



# Chapitre 11 : Ceci est un réseau



## Initiation aux réseaux

Cisco | Networking Academy®  
Mind Wide Open™



# Chapitre 11

- 11.1 Création et développement
- 11.2 Assurer la sécurité du réseau
- 11.3 Les performances réseau de base
- 11.4 Gérer les fichiers de configuration IOS
- 11.5 Les routeurs à services intégrés
- 11.6 Résumé



# Chapitre 11 : Les objectifs

- Identifier les périphériques et les protocoles utilisés dans un réseau de petite taille
- Expliquer comment un petit réseau sert de base aux réseaux plus importants
- Expliquer l'utilité des mesures de sécurité de base sur les périphériques réseau
- Identifier les failles de sécurité et les techniques employées pour limiter les risques



## Chapitre 11 : Les objectifs (suite)

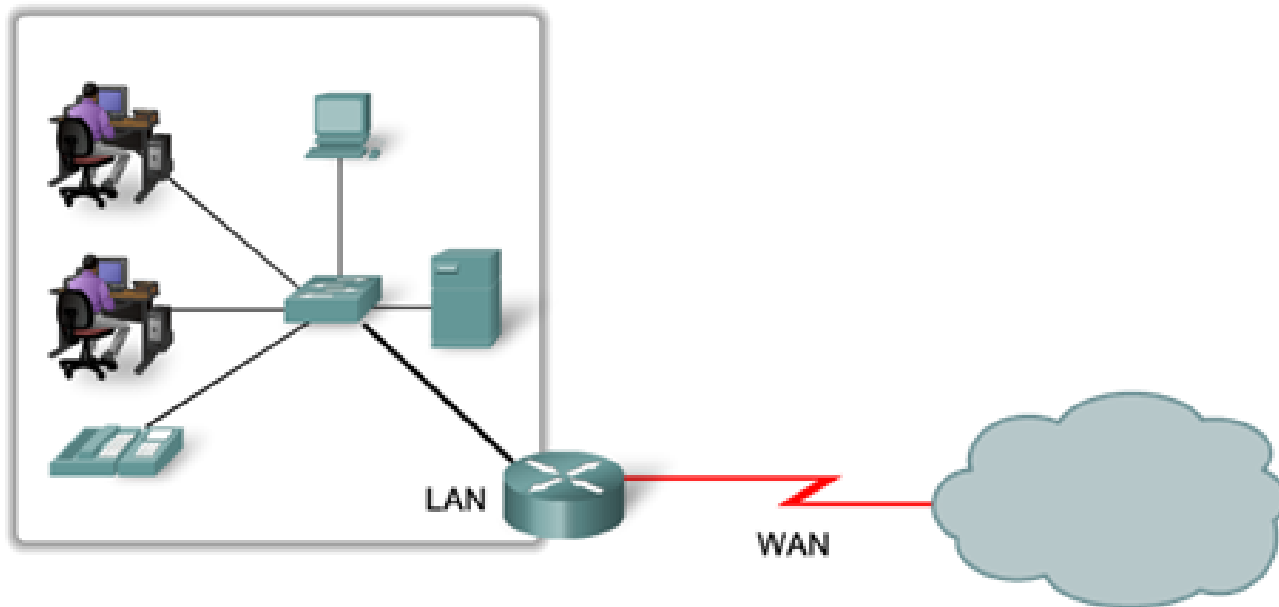
- Utiliser le résultat des commandes ping et tracer pour déterminer les performances réseau relatives
- Utiliser des commandes show de base pour vérifier la configuration et l'état de l'interface d'un périphérique
- Expliquer les systèmes de fichiers des routeurs et des commutateurs
- Appliquer les commandes pour sauvegarder et restaurer un fichier de configuration IOS



Périphériques d'un petit réseau

# Topologies de petits réseaux

- Topologie typique d'un petit réseau



## Périphériques d'un petit réseau

# Sélection de périphériques pour un petit réseau

- Facteurs à prendre en compte lors de la sélection des périphériques intermédiaires



COST



PORTS



SPEED



EXPANDABLE/ MODULAR



MANAGEABLE



## Périphériques d'un petit réseau

# Adressage pour un petit réseau

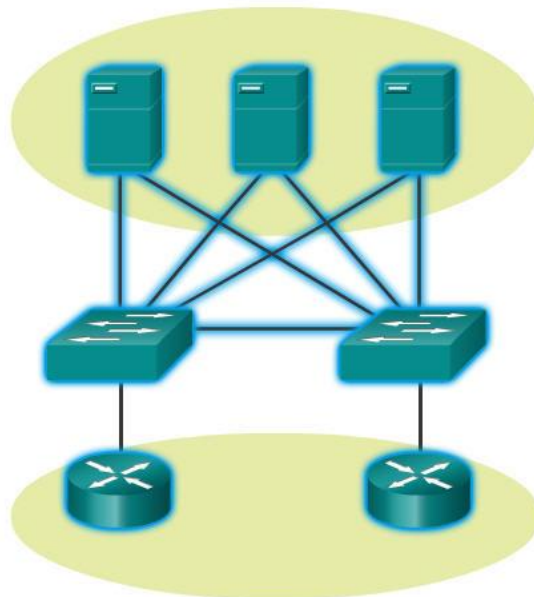
- Le schéma d'adressage IP doit être planifié, documenté et mis à jour en fonction du type de périphériques recevant l'adresse.
- Exemples de périphériques qui feront partie de la conception IP :
  - Périphériques finaux des utilisateurs
  - Serveurs et périphériques
  - Hôtes accessibles depuis Internet
  - Périphériques intermédiaires
- Les schémas IP planifiés aident l'administrateur pour :
  - Le suivi des périphériques et le dépannage
  - Le contrôle de l'accès aux ressources

## Périphériques d'un petit réseau

# Redondance dans un petit réseau

- La redondance permet d'éliminer les points de défaillance uniques.
- Elle améliore la fiabilité du réseau.

Redondance dans une batterie de serveurs







## Périphériques d'un petit réseau

# Considérations liées à la conception d'un petit réseau

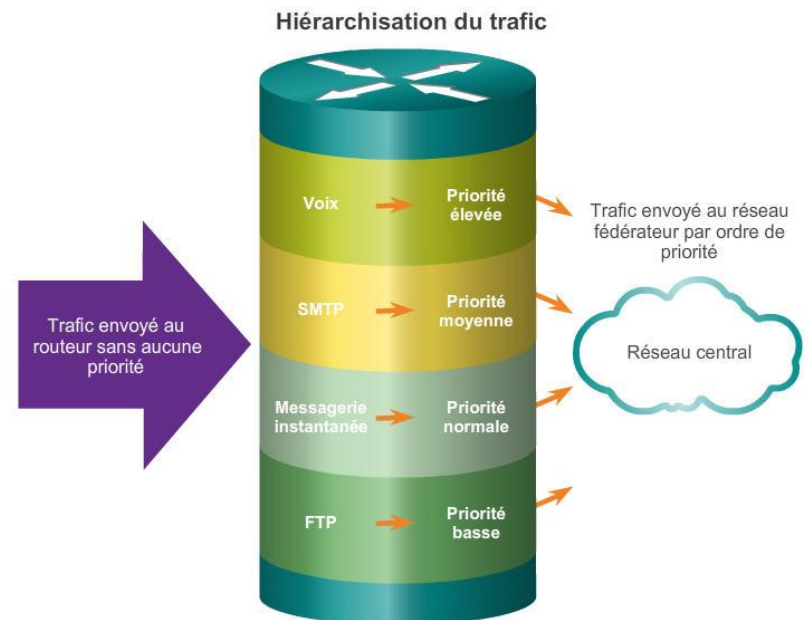
- Voici ce qu'il faut prévoir dans la conception du réseau :

Assurez-vous que les serveurs de messagerie et de fichiers sont dans un emplacement centralisé.

Protégez cet emplacement en utilisant des dispositifs de sécurité matériels et logiciels.

Créez la redondance dans la batterie de serveurs.

Configurez des chemins d'accès redondants vers les serveurs.





Protocoles d'un petit réseau

# Applications courantes d'un petit réseau

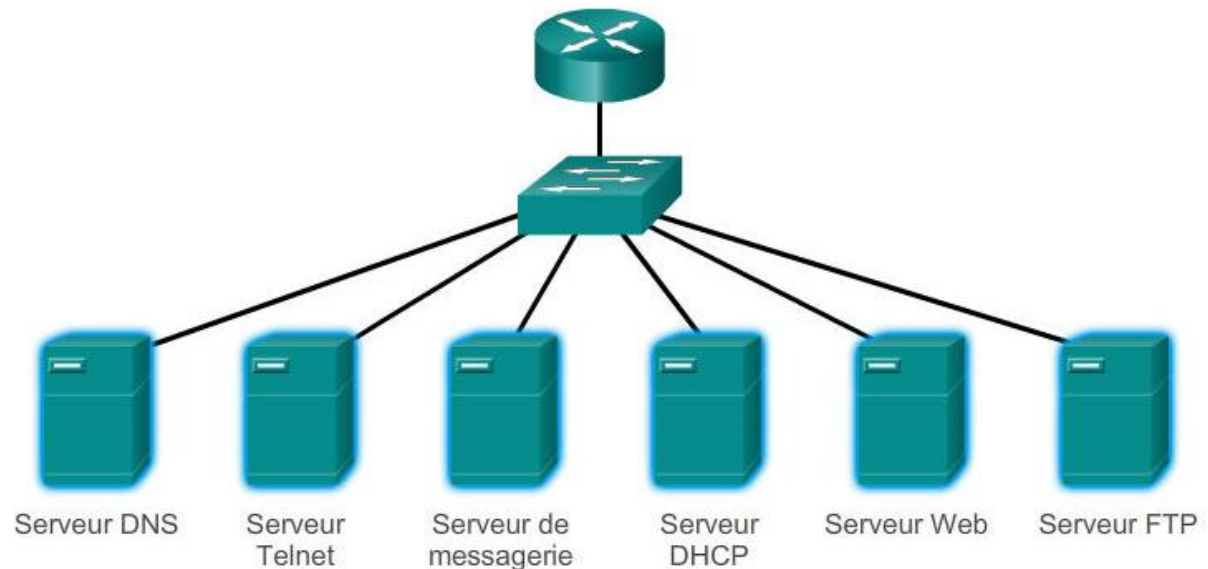
- **Applications orientées Réseau** : logiciels qui permettent de communiquer sur le réseau.
- **Services de couche application** : programmes qui communiquent avec le réseau et préparent les données à transférer.



## Protocoles d'un petit réseau

# Protocoles courants d'un petit réseau

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





## Protocoles d'un petit réseau

# Applications en temps réel pour un petit réseau

- **Infrastructure** : doit être évaluée pour vérifier qu'elle prend en charge les applications en temps réel proposées.
- La téléphonie IP (VoIP) est mise en œuvre dans les entreprises qui utilisent encore des téléphones traditionnels.
- Téléphonie IP : le téléphone IP exécute lui-même la conversion voix-vers-IP.
- Protocoles de vidéo en temps réel : utilisent le protocole RTP et le protocole RTCP.



Évolution vers de plus grands réseaux

## Évolutivité d'un petit réseau

Facteurs importants à prendre en compte lors de l'évolution vers un plus grand réseau :

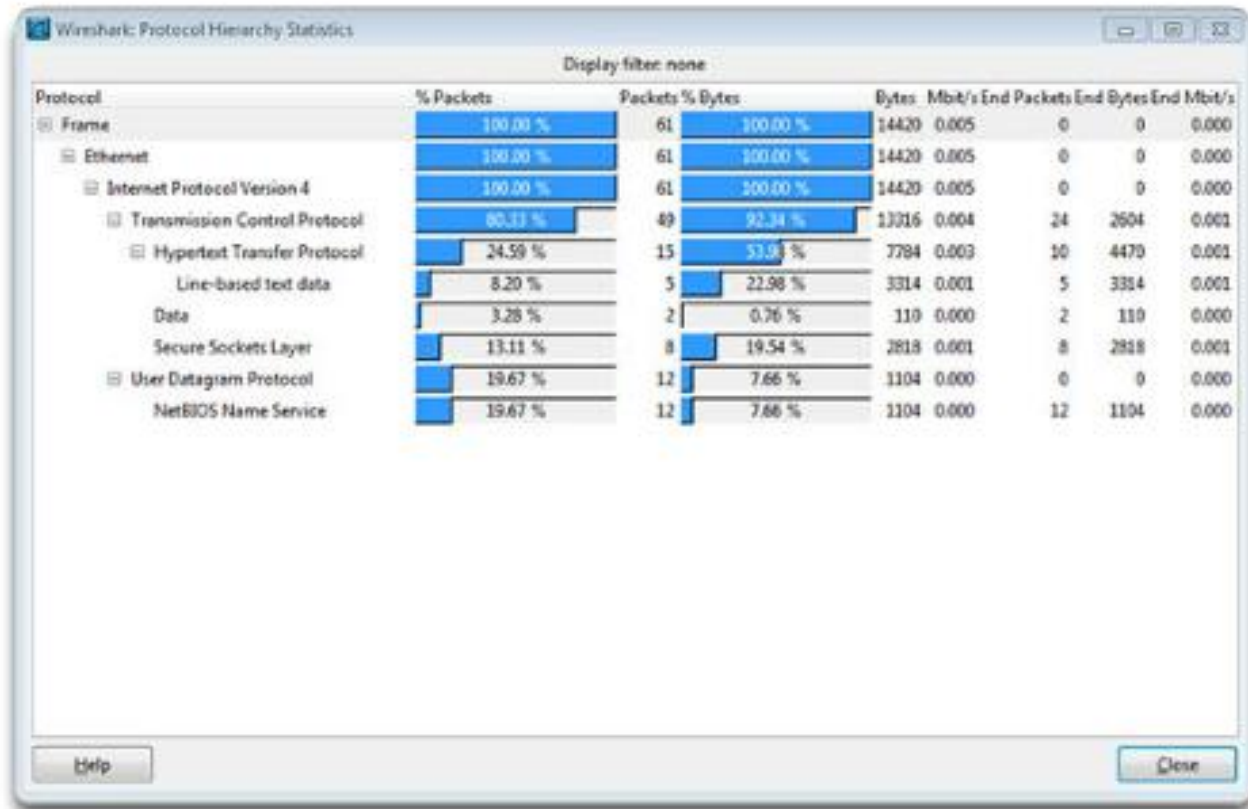
- Documentation : topologies logiques et physiques
- Inventaire des équipements : liste des périphériques qui utilisent ou constituent le réseau
- Budget : budget informatique détaillé, y compris les achats d'équipements pour l'année fiscale
- Analyse du trafic : documentation des protocoles, applications et services, avec leurs besoins respectifs quant au trafic



Évolution vers de plus grands réseaux

# Analyse des protocoles d'un petit réseau

- Les informations collectées par l'analyse des protocoles permettent de prendre des décisions sur la façon de gérer le trafic plus efficacement.

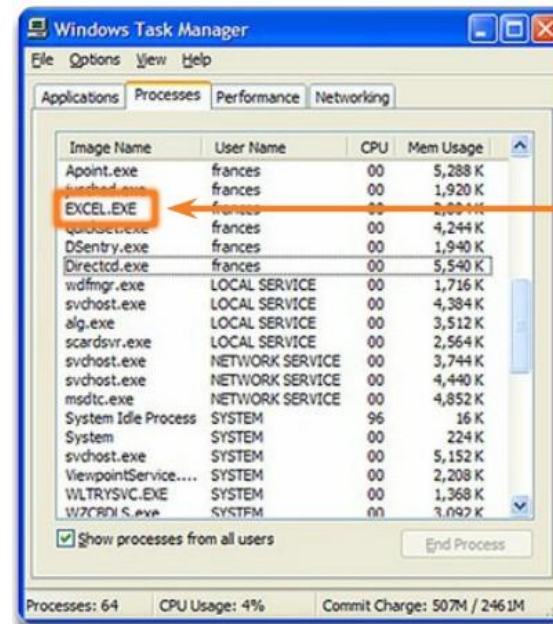




## Évolution vers de plus grands réseaux

# Évolution des exigences liées aux protocoles

- L'administrateur réseau peut obtenir des « instantanés » sur l'utilisation des applications par les employés.
- Ces instantanés permettent de suivre l'utilisation du réseau et les besoins en matière du flux du trafic.
- Ils aident à anticiper les modifications de réseau nécessaires.



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





## Évaluation de la sécurité des périphériques réseau

# Menaces pour la sécurité du réseau

- Les catégories de menaces à la sécurité du réseau



Vol d'informations



Perte et manipulation de données



Usurpation d'identité



Interruption de service





## Évaluation de la sécurité des périphériques réseau

# Sécurité physique

Les quatre catégories de menaces physiques sont les suivantes :

- Menaces matérielles : entraînant des dommages physiques sur les serveurs, routeurs, commutateurs, installations de câblage et stations de travail.
- Menaces environnementales : variations extrêmes de la température ou du taux d'humidité.
- Menaces électriques : pointes de tension, tension d'alimentation insuffisante (chutes), alimentation non contrôlée (bruit) et panne totale.
- Menaces liées à la maintenance : mauvaise manipulation des composants électriques principaux (décharges électrostatiques), pénurie de pièces de rechange importantes, câblage mal effectué et étiquetage médiocre.



## Évaluation de la sécurité des périphériques réseau

# Types de failles de sécurité

- Faiblesses technologiques
- Faiblesses de configuration
- Faiblesses dans la stratégie de sécurité

### Faiblesses de sécurité des réseaux :

#### Faiblesse des protocoles TCP/IP

- Les protocoles HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) et ICMP (Internet Control Message Protocol) ne sont pas sécurisés.
- Les protocoles SNMP (Simple Network Management Protocol) et SMTP (Simple Mail Transfer Protocol) sont liés à la structure intrinsèquement non sécurisée sur laquelle le protocole TCP a été conçu.

#### Faiblesses du système d'exploitation

- Chaque système d'exploitation présente des problèmes de sécurité qui doivent être résolus.
- UNIX, Linux, MacOS, MacOSX, Windows Server2012, Windows7, Windows8
- Ils sont documentés dans les archives de la CERT (Computer Emergency réponse Team) à l'adresse <http://www.cert.org>

#### Faiblesse des équipements réseau

Différents types d'équipement réseau tels que les routeurs, les pare-feu et les commutateurs présentent des failles de sécurité qui doivent être identifiées et protégées. Ces faiblesses concernent la protection des mots de passe, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feu.



## Failles et attaques du réseau

# Virus, vers et chevaux de Troie

- Virus : logiciel malveillant associé à un autre programme pour exécuter des fonctions indésirables sur une station de travail.
- Cheval de Troie : entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un outil de piratage.
- Vers : programmes autonomes qui attaquent un système et essaient d'exploiter une vulnérabilité spécifique. Le ver recopie son programme de l'hôte assaillant sur les systèmes qu'il vient d'attaquer, et le cycle recommence.



## Failles et attaques du réseau

# Attaques par reconnaissance



Requêtes Internet



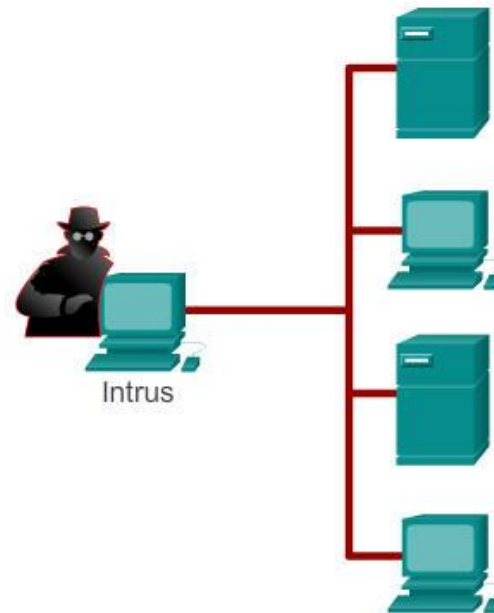
Balayages ping



Balayages de ports



Analyseurs de paquets





# Failles et attaques du réseau

## Attaques par accès

### Attaque de mot de passe

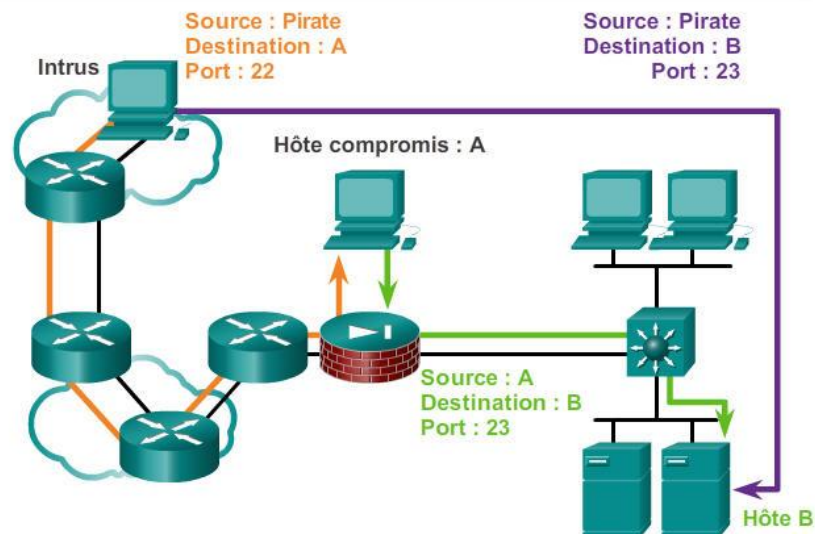
Les pirates peuvent lancer différents types d'attaques de mots de passe :

- Attaques en force
- Chevaux de Troie
- Analyseurs de paquets



### Redirection de port

La redirection de port est une attaque du type « exploitation de la confiance » qui utilise un hôte compromis pour faire passer, au travers d'un pare-feu, un trafic qui serait normalement bloqué. Ce type d'attaque est principalement limité par l'utilisation de modèles de confiance appropriés. Un logiciel antivirus et un système IDS sur l'hôte permettent de détecter et d'empêcher l'installation



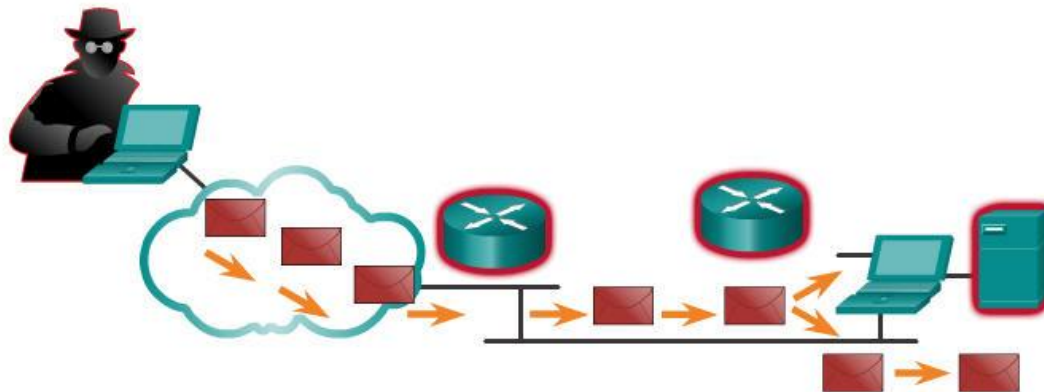


## Faibles et attaques du réseau

# Attaques par déni de service (DoS)

### Attaque par déni de service (DoS)

Surcharge des ressources	Données mal formées
Espace disque, bande passante, tampons	Paquets surdimensionnés (ping fatal)
Inondation de paquets ping (Smurf)	Chevauchement de paquets (Winuke)
Inondations de paquets (bombes UDP, attaques Fraggle)	Données non traitées (Teardrop)



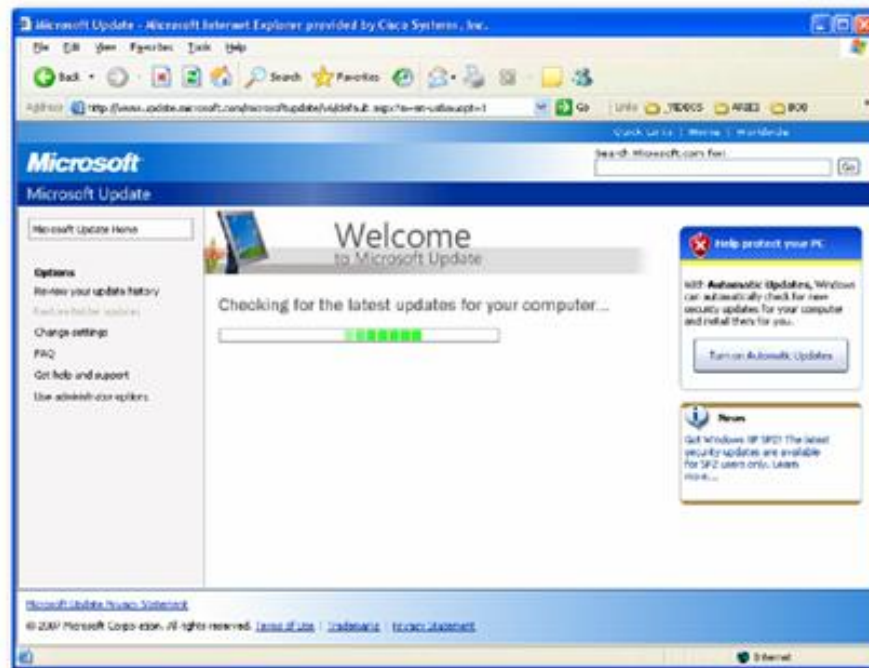
Les attaques par déni de service empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système.



Réduction du risque d'attaques du réseau

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

- Faites en sorte de toujours utiliser les versions les plus récentes des antivirus.
- Installez les derniers correctifs de sécurité.





Réduction du risque d'attaques du réseau

# Authentification, autorisation et gestion des comptes

Authentification, autorisation et gestion des comptes

- **Authentification** : les utilisateurs et les administrateurs doivent prouver leur identité. L'authentification peut être implémentée à l'aide de combinaisons de nom d'utilisateur et de mot de passe, de questions d'authentification, de jetons et d'autres méthodes.
- **Autorisation** : les ressources auxquelles les utilisateurs peuvent accéder et les opérations qu'ils sont autorisés à effectuer.
- **Gestion des comptes** : enregistrements auxquels l'utilisateur a accédé, durée de l'accès aux ressources et modifications apportées.





## Réduction du risque d'attaques du réseau

# Les pare-feu

Un pare-feu se trouve entre deux réseaux ou plus. Il contrôle le trafic et contribue à éviter les accès non autorisés. Méthodes utilisées :

- Filtrage des paquets
- Filtrage des applications
- Filtrage des URL
- Inspection dynamique de paquets (SPI) - Les paquets entrants doivent constituer des réponses légitimes aux requêtes des hôtes internes.



Appareils de sécurité Cisco



Pare-feu basé sur serveur



Routeur sans fil Linksys avec pare-feu intégré



Pare-feu personnel



## Réduction du risque d'attaques du réseau

# Sécurité des terminaux

- Les terminaux courants sont les ordinateurs portables, les ordinateurs de bureau, les serveurs, les smartphones ou encore les tablettes.
- Les employés doivent respecter les politiques de sécurité établies par les entreprises afin d'assurer la sécurité de leurs appareils.
- Ces politiques incluent souvent antivirus et la prévention des





## Sécurisation des périphériques

# Initiation à la sécurisation des périphériques

- La sécurité du réseau repose en partie sur la sécurisation des équipements, y compris les appareils des utilisateurs et les périphériques intermédiaires.
- Les noms d'utilisateur et les mots de passe par défaut doivent être changés immédiatement.
- L'accès aux ressources du système doit être limité strictement aux personnes autorisées à les utiliser.
- Dans la mesure du possible, les services et les applications qui ne sont pas nécessaires doivent être désactivés et désinstallés.
- Les correctifs de sécurité doivent être appliqués dès qu'ils sont disponibles.



## Sécurisation des périphériques

# Les mots de passe

Mot de passe faible	Raison de sa faiblesse
secret	Mot de passe simple tiré du dictionnaire
smith	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 une espace



## Sécurisation des périphériques

# Mesures de sécurité élémentaires

- Chiffrement des mots de passe
- Longueur minimale à respecter pour les mots de passe
- Blocage des attaques en force
- Utilisation d'un message de bannière
- Définition d'un délai d'expiration EXEC

```
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
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

# Sécurisation des périphériques

## Activation de 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.






## Ping

# Interprétation des messages ICMP


- **!** – 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.

Test de la pile TCP/IP locale

L'envoi d'une requête ping à l'hôte local confirme que la suite de protocoles TCP/IP est installée et fonctionne sur la carte réseau locale.



Envoyer une requête ping à l'adresse **127.0.0.1** revient à ce que le périphérique s'envoie la requête ping à lui-même.





## Ping

# Les extensions de la commande ping

- Le logiciel Cisco IOS offre un mode « étendu » de la commande ping.

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]:





# Ping

## Planification initiale du réseau

### Exécuter le même test...

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 mar 2013 14:41:06

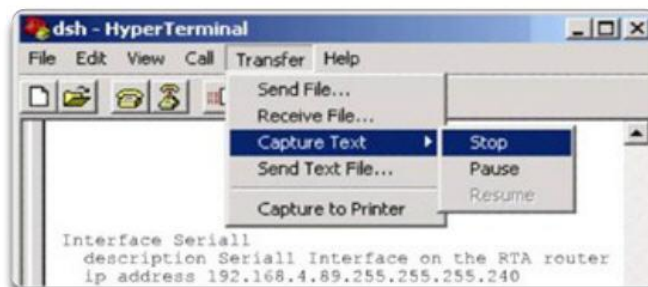
```
C:\>ping 10.66.254.159
```

```
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
```

### Capture des résultats de la commande ping à partir d'un routeur - Enregistrement dans un fichier texte



#### Dans la session de terminal :

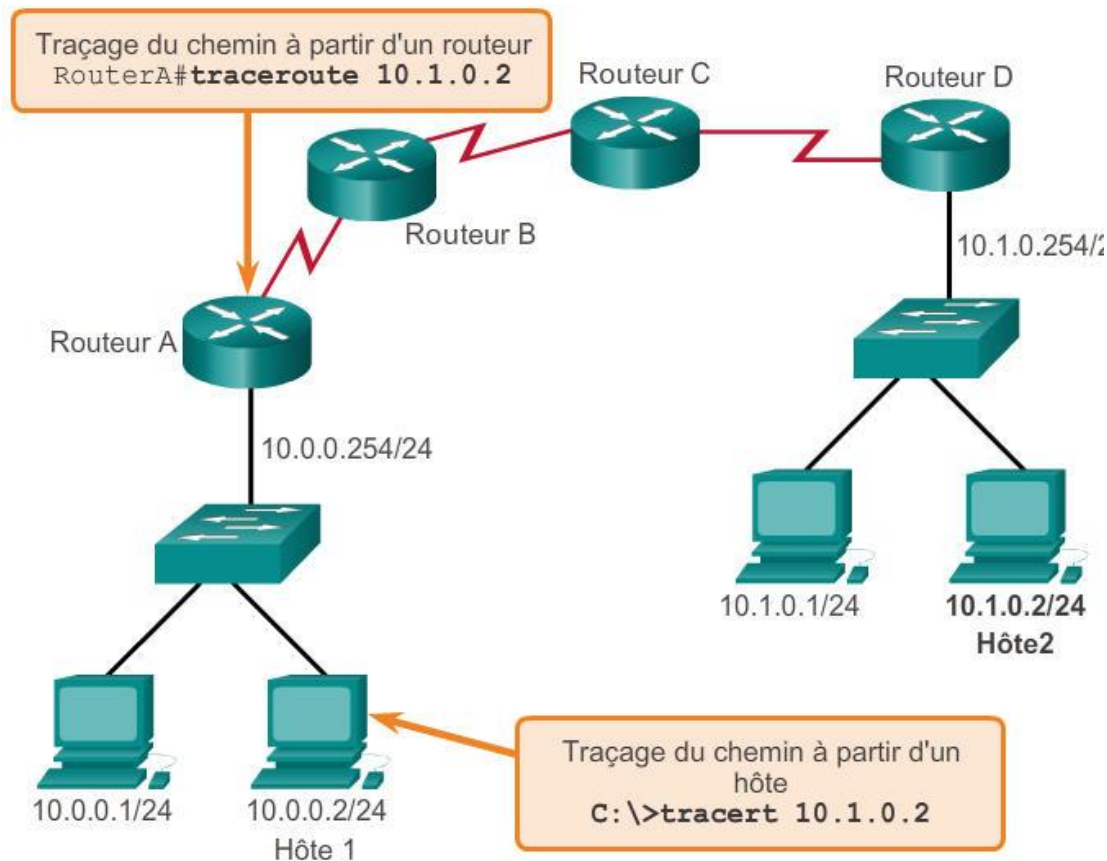
1. Démarrez le processus de capture de texte.
2. Exécutez la commande **ping** <adresse ip> .
3. Arrêtez le processus de capture.
4. Enregistrez le fichier texte.



## Tracert

# Interprétation des messages tracert

Test du chemin vers un hôte distant





Les commandes show

# Révision des commandes show courantes

- Vous pouvez afficher l'état de presque tous les processus ou fonctions du routeur à l'aide de la commande **show**.
- Commandes show fréquemment utilisées :
  - show running-config**
  - show interfaces**
  - show arp**
  - show ip route**
  - show protocols**
  - show version**



Les commandes show

# Affichage des paramètres du routeur avec la commande show version

Version de Cisco IOS

Bootstrap du système

Image Cisco IOS

Processeur et RAM

Nombre et type d'interfaces

Quantité de mémoire vive non volatile

Quantité de mémoire flash

Registre de configuration

```
Router#show version
Cisco Internetwork Operating System Software
IOS(tm)2500 Software (C2500-I-L),Version 12.0(17a),RELEASE
SOFTWARE (fc1)
Copyright (c)1986-2002 by cisco Systems,Inc.
Compiled Mon 11-Feb-02 05:55 by kellythw
image text-base:0x00001000
ROM:system Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH :3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c),RELEASE SOFTWARE (fc1)
System image file is "flash:c2500-i-l.120-17a.bin"
cisco 2500 (68030 processor(revision N) With 2048K/2048K
bytes of memory.
processor bord ID 08860060,with hardware revision 00000000
Bridging software.
X.25 software,version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile Configuration memory.
8192K bytes of processor board system flash (Read ONLY)
Configuration register is 0x2102
Router#
```



Les commandes show

# Affichage des paramètres du commutateur avec la commande show version

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z9ZN
Last reset from power-on
1 Virtual Ethernet interface
```



## Commandes hôtes et IOS

# Options de commande ipconfig

- ipconfig : affiche l'adresse IP, le masque de sous-réseau et la passerelle par défaut.
- ipconfig /all : affiche également l'adresse MAC.
- ipconfig /displaydns : affiche toutes les entrées DNS stockées dans la mémoire cache d'un système Windows.

```
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

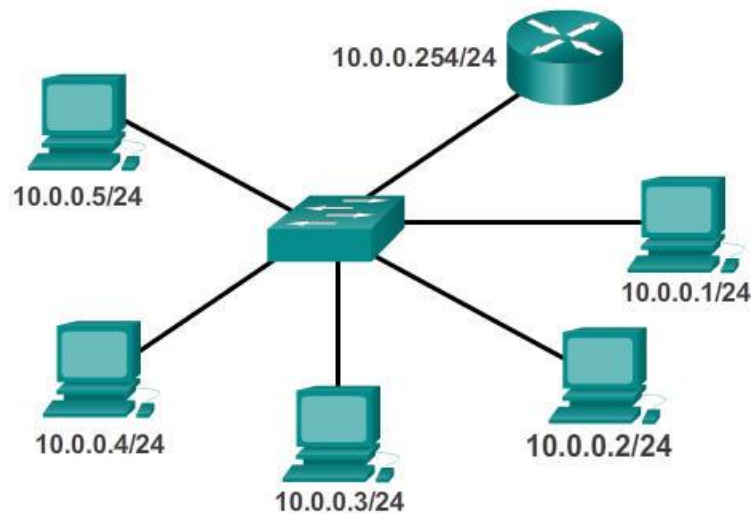
C:\>
```





## Commandes hôtes et IOS

# Options de commande arp



```

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



## Commandes hôtes et IOS

# Options de commande show cdp neighbors

```
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

Device ID         Local Intrfce   Holdtme    Capability Platform  Port ID
S3                 Fas 0/0         151        S I       WS-C2950  Fas 0/6
R2                 Ser 0/0/1       125        R         1841      Ser 0/0/1

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
```





## Commandes hôtes et IOS

# Utilisation de la commande show ip interface brief

- Cette commande peut être utilisée pour vérifier l'état de toutes les interfaces réseau sur un routeur ou un commutateur.

```
Router1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.254.254	YES	NVRAM	up	up
FastEthernet0/1/0	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

---

```
Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

---

```
Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
 1 172.16.0.253 8 msec 4 msec 8 msec
 2 10.0.0.254 16 msec 16 msec 8 msec
 3 192.168.0.1 16 msec * 20 msec
```



## Systèmes de fichiers du routeur et du commutateur

# Systèmes de fichiers du routeur

- **show file systems** : répertorie tous les systèmes de fichiers disponibles sur un routeur Cisco 1941

```
Router# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -          -          -      -      -
      -          -          opaque  rw      archive:
      -          -          opaque  rw      system:
      -          -          opaque  rw      tmosvs:
      -          -          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:
```

- \* L'astérisque indique qu'il s'agit du système de fichiers par défaut



## Systèmes de fichiers du routeur et du commutateur

# Systèmes de fichiers du commutateur

- **show file systems** : répertorie tous les systèmes de fichiers disponibles sur un commutateur Catalyst 2960

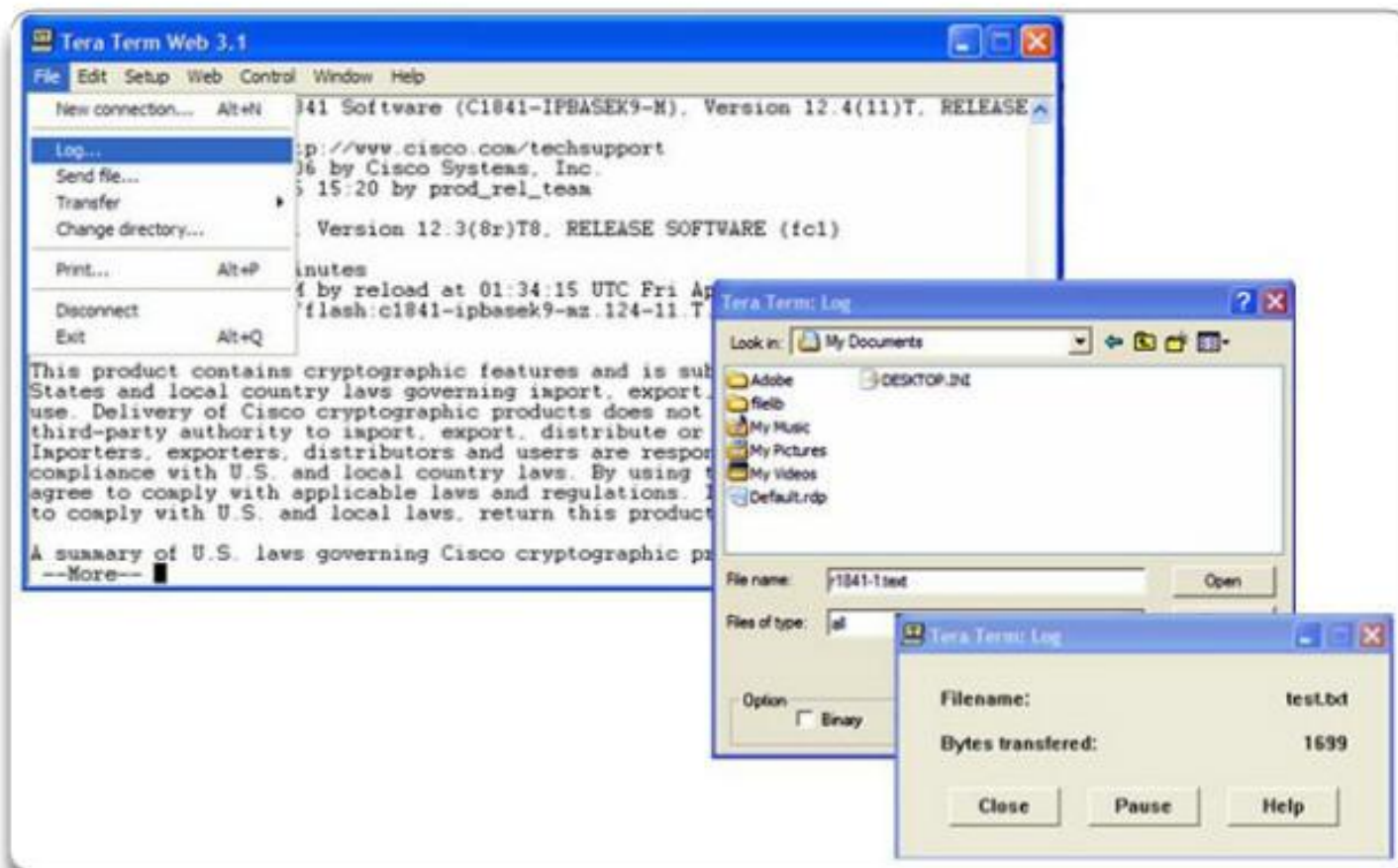
```
Switch#show file systems
File Systems:

  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 des fichiers de configuration

## Sauvegarde et restauration à l'aide de fichiers texte

Enregistrement vers un fichier texte dans Tera Term





## Sauvegarde et restauration des fichiers de configuration

# Sauvegarde et restauration via TFTP

- Les fichiers de configuration peuvent être stockés sur un serveur TFTP (Trivial File Transfer Protocol)
- `copy running-config tftp` : enregistre la configuration en cours sur un serveur TFTP
- **`copy startup-config tftp`** : enregistre la configuration initiale sur un serveur TFTP

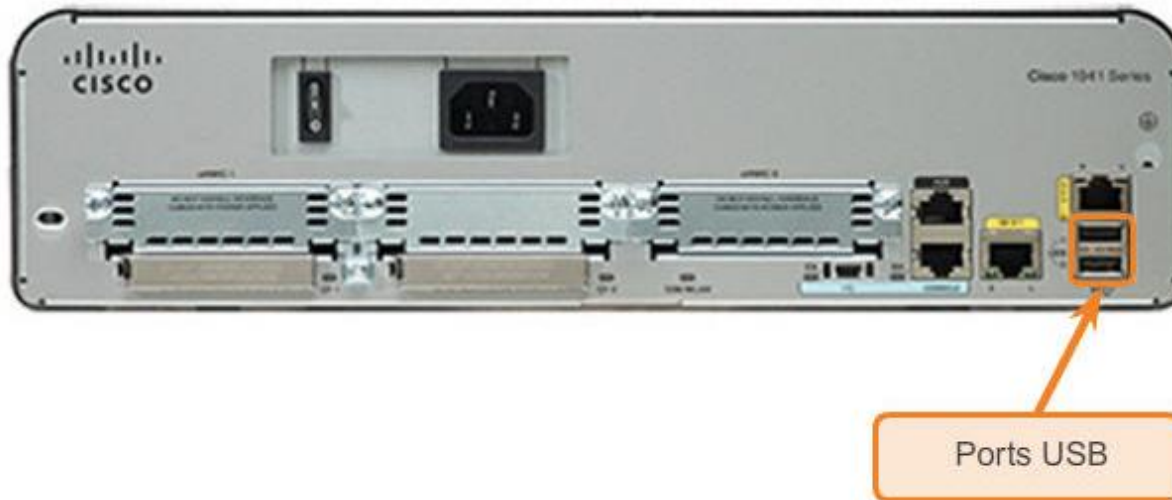
```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!! [OK]
```



## Sauvegarde et restauration des fichiers de configuration

# Utilisation des ports USB d'un routeur Cisco

- Le lecteur Flash USB doit être formaté en FAT16.
- Peut contenir plusieurs copies de Cisco IOS et plusieurs configurations de routeur.
- Permet à l'administrateur de déplacer plus facilement les configurations d'un routeur à l'autre.





## Sauvegarde et restauration des fichiers de configuration

# Sauvegarde et restauration via une connexion USB

```
R1#copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copier vers le disque Flash USB qui ne contient pas de fichier du même nom.

```
R1#copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copier vers le disque Flash USB contenant déjà le même fichier de configuration.



## Routeur intégré

# Périphérique multifonction

- Intègre un commutateur, un routeur et un point d'accès sans fil.
- Assure le routage, la commutation et la connectivité sans fil.
- Les routeurs sans fil Linksys sont de conception simple et sont utilisés dans les réseaux domestiques.
- La gamme de routeurs à services intégrés (ISR) de Cisco offre un large choix de modèles conçus aussi bien pour les petits bureaux que pour les réseaux plus grands.

Linksys : modèle WRT300N2

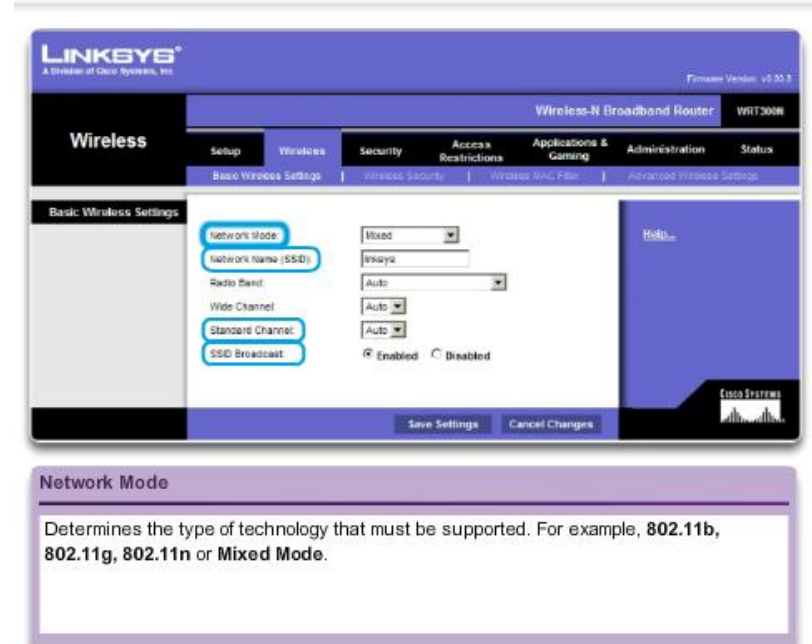




## Routeur intégré

# Connectivité sans fil

- **Mode sans fil** : la plupart des routeurs sans fil intégrés prennent en charge les normes 802.11b, 802.11g et 802.11n
- **SSID (Service Set Identifier)** : nom alphanumérique, avec distinction majuscules/minuscules, pour votre réseau domestique sans fil
- **Canal sans fil** : spectre des radiofréquences (RF) divisé en canaux





Routeur intégré

# Sécurité de base des connexions sans fil

- Modifiez les valeurs par défaut
- Désactivez la diffusion SSID
- Configurez le chiffrement WEP ou WPA
- **Protocole WEP (Wired Equivalency Protocol) :** clés préconfigurées utilisées pour chiffrer et déchiffrer les données Chaque périphérique sans fil autorisé à accéder au réseau doit avoir fourni la même clé WEP.
- **WPA (Wi-Fi Protected Access) :** utilise également des clés de chiffrement comprises entre 64 et 256 bits. De nouvelles clés sont générées chaque fois qu'une connexion est établie avec le point d'accès. Cette méthode est donc plus sûre.



## Routeur intégré

# Configuration du routeur intégré

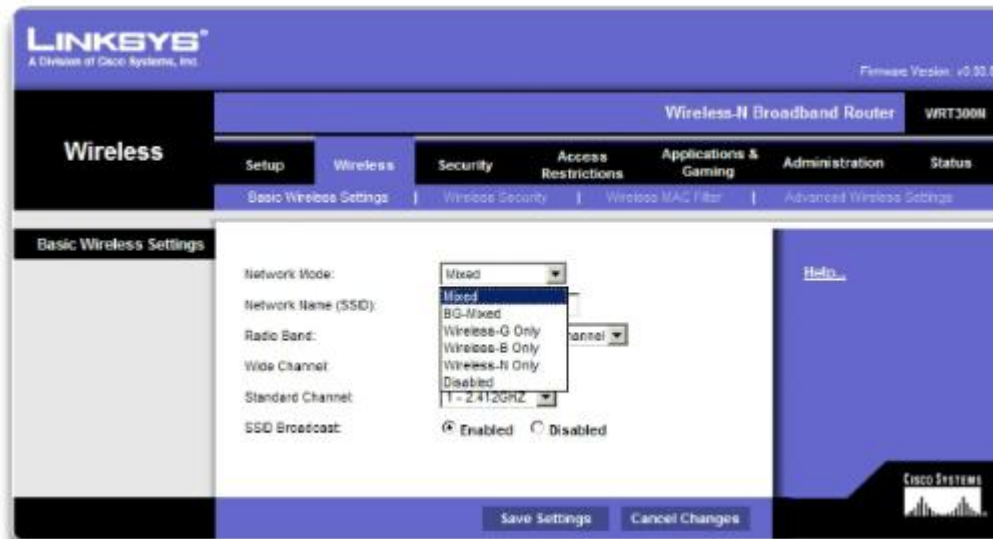
- Accédez au routeur en raccordant un ordinateur à l'un de ses ports LAN Ethernet à l'aide d'un câble.
- L'appareil connecté recevra automatiquement les informations d'adressage IP depuis le routeur intégré.
- Par sécurité, changez le nom d'utilisateur et le mot de passe par défaut, ainsi que l'adresse IP Linksys par défaut.



## Routeur intégré

# Activation de la connectivité sans fil

- Configurez le mode sans fil
- Configurez le SSID
- Configurez le canal RF
- Configurez le mécanisme de chiffrement souhaité





## Routeur intégré

# Configuration d'un client sans fil

- Les paramètres de configuration du client sans fil doivent correspondre à ceux du routeur sans fil.

SSID

Security Settings (Paramètres de sécurité)

Channel

- Le logiciel client sans fil peut être intégré au système d'exploitation ou être un utilitaire sans fil autonome et téléchargeable.





# Résumé du chapitre 11

- Une bonne conception de réseau intègre la fiabilité, l'évolutivité, ainsi que la disponibilité.
- Les réseaux doivent être à l'abri des virus, des chevaux de Troie, des vers et des attaques.
- Documentez les performances réseau de base.
- Testez la connectivité réseau avec les commandes ping et traceroute.
- Utilisez les commandes IOS pour contrôler et afficher des informations sur le réseau et ses périphériques.
- Sauvegardez les fichiers de configuration via TFTP ou USB.
- Les réseaux domestiques et les PME utilisent souvent des routeurs intégrés. Ceux-ci leur procurent des fonctionnalités de commutateur, de routeur et de point d'accès sans fil.



# Cisco | Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>