

Télécommunications et Réseaux

Chapitre 5 : Système d'exploitation de réseau

Cours de M. Pétein Thomas

Email : thomas.petein@heh.be

Introduction

Les réseaux domestiques relient généralement une grande variété de périphériques finaux, notamment des ordinateurs de bureau, des ordinateurs portables, des tablettes, des smartphones, des télévisions connectées, des lecteurs multimédias réseau compatibles DLNA,...

DLNA (*Digital Living Network Alliance*) est une alliance de plus de 250 sociétés, fabricants d'appareils électroniques, de périphériques informatiques, d'ordinateurs personnels, de téléphones mobiles et opérateurs de services et de contenus.

DLNA définit un standard d'interopérabilité permettant la lecture, le partage et le contrôle d'appareils multimédia indépendamment de leur marque ou de leur nature.



Système d'exploitation de réseau

Tous ces périphériques finaux se connectent généralement à un routeur domestique. Les routeurs domestiques regroupent en fait 4 périphériques en un :

- **Router** - Transfère les paquets de données vers Internet et reçoit des paquets depuis Internet.
- **Switch** - Connecte des périphériques finaux à l'aide de câbles réseau.
- **Point d'accès sans fil** - Se compose d'un émetteur radio capable de connecter des périphériques finaux sans fil.
- **Pare-feu** - Sécurise le trafic sortant et contrôle le trafic entrant.

Bien entendu, dans les réseaux d'entreprise comportant beaucoup plus de périphériques et gérant plus de trafic, ces périphériques sont souvent intégrés comme des périphériques indépendants et autonomes, assurant un service spécifique.

Chaque périphérique est très différent en termes de matériel, d'utilisation et de fonctionnalités. Cependant, dans tous les cas, c'est le système d'exploitation qui permet au matériel de fonctionner !

Système d'exploitation de réseau

Les systèmes d'exploitation sont utilisés sur tous les périphériques, depuis les périphériques utilisateur comme les smartphones, les tablettes, les ordinateurs de bureau, les ordinateurs portables jusqu'aux périphériques réseau tel que les commutateurs, les routeurs, les points d'accès sans fil et les pare-feu.

Bien sûr nous n'allons pas utiliser le même système d'exploitation sur des périphériques complètement différents, il faut que ce système soit adapté aux fonctionnalités et aux performances spécifique du matériel qu'il va devoir gérer.

Ce qui va nous intéresser dans ce chapitre, c'est le système d'exploitation que l'on peut retrouver sur des périphériques réseaux.

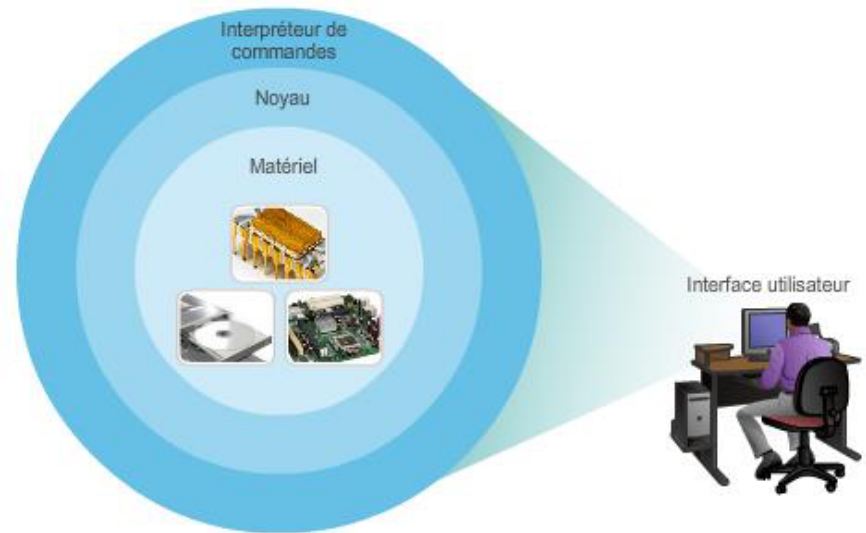
Cisco IOS

Cisco Internetwork Operating System (IOS) est un terme générique utilisé pour désigner l'ensemble des systèmes d'exploitation réseau utilisés sur les périphériques réseau Cisco.

Lorsqu'un ordinateur est mis sous tension, il charge, à partir d'un disque dur, le système d'exploitation dans la mémoire vive (RAM).

La partie du code du système d'exploitation directement liée au matériel informatique s'appelle le noyau.

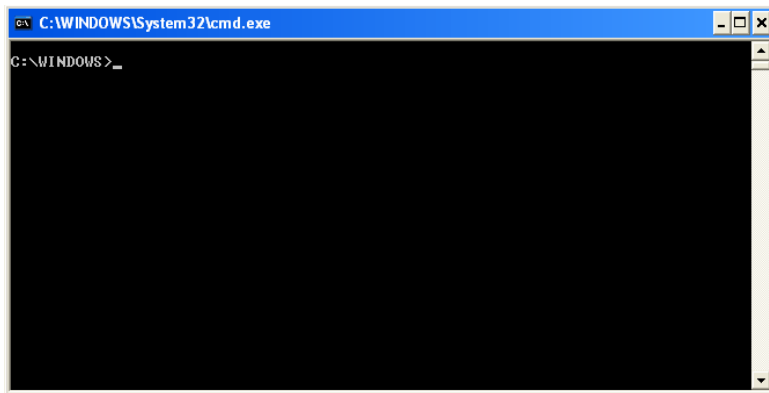
La partie liée aux applications et à l'utilisateur s'appelle l'interpréteur de commandes. L'utilisateur accède à l'interpréteur de commandes à l'aide de l'interface de ligne de commande (CLI) ou de l'interface graphique utilisateur.



Système d'exploitation de réseau

Lorsqu'il utilise l'interface de ligne de commande, l'utilisateur accède directement au système dans un environnement textuel, en entrant des commandes au clavier, dans une invite de commande.

En règle générale, le système exécute la commande en fournissant une sortie textuelle. L'interface graphique permet à l'utilisateur d'accéder au système dans un environnement qui offre des images, du contenu multimédia et du texte. Les actions sont exécutées par le traitement des images à l'écran.



Interface en ligne de commande de Windows



Interface graphique de Windows

Système d'exploitation de réseau




La plupart des systèmes d'exploitation des périphériques finaux sont accessibles via une interface graphique (et certains proposent les deux).

Lorsqu'on parle du système d'exploitation des routeurs domestiques, vous entendrez parler de « firmware ». La méthode la plus courante pour configurer un routeur domestique est d'utiliser un navigateur Web pour accéder à une interface graphique conviviale.


Cisco IOS est utilisé par la plupart des périphériques Cisco, quels que soient leur taille et leur type. La méthode la plus courante pour accéder à ces périphériques est d'utiliser la CLI.

Cisco IOS étant un terme qui fait référence aux différents systèmes d'exploitation qui s'exécutent sur divers périphériques réseau, il existe de nombreuses versions différentes de Cisco IOS :

Cisco Catalyst 2960-48TT-L Switch

Search...  **Release 12.2.55-SE9 ED** ☆☆☆☆☆ Write a Review [Release Notes for 12.2\(55\)SE9](#)  Add Devices  Add Notification

Expand All | Collapse All

▼ Suggested
12.2.55-SE9(ED) 



► Latest

▼ All Releases

▼ 15.0

▼ **15.0SE**

- 15.0.2-SE6(ED)
- 15.0.2-SE5(ED)
- 15.0.2-SE4(ED)
- 15.0.2-SE2(ED)
- 15.0.2-SE1(ED)
- 15.0.2-SE(ED)
- 15.0.1-SE3(ED)
- 15.0.1-SE2(ED)
- 15.0.1-SE1(ED)
- 15.0.1-SE(ED)

File Information ▲	Release Date	DRAM/Flash	
LAN BASE  c2960-lanbase9-mz.122-55.SE9.bin	18-MAR-2014	64 / 32	Download Add to cart
LAN BASE WITH WEB BASED DEV MGR  c2960-lanbase9-tar.122-55.SE9.tar	18-MAR-2014	64 / 32	Download Add to cart

De la même façon qu'un PC peut exécuter Microsoft Windows 10, un périphérique réseau Cisco exécute une version spécifique de Cisco IOS. La version de l'IOS dépend du type de périphérique utilisé et des fonctions nécessaires. Il est d'ailleurs possible de mettre à niveau l'IOS pour obtenir de nouvelles fonctionnalités par exemple.

Le fichier IOS proprement dit, dont la taille atteint plusieurs méga-octets, est stocké dans une zone de mémoire semi-permanente appelée **Flash**.

La mémoire Flash assure un stockage non volatil. En d'autres termes, cette mémoire conserve son contenu lorsque le périphérique n'est plus sous tension.

Bien que le contenu de la mémoire Flash ne soit pas perdu en cas de perte d'alimentation, il peut être modifié ou remplacé si nécessaire. Cela permet de mettre à niveau l'IOS.

Dans de nombreux périphériques Cisco, l'IOS est copié de la mémoire Flash vers la mémoire vive (RAM) lorsque le périphérique est mis sous tension.

L'IOS s'exécute alors depuis la mémoire vive lorsque le périphérique fonctionne. L'exécution de l'IOS sur la mémoire vive augmente les performances du périphérique, c'est pourquoi il est copié dans celle-ci.

Cependant attention, la mémoire vive est considérée comme de la mémoire volatile ce qui signifie que les données sont perdues en cas de coupure d'alimentation.

Les quantités de mémoire Flash et de mémoire vive requises varient selon la version de l'IOS. Dans le cadre de la maintenance et de la planification réseau, il est important de déterminer les besoins relatifs à la mémoire Flash et à la mémoire vive pour chaque périphérique car il est possible que les nouvelles versions d'IOS requièrent plus de mémoire vive et de mémoire Flash que la quantité disponible sur les périphériques...

Système d'exploitation de réseau

Les routeurs et les commutateurs Cisco assurent principalement les fonctions suivantes, ou permettent de les effectuer :

- Garantir la sécurité du réseau
- L'adressage IP des interfaces virtuelles et physiques
- Les configurations spécifiques aux interfaces pour optimiser la connectivité des supports respectifs
- Routage
- Les technologies de qualité de service (QoS)
- La prise en charge des technologies de gestion de réseau

Il y a plusieurs moyens d'accéder à l'interface CLI :

- via le port console
- via telnet ou SSH
- via le port AUX

Console

On peut accéder au CLI via une session **console**, aussi appelée **ligne CTY**. La console connecte directement un ordinateur ou un terminal au port de console du routeur ou du commutateur via une liaison série lente.

Le port de console est un port de gestion permettant un accès hors réseau à un routeur.

La console s'utilise en particulier dans les circonstances suivantes :

- ✓ configuration initiale du périphérique réseau
- ✓ procédures de reprise après sinistre, dépannage lorsque l'accès distant est impossible
- ✓ procédures de récupération des mots de passe

Telnet et SSH

Une autre méthode d'accès distant à une session CLI consiste à établir une connexion **Telnet** avec le routeur.

À la différence des connexions console, les sessions Telnet requièrent des services réseau actifs sur le périphérique.

→ On ne peut accéder au périphérique Cisco que lorsque celui-ci possède une interface active configurée avec une adresse de couche 3, par exemple une adresse IPv4.

Un hôte doté d'un client Telnet peut accéder aux **sessions vty** en cours d'exécution sur le périphérique Cisco. *Pour des raisons de sécurité, IOS exige l'emploi d'un mot de passe dans la session Telnet en guise de méthode d'authentification minimale.*

Le protocole **Secure Shell** (noté **SSH**) permet un accès distant plus sécurisé aux périphériques.

SSH est la version sécurisée de Telnet. Il fournit une authentification par mot de passe plus résistante que celle de Telnet et il emploie un chiffrement lors du transport des données de la session.

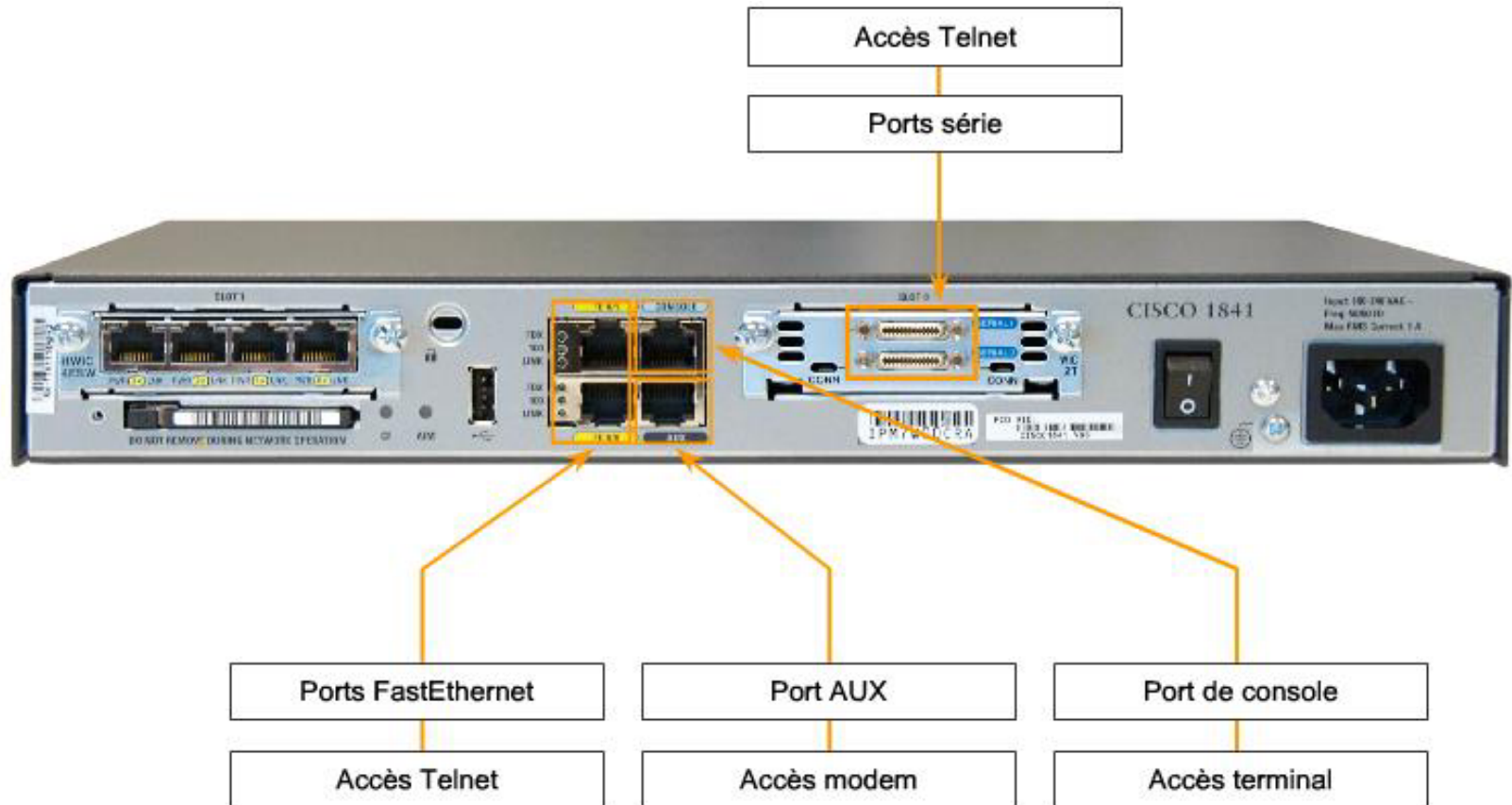
→ **Il est conseillé de toujours utiliser SSH à la place de Telnet dans la mesure du possible.**

AUX

La dernière façon d'ouvrir une session CLI à distance consiste à établir une connexion téléphonique commutée à travers un modem connecté au **port AUX** du routeur.

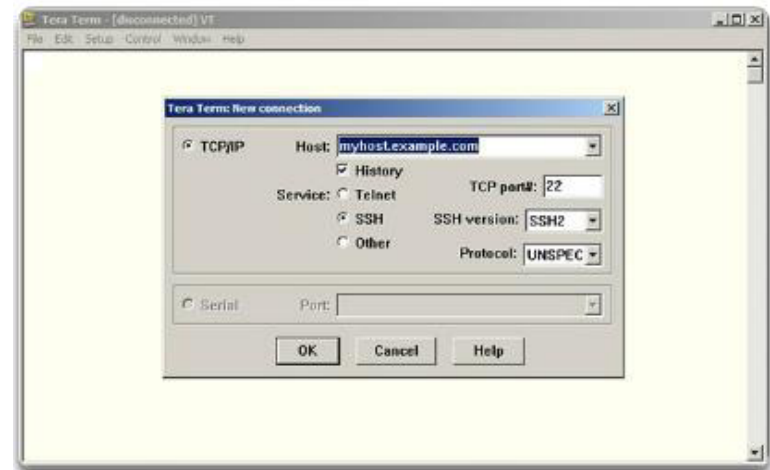
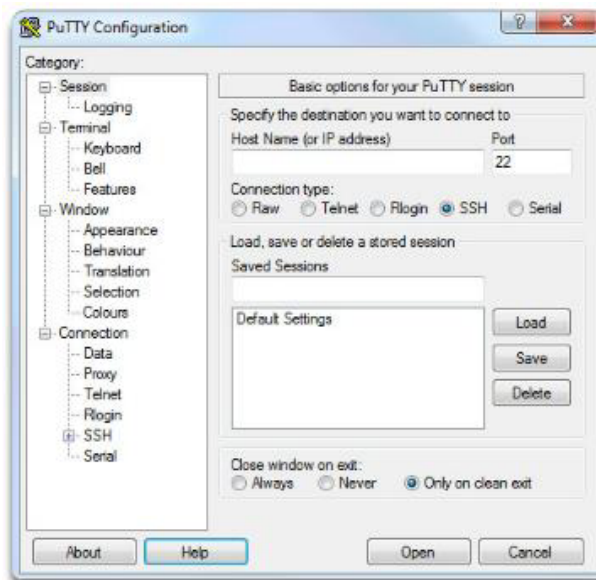
Comme le port console, cette méthode ne requiert ni la configuration, ni la disponibilité de services réseau sur le périphérique. Néanmoins, il ne s'utilise localement à la place du port de console qu'en cas de problèmes liés au port de console !

Système d'exploitation de réseau



Il existe d'excellents programmes d'émulation de terminal disponibles pour se connecter à un périphérique réseau via une connexion série sur un port de console ou via une connexion Telnet/SSH.

Exemples : PuTTY, Tera Term, HyperTerminal



Les périphériques réseau ont besoin de deux types de logiciels pour fonctionner : le système d'exploitation et le logiciel de configuration.

Les fichiers de configuration contiennent les commandes du logiciel Cisco IOS utilisées pour personnaliser les fonctionnalités d'un périphérique Cisco.

Un périphérique réseau Cisco contient deux fichiers de configuration :

- le fichier de configuration en cours, utilisé par le périphérique en fonctionnement normal.
- le fichier de configuration initiale, qui est chargé dans la mémoire vive, quand le périphérique démarre. Il sert également de copie de sauvegarde de la configuration.

Remarque : Il est également possible de stocker un fichier de configuration à distance (sur un serveur FTP par exemple) en guise de copie de sauvegarde.

1. Le fichier de configuration initiale

Le fichier de configuration initiale (« **startup-config** ») est utilisé au démarrage du système pour configurer le périphérique. Il est stocké en mémoire vive non volatile (NVRAM), ce qui implique que ce fichier reste intact lorsque le périphérique Cisco est mis hors tension.

Lors du démarrage (ou du redémarrage), les fichiers « startup-config » sont chargés en mémoire vive.

Une fois chargé en mémoire vive, le fichier de configuration initiale est considéré comme étant la configuration en cours, également appelée « running-config ».

2. Le fichier de configuration en cours

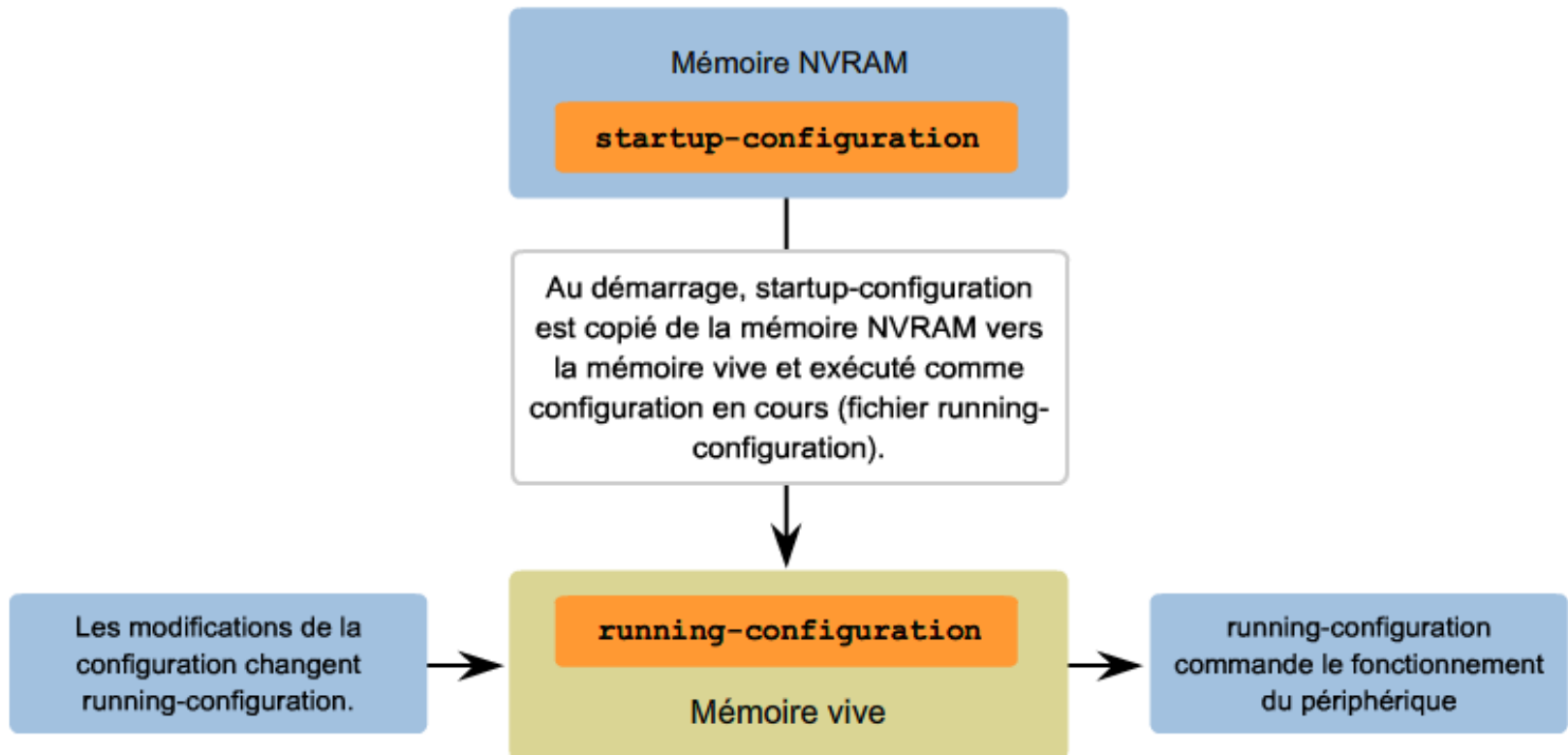
La « running-config » est modifiée lorsque l'administrateur réseau configure le périphérique. *Les modifications de la configuration en cours produisent immédiatement leurs effets sur le fonctionnement du périphérique Cisco.*

Comme le fichier de configuration en cours se trouve en mémoire vive, son contenu est perdu si le périphérique est éteint ou redémarre. Cependant, l'administrateur a la possibilité de les enregistrer dans le fichier startup-config afin qu'elles soient réutilisées lors du redémarrage suivant du périphérique !

Pour sauvegarder le fichier de configuration en cours en tant que fichier de configuration initial, il suffit d'utiliser la commande :

S1# copy running-config startup-config

Système d'exploitation de réseau



Cisco IOS a été conçu comme un système d'exploitation offrant différents modes d'exploitation (ayant chacun son propre domaine de fonctionnement) organisés selon une structure hiérarchique.

Dans l'ordre de haut en bas, les principaux modes sont les suivants :

- mode d'exécution utilisateur
- mode d'exécution privilégié
- mode de configuration globale
- autres modes de configuration spécifiques

Chaque mode permet d'effectuer des tâches particulières et possède un jeu de commandes spécifiques qui sont disponibles lorsque le mode est en vigueur

Certaines commandes sont à la disposition de tous les utilisateurs ; d'autres ne peuvent être exécutées qu'après passage au mode dans lequel elles sont disponibles.

Chaque mode est identifié par une invite distincte qui ne permet d'entrer que les commandes appropriées pour ce mode et une authentification différente peut être requise pour chaque mode hiérarchique.

User EXEC Command-Router>

ping
show (limited)
enable
etc...

Privileged EXEC Commands-Router#

all User EXEC Commands
debug commands
reload
configure
etc..

Global Configuration Commands-Router(config)#

hostname
enable secret
ip route

interface ethernet
serial
bri
etc.

Interface Commands-Router(config-if)#

ip address
ipx network
encapsulation
shutdown/ no shutdown
etc..

router rip
ospf
eigrp

Routing Engine Commands-Router(config-router)#

network
version
auto summary

Invite de commande du mode d'exécution utilisateur

```
Router>ping 192.168.10.5
```

Invite de commande du mode d'exécution privilégié

```
Router#show running-config
```

Invite de commande du mode de configuration globale

```
Router (config) #Interface FastEthernet 0/0
```

Invite de commande d'un mode de configuration spécifiques

```
Router (config-if) #ip address 192.168.10.1 255.255.255.0
```

1. Le mode d'exécution utilisateur

Le mode d'exécution utilisateur est le point d'entrée de l'environnement CLI.

→ Il a des pouvoirs restreints !

Il n'autorise aucune commande susceptible de modifier la configuration du périphérique, juste des commandes de visualisation.

Par défaut, il est accessible sans authentification mais il est néanmoins conseillé d'en définir une lors de la configuration initiale.

2. Le mode d'exécution privilégié

Ce mode avancé permet d'accéder aux informations détaillées et aux commandes de configuration et de gestion du périphérique.

Pour accéder à ce mode privilégié, il faut, à partir du mode utilisateur, utiliser la commande « **enable** ». La commande « disable » permet quant à elle de repasser du mode d'exécution privilégié au mode d'exécution utilisateur.

Tout comme le premier, il est accessible sans authentification par défaut, mais il est néanmoins vivement conseillé de définir un mot de passe pour y accéder lors de la configuration initiale du matériel.

3. Le mode de configuration globale

Ce mode permet d'effectuer des commandes de configuration globales sur l'équipement.

Il est accessible à partir du mode de configuration privilégié via la commande **S1#configure terminal**

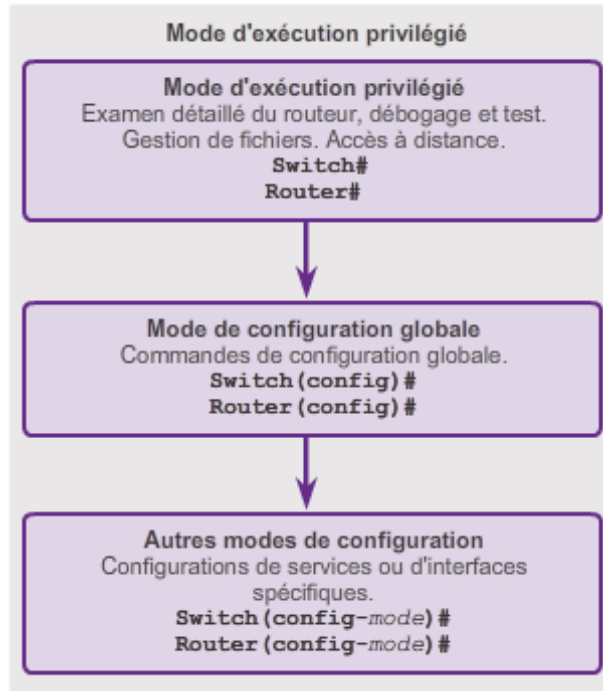
4. Les autres modes de configuration

Ce mode permet d'effectuer des commandes de configuration d'un service ou d'une interface spécifique tel que :

- Mode interface : pour configurer l'une des interfaces réseau (Fa0/0, S0/0/0,...)
- Mode ligne : pour configurer l'une des lignes physiques ou virtuelles (console, VTY,...)
- Mode routeur : pour configurer les paramètres de l'un des protocoles de routage.

Remarque : Pour quitter un mode de configuration, taper la commande **end** ou **exit**.

Système d'exploitation de réseau



Exemple :

```
Router>ping 192.168.10.5

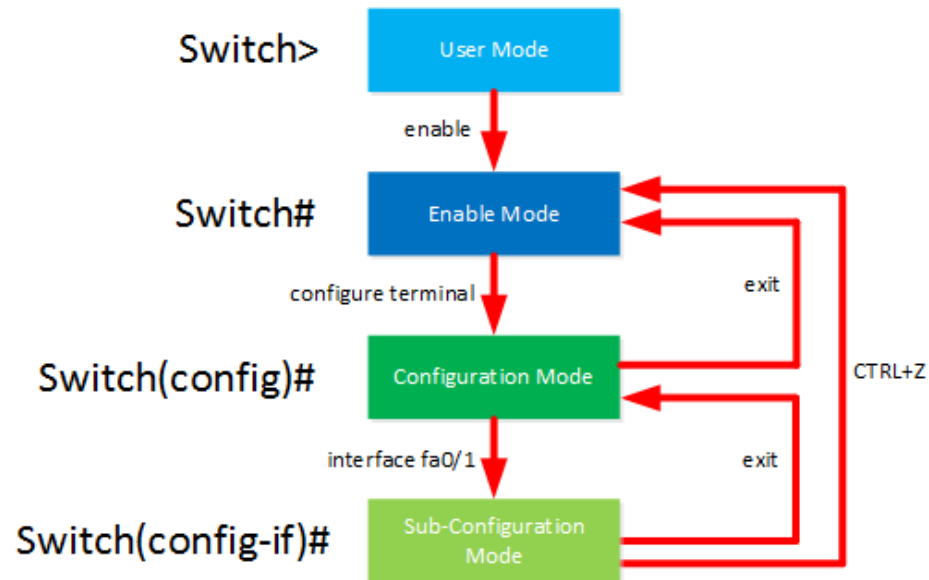
Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

Système d'exploitation de réseau

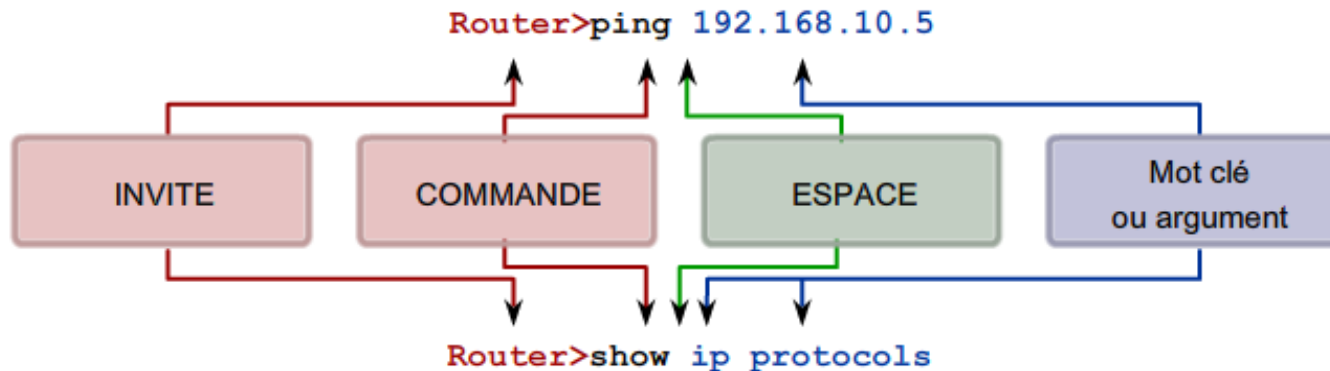
Passage d'un mode de configuration à l'autre :



Syntaxe de commandes

Un périphérique Cisco IOS prend en charge de nombreuses commandes. Chaque commande IOS a un format ou une syntaxe spécifique et ne peut être exécutée que dans le mode approprié.

En général, vous entrez une commande en tapant un nom de commande suivi des *mots-clés* et des *arguments* appropriés.



Les mots-clés décrivent des paramètres spécifiques à l'interpréteur de commandes. Par exemple, la commande **show** affiche des informations sur le périphérique.

Cette commande admet divers mots-clés permettant de préciser le type d'informations à afficher.

Exemple : S1# **show running-config**

La commande **show** est suivie du mot-clé **running-config**. Ce mot-clé spécifie que vous voulez afficher la configuration en cours.

Une commande peut exiger un ou plusieurs arguments. Un argument n'est généralement pas un mot prédéfini, contrairement à un mot clé. Un argument est une valeur ou une variable définie par l'utilisateur.

Conventions typographiques utilisées dans les commandes Cisco

Par exemple, la syntaxe d'une commande **description** est :

Switch(config-if)# **description** *chaîne*

Dans cet exemple, le texte en gras indique les commandes et les mots-clés à saisir tels quels et le texte en italique indique un argument pour lequel vous devez fournir une valeur.

Switch(config-if)# **description** Commutateur du QG

commande ← → argument

Convention	Description
boldface	Le texte en gras indique des commandes et des mots clés que l'utilisateur entre tels quels.
<i>italics</i>	Le texte en italique indique des arguments dans lesquels l'utilisateur fournit des valeurs.
[X]	Les crochets encadrent un élément facultatif (mot clé ou argument).
	Un trait vertical indique un choix dans un ensemble de mots clés ou d'arguments facultatifs ou obligatoires.
[X Y]	Les crochets encadrent un élément facultatif (mot clé ou argument).
{X Y}	Les accolades encadrant des mots clés ou des arguments séparés par un trait vertical indiquent un choix obligatoire.

Remarque : Lorsque vous utilisez une commande dans le CLI, il n'y a pas de distinction entre les majuscules et les minuscules.

La liste des commandes est la source d'informations de référence pour trouver une commande IOS particulière, de la même manière qu'un dictionnaire est la source de référence pour obtenir des informations sur un mot particulier.

On peut donc aller sur le site www.cisco.com pour obtenir des versions PDF (téléchargeables) des listes complètes de commandes disponibles pour un certain matériel et une certaine version d'IOS.

Aide dans l'IOS

IOS propose plusieurs formes d'aide :

- **aide contextuelle** : permet, grâce à « ? », d'afficher la liste des commandes, des mots clés et des arguments disponibles dans le contexte du mode en vigueur.

```
Cisco#cl?  
clear  clock  
Cisco#clock ?  
set    Set the time and date
```

- **vérification de la syntaxe d'une commande** : Lorsque vous soumettez une commande, l'interpréteur de commandes analyse la commande de gauche à droite pour déterminer l'action demandée.

S'il comprend la commande, alors il l'exécute.

S'il y a une erreur, il affiche un message.

Il existe trois types de messages d'erreur :

- commande ambiguë : l'interpréteur indique que vous n'avez pas entré assez de caractères pour permettre de reconnaître la commande

```
Switch#c  
% Ambiguous command: 'c'
```

- commande incomplète : quand il manque des mots clés ou des arguments obligatoires à la fin de la commande.

```
Switch#>clock set  
% Incomplete command.
```

- commande incorrecte : il renvoie un accent circonflexe (« ^ ») pour indiquer l'emplacement de l'erreur.

```
Switch#clock set 19:50:00 25 6  
                                     ^  
% Invalid input detected at '^' marker.
```

- **touches d'accès rapides et raccourcis**

Les plus importantes sont les suivantes :

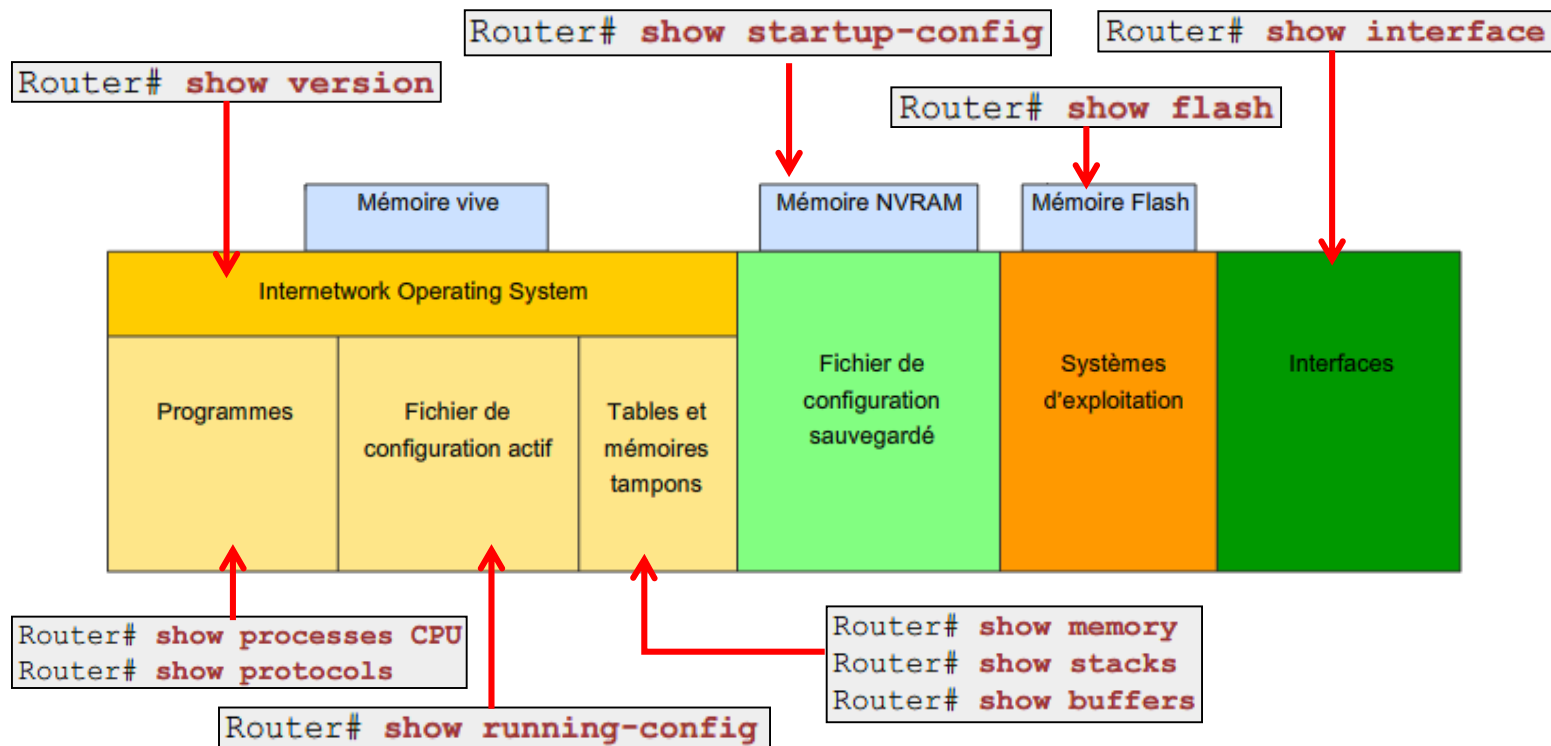
- **Flèche Bas** – permet à l'utilisateur de faire défiler les commandes précédentes, de la plus ancienne à la plus récente
- **Flèche Haut** – permet à l'utilisateur de faire défiler les commandes précédentes, de la plus récente à la plus ancienne
- **TAB** – permet de compléter automatiquement une commande ou un paramètre abrégé si l'abréviation contient suffisamment de lettres pour exclure toute ambiguïté par rapport aux autres commandes disponibles.
- **Ctrl + Z** – permet de passer du mode de configuration au mode d'exécution utilisateur privilégié
- **Ctrl + C** – quitte le mode de configuration ou annule la commande actuelle
- **Ctrl + Maj + 6** (avec un clavier QWERTY) - Permet à l'utilisateur d'interrompre un processus IOS comme ping ou traceroute. Avec un clavier AZERTY, il faudra utiliser le raccourci : **Ctrl + Maj + 9**.

Il y a d'autres touches de raccourcis comme par exemple :

- **Ctrl + A** – place le curseur au début de la ligne
- **Ctrl + E** – place le curseur à la fin de la ligne
- **Ctrl + R** - Afficher à nouveau la ligne permet d'actualiser la ligne qui vient d'être saisie. Par exemple, il peut arriver qu'un message IOS s'affiche dans l'interface CLI juste au moment où vous tapez une ligne. Vous pouvez alors utiliser **Ctrl-R** pour rappeler votre ligne afin d'éviter de la retaper.

Commandes IOS d'examen

Pour contrôler et dépanner le réseau, il est nécessaire d'examiner le fonctionnement des périphériques. La commande d'examen de base est la commande **show**.



Parmi les plus fréquentes au niveau des commandes show, on peut citer :

show version : Affiche des informations sur la version du logiciel chargé actuellement ainsi que des renseignements sur le matériel et le périphérique.

show arp : Affiche la table ARP du périphérique.

show mac-address-table : (uniquement pour les commutateurs) Affiche la table MAC d'un commutateur.

show startup-config : Affiche la configuration enregistrée en mémoire NVRAM.

show running-config : Affiche le contenu du fichier de configuration en cours, la configuration d'une interface spécifique, ou des informations sur les classes de mappage.

show ip interfaces : Affiche des statistiques IPv4 pour toutes les interfaces d'un routeur. Tandis que la commande **show ip interface brief** permet d'obtenir un bref résumé des interfaces et de leur état de fonctionnement.

Système d'exploitation de réseau

Version de l'IOS utilisé

```
Switch#sh version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
```

Version du boot loader

```
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
```

Type de processeur et sa mémoire vive

Type et nombre
d'interfaces

```
System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
```

Mémoire Flash
disponible

```
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 000A.4106.05B7
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number       : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC103321EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	26	WS-C2960-24TT	12.2	C2960-LANBASE-M

Configurations de base

Un commutateur est également l'un des éléments fondamentaux utilisés lors de la création d'un petit réseau. En reliant deux PC à un commutateur, ces ordinateurs disposeront d'une interconnectivité instantanée.

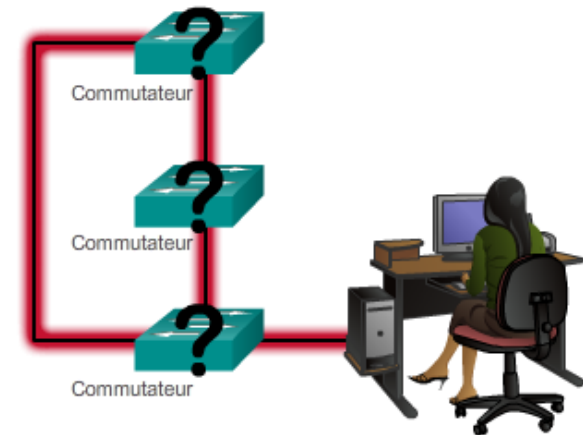
Pour ces raisons, le reste de ce chapitre porte sur la configuration de paramètres de base tels que l'attribution d'un nom d'hôte, la limitation de l'accès à la configuration du périphérique, la configuration des messages de bannière et l'enregistrement de la configuration.

Noms des périphériques

Par défaut, dans l'interface CLI, les noms d'hôtes de tout les commutateurs (ou des routeurs) seront les mêmes...

Le nom par défaut d'un commutateur Cisco IOS est « Switch ». Imaginez un interréseau disposant de plusieurs commutateurs portant le nom par défaut « Switch ».

Pas pratique pour les différencier et peu évident aussi de s'y retrouver !



→ Il est conseillé de les renommer correctement après avoir créer une convention d'attribution de noms, et cela en même temps que le schéma d'adressage afin d'assurer la continuité dans l'organisation.

Pour nommer les périphériques de façon cohérente et utile, il est nécessaire d'établir une convention d'attribution de noms applicable dans toute l'entreprise ou tout au moins à l'emplacement géographique des périphériques.

Il est conseillé de créer la convention d'attribution de noms en même temps que le schéma d'adressage afin d'assurer l'homogénéité au sein de l'entreprise.

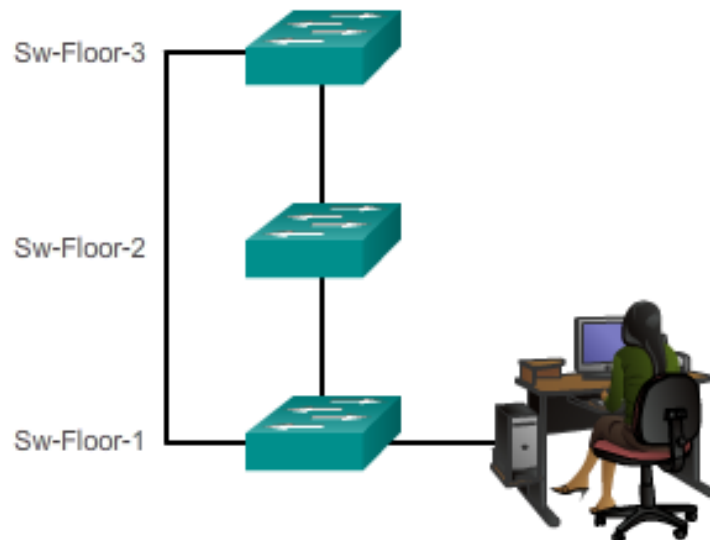
Exemple de conventions d'attribution des noms :

- Commencent par une lettre
- Ne contiennent pas d'espaces
- Se terminent par une lettre ou un chiffre
- Ne comportent que des lettres, des chiffres et des tirets
- Comportent moins de 64 caractères

Système d'exploitation de réseau

Si l'on reprend l'exemple précédent :

Pour créer une convention d'attribution de noms pour les commutateurs, vous devez prendre en compte leur emplacement et le rôle qu'ils jouent.



Pour configurer un nom à un switch (ou un routeur), il faut être dans le mode d'exécution privilégié et utiliser les commandes suivantes :

```
Switch#configure terminal  
Switch(config)#hostname Sw-Floor-1  
Sw-Floor-1(config)#
```

Si l'on veut supprimer le nom attribué à un périphérique, on utilisera la commande :

```
Sw-Floor-1(config)#no hostname  
Switch(config)#
```

Mots de passe et authentification

Ensuite, comme nous l'avons vu lorsque nous avons discuté des mesures de sécurité : tout périphérique doit être protégé par des mots de passe configurés localement afin d'en limiter l'accès.

Au niveau du choix des mots de passe, il est recommandé d'utiliser des mots de passe différents pour chacun des niveaux d'accès. En effet, bien que l'utilisation de plusieurs mots de passe différents ne facilite pas l'ouverture d'une session, cette précaution est nécessaire pour protéger convenablement l'infrastructure réseau contre l'accès non autorisé.

De plus il faut impérativement utiliser des mots de passe forts (c-à-d qui ne sont pas faciles à deviner).

Pour choisir les mots de passe, respectez les règles suivantes :

- Utilisez des mots de passe de plus de 8 caractères.
- Utilisez une combinaison de lettres majuscules et minuscules, des chiffres, des caractères spéciaux et/ou des séquences de chiffres dans les mots de passe.
- Evitez d'utiliser le même mot de passe pour tous les périphériques.
- Abstenez-vous d'employer des mots communs

1) Limiter l'accès au mode privilégié

On a dans ce cas deux possibilités :

- la commande **enable password**
- la commande **enable secret**

La seule différence entre les deux est que la commande **enable secret** offre une plus grande sécurité dans la mesure où le mot de passe est chiffré !

→ Il est donc recommandé d'utiliser celle-ci plutôt que l'autre.

Exemple :

```
Sw-Floor-1>enable
Sw-Floor-1#configure terminal
Sw-Floor-1(config)#enable password class
Sw-Floor-1(config)#exit
Sw-Floor-1#disable
Sw-Floor-1>
```

```
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

2) Limiter l'accès au périphérique via une connexion console

Pour ce faire, vous devez être en mode de configuration globale et taper la commande **line console 0**

Cette commande permet d'entrer en mode de configuration de ligne pour la console. Le zéro sert à représenter la première (et le plus souvent, la seule) interface de console.

Une fois dans le mode de configuration de la console, il vous suffira alors de taper la commande **password** suivie du mot de passe que vous désirez mettre..

Finalement, tapez la commande **login**

Cette dernière commande est très importante, c'est elle qui rend l'authentification obligatoire.

Exemple :

```
Sw-Floor-1(config)#line console 0  
Sw-Floor-1(config-line)#password cisco  
Sw-Floor-1(config-line)#login  
Sw-Floor-1(config-line)# exit
```

3) Limiter l'accès au périphérique via une connexion Telnet

Les lignes **VTY** permettent d'accéder à un routeur via Telnet. Par défaut, de nombreux périphériques Cisco prennent en charge jusqu'à 16 lignes VTY qui sont numérotées de 0 à 15. Vous devez définir un mot de passe pour toutes les lignes VTY disponibles.

Etre en mode de configuration globale et taper la commande **line vty 0 15**

Vous arrivez dans le mode de configuration particulier concernant les lignes VTY.

Il vous suffira alors de taper la commande **password** suivie du mot de passe que vous désirez mettre.

Comme pour limiter l'accès à la console, n'oubliez pas de finir en tapant la commande **login**

Exemple :

```
Sw-Floor-1(config)#line vty 0 15
```

```
Sw-Floor-1(config-line)#password cisco
```

```
Sw-Floor-1(config-line)#login
```

```
Sw-Floor-1(config-line)# exit
```

4) Chiffrement de l'affichage des mots de passe

Une autre commande utile permet d'empêcher l'affichage des mots de passe en clair lorsqu'un utilisateur consulte les fichiers de configuration. Il s'agit de la commande **service password-encryption**

Cette commande provoque le chiffrement simple des mots de passe déjà configurés (et non chiffrés) afin d'empêcher les personnes non autorisées de lire les mots de passe dans le fichier de configuration.

Avant :

```
Sw-Floor-1#show run
<résultat omis>
!
line con 0
  password class
  login
!
<résultat omis>
```

Après :

```
Sw-Floor-1(config)#service password-encryption
Sw-Floor-1#show run
<résultat omis>
!
line con 0
  password 7 094F471A1A0A
  login
!
<résultat omis>
```

5) Message de bannière

En plus des mots de passe pour empêcher l'accès non autorisé, il est également intéressant de mettre en place une méthode pour déclarer que l'accès à un périphérique est réservé aux personnes autorisées.

On peut donc afficher une bannière qui sera visible par n'importe quelle personne essayant d'ouvrir une session.

Pour afficher une bannière, utilisez la commande **banner motd**

Cette commande banner motd requiert l'utilisation de délimiteurs pour identifier le contenu du message de bannière.

→ La commande banner motd est suivie d'un espace et d'un caractère de délimitation (« # »). Ensuite, une ou plusieurs lignes de texte constituent le message de bannière. Enfin, le caractère de délimitation apparaît une seconde fois pour marquer la fin du message.

Exemple :

Sw-Floor-1(config)#**banner motd** # This is a secure system. Authorized Access Only ! #

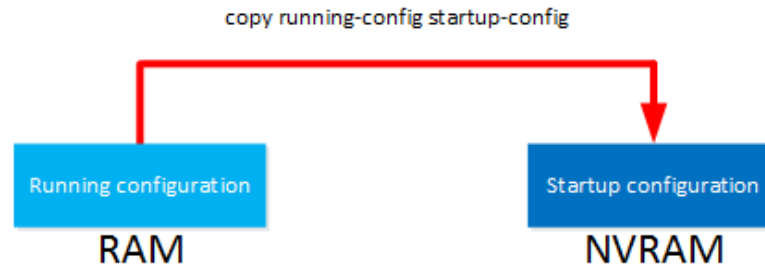
6) Gestion des fichiers de configuration

Une fois que vous avez modifié le fichier de configuration en cours (running-config), qui je vous le rappelle est stocké en mémoire vive (RAM), trois possibilités s'offrent à vous :

- adopter la configuration modifiée comme nouvelle configuration initiale

Vous n'effectuerez cette opération qu'après avoir vérifié que toutes les modifications que vous avez faites fonctionnent correctement.

Pour sauver la configuration en cours en tant que configuration initiale, tapez la commande **copy running-config startup-config**



Le fichier de configuration actuel remplacera donc le fichier configuration initial.

2^{ème} possibilité :

➤ restaurer la configuration d'origine du périphérique

Si les modifications apportées à la configuration en cours n'ont pas l'effet souhaité, il peut s'avérer nécessaire de revenir à la configuration antérieure du périphérique.

Le meilleur moyen de le faire consiste à redémarrer le périphérique en entrant la commande **reload** en mode d'exécution privilégié.

Exemple :

Sw-Floor-1#**reload**

Proceed with reload? [confirm]

3^{ème} possibilité :

➤ supprimer toute configuration du périphérique

On utilisera cette méthode si des modifications indésirables sont enregistrées dans la configuration initiale.

Dans ce cas il faut effacer la configuration initiale, via la commande **erase startup-config** et redémarrer le périphérique.

Exemple :

Sw-Floor-1#**erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Sw-Floor-1#**reload**

Proceed with reload? [confirm]

Switch>

7) Sauvegarde des configurations hors connexion

Afin d'être parer à toute éventualité, on conseille de sauvegarder les fichiers de configuration à un autre endroit, comme sur un serveur TFTP ou sur un support conservé en lieu sûr.

Pour sauver vos fichiers de configuration en cours (ou de configuration initiale) sur un serveur TFTP, il vous suffit de faire comme ceci :

- Taper **copy running-config tftp** (ou **copy startup-config tftp**)
- Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stockée
- Entrez le nom à attribuer au fichier de configuration

Exemple :

```
Sw-Floor-1#copy startup-config tftp
Address or name of remote host [ ] ? 192.168.1.10
Destination filename [Sw-Floor-1-config] ?
Writing startup-config..... [OK]
```

Adresses, interfaces et ports

L'utilisation d'adresses IP (IPv4 ou IPv6) est le principal moyen permettant aux périphériques de se localiser les uns les autres et d'établir la communication de bout en bout sur Internet. En fait, dans tout inter-réseau, les adresses IP sont essentielles pour que les périphériques communiquent de la source à la destination et inversement.

Chaque périphérique final d'un réseau (ordinateurs, imprimantes réseau, téléphones VoIP,...) doit comporter une adresse IP.

Si l'on prend le cas d'une adresse l'IPv4, sa structure est appelée « notation décimale à point » et est composée de quatre nombres décimaux compris entre 0 et 255.

Les adresses IPv4 sont des numéros affectés à des périphériques connectés à un réseau. Ces adresses sont logiques par nature, dans la mesure où elles fournissent des informations sur l'emplacement des périphériques.

En plus d'une adresse IP, un masque de sous-réseau est également nécessaire. Un masque de sous-réseau est un type spécial d'adresse IPv4 qui, allié à l'adresse IP, détermine à quel sous-réseau spécifique (qui fait partie d'un réseau plus grand) le périphérique appartient.

Système d'exploitation de réseau

En plus des adresses, les communications réseau dépendent des interfaces des périphériques utilisateur, des interfaces des périphériques réseau et des câbles de connexion.

Chaque interface a des caractéristiques, ou des normes, qui la définissent : un câble de connexion à l'interface doit donc être adapté aux normes physiques de l'interface.

Les supports réseaux, tels que les commutateurs ou les routeurs incluent les câbles en cuivre à paires torsadées, les câbles à fibres optiques, les câbles coaxiaux ou la technologie sans fil.



Les différents types de supports réseau possèdent divers avantages et fonctionnalités et tous les supports réseau ne possèdent pas les mêmes caractéristiques et ne conviennent pas pour les mêmes objectifs.

Pouvez-vous me donner des caractéristiques vis-à-vis desquelles on peut avoir une différence entre ces supports de transmission ?

- la distance sur laquelle les supports peuvent transporter correctement un signal
- l'environnement dans lequel les supports doivent être installés
- la quantité de données et le débit de la transmission
- le coût des supports et de l'installation

Les commutateurs sont équipés de ports physiques (12, 24 ou 48 ports) pour la connexion, mais intègrent également une ou plusieurs interfaces virtuelles de commutateur (notée SVI).

Ce sont des interfaces virtuelles car il n'existe aucun matériel sur le périphérique associé : une interface SVI est créée au niveau logiciel.

L'interface virtuelle est un moyen de gérer à distance un commutateur sur un réseau grâce à l'IPv4. Chaque commutateur dispose d'une interface SVI apparaissant dans la configuration initiale par défaut prête à l'emploi . L'interface SVI par défaut est l'interface VLAN1.

Configuration d'une interface sur un commutateur

Comme nous l'avons déjà évoqué auparavant, afin de pouvoir se connecter et gérer à distance un matériel réseau, une adresse IP et un masque de sous-réseau doivent être configurés sur une interface virtuelle (SVI).

Premièrement, pour accéder à une l'interface virtuelle, il faut, à partir du mode de configuration globale, utiliser la commande **interface** suivie du *nom de l'interface*.

Pour configurer une adresse IP et un masque de sous-réseau il faut utiliser la commande **ip address @ip @mask**

Une fois que l'on est dans le mode de configuration de l'interface, on peut désactiver celle-ci à l'aide de la commande **shutdown** ou au contraire, si on souhaite (ré)activé une interface, on utilisera la commande **no shutdown**

Exemple :

```
Sw-Floor-1(config)#interface vlan 1  
Sw-Floor-1(config-if)#ip address 192.168.10.1 255.255.255.0  
Sw-Floor-1(config-if)#no shutdown
```

De même que le nom d'hôte facilite l'identification du périphérique sur un réseau, une description d'interface indique le but de l'interface.

Il est donc possible d'ajouter, à chaque interface, un message descriptif à l'aide de la commande **description**

Exemple :

```
Sw-Floor-1(config)#interface vlan 1
```

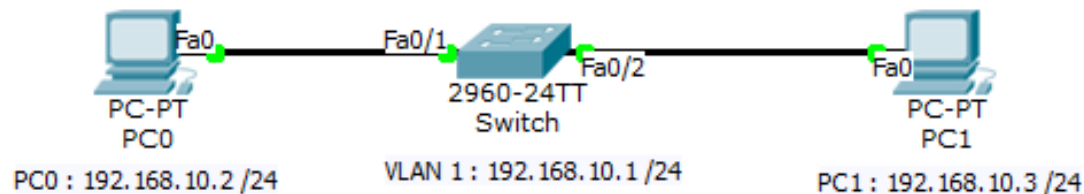
```
Sw-Floor-1(config-if)#description Interface de gestion à distance
```

```
Sw-Floor-1(config-if)#ip address 192.168.10.1 255.255.255.0
```

```
Sw-Floor-1(config-if)#no shutdown
```


Système d'exploitation de réseau

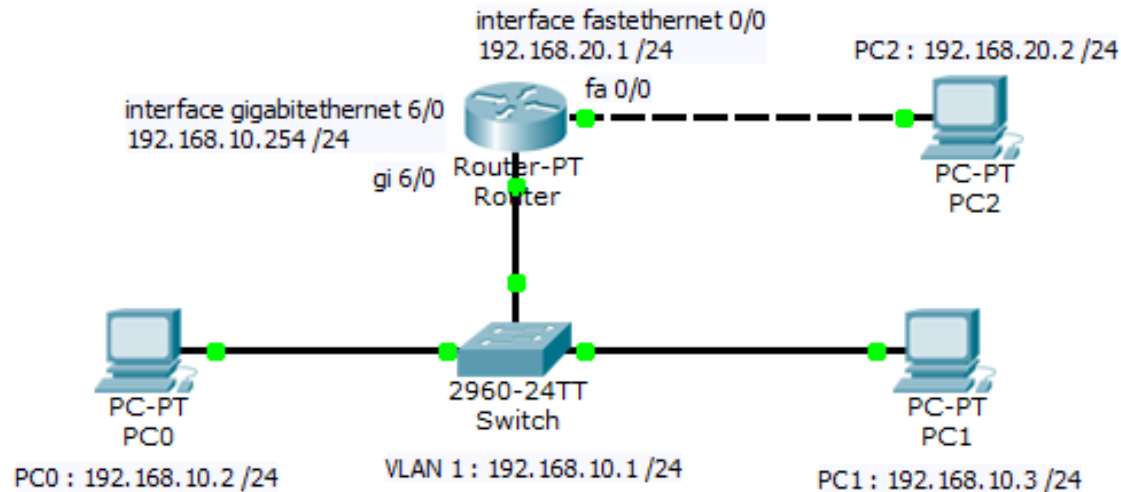
Un commutateur de réseau local étant un périphérique intermédiaire qui interconnecte des segments d'un réseau, ces interfaces physiques ne possèdent pas d'adresses IP, contrairement aux routeurs, dont les interfaces sont connectées à différents réseaux.



Dans ce schéma, le commutateur et les 2 ordinateurs font partie du même réseau. Ils peuvent donc tous communiquer ensemble.

Par contre, aucun d'entre eux ne peut communiquer en dehors du réseau local sauf s'ils ont préalablement été configurés avec une adresse de passerelle !

Système d'exploitation de réseau



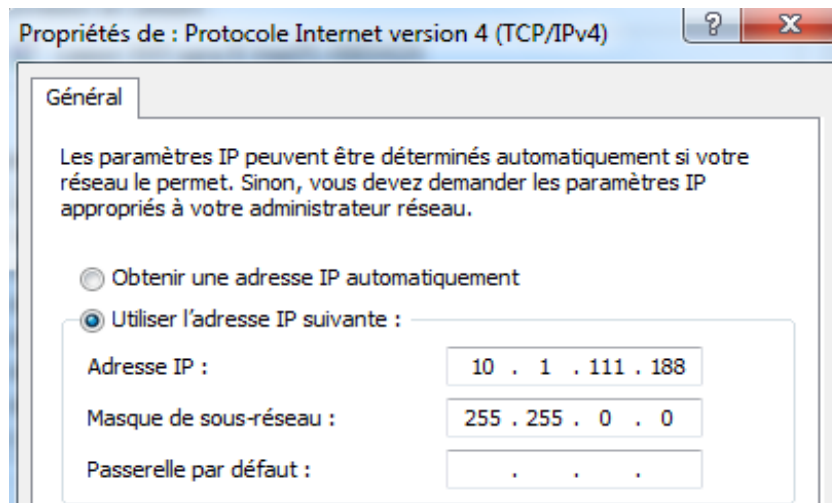
Cette adresse de passerelle doit donc être configurée à la fois sur les ordinateurs et sur le commutateur si l'on souhaite qu'ils puissent communiquer en dehors du réseau dans lequel ils se trouvent.

Concernant le commutateur, cela se fait à partir du mode de configuration globale, via la commande **ip default-gateway @IP**

Exemple :

Sw-Floor-1(config)#**ip default-gateway 192.168.10.254**

Attribution statique => Configuration IP manuelle



➔ **Sous Windows**

Pour afficher la configuration IP :
C:> ipconfig/all

➔ **Sous Linux** : *ifconfig eth0 x.x.x.x/N*

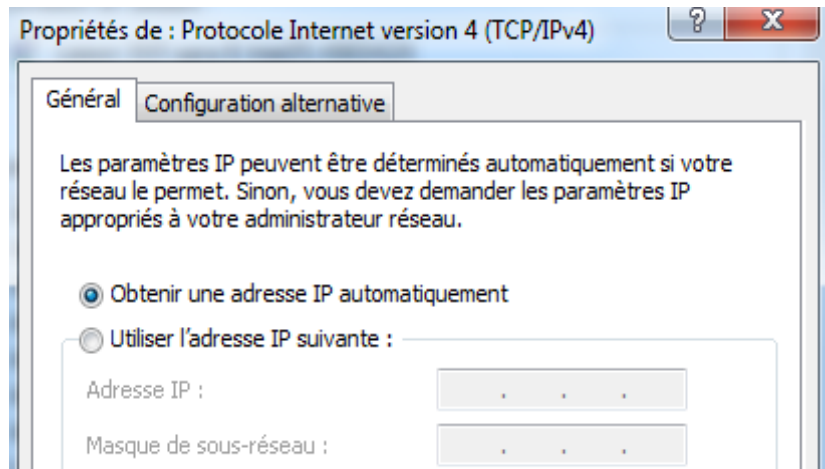
L'attribution statique convient pour les imprimantes, les serveurs et d'autres périphériques réseau, qui doivent être accessibles pour les clients d'un réseau.

Attribution dynamique => Configuration IP automatique

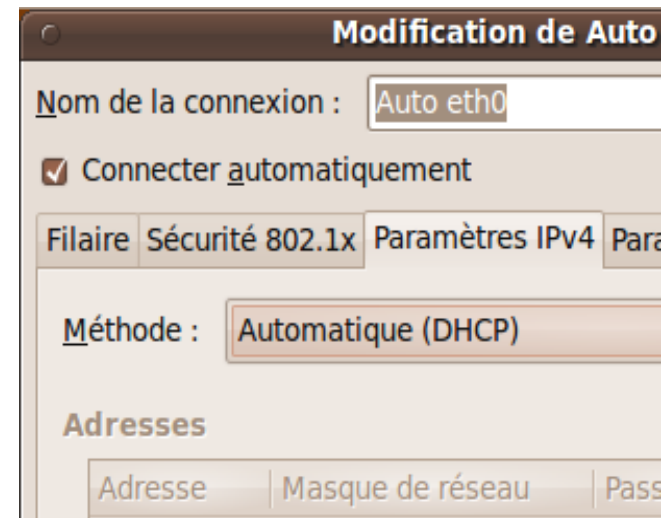
Utilisation du protocole DHCP (Dynamic Host Configuration Protocol)

→ La machine obtient dynamiquement une adresse via un serveur DHCP

Sous Windows



Sous Linux (Ubuntu)



L'autre avantage de l'attribution dynamique réside dans le fait que les adresses ne sont pas permanentes pour les hôtes.

Elles sont uniquement « louées » pour une certaine durée.

Si l'hôte est mis sous tension ou retiré du réseau, son adresse est renvoyée au pool et sera réutilisée.

Commandes *ipconfig* :

ipconfig/all

Affiche la configuration TCP/IP complète de toutes les cartes.

ipconfig/release [Carte]

Envoie un message *DHCPRELEASE* au serveur DHCP pour libérer la configuration DHCP actuelle et annuler la configuration d'adresse IP de toutes les cartes (si aucune carte n'est spécifié) ou d'une carte spécifique si le paramètre *Carte* est inclus.

ipconfig/renew [Carte]

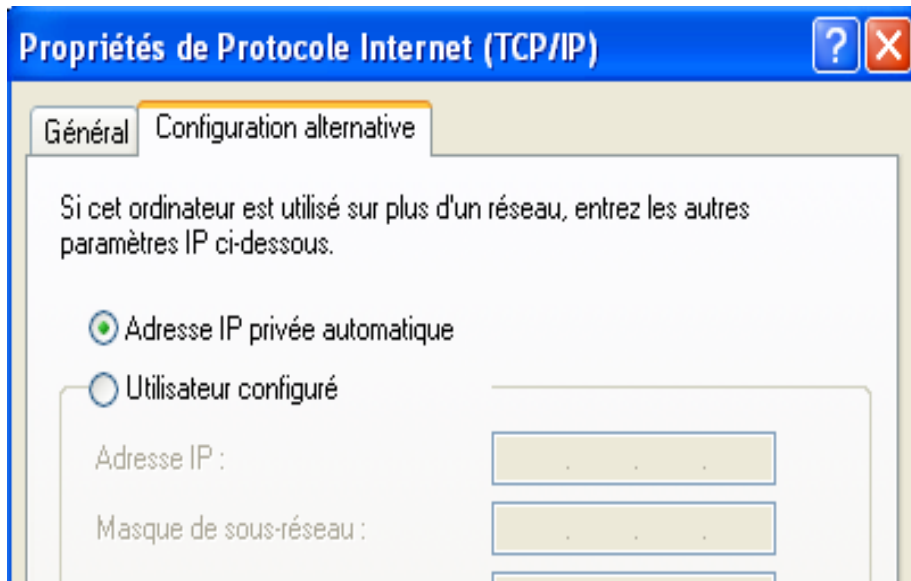
Renouvelle la configuration DHCP de tous les cartes (si aucune carte n'est spécifiée) ou d'une carte spécifique si le paramètre *Carte* est inclus.

Système d'exploitation de réseau

Elle permet de définir quelle adresse IP vous devez utiliser lorsqu'aucun serveur n'est en mesure de vous en fournir une !

Dans ce cas, le client (Windows) dispose de deux solutions :

- Adressage interne Microsoft (APIPA = Adressage IP Privé Automatique, par défaut)
- Adressage manuel d'une adresse IP fixe



Adressage APIPA :

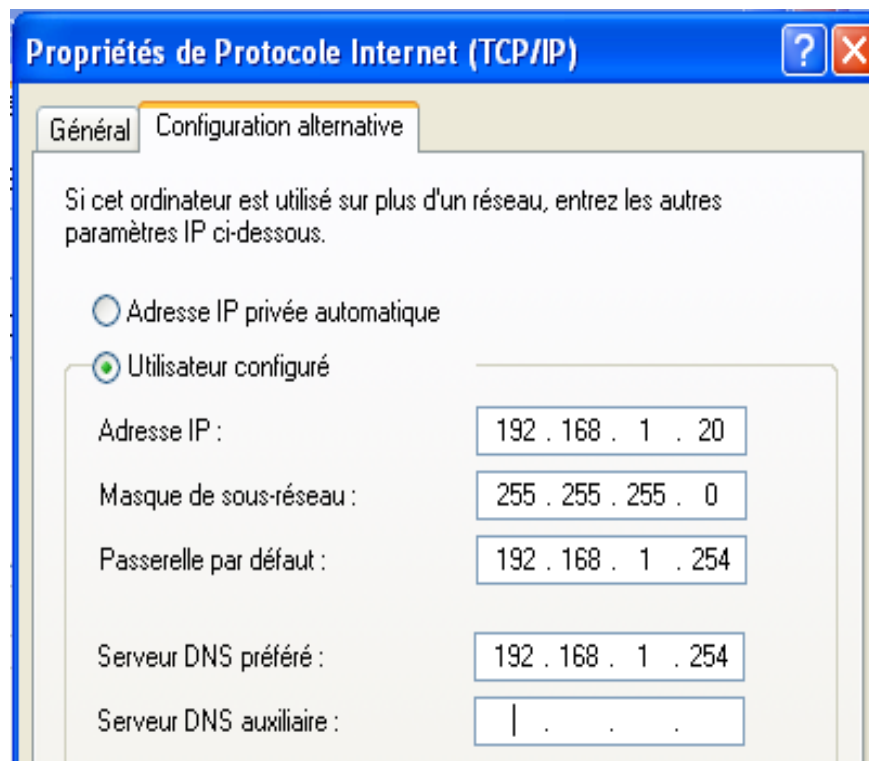
Cette configuration limitera la station à ne communiquer qu'avec les autres machines disposant d'une adresse APIPA.

Plage IP :

169.254.0.1 - 169.254.255.254

Système d'exploitation de réseau

Cette option peut s'avérer utile si vous souhaitez permettre à certains postes clients bien **identifiés** de continuer à pouvoir accéder aux serveurs lorsque le serveur DHCP n'est plus disponible.



Commande ping et traceroute

Pour diagnostiquer un problème on peut utiliser deux commandes :

- la commande ping
- la commande de trace

Celles-ci peuvent s'utiliser conjointement pour diagnostiquer un problème car elles ne fourniront pas forcément les mêmes indices concernant le problème.

Ping

La commande permet de tester l'accessibilité d'une autre machine à travers un réseau IP. Elle utilise une requête ICMP *Echo* et attend une réponse *Echo reply*.

Traceroute

La commande **tracert** montre l'itinéraire et là où se trouve le défaut dans l'inter-réseau au-delà du réseau local.