



Chapitre 2 : Conception et dépannage d'un réseau



Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™



Chapitre 2 – Sections et objectifs

- 2.1 Conception du réseau
 - Identifier les équipements entrant dans la conception d'un réseau
 - Identifier les protocoles utilisés dans un réseau
 - Expliquer comment un petit réseau sert de base aux réseaux plus importants
- 2.2 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



Chapitre 2 : Sections et objectifs (suite)

- 2.3 Les commandes réseau de base
 - 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 la commandes ipconfig pour vérifier la configuration des périphériques réseau
 - Utiliser la commandes arp pour obtenir des informations sur les périphériques réseau
 - Utiliser la commande netstat pour obtenir des informations et des statistiques sur les connexions réseau
- 2.4 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



2.1 Conception du réseau



Cisco | Networking Academy®
Mind Wide Open™



Conception du réseau

Les appareils d'un réseau

- Topologies de réseaux
 - Se composent de routeurs, de commutateurs, de serveurs, des copieurs/imprimantes et des appareils des utilisateurs : les ordinateurs (PC/portable) + tablettes, smartphone, objets connectés...
 - L'utilisateur accède à Internet par une liaison WAN, par câble, par DSL ou fibre optique.
 - La gestion est assurée par une entreprise tierce ou un service interne.
- Critères de compatibilité des périphériques d'un réseau
 - 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).



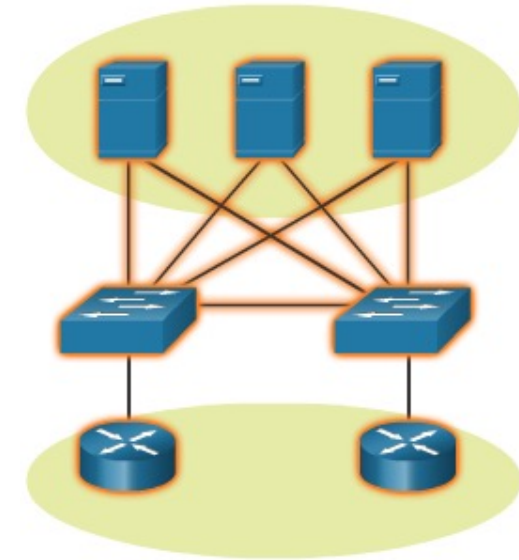


Conception du réseau

Les appareils d'un réseau (suite)

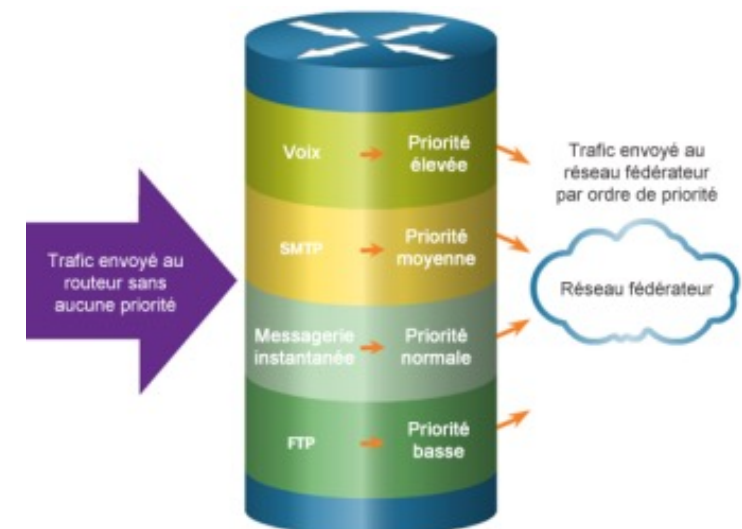
■ Redondance dans un réseau

- 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.

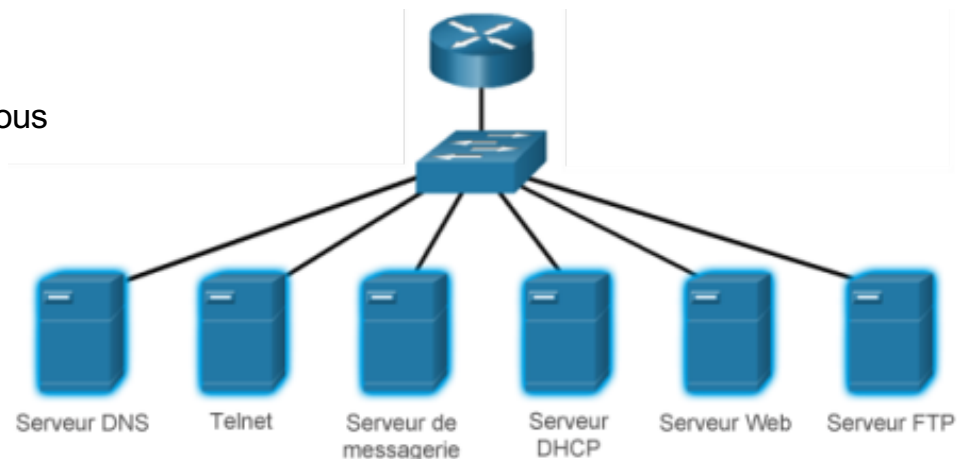




Conception du réseau

Les applications et les protocoles des réseaux

- 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
 - Applications en temps réel
 - Téléphonie IP
 - Visioconférence
 - Nécessitent une infrastructure performante





Conception du réseau

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 » sur l'utilisation des applications par les collaborateurs.





2.2 Sécurité du réseau



Cisco | Networking Academy®
Mind Wide Open™



Sécurité du réseau

Menaces pour la sécurité et vulnérabilités

■ Types de menaces

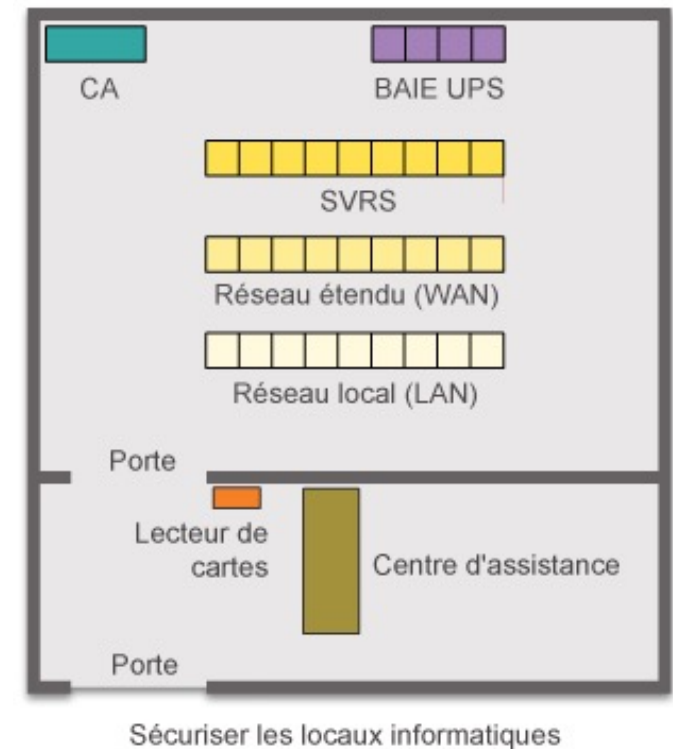
- Les intrusions électroniques peuvent coûter très cher.
- Elles sont souvent le résultat de vulnérabilités logicielles, d'attaques du matériel ou d'usurpation d'informations d'identification.
- Les menaces électroniques les plus courantes sont celles présentées dans l'illustration.

■ 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.





Sécurité du réseau

Attaques réseau

■ Types de programme malveillant

- Virus
- Vers
- Chevaux de Troie



■ Attaques de reconnaissance

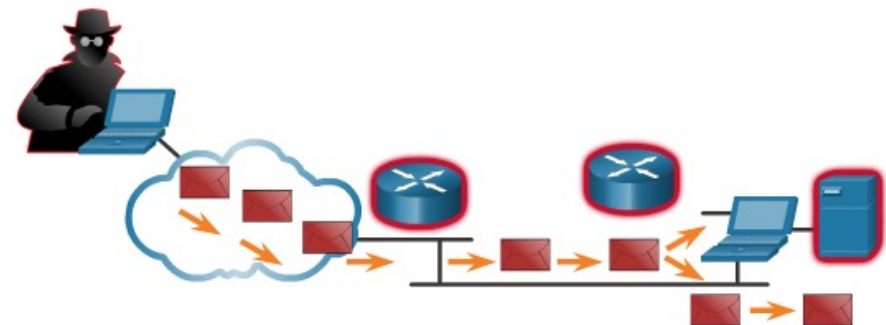
- Détection et mappage de systèmes et de services.
- Acquérir suffisamment d'informations sur le système ou le réseau cible pour identifier les vulnérabilités plus facilement.
- Les outils les plus courants fonctionnent souvent avec des services Internet publics et gratuits, tels que DNS et Whois.
-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



Sécurité du réseau

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





Sécurité du réseau

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 (Accounting) : les actions exécutées lors de l'accès à la ressource
 - Le cadre AAA peut être très utile pour réduire les attaques réseau.



Sécurité du réseau

Réduction des attaques réseau (suite)

■ Pare-feu

- 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 du réseau

Sécurité des appareils

- Présentation de la sécurité des périphériques
 - Les paramètres par défaut sont dangereux, car ils sont connus.
 - De plus, les paramètres suivants doivent être appliqués sur les systèmes avant leur mise en production :
 - 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
 - Ou alors faire l'utilisation d'une expression composée de plusieurs mots que l'on appelle « phrase secrète » ou « phrase de passe »



Sécurité du réseau

Sécurité des appareils (suite)

- Principes de sécurité de base
 - Les mots de passe forts sont efficaces uniquement s'ils sont secrets.
 - Les mots de passe doivent être chiffrés dans la configuration.
 - Les règles de gestion doivent 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.
 - Le système doit bloquer les tentatives de connexion pendant 120 secondes après trois échecs de connexion en l'espace de 60 secondes (par exemple)
 - Le réseau doit déconnecter automatiquement les utilisateurs inactifs sur un poste au bout d'un certain temps d'inactivité.
- Administration sécurisée à distance en ligne de commande
 - Telnet n'est pas sécurisé.
 - Il est fortement recommandé d'utiliser SSH à la place.
 - Pour configurer la prise en charge de SSH sur un périphérique, il faut suivre quatre étapes :
 - Étape 1. S'assurer que le périphérique a un nom d'hôte et une adresse IP uniques.
 - Étape 2. Générer les clés SSH.
 - Étape 3. Créer un nom d'utilisateur associé à un mot de passe.
 - Étape 4. Choisir un mode d'authentification (utilisateur/mot de passe ou certificats)



2.3 Les commandes réseau de base



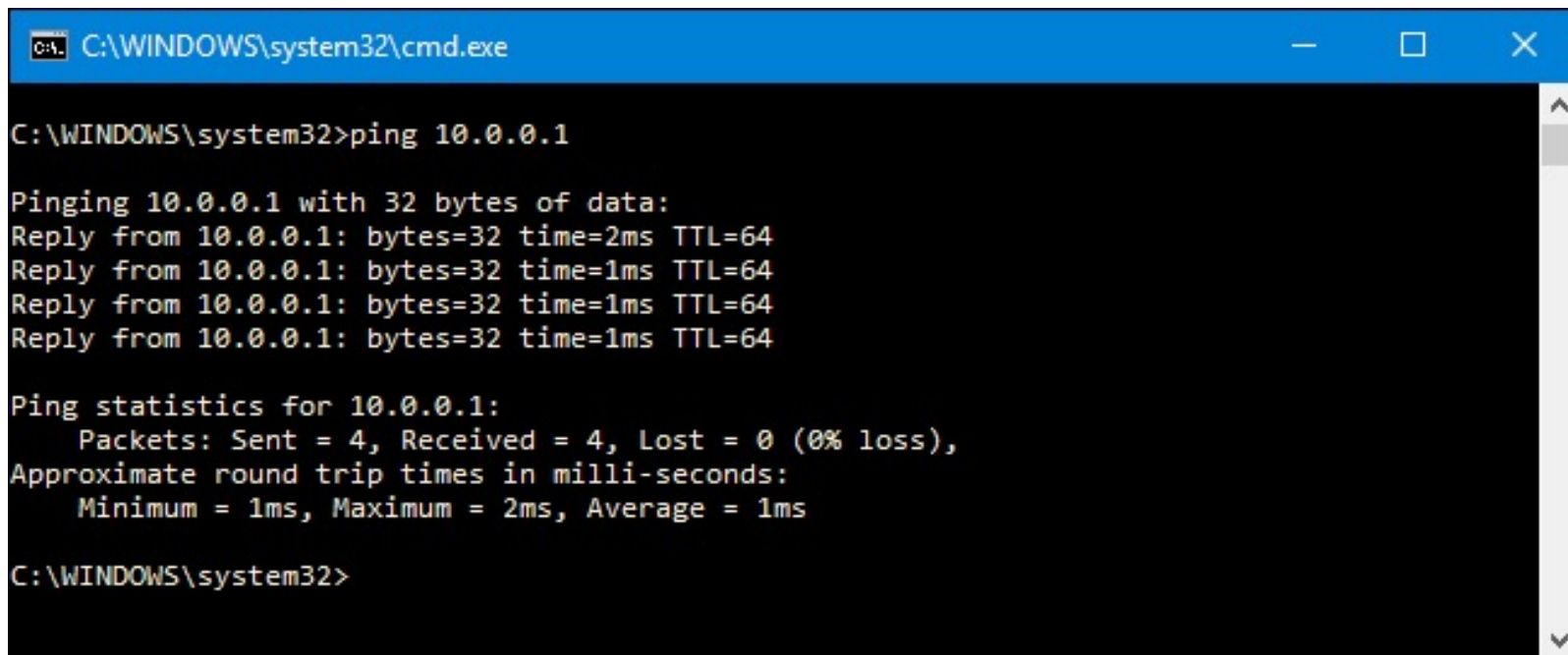
Cisco | Networking Academy®
Mind Wide Open™



Les commandes réseau de base

La commande ping

- Interprétation des résultats de requête ping
 - La commande ping permet de tester efficacement la connectivité.
 - Le protocole ICMP (Internet Control Message Protocol) vérifie la connectivité de la couche 3.
 - Un délai de réponse plus long peut être signe d'un problème de latence.



```

C:\WINDOWS\system32\cmd.exe

C:\WINDOWS\system32>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\WINDOWS\system32>
  
```




Les commandes réseau de base

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/Linux.

```

C:\> Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Chris>tracert google.com

Tracing route to google.com [173.194.33.169]
over a maximum of 30 hops:
  0  1 ms  1 ms  1 ms  192.168.1.254
  1  7 ms  7 ms  9 ms  10.31.188.1
  2  11 ms 34 ms 19 ms STILWAWBCI01.bb.telus.com [75.154.217.108]
  3  11 ms 11 ms 10 ms 74.125.49.177
  4  11 ms 11 ms 10 ms 209.85.249.34
  5  11 ms 11 ms 11 ms 209.85.244.65
  6  11 ms 10 ms 11 ms sea09s18-in-f9.1e100.net [173.194.33.169]

Trace complete.

C:\Users\Chris>
    
```



Les commandes réseau de base

La commande ipconfig

- La commande ipconfig de Windows donne la configuration réseau de l'ordinateur
- ipconfig affiche un résumé de la configuration (adresse IP, masque, passerelle)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Alain>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion linksys:

    Suffixe DNS propre à la connexion :
    Adresse IP. . . . . : 192.168.1.10
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.1

C:\Documents and Settings\Alain>
```



Les commandes réseau de base

La commande ipconfig (suite)

- La commande ipconfig /all donne la configuration réseau détaillée de l'ordinateur

```

C:\WINNT\System32\cmd.exe

C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . : WOLFPACK
        Primary DNS Suffix . . . . . :
        Node Type . . . . . : Hybrid
        IP Routing Enabled. . . . . : No
        WINS Proxy Enabled. . . . . : No
        DNS Suffix Search List. . . . . :

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix . :
        Description . . . . . : 3Com 3C920 Integrat
        Controller (3C905C-TX Compatible)
        Physical Address. . . . . : 00-B0-D0-12-34-56
        DHCP Enabled. . . . . : Yes
        Autoconfiguration Enabled . . . . . : Yes
        IP Address. . . . . : 152.7.x.x
        Subnet Mask . . . . . : 255.255.254.0
        Default Gateway . . . . . : 152.7.x.1
        DHCP Server . . . . . : 152.1.1.102
        DNS Servers . . . . . : 152.1.1.206
                                152.1.1.161
        Lease Obtained. . . . . : Tuesday, November 19, 2002 10:00:00 AM
        Lease Expires . . . . . : Monday, January 18, 2003 10:00:00 AM

C:\>_
  
```



Les commandes réseau de base

La commande ipconfig

- D'autres options
 - Permettent la gestion de la résolution de noms (protocole DNS) et de la configuration réseau automatique (protocole DHCP)
 - ipconfig /flushdns
 - ipconfig /displaydns
 - ipconfig /release
 - ipconfig /renew



Les commandes réseau de base

La commande arp

- ARP est le protocole assurant la correspondance entre les adresses MAC et les adresses IP des hôtes sur le réseau local
 - 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.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>arp -a

Interface: 10.1.10.55 --- 0xc
Internet Address      Physical Address      Type
10.1.10.1             00-13-f7-f8-94-12    dynamic
10.1.10.129           00-24-d2-8a-e8-fd    dynamic
10.1.10.255           ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.60            01-00-5e-00-01-3c    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Andrew>
    
```




Les commandes réseau de base

La commande netstat

- netstat est un utilitaire réseau affichant des informations sur les connexions et les configurations réseau ainsi que leurs statistiques
- De nombreuses options sont possibles

```
C:\>netstat -ano

Active Connections

    Proto Local Address          Foreign Address         State       PID
    TCP    0.0.0.0:135             0.0.0.0:0               LISTENING   680
    TCP    0.0.0.0:445             0.0.0.0:0               LISTENING   4
    TCP    0.0.0.0:3389            0.0.0.0:0               LISTENING   1128
    TCP    0.0.0.0:49152           0.0.0.0:0               LISTENING   348
    TCP    0.0.0.0:49153           0.0.0.0:0               LISTENING   772
    TCP    0.0.0.0:49154           0.0.0.0:0               LISTENING   896
    TCP    0.0.0.0:49155           0.0.0.0:0               LISTENING   432
    TCP    0.0.0.0:49156           0.0.0.0:0               LISTENING   448
    TCP    10.0.2.15:139           0.0.0.0:0               LISTENING   4
    TCP    [::]:135                [::]:0                  LISTENING   680
    TCP    [::]:445                [::]:0                  LISTENING   4
    TCP    [::]:3389               [::]:0                  LISTENING   1128
    TCP    [::]:49152              [::]:0                  LISTENING   348
    TCP    [::]:49153              [::]:0                  LISTENING   772
    TCP    [::]:49154              [::]:0                  LISTENING   896
    TCP    [::]:49155              [::]:0                  LISTENING   432
    TCP    [::]:49156              [::]:0                  LISTENING   448
    UDP    0.0.0.0:5355            *:*                      1128
```



2.4 Dépannage du réseau



Cisco | Networking Academy®
Mind Wide Open™



Dépannage du réseau

Méthodes de dépannage

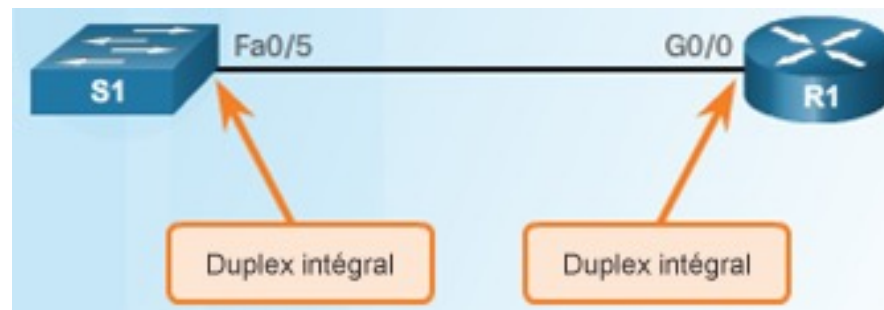
- Méthodes de dépannage de base
 - Identifier le problème
 - Élaborer une théorie des causes probables
 - Tester la théorie pour déterminer la cause
 - Établir un plan d'action pour résoudre le problème et implémenter la solution
 - Vérifier l'intégralité des fonctionnalités du système et implémenter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



Dépannage du réseau

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 des logs peuvent signaler un problème de correspondance du mode duplex.





Dépannage du réseau

Scénarios de dépannage

- Problèmes d'adressage IP sur périphériques
 - Erreurs d'affectation manuelle
 - Erreurs liées à DHCP
 - Adresses en double (conflit)
- 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



```

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:\>
    
```




2.5 Synthèse du chapitre



Cisco | Networking Academy®
Mind Wide Open™



