6e partie :
Création et sécurisation de petits réseaux

Modules 16 - 17

AVIGNON UNIVERSITÉ

Module 16 : Fondamentaux de la sécurité des réseaux

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

Menaces pour la sécurité du réseau

- Les catégories de menaces à la sécurité du 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.

Types de failles de sécurité

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

Faiblesses de sécurité des réseaux :

Faiblesse des protocolesTCP/IP
- Les protocoles HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol (FTP) 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.

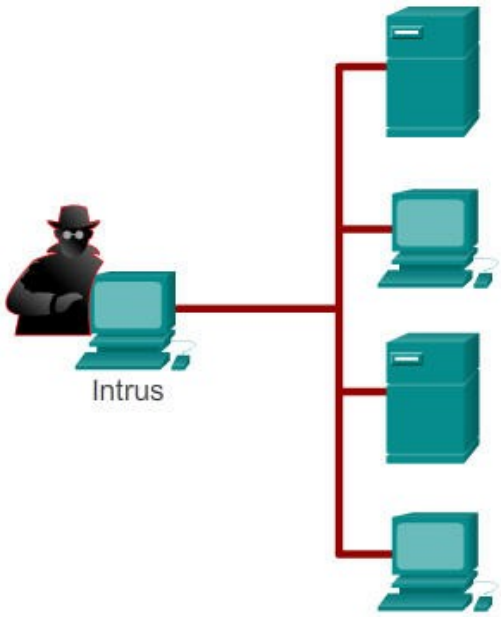
Faiblesses du système d'exploitation
- Chaque système d'exploitation présente des problèmes de sécurité qui doivent être résolus.
- UNIX, Linux, MacOS, MacOSX, Windows Server2012, Windows7, Windows8
- Ils sont documentés dans les archives de la CERT (Computer Emergency réponse Team) à l'adresse http://www.cert.org

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.

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.

Attaques par reconnaissance

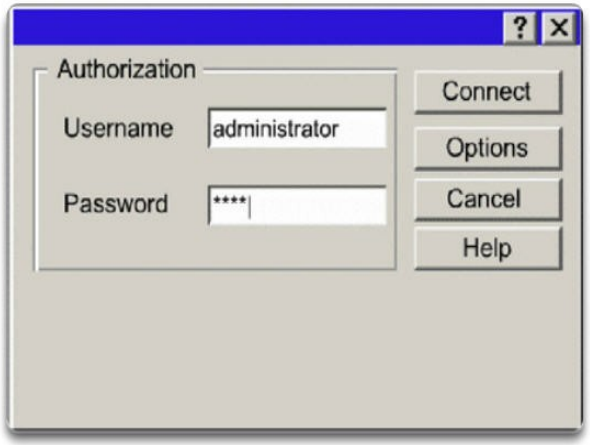


Attaques par accès

Attaque de mot de passe

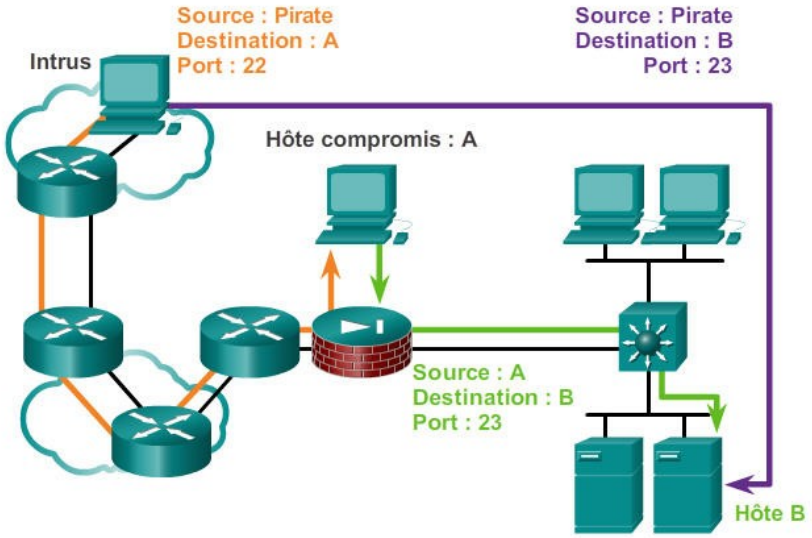
Les pirates peuvent lancer différents types d'attaques de mots de passe :

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



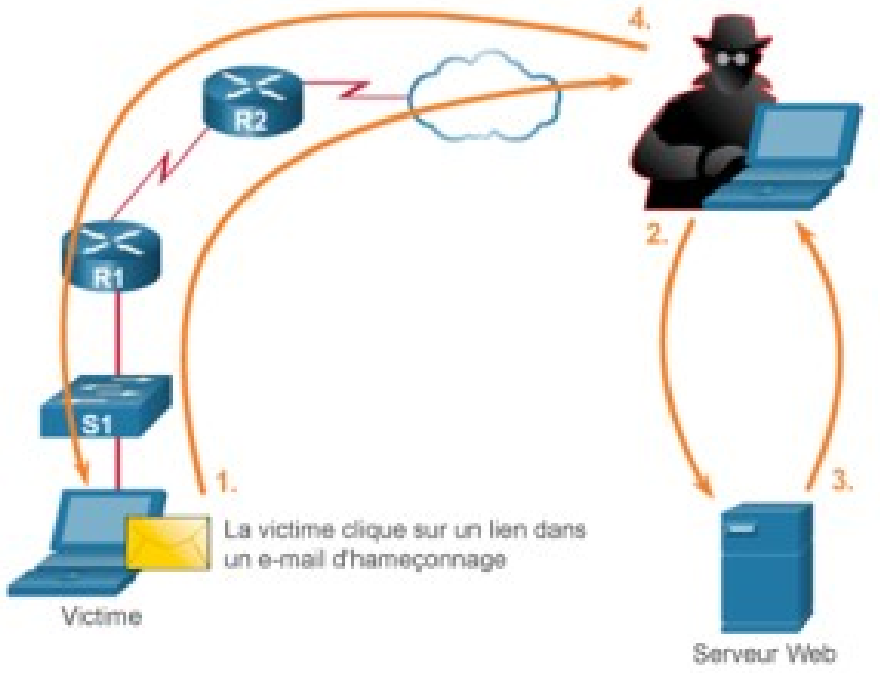
Redirection de port

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



Attaques par accès (suite)

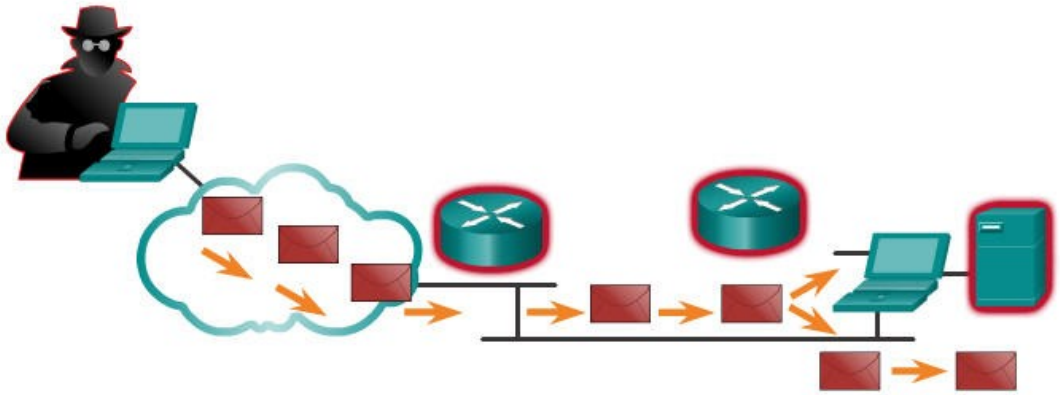
L'homme du milieu (*Man in the middle*)



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.

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.

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.

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 l'utilisation d'un logiciel antivirus et la prévention des intrusions sur les hôtes.

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

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
```

Activation de SSH

1. **Configurer un nom d'hôte unique pour l'appareil**. Un appareil doit avoir un nom d'hôte unique autre que celui par défaut.
2. **Configurer le nom de domaine IP**. Configurez le nom de domaine IP du réseau en utilisant la commande **ip-domain name**. **du mode de configuration globale.**
3. **Générer une clé pour chiffrer le trafic SSH**. SSH crypte le trafic entre la source et la destination. Cependant, pour ce faire, une clé d'authentification unique doit être générée à l'aide de la commande de configuration globale **crypto key generate rsa modulus** *bits*. Le module de *bits* détermine la taille de la clé et peut être configuré de 360 bits à 2048 bits. Plus la valeur du bit est grande, plus la clé est sécurisée. Cependant, les valeurs de bits plus importantes prennent également plus de temps pour chiffrer et déchiffrer les informations. Il est recommandé d'utiliser un module d'au moins 1 024 bits.
4. **Vérifiez ou créez une entrée de base de données locale**. Créez une entrée de nom d'utilisateur dans la base de données locale à l'aide de la commande de configuration globale **username** .
5. **S'authentifier par rapport à la base de données locale**. Utilisez la commande **login local** line configuration pour authentifier la ligne vty par rapport à la base de données locale.
6. **Activer des sessions SSH vty entrantes**. Par défaut, aucune session d'entrée n'est autorisée sur les lignes vty. Vous pouvez spécifier plusieurs protocoles d'entrée, y compris Telnet et SSH, à l'aide de la commande **transport input [ssh | telnet]** .

Principe des clés asymétriques

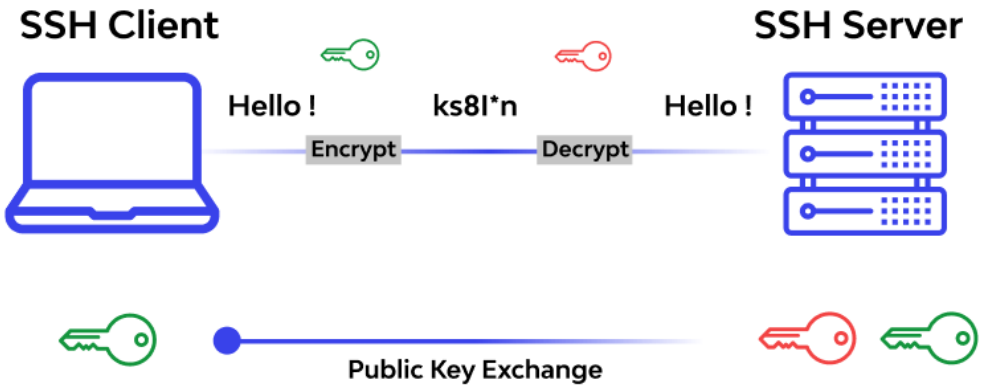
Chiffrement RSA : algorithme de cryptographie asymétrique

- **Clé publique**
  - Utilisée pour chiffrer les messages
  - Distribuée aux destinataires
- **Clé privée**
  - Utilisée pour déchiffrer les messages
  - Secrète et réservée à la machine hôte
- **Principe :** il est calculatoirement impossible de déchiffrer à l'aide de la seule clé publique
  - Dépend de l'algorithme de chiffrement et de la taille de la clé

Utilisation des clés

Client vers serveur

- Génération d'une paire de clés par le serveur
- Schéma de fonctionnement



Serveur vers client

- Génération d'une paire de clés par le client

Résumé

- Expliquer pourquoi des mesures de sécurité de base sont nécessaires pour les périphériques réseau.
- Identifier les vulnérabilités
- Identifier les techniques générales de maîtrise des menaces
- Configurer les périphériques réseau en utilisant des fonctionnalités de sécurisation renforcées pour maîtriser les menaces pour la sécurité

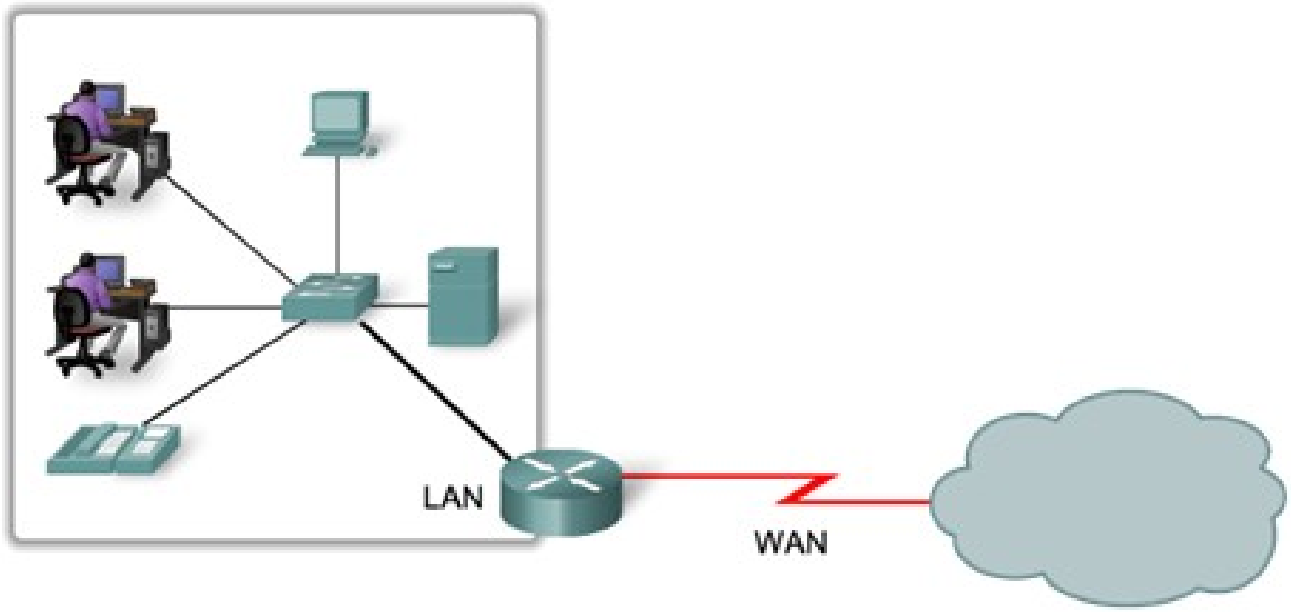
Module 17 : Conception d’un réseau de petite taille

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

Topologies de petits réseaux

- Topologie typique d'un petit réseau

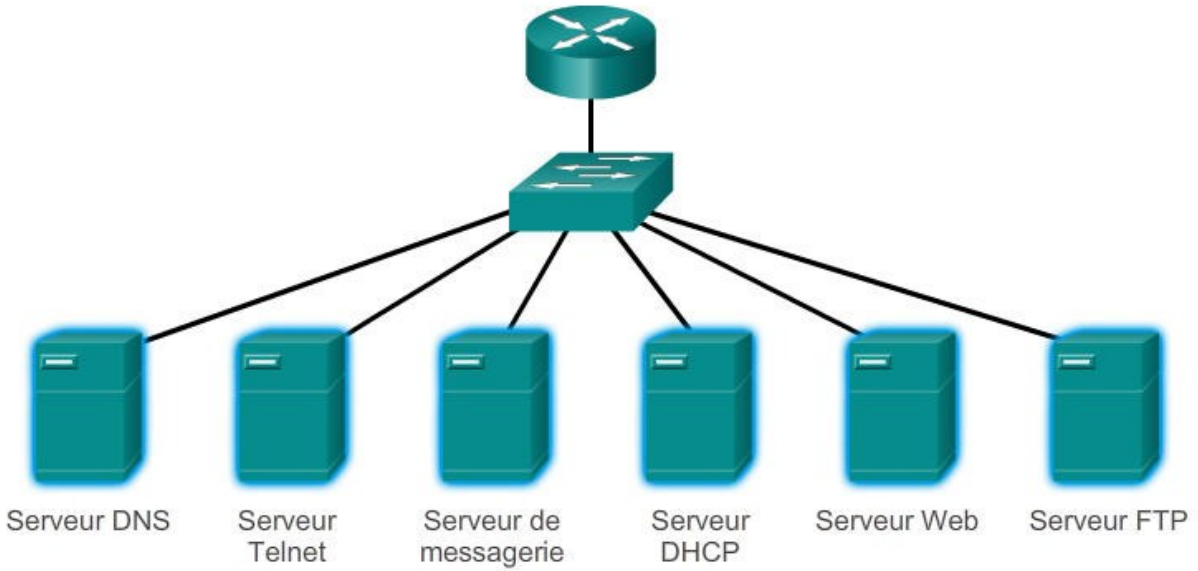


Adressage pour un petit réseau

- 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

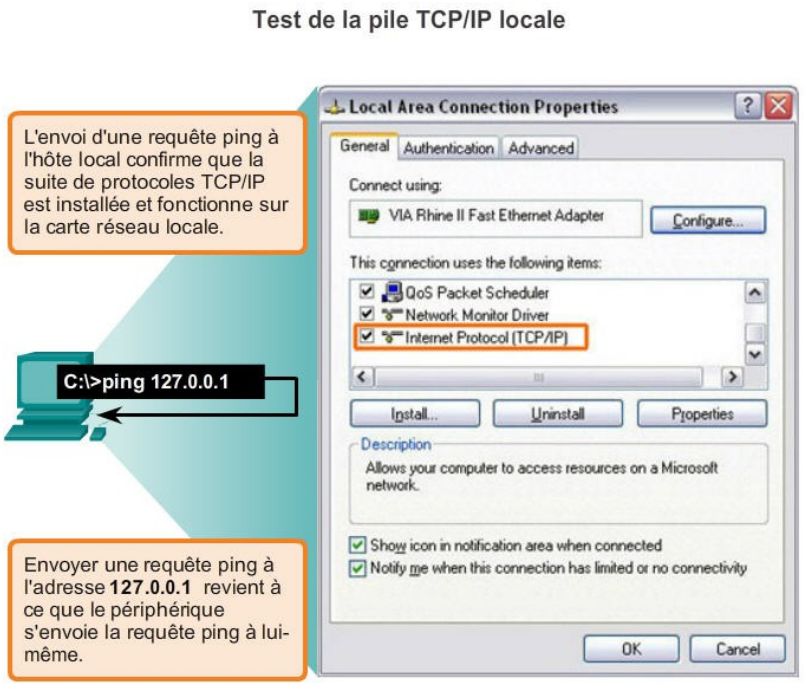
Applications courantes d'un petit réseau

- **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

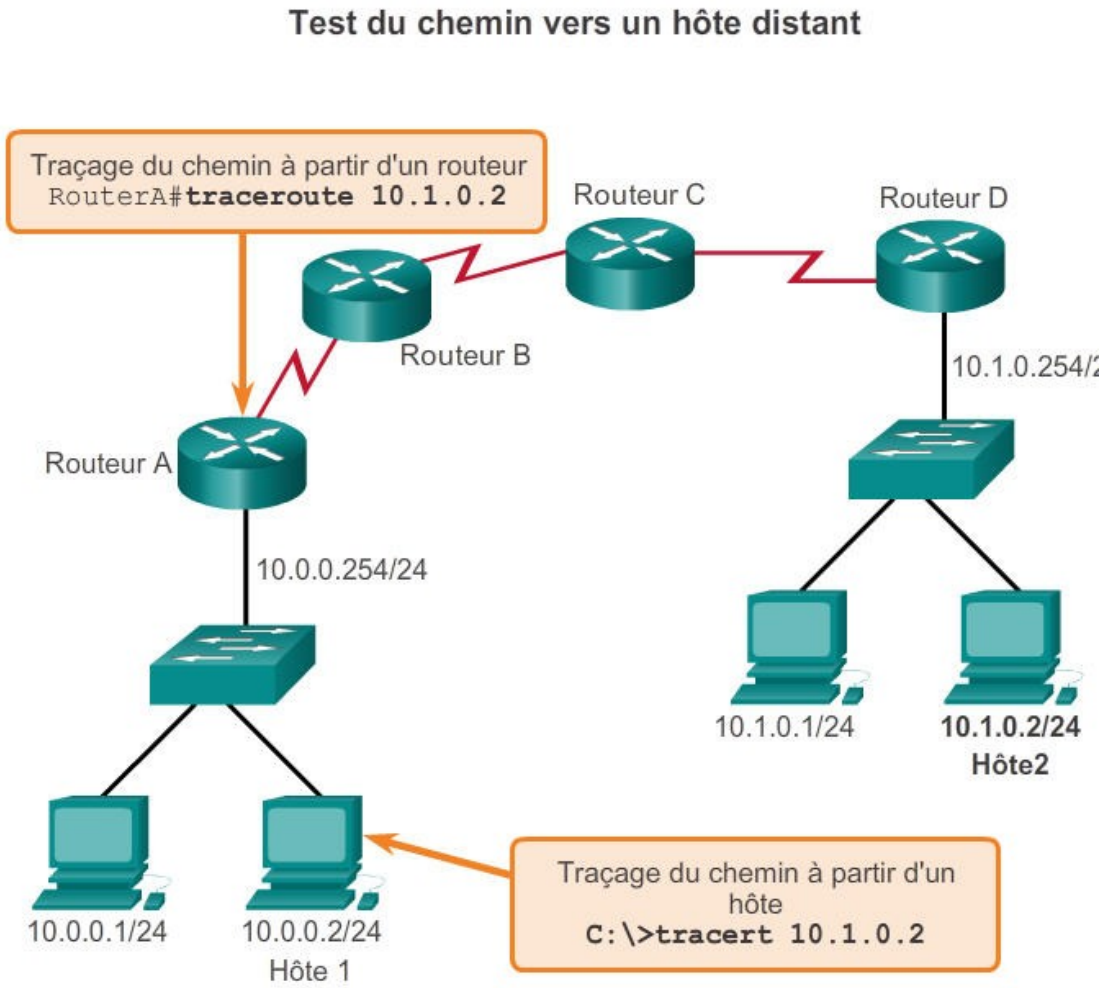


Ping : interprétation des messages ICMP

- **!** – 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.



Interprétation des messages tracert



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**

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:\>
```

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]
```

Scénarios de dépannage

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

```
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd4c:6609:6733:c5cc%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

C:\>
```

- 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

Périphérique multifonction

- Intègre un modem, un routeur, un serveur et un point d'accès sans fil
- Établit la connexion avec le FAI (fournisseur d’accès à Internet)
- Assure le routage, la commutation et la connectivité sans fil
- Est un serveur sur lequel sont installés des services courants : web, DHCP, VoIP ...

Résumé

- 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