CISCO

CCNA 2

Routers & Routing Basics

SOMMAIRE

Module 1

Réseaux WAN & routeurs

Introduction au réseau WAN :

Un réseau WAN est un réseau de communication de données qui couvre une zone géographique étendue, comme un département, une région ou un pays par exemple.

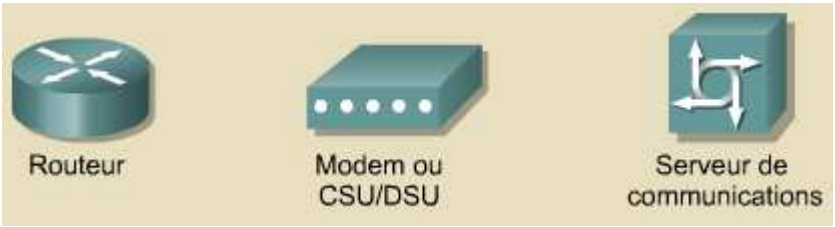
Distance entre les unités	Emplacement des hôtes	Nom
10m	Pièce	Réseau LAN Salle de classe
100m	Bâtiment	Réseau LAN École
1000m = 1km	Campus	Réseau LAN Université
10,000m = 10km	Ville	Réseau métropolitain
100,000m = 100km	Pays	Réseau WAN Cisco Systems, Inc.
1,000,000m = 1,000km	Continent	Réseau WAN Afrique
10,000,000m = 10,000km	Planète	Réseau WAN Internet
100,000,000m = 100,000km	Systèmes terre-lune	Réseau WAN Satellites terrestres et artificiels

Caractéristiques :

- Ils relient des équipements géographiquement *éloignés*.
- Ils utilisent les services de *porteuse d'opérateurs* tels que RBOC (Regional Bell Operating Company), Sprint, MCI et VPM Internet Services, Inc.
- Ils utilisent divers types de *connexions série* pour accéder à la bande passante.

Un réseau WAN fonctionne au niveau de la *couche physique* et de la *couche liaison de données* du modèle de référence OSI.

Les équipements utilisés dans un WAN :



- Des **routeurs**, qui offrent de nombreux services, y compris l'interconnexion.
- Le terme «**modems**» inclut des services d'interface de qualité voix, des unités CSU/DSU servant d'interface pour les services T1-E1 …
- Des **serveurs** de communication, qui concentrent les communications utilisateur entrantes et sortantes via le RTC.

Les protocoles de liaison de données WAN spécifient la façon dont les trames sont transportées entre les systèmes sur une même liaison. Il s'agit notamment des protocoles conçus pour fonctionner avec des services *point à point*, *multipoints* et *commutés multi-accès*, tels que les services Frame Relay.

Organismes gérant les normes :

- L'**UIT-T** (Union Internationale des Télécommunications – Télécommunications)
- L'Organisation internationale de normalisation (**ISO**).
- L'Internet Engineering Task Force (**IETF**).
- L'Electrical Industries Association (**EIA**).

Introduction aux routeurs dans un réseau WAN

Un routeur est un type spécial d'ordinateur. Il possède les mêmes composants de base qu'un ordinateur de bureau standard. Il est doté d'un processeur, de mémoire, d'un système de bus, ainsi que de diverses interfaces d'entrée/sortie.

Les routeurs doivent être équipés d'une plate-forme logicielle *IOS* (*Internetworking Operating Software*) pour exécuter les *fichiers de configuration*. Ces fichiers contiennent les instructions et les paramètres qui contrôlent le trafic entrant et sortant des routeurs.

Les principaux composants internes d'un routeur :

UC:

Le processeur (UC) exécute les instructions du système d'exploitation IOS. Ses principales fonctions sont, entre autres, l'initialisation du système, le routage et le contrôle de l'interface réseau.

La mémoire vive (RAM) ou DRAM :

- elle contient les tables de routage.
- elle contient le cache ARP.
- elle contient la mémoire cache à commutation rapide.
- elle effectue la mise en mémoire tampon des paquets (Mémoire d'E/S partagée).
- elle gère les files d'attente de paquets.
- elle sert de mémoire temporaire pour le fichier de configuration.
- elle perd son contenu à la mise hors tension ou au redémarrage du routeur.

La mémoire vive rémanente (NVRAM) :

- elle assure le stockage du fichier de configuration de démarrage,
- elle conserve son contenu à la mise hors tension ou au redémarrage du routeur.

La mémoire flash :

- elle contient l'image du système d'exploitation (IOS),

- elle permet de mettre à jour le logiciel sans suppression ni remplacement de puces.
- elle conserve son contenu à la mise hors tension ou au redémarrage du routeur,
- elle peut stocker plusieurs versions de la plate-forme logicielle IOS,
- elle constitue un type de ROM (EEPROM).

L'ajout ou le remplacement des modules SIMM de mémoire flash ou des cartes PCMCIA permet de mettre à niveau la quantité de mémoire flash.

La mémoire morte (ROM) :

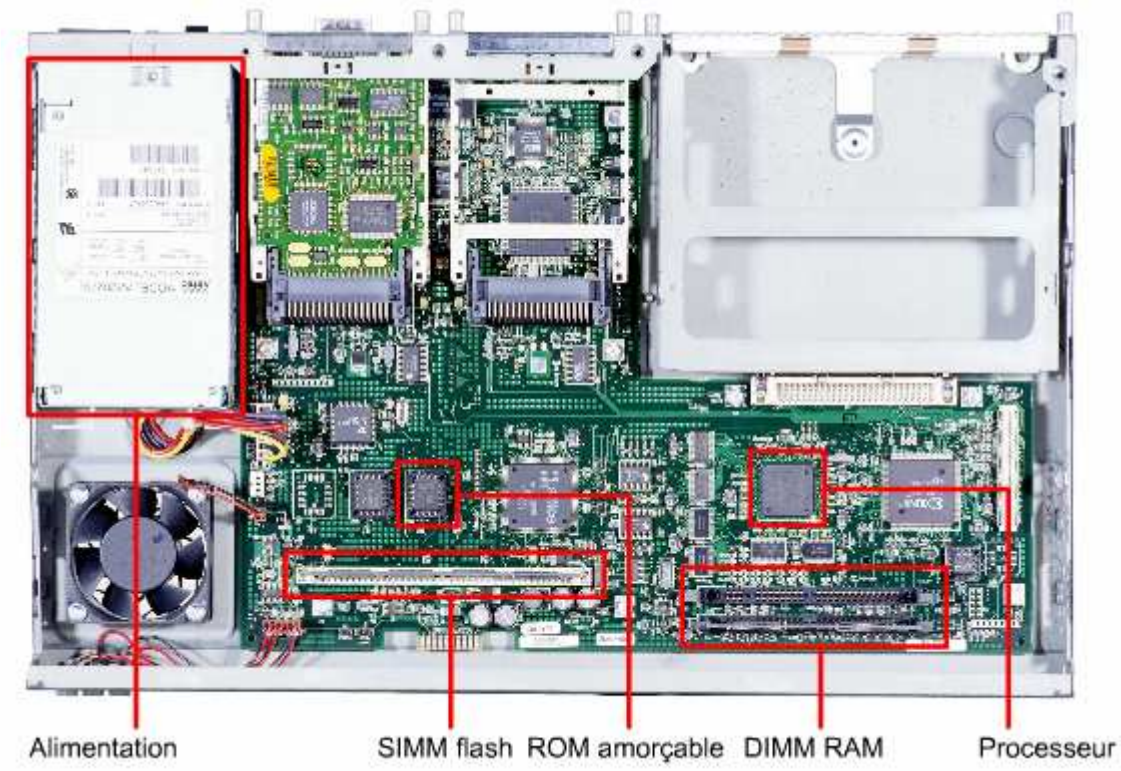
- elle gère les instructions du test automatique de mise sous tension (POST).
- elle stocke le programme d'amorçage (bootstrap) et le logiciel de système de base.
- elle nécessite un remplacement des puces enfichables sur la carte mère pour procéder aux mises à jour logicielles.

Bus:

- Les routeurs comportent un bus système et un bus processeur.
- Le bus système est utilisé pour transférer les paquets vers et depuis les interfaces.
- le bus processeur est utilisé pour transfère les instructions et les données vers ou depuis les adresses mémoire spécifiées.

Les interfaces :

- elles connectent le routeur au réseau pour l'entrée et la sortie des paquets,
- elles peuvent se trouver sur la carte mère ou sur un module séparé.



Les connexions externes des routeurs :

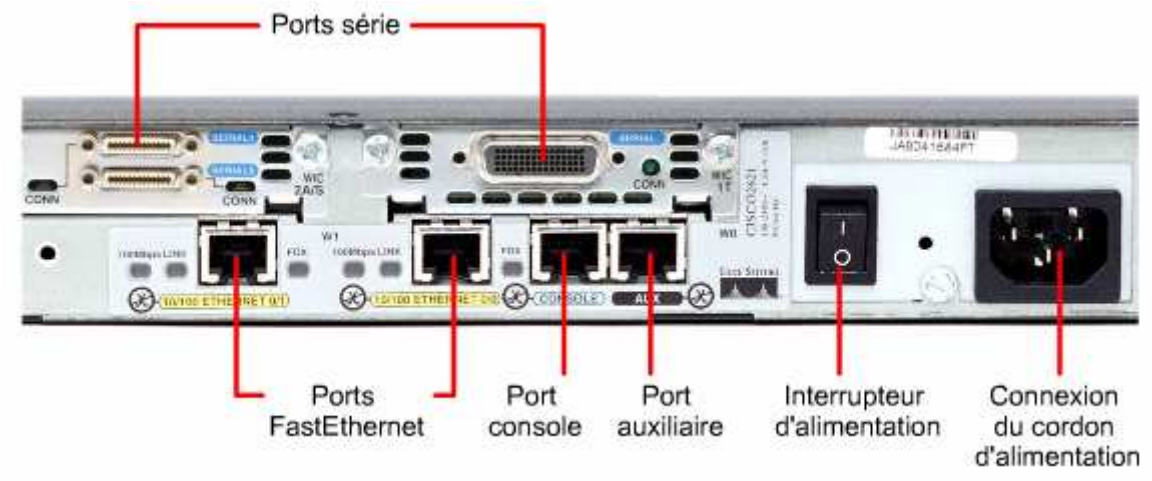
Le routeur possède trois types d'interfaces: LAN, WAN et Console/AUX.

→ Les interfaces LAN (Ethernet ou Token Ring standard …).

→ Les interfaces WAN (ports série, RNIS et une unité de transmission de données (CSU).

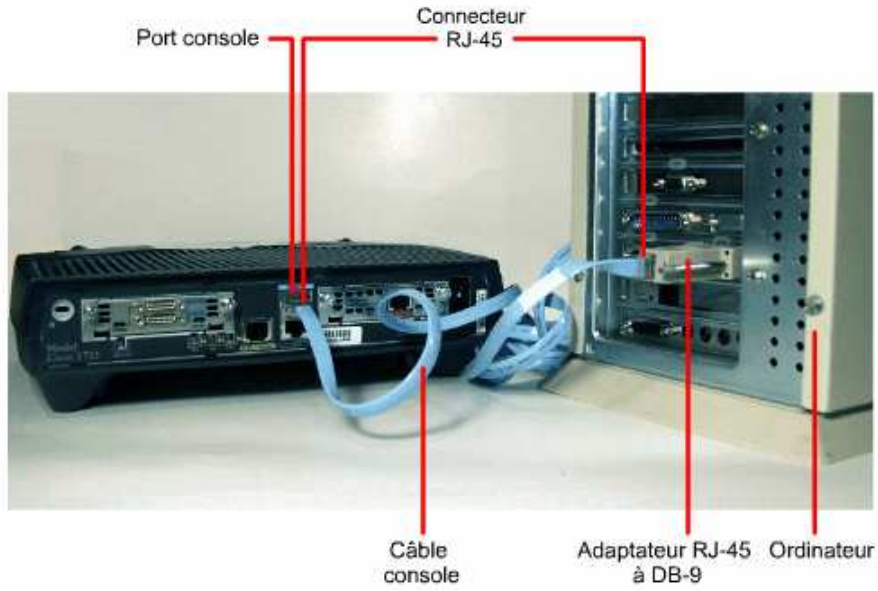
→ Les ports de gestion sont des ports série utilisés pour la configuration initiale (Aux, Console …)

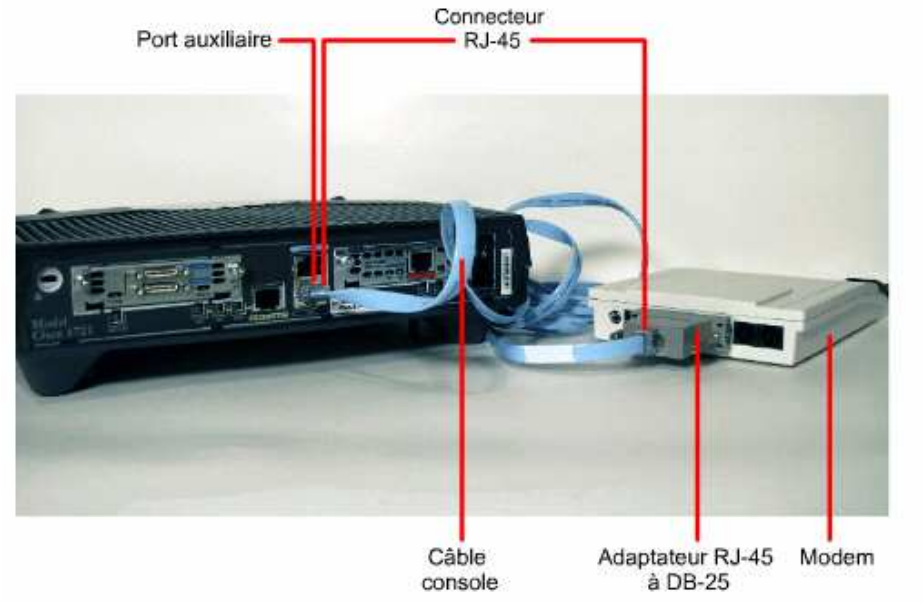
** les ports de gestion sont des ports série asynchrones EIA-232.



Connexion des ports de gestion :

Pour le dépannage, il est préférable d'utiliser le port console plutôt que le port auxiliaire, car il permet par défaut d'afficher les messages de démarrage, de débogage et les messages d'erreur du routeur.





Connexion des interfaces en mode console :

Le port console est un port de gestion qui fournit un accès hors bande au routeur. Il est utilisé pour la configuration initiale du routeur, pour la surveillance, et pour les procédures de reprise après sinistre.

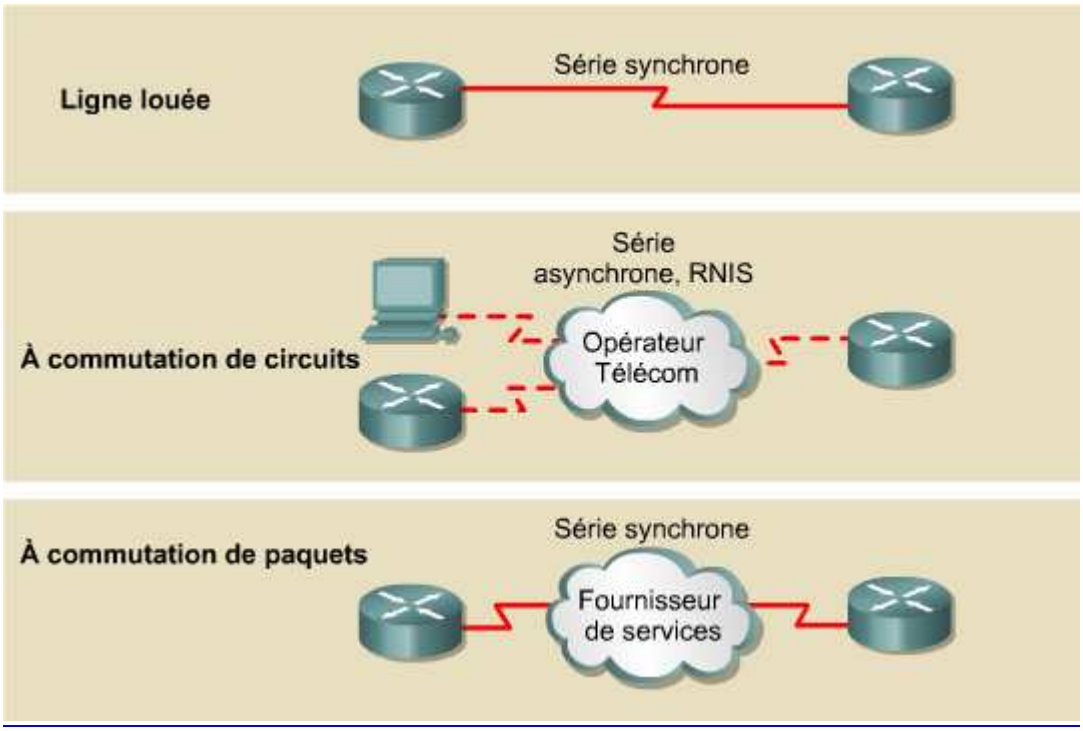
Pour connecter le PC à un routeur:

1. Configurez le logiciel d'émulation de terminal sur le PC pour:
   - Le port COM approprié
   - 9600 bauds
   - 8 bits de données
   - Aucune parité
   - 1 bit d'arrêt
   - Aucun contrôle de flux
2. Connectez le connecteur RJ-45 du câble à paires inversées au port console du routeur.
3. Connectez l'autre extrémité du câble à paires inversées à l'adaptateur RJ-45 à DB-9.
4. Connectez l'adaptateur DB-9 femelle à un PC.

Connecteurs 8 broches sur les routeurs CISCO :

Port ou connexion	Type de port	Couleur	Connecté à	Câble
Ethernet	RJ-45	jaune	Concentrateur ou commutateur Ethernet	Droit
WAN T1/E1	RJ-48C/ CA81A	vert clair	Réseau T1 ou E1	RJ-48 T1
Console	8 broches	bleu clair	Port COM d'un ordinateur	Console (à paires inversées)
AUX	8 broches	noir	Modem	Console (à paires inversées)
BRI S/T	RJ-48C/ CA81A	orange	Unité NT1 ou PINX (Private Integrated Network eXchange)	RJ-48
BRI U WAN	RJ-49C/ CA11A	orange	Réseau RNIS	RJ-49
Token	UTP, STP	violet	Unité Token Ring	Token Ring RJ-45

Types de réseau WAN :



Routeurs de réseaux LAN & WAN :

Bien qu'un routeur puisse servir pour *segmenter des réseaux LAN*, son utilisation première est celle d'une *unité WAN*.

Les deux fonctions principales d'un routeur sont de sélectionner le meilleur chemin pour les paquets et de commuter ces paquets vers l'interface appropriée.

Un interréseau correctement configuré fournit les éléments suivants :

- un adressage cohérent de bout en bout.
- des adresses représentant les topologies réseau.
- une sélection du meilleur chemin.
- un routage dynamique ou statique.
- la commutation.

Rôle d'un routeur dans un réseau WAN :

Les caractéristiques qui distinguent un réseau WAN d'un réseau LAN se situent en général au niveau de la couche *physique* et de la couche *liaison de données*. Autrement dit, les normes et les protocoles des couches 1 et 2 des réseaux WAN sont différents de ceux des mêmes couches des réseaux LAN.

La couche physique WAN décrit l'interface entre *l'ETTD* (*équipement terminal de traitement de données*) et *l'ETCD* (*équipement de terminaison de circuit de données*). En règle générale, l'ETCD est le réseau du fournisseur d'accès et l'ETTD, l'unité connectée.

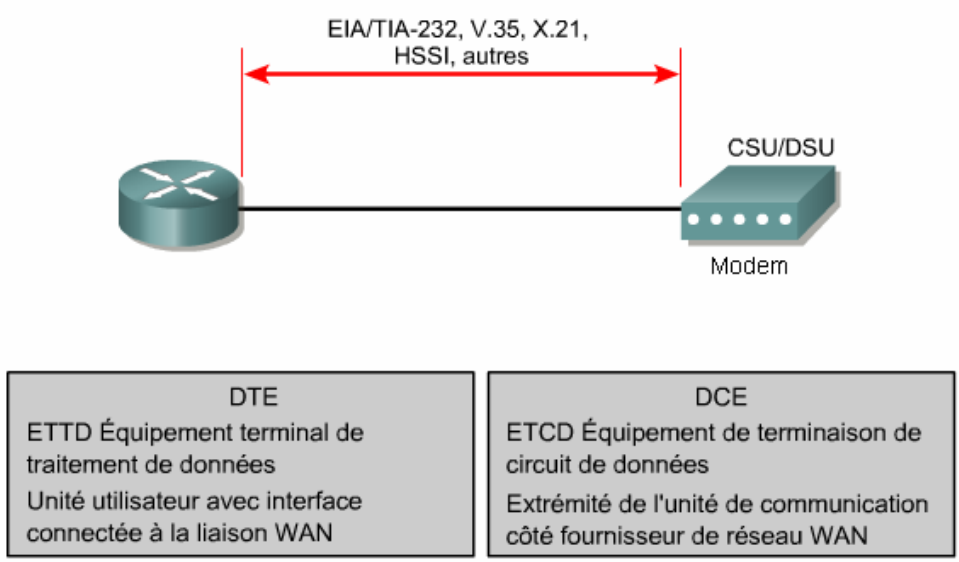
Le rôle principal d'un routeur dans un WAN n'est donc pas le routage, mais la compatibilité des connexions vers et entre les diverses normes physiques et de liaison de données d'un réseau WAN.

Normes et protocoles de la couche physique WAN:

- EIA/TIA-232
- V.24
- V.35
- X.21
- RNIS
- T1, T3, E1 et E3
- xDSL
- SONET

Normes et protocoles de la couche liaison de données WAN:

- HDLC (High-level Data Link Control)
- Frame Relay
- PPP (protocole point à point)
- SDLC (Synchronous Data Link Control)
- SLIP (Serial Line Internet Protocol)
- X.25
- ATM



Module 2

Introduction aux routeurs

L'objectif de la plate-forme logicielle Cisco IOS

Cisco a nommé son système d'exploitation Cisco Internetwork Operating System ou **Cisco IOS** (pour les routeurs / commutateurs), L'IOS fournit les services réseau suivants:

- fonctions de routage et de commutation de base
- accès fiable et sécurisé aux ressources en réseau
- évolutivité du réseau.

Modes d'interface utilisateur des routeurs

L'IOS fournit un service d'interpréteur de commande baptisé programme d'exécution des commandes (EXEC). À chaque entrée de commande, le programme d'exécution valide puis exécute la commande.

Par mesure de sécurité, l'IOS sépare les sessions d'exécution en deux niveaux d'accès. Ces niveaux sont le mode utilisateur et le mode privilégié (enable).

→ *Le mode utilisateur* n'autorise qu'un nombre limité de commandes de surveillance de base « visualisation seule ». Le niveau utilisateur n'autorise aucune commande susceptible de modifier la configuration du routeur

Router>

→ *Le mode privilégié* accède à toutes les commandes du routeur. Protéger par un mot de passe (et même une ID utilisateur). Ainsi, seuls les utilisateurs autorisés peuvent accéder au routeur

Router#

Remarque : Deux commandes permettent de définir un mot de passe d'accès au mode privilégié: **enable password** et **enable secret**. Si les deux commandes sont utilisées, la commande enable secret a préséance.

Ctrl-Z → permet de retourner vers le mode privilégié.

```
User Access Verification
Password:
Router>                          <-- Invite du mode utilisateur
Router>enable
Password:
Router#                          <-- Invite du mode privilégié
Router#disable
Router>
Router>exit
```

Caractéristiques de la plate-forme logicielle Cisco IOS

Cisco développe différentes images IOS. Chaque image représente un jeu de fonctions adapté aux différentes plates-formes, aux ressources mémoire disponibles, ainsi qu'aux besoins du client. (La structure de commande de configuration de base reste identique).

Show version → pour vérifier l'image en cours et la mémoire flash disponible.

```
... <output omitted> ... Cisco 1721 (68380) processor (revision C) with
3584K/512K bytes of memory.
```

Cette ligne indique quelle quantité de mémoire principale et de mémoire partagée est installée dans le routeur.

Show flash → pour trouver la quantité de mémoire flash.

```
... <output omitted> ...
15998976 bytes total (10889728 bytes free)
```

Fonctionnement de la plate-forme logicielle Cisco IOS

Les équipements Cisco ISO possèdent 3 environnements d'exploitation ou modes distincts :

- Moniteur ROM
- Mémoire ROM amorçable
- Cisco IOS

Le processus de démarrage du routeur se charge normalement en mémoire RAM et exécute l'un de ces environnements d'exploitation (selon la valeur du registre de configuration)

Le moniteur ROM exécute le processus de bootstrap et fournit des fonctions et des diagnostics de bas niveau. Il sert au redémarrage suite à une panne système et à la récupération des mots de passe perdus (accessible qu'au moyen d'une connexion physique directe à travers le port console).

Le mode ROM amorçable, seul un sous-ensemble limité des fonctions de l'IOS est disponible. La mémoire ROM amorçable permet les opérations d'écriture en mémoire flash et est principalement utilisée pour remplacer l'image IOS qui est stockée en mémoire flash.

Cisco IOS : la version complète de l'IOS chargé à partir de la mémoire flash.

Show version → pour voir l'image et la version de l'IOS qui s'exécute + le paramètre du registre de configuration

Remarque : Sur certains équipements, l'IOS est directement exécuté à partir de la mémoire flash. Cependant, certains routeurs Cisco requièrent le chargement d'une copie de l'IOS dans la mémoire RAM et son exécution à partir de celle-ci

Démarrage initial des routeurs Cisco

Les routines de démarrage effectuent les opérations suivantes :

- vérifier que le matériel de routeur a été testé et est opérationnel (POST).
- trouver et charger l'IOS.
- trouver et appliquer le fichier de configuration de démarrage

1 → le routeur exécute un test POST en exécutant les diagnostics chargés en mémoire ROM. (le fonctionnement de base du processeur, de la mémoire et des ports d'interface réseau).

2 → le chargeur de bootstrap générique de la mémoire ROM s'exécute pour initialiser l'IOS « selon la valeur du registre de configuration ».
Lorsque l'IOS est chargé et opérationnel, une liste des composants matériels et logiciels s'affiche sur l'écran.

3 → Le fichier de configuration stocké dans la mémoire NVRAM est chargé dans la mémoire principale, puis il est exécuté ligne par ligne (protocoles, adresses, services …).
Sinon (pas de fichier en NVRAM), le système d'exploitation recherche un serveur TFTP disponible. S'il n'en trouve aucun, le dialogue de configuration (SETUP) est établi.

Mode Setup :

Le mode SETUP a pour but de donner une configuration de base afin de démarrer le routeur.

Dans le mode setup, les réponses par défaut apparaissent entre crochets **[ ]** à la suite de la question. → Appuyez sur la touche **Entrée** pour accepter les valeurs par défaut.

Ctrl-C → mettre fin au processus SETUP.

A la fin, il faut savoir que toutes les interfaces sont administrativement désactivées

Indicateurs LED du routeur (informations de statut) :

→ Une LED d'interface indique l'activité de l'interface correspondante.
Si une interface est occupée en permanence, sa LED reste toujours allumée.
→ La LED OK de couleur **verte** située à droite du port AUX s'allume lorsque le système s'initialise correctement.

Examen du démarrage initial d'un routeur

La valeur configurée en usine pour le registre de configuration est **0x2102**, ce qui indique que le routeur doit tenter de charger l'IOS selon les commandes Boot System

L'utilisateur peut déterminer la version bootstrap et la version de l'IOS que le routeur utilise + le modèle de routeur + le processeur + la quantité de mémoire + le nombre d'interfaces + les types d'interfaces + la quantité des mémoires NVRAM & flash….

Le message "*NVRAM invalid, possibly due to write erase*" → indique à l'utilisateur que ce routeur n'a pas encore été configuré ou que la mémoire NVRAM a été effacée

Aide au clavier dans l'interface CLI du routeur

? → Afficher la liste des commandes disponibles du mode courant.

→ L'invite `--More--` indique la présence de plusieurs écrans.

Le bouton Entrée → Afficher la ligne suivante.
Le bouton Espace → Afficher l'écran suivante.

→ L'indice ^ indique la position de l'erreur.

→ Le symbole du dollar **$** indique que la ligne a été déplacée vers la gauche.

Commandes d'édition avancée

L'interface utilisateur offre un mode d'édition avancée vous permettant de modifier une ligne de commande au cours de la frappe (automatiquement activé).

Commande	Description
Ctrl-A	Permet de revenir au début de la ligne de commande.
Esc-B	Permet de reculer d'un mot.
Ctrl-B (ou flèche gauche)	Permet de reculer d'un caractère.
Ctrl-E	Permet d'atteindre la fin de la ligne de commande.
Ctrl-F (ou flèche droite)	Permet d'avancer d'un caractère.
Esc-F	Permet d'avancer d'un mot.

Historique des commandes du routeur

La fonction d'historique des commandes vous permet d'accomplir les tâches suivantes:

- définir la capacité du tampon d'historique des commandes.
- rappeler des commandes.
- désactiver la fonction d'historique des commandes.

Par défaut, la fonction d'historique des commandes est active et le système enregistre 10 lignes de commandes dans son tampon (**maximum 256**).

Commande	Description
Ctrl-P ou flèche vers le haut	Rappelle la dernière commande (commande précédente).
Ctrl-N ou flèche vers le bas	Rappelle la dernière commande la plus récente.
Router>**show history**	Affiche la mémoire tampon des commandes.
Router>**terminal history size** *number-of-lines*	Définit la taille de la mémoire tampon historique des commandes*
Router>**terminal no editing**	Désactive les fonctions d'édition avancées.
Router>**terminal editing**	Re-enables advanced editing
<Tab>	Complète l'entrée.

Clock set `{heure} {date}` → pour configurer l'heure et la date du routeur.

Informations affichées par la commande show version :

- la version de l'IOS et informations descriptives.
- la version de ROM du bootstrap.
- la version de la ROM amorçable.
- le temps de fonctionnement du routeur.
- la dernière méthode de redémarrage.
- le fichier et l'emplacement de l'image système.
- la plate-forme de routeur.
- la valeur du registre de configuration.

Module 3

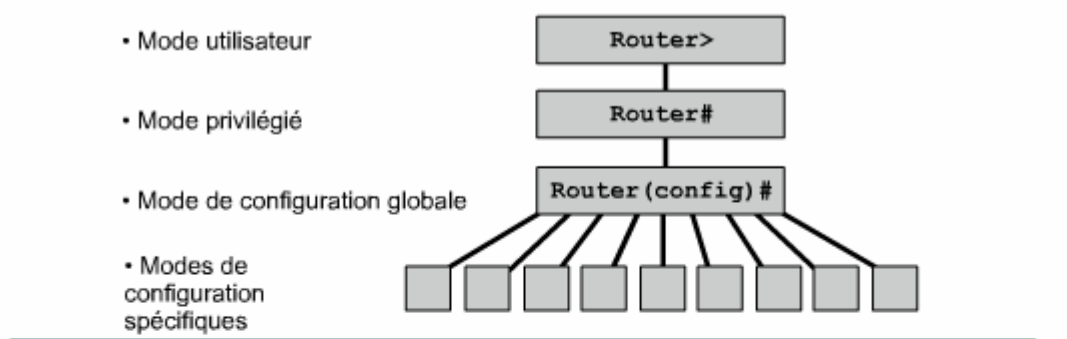
Configuration d'un routeur

Modes de commandes CLI :

Toutes les modifications de la configuration apportées sur un routeur Cisco sont effectuées en mode de configuration globale.

```
Router#configure terminal
Router(config)#
```

Voici quelques-uns des modes auquel vous pouvez accéder à partir du mode de configuration globale :



Mode de configuration	Invite
Interface	Router(config-if)#
Sous-interface	Router(config-subif)#
Contrôleur	Router(config-controller)#
Liste de mise en correspondance	Router(config-map-list)#
Classe de mise en correspondance	Router(config-map-class)#
Ligne	Router(config-line)#
Routeur	Router(config-router)#
Routeur IPX	Router(config-ipx-router)#
Mise en correspondance de route	Router(config-route-map)#

Configuration du nom d'un routeur

```
Router(config)#hostname Tokyo
Tokyo(config)#
```

Configuration des mots de passe d'un routeur

La commande **service password-encryption** applique un cryptage simple à tous les mots de passe non cryptés. La commande **enable secret** <*password*> utilise un puissant algorithme MD5 pour le cryptage.

Mot de passe de console

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

Mot de passe de terminal virtuel

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

Mot de passe enable

```
Router(config)#enable password san-fran
```

Cryptage d'un mot de passe

```
Router(config)#service password-encryption
Router(config)#enable secret <password>
```

Examen des commandes show

Plusieurs commandes **show** peuvent être utilisées pour *examiner* le contenu des fichiers du routeur ou pour le *dépannage*.

Show interfaces → Affiche les statistiques relatives à toutes les interfaces du routeur.

Show controllers serial → Affiche les caractéristiques de l'interface.

Show clock → Indique l'heure définie sur le routeur

Show hosts → Affiche une liste de noms et d'adresses d'hôtes se trouvant en mémoire cache

Show users → Indique tous les utilisateurs connectés au routeur

Show flash → Affiche des informations sur la mémoire flash ainsi que la liste des fichiers IOS qui y sont stockés

Show ARP → Affiche la table ARP du routeur

Show protocols → Affiche l'état général et propre aux interfaces de tous les protocoles de couche 3 configurés.

Show startup-config → Affiche le contenu de la NVRAM.

Show running-config → Affiche le contenu du fichier de configuration exécuté actuellement.

Configuration d'une interface série

```
Router(config)#interface serial {slot/port]                → sélectionner l'interface
Router(config-if)#ip address <ip address> <net mask>       → définir l'@ IP + le masque
Router(config-if)#clock rate {valeur d'horloge}            → s'il s'agit de l'ETCD
Router(config-if)#no shutdown                              → activer l'interface
```

Faire des changements de configuration

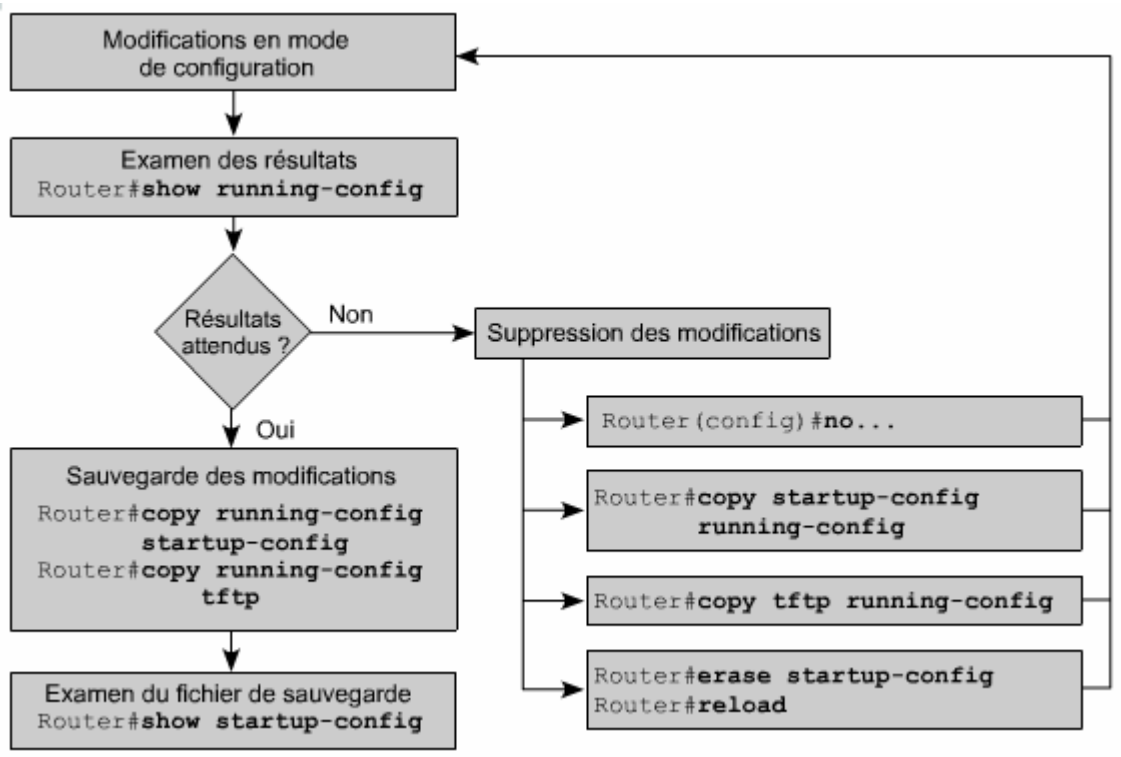
En cas d'erreur, vous pouvez corriger l'environnement en effectuant une ou plusieurs des opérations suivantes:

No {*commande*}→ désactiver la commande.

Copy startup-config running-config → recharger le système de la mémoire NVRAM.

Copy tftp running-config → copier un fichier de configuration archivé via un serveur TFTP.

Erase startup-config → supprimer le fichier de configuration + Reload



Configuration d'une interface Ethernet

```
Router(config)#interface {Type} {slot/port}          → sélectionner l'interface
Router(config-if)#ip address <ip address> <net mask>  → définir l'@ IP + le masque
Router(config-if)#no shutdown                         → activer l'interface
```

Résolution de nom d'hôte

La résolution de nom d'hôte est le processus qu'utilise le système informatique pour associer un nom d'hôte à une adresse IP.

Contrairement aux noms DNS, les noms d'hôtes ne sont significatifs que sur le routeur sur lequel ils sont configurés.

```
Router(config)#ip host {nom du routeur} {@1] {@2} …
```

Configuration facultative:

Descriptions d'interface

Il est indispensable d'utiliser une description d'interface afin d'identifier des informations importantes concernant cet interface.

```
Router(config-if)#description {commentaire}
```

Bannières de connexion

Une bannière de connexion s'affiche lors de la connexion, et permet de transmettre un message destiné à tous les utilisateurs du routeur (pour les avertir, par exemple, d'un arrêt imminent du système).

```
Router(config)#banner motd # le message ici # .
```

Sauvegarde de la configuration et documentation

Les fichiers de configuration doivent être stockés en tant que fichiers de sauvegarde pour parer à toute éventualité.

Enregistrez les fichiers de configuration sur :
- Un serveur TFTP
- Un serveur de réseau
- Un disque conservé dans un endroit sûr

Copie, édition et collage des configurations

Copy running-config tftp → Pour sauvegarder une copie de fichier de configuration sur un serveur tftp

→ Indiquer l'@ IP du serveur tftp.
→ Indiquer un nom pour le fichier.
→ Confirmez vos choix.

Copy tftp running-config → Pour utiliser une copie de fichier de configuration stocké sur un serveur tftp

→ Sélectionner fichier d'hôte / ficher de réseau.
→ Entrer l'@ IP du serveur.
→ Entrer le nom du fichier de configuration ou acceptez le nom par défaut

Module 4

Informations sur les autres équipements

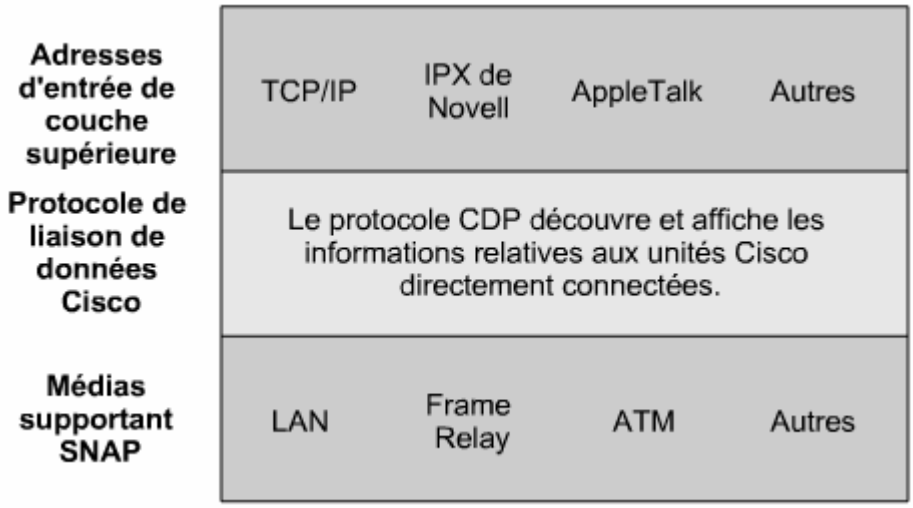
Introduction au protocole CDP

CDP (Cisco Discovery Protocol) est un protocole de couche 2 qui relie des médias physiques de niveau inférieur et des protocoles de couche réseau de niveau supérieur.

→ Il permet d'obtenir des informations sur les équipements voisins.
→ CDP est indépendant du média comme du protocole
→ CDP Version 2 (CDPv2) est la version la plus récente de ce protocole.
→ Une trame CDP est de petite taille ne surchargeant pas les réseaux.

Lors du démarrage d'un équipement Cisco, CDP démarre de façon automatique et permet à l'équipement de détecter les équipements voisins qui exécutent comme lui ce protocole.

Chaque équipement configuré pour CDP envoie périodiquement des messages, appelés annonces, aux équipements réseau directement connectés. Les annonces contiennent également des informations de « durée de vie » ou durée de conservation, indiquant pendant combien de temps les équipements récepteurs doivent conserver les informations CDP avant de les éliminer.



Informations obtenues avec CDP

Show cdp neighbors → pour afficher les informations sur les réseaux directement connectés.

```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform  Port ID
Rt3      Ser0/1        152     R        2500      Ser1
Rt1      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

CDP fournit des informations sur chaque équipement CDP voisin en transmettant des TLV (*Type Length Value*), c'est-à-dire des blocs d'informations incorporés dans des annonces.

Les TLV affichées par les commandes **show cdp neighbors** sont notamment:

- l'identifiant
- l'interface locale
- la durée de conservation
- la capacité
- la plate-forme
- l'ID du port

Les TLV suivantes ne sont comprises que dans CDPv2:

- le nom de domaine de gestion VT
- le VLAN natif
- le mode Full-Duplex ou Half-Duplex

Mise en œuvre, surveillance et maintenance du protocole CDP

Commande	Mode	Usage
`cdp run`	Mode de configuration globale	Active CDP globalement sur le routeur.
`cdp enable`	Mode de configuration d'interface	Active CDP sur une interface.
`clear cdp counters`	Mode privilégié	Remet à zéro les compteurs de trafic.
`show cdp`	Mode utilisateur ou privilégié	Indique l'intervalle entre les transmissions des annonces CDP, la durée de validité d'une annonce CDP pour un port donné (en secondes) et la version de l'annonce.
`show cdp entry {* | device-name [*] [protocol | version]}`	Mode utilisateur ou privilégié	Affiche les informations relatives à un voisin spécifique. L'affichage peut être limité aux informations de version ou de protocole.
`show cdp interface [type number]`	Mode utilisateur ou privilégié	Affiche les informations relatives aux interfaces sur lesquelles le protocole CDP est activé.
`show cdp neighbors [type number] [detail]`	Mode utilisateur ou privilégié	Indique le type et le nom de l'unité détectée, le numéro et le type de l'interface locale (port), la durée de validité de l'annonce CDP pour le port (en secondes), le numéro de produit de l'unité et l'ID du port. L'utilisation du mot-clé " detail " permet d'afficher des informations sur l'ID du VLAN natif, le mode duplex et le nom de domaine VTP associé aux unités voisines.

La commande **cdp enable** est utilisée pour activer CDP sur une interface particulière. Sur la version 10.3 de la plate-forme logicielle Cisco IOS, CDP est activé par défaut. Toutefois, sur certaines interfaces, telles que les interfaces asynchrones, CDP est désactivé par défaut.

No CDP run → Pour désactiver CDP au niveau global.
No CDP enable → désactiver CDP en mode de configuration d'interface

Dépannage du protocole CDP

Commande	Description
`clear cdp table`	Supprime la table d'informations CDP relative aux unités voisines.
`clear cdp counters`	Remet à zéro les compteurs de trafic.
`show cdp traffic`	Affiche les compteurs CDP, notamment le nombre de paquets envoyés et reçus, ainsi que les erreurs de somme de contrôle.
`show debugging`	Affiche l'information concernant les types de débogage qui sont présentement actifs.
`debug cdp adjacency`	Informations CDP sur les unités voisines
`debug cdp events`	Événements CDP
`debug cdp ip`	Informations IP CDP
`debug cdp packets`	CDP packet-related information
`cdp timer`	Indique la fréquence d'envoi de mises à jour CDP par la plate-forme logicielle Cisco IOS.
`cdp holdtime`	Indique le délai de conservation à envoyer dans le paquet de mises à jour CDP.
`show cdp`	Affiche des informations CDP globales, notamment sur les compteurs et les délais de conservation.

Introduction à Telnet :

Telnet est un protocole de couche 7 du modèle OSI « sous forme d'une commande EXEC de l'IOS » qui sert à établir une connexion à distance.

On peut utiliser Telnet pour se connecter à des hôtes distants pour le but de :

- configurer des équipements réseau à distance
- tester la connectivité (parce que Telnet offre un test complet)

→ Telnet s'appuie sur l'utilisation du protocole TCP au niveau de la couche Transport.

Les commandes Telnet peuvent être exécutées en mode utilisateur ou en mode privilégié

Etablir une session :

Utilisez l'un des commandes suivantes pour établir une session Telnet :

Router> **connect {@IP | Nom du routeur}**
Router> **{nom du routeur}**
Router> **{@IP du routeur}**
Router> **telnet {@IP | Nom du routeur}**

Vérifier la connexion Telnet :

Causes d'échec de la connexion telnet :

- problèmes spécifiques d'adressage
- Problèmes attribution de noms
- Problèmes d'autorisation d'accès

→ Dans ce cas, essayez d'exécuter la commande **ping** ou **tracert** (pour connaitre la cause)

Se déconnecter d'une session Telnet :

Utilisez l'un des commandes suivantes pour se déconnecter d'une session Telnet :

Router> **logout**
Router> **exit**

Interruption d'une session Telnet :

➔ Pour interrompre une session sans la fermer : **Ctrl-Shift-6**, puis sur **x**
Revenir au précédent routeur.

➔ Pour afficher les connexions actives : **show sessions**

```
Denver#show sessions
 Conn    Host    Address            Idle    Conn Name
 1       Paris   131.108.100.152    0       Paris
 2       Tokyo   126.102.57.63      0       Tokyo
```

➔ Pour reprendre la dernière session Telnet interrompue : la touche **Entrée**

`[Resuming connection 1 to 192.168.15.2 ... ]` → **la dernière connexion** Entrée

Pour reprendre une session précise → **resume {identifiant de connexion}**

➔ Pour se déconnecter d'une session Telnet interrompue : **disconnect {nom de routeur}**

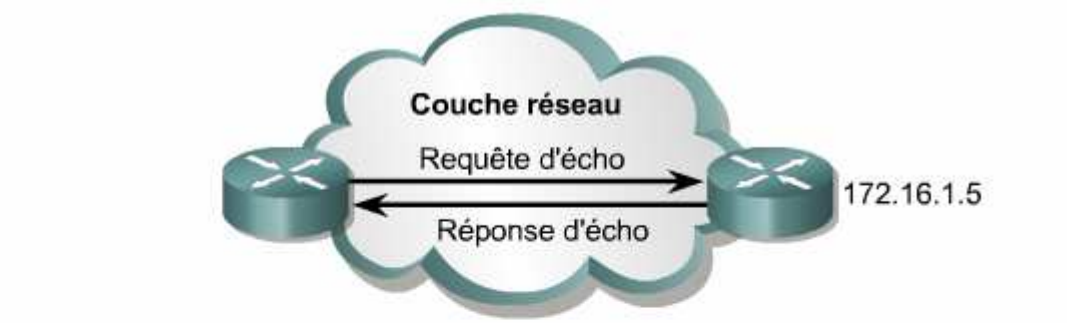
→ Le nombre de sessions ouvertes simultanément est défini par la commande **session limit**

Tests de connectivité alternative

Ping :

La commande **ping** permet de tester la connectivité de bout en bout.

→ Cette opération peut être exécutée en mode utilisateur ou en mode privilégié.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

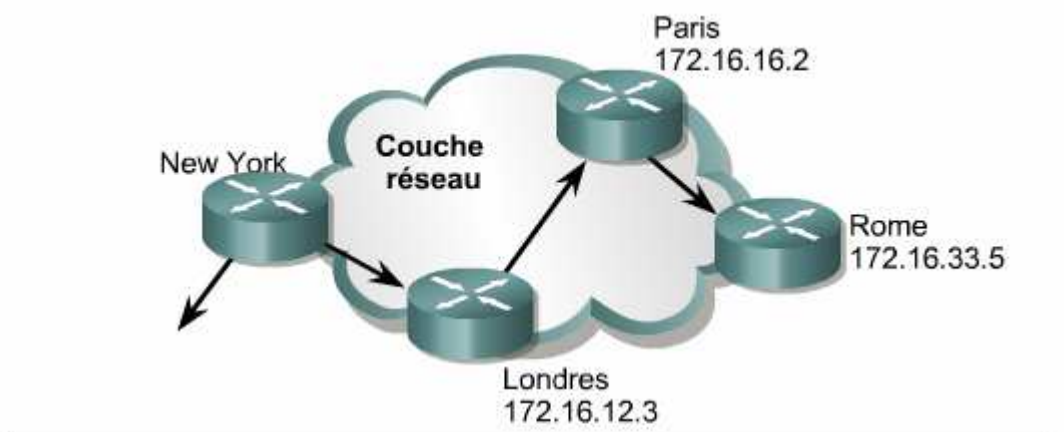
Les points d'exclamation (**!**) → indiquent chaque écho réussi.
Un point (**.**) → signifie que l'application de votre routeur a été temporisée.

Traceroute :

La commande **traceroute** permet de tester chaque étape de l'acheminement.

→ Cette opération peut être exécutée en mode utilisateur ou en mode privilégié.

Si l'un de ces routeurs est inaccessible, trois astérisques s'affichent (*****) à la place du nom du routeur.




```
York#traceroute ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
  1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
  2 PARIS (172.16.16.2) 8 msec 8msec 8msec
  3 ROME (172.16.33.5) 8msec 8msec 4msec

York#
```

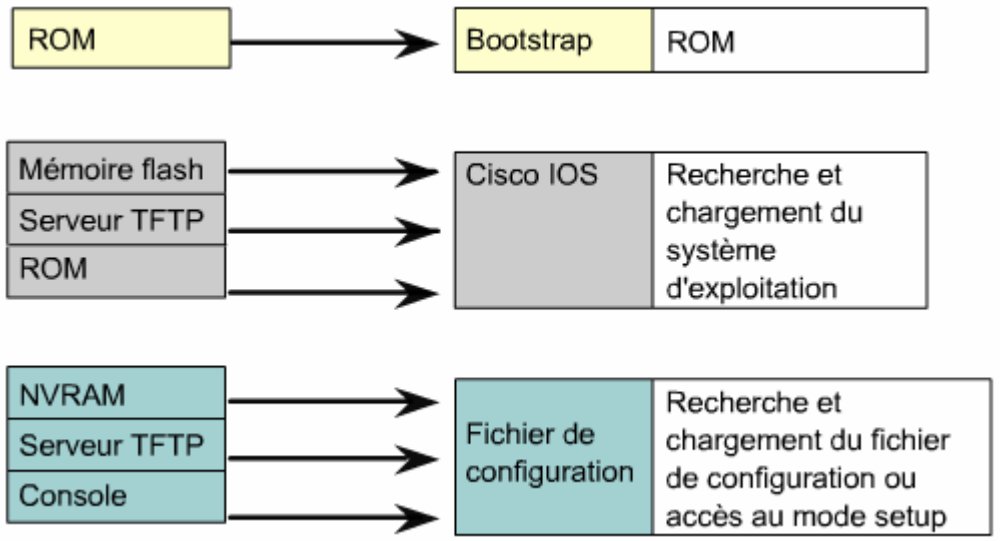
Show ip route :

Pour déterminer s'il existe une entrée correspondant au réseau cible dans la table de routage.

Module 5

Gestion de la plate-forme logicielle Cisco IOS

Étapes de la séquence d'amorçage du routeur



Comment un équipement Cisco localise et charge l'IOS ?

L'ordre suivant lequel le routeur cherche les informations de bootstrap est déterminé par la valeur du champ d'amorçage du registre de configuration.

Config-register {valeur en hexa}→ Modifier la valeur du registre de configuration (mode de config globale)

Le registre de configuration est un registre de 16 bits qui se trouve dans la mémoire NVRAM. Les quatre derniers bits du registre de configuration forment le champ d'amorçage (affiché par la commande Show version)

Valeur	Description
0xnnn0	Utilisation du mode moniteur ROM (démarrage manuel à l'aide de la commande `b`)
0xnnn1	Amorce la première image dans la flash. Cependant, sur des plateformes plus anciennes, l'amorçage se fera sur une version de l'IOS plus ancienne située dans la ROM
0xnnn2 à 0xnnnF	Recherche des commandes "`boot system`" dans la mémoire NVRAM (0xnnn2 est la valeur par défaut si le routeur a une mémoire flash)"

Modification du champ d'amorçage :

- Il faut passer en mode moniteur ROM → amorcer manuellement en entrant la commande **b** à l'invite du mode.
- Changer la valeur noté X seulement « 0x*nnn***X** » au registre de configuration selon le besoin.

Utilisation de la commande boot system

Les trois exemples suivants illustrent l'utilisation de plusieurs commandes **boot system** pour préciser la séquence d'amorçage de secours de la plate-forme logicielle Cisco IOS

```
Router#configure terminal
Router(config)#boot system flash IOS_filename
Router(config)#boot system tftp IOS_filename tftp_address
Router(config)#boot system ROM
[Ctrl-Z]
Router#copy running-config startup-config
```

→ Si la mémoire NVRAM ne contient pas de commandes boot system.

Par défaut : Flash → TFTP → ROM

Dépannage d'une panne d'amorçage de l'IOS :

Plusieurs éléments peuvent être à l'origine du mauvais amorçage d'un routeur:

- une instruction **boot system** manquante ou incorrecte.
- une valeur du registre de configuration est incorrecte
- l'image flash est corrompue
- une panne matérielle

→ Pour identifier la source de l'image d'amorçage, tapez la commande **show version** et cherchez la ligne qui identifie la source de l'image d'amorçage.

```
Router#show version
Cisco Internetwork Operating System Software  IOS
(tm) 2500 Software (C2500-JS-L), Version 12.1(5),
RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18
by cmong Image text-base: 0x03071DB0, data-base:
0x00001000
ROM: System Bootstrap, Version 5.2(8a), RELEASE
```

→ Utilisez la commande **show running-config** et recherchez une instruction **boot system** au début de la configuration.

→ Examiner la dernière ligne du « registre de configuration » par **show version**

Si le problème persiste, il se peut que le fichier d'image flash du routeur soit corrompu, Exemples :

- open: read error...requested 0x4 bytes, got 0x0
- trouble reading device magic number

- boot: cannot open "flash:"
- boot: cannot determine first file name on device "flash:"

→ Sinon panne matérielle.

Vue d'ensemble du système de fichiers IOS :

Les deux types de logiciels nécessaires pour fonctionner un routeur sont les systèmes d'exploitation et de configuration.

→ Le fichier de l'IOS occupe plusieurs méga-octets.
→ Le fichier de configuration occupe quelques centaines à quelques milliers d'octets.

IFS :

À compter de la version 12 de l'IOS, les routeurs utilisent le système de fichiers (**IFS**).

L'IFS fournit une méthode unique pour la gestion de l'ensemble des systèmes de fichiers utilisés par un routeur (Système de fichier de mémoire flash, des systèmes de fichiers réseau (TFTP, RCP et FTP) et des systèmes de fichier de lecture ou d'écriture de données (NVRAM, configuration courante, ROM).

IFS utilise la convention URL pour spécifier les fichiers sur les unités du réseau. La convention URL identifie l'emplacement des fichiers de configuration à la suite du point-virgule sous la forme [[[//emplacement]/répertoire]/nomdefichier].

Préfixes les plus courants :

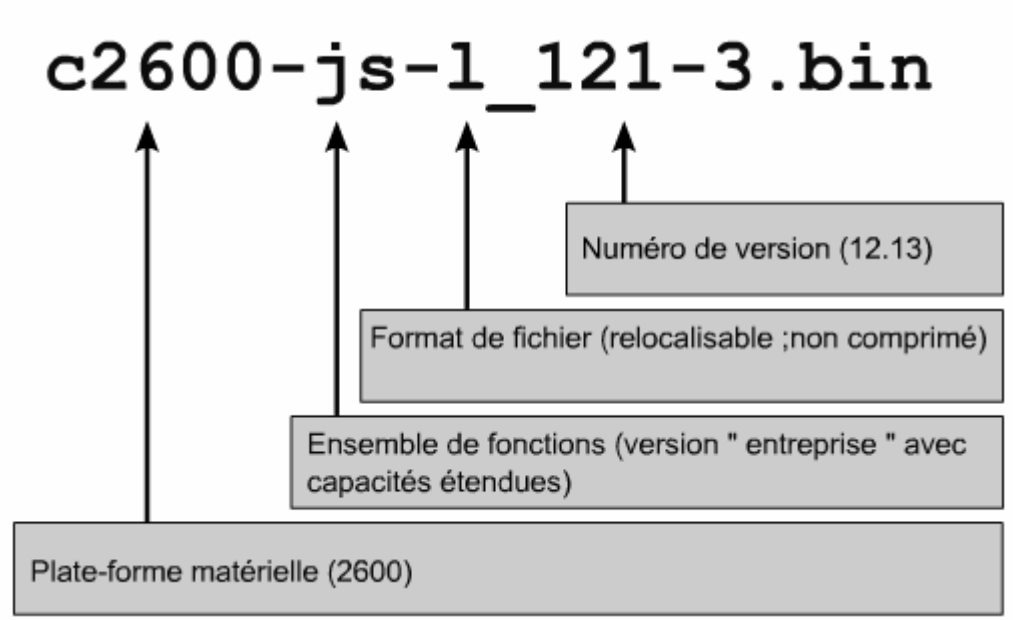
Prefixe	Description
bootflash:	Mémoire bootflash
flash:	Mémoire flash. Ce préfixe est disponible sur toutes les plates-formes. Pour les plates-formes sans unité appelée flash, le préfixe flash: est associé à slot0:. Ainsi, le préfixe flash: peut être utilisé pour faire référence à la zone de mémoire flash principale sur toutes les plates-formes.
flh:	Fichiers journaux de chargement de la mémoire flash
ftp:	File Transfer Protocol (FTP) network server
nvram:	NVRAM
rcp:	Serveur de réseau RCP (Remote Copy Protocol)
Slot0:	Première carte mémoire flash PCMCIA (Personal Computer Memory Card International Association)
Slot1:	Deuxième carte mémoire flash PCMCIA
system:	Contient la mémoire système, y compris la configuration courante
Tftp:	Serveur de réseau TFTP

Exemples des commandes (différences) :

Pre IOS Version 12.0 Commands	IOS Version 12.x Commands
configure network (pre-Cisco IOS Release 10.3) copy rcp running-config copy tftp running-config	copy ftp: system:running-config copy rcp: system:running-config copy tftp: system:running-config
configure overwrite-network (pre-Cisco IOS Release 10.3) copy rcp startup-config copy tftp startup-config	copy ftp: nvram:startup-config copy rcp: nvram:startup-config copy tftp: nvram:startup-config
show configuration (pre-Cisco IOS Release 10.3) show startup-config	more nvram:startup-config
Pre IOS Version 12.0 Commands	**IOS Version 12.x Commands**
write erase (pre-Cisco IOS Release 10.3) erase startup-config	erase nvram:
write memory (pre-Cisco IOS Release 10.3) copy running-config startup-config	copy system:running-config nvram:startup-config
write network (pre-Cisco IOS Release 10.3) copy running-config rcp copy running-config tftp	copy system:running-config ftp: copy system:running-config rcp: copy system:running-config tftp:
write terminal (pre-Cisco IOS Release 10.3) show running-config	more system:running-config

Conventions d'attribution de noms de l'IOS :

Cisco utilise une convention d'attribution de noms pour les fichiers IOS. Cette convention spécifie différents champs dans les noms.



Remarque : La troisième partie indique si l'IOS est stocké en mémoire flash dans un fichier compressé et s'il est transférable. Une image transférable est copiée de la mémoire flash dans la mémoire RAM pour y être exécutée. Une image non transférable est directement exécutée dans la mémoire flash.

Gestion des fichiers de configuration :

À l'aide de TFTP :

Copy running-config tftp → pour sauvegarder une copie sur un serveur tftp
Copy tftp running-config → Pour restaurer la copie sauvegardée.

Par copier-coller :

→ Capturer la configuration courante → Enregistrer dans un fichier texte → Modifier le fichier.

Pour capturer la configuration :

1. Sélectionnez **Transfert**
2. Sélectionnez **Capturer le texte** → Indiquez le nom du fichier texte
3. Sélectionnez **Démarrer** pour commencer la capture du texte
4. Affichez la configuration à l'écran en entrant **show running-config**
5. Appuyez sur la **barre d'espacement** chaque fois que l'invite **"- More –"** apparaît.

Lorsque la configuration complète est affichée, arrêtez la capture en procédant comme suit:

1. Sélectionnez **Transfert**
2. Sélectionnez **Capturer le texte**

3. Sélectionnez **Arrêter**

Vous devez modifier le fichier de configuration en supprimant :

- show running-config
- Building configuration...
- Current configuration:
- - More -
- Ainsi que les lignes qui suivent le mot “End”.

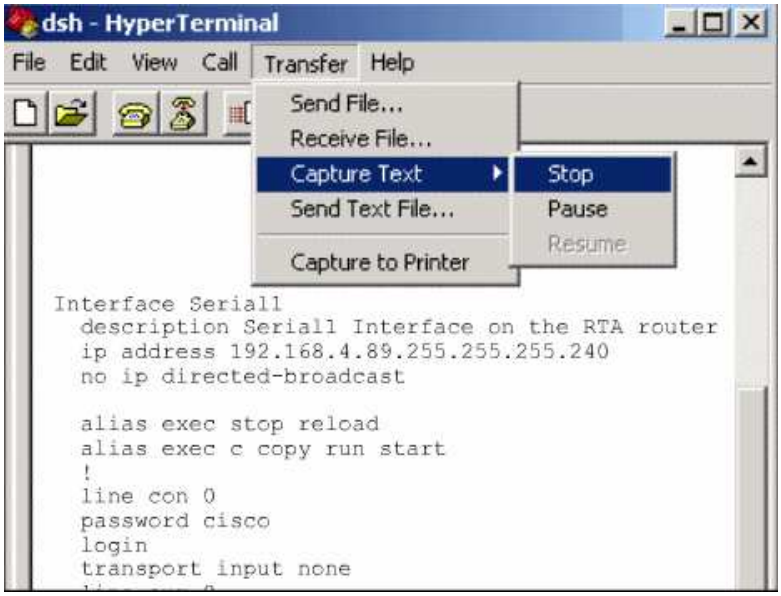
À la fin de chaque section d’interface, ajoutez la commande **no shutdown**.

Vous pouvez ajouter des commentaires à la configuration afin d’en expliquer certaines parties. Il suffit pour cela de placer un point d’exclamation “**!**” en début de ligne.

La restauration :

Erase startup-config → supprimer toute trace de configuration.
Reload → pour redémarrer le routeur.

- Passez en mode de configuration globale du routeur.
- cliquez sur **Transfert** > **Envoyer un fichier texte**.
- Sélectionnez le nom du fichier.
- **Copy running-config startup-config** → pour sauvegarder.



Gestion des images IOS via TFTP :

Copy flash tftp → sauvegarder une copie de l’IOS sur un serveur tftp (@IP + nom fichier)

Copy tftp flash → restaurer un IOS à partir d’un serveur tftp (@IP + nom fichier + formatage)

```
GAD#copy tftp flash
Address or name of remote host []?192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee…eeeeeeeeeeeee…erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!…!!!!!!!!!!!!!!!!!!
Verifying Check sum ............OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#
```

Gestion des images IOS via Xmodem

Si l'image IOS en mémoire flash a été effacée ou altérée, il peut être nécessaire de restaurer l'IOS à partir du mode moniteur ROM (ROMmon 1>).

1 → Connaître la cause de l'altération : **dir flash**
2 → Si vous détectez une image qui semble être valide, tentez de démarrer à partir de cette image. **boot flash: {nom de fichier}** exemple : rommon 1>*boot flash:c2600-is-mz.121-5*
3 → Utilisez la commande **show version** pour vérifier la valeur du registre de configuration
4 → si le problème persiste → vous devrez télécharger un nouveau IOS (à l'aide de xmodem)

Comment télécharger un IOS ?

Eléments requises :

Un PC contenant une copie du fichier IOS à restaurer + Un câble console + un programme d'émulation de terminal tel qu'Hyper Terminal (la vitesse par défaut de 9600 bps).

Confreg → pour modifier les paramètres de transfère (la vitesse jusqu'à 115200 bps)

Xmodem **-c {image_file_name}** → pour télécharger un IOS à partir du mode ROM Monitor

Le **-c** indique d'utiliser le code de redondance cyclique (CRC) pour contrôler les erreurs.

```
rommon 2 >xmodem -c c2600-is-mz.122-10a.bin

Do not start the sending program yet...

  Warning:  All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y
Ready to receive file c2600-is-mz.122-10a.bin ...
```

Vous devez alors lancer le transfert à partir de l'HyperTerminal :

→ **Transfert** > **Envoyer un fichier** + indiquez le nom/emplacement de l'image, sélectionnez Xmodem comme protocole, puis lancez le transfert.

Avant de redémarrer le routeur, vous devez à nouveau paramétrer la vitesse à 9600 bps et le registre de configuration à 0x2102 : #config-register **0x2102**

Variables d'environnement :

L'IOS peut être restauré à partir d'une session TFTP (le moyen le plus rapide)

Les variables d'environnement fournissent une configuration minimale qui permet le transfert via TFTP de l'IOS.

Le transfert ROMmon TFTP ne fonctionne que sur le premier port LAN (un jeu simple de paramètres IP a été défini pour cette interface).

Pour définir une variable d'environnement ROMmon, vous devez taper le nom de la variable, le signe égal (=), puis la valeur de la variable.

```
rommon 10>set
 IP_ADDRESS=10.0.0.1
 IP_SUBNET_MASK=255.255.255.0
 DEFAULT_GATEWAY=10.0.0.254
 TFTP_SERVER=192.168.1.1
 TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

Set → Pour vérifier les variables d'environnement ROMmon.

Tftpdnld → pour démarrer le téléchargement de l'IOS

i → pour redémarrer le routeur

Module 6

Routage & Protocoles de routage

Présentation du routage :

Le routage est le processus qu'un routeur utilise pour transmettre des paquets vers un réseau de destination.

→ Un routeur prend des décisions en fonction de l'adresse IP de destination d'un paquet.

Lorsque les routeurs utilisent le *routage dynamique*, ces informations sont fournies par les autres routeurs. Lorsque le *routage statique* est utilisé, un administrateur réseau configure manuellement les informations sur les réseaux distants.

Utilisation de la route statique

Puisqu'une route statique est configurée manuellement, l'administrateur doit la configurer sur le routeur à l'aide de la commande **ip route**

Router(config)#**ip route {réseau destination} {masque} {passerelle} {distance administrative}**

La passerelle : 1- Soit l'interface de sortie du routeur local
2- Soit l'adresse IP de l'interface du saut suivant

Exemple : 1- Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Ou 2- Router(config)#ip route 10.0.0.0 255.0.0.0 S1

La distance administrative est un paramètre optionnel qui donne une mesure de la fiabilité de la route. *Plus la valeur de la distance administrative est faible et plus la route est fiable*.
La distance administrative par défaut est **1** quand on utilise une route statique (Entre 0 et 255).

Show ip route {adresse} → Pour vérifier la distance administrative d'une route donnée.

Remarque : Si le routeur ne peut pas atteindre l'interface sortante qui est empruntée sur la route, la route n'est pas installée dans la table de routage.

Il est possible de configurer sur un routeur une route statique qui ne sera utilisée qu'en cas d'échec de la route acquise de façon dynamique → attribuez une *valeur de distance administrative supérieure* à celle du protocole de routage dynamique utilisé.

Configuration de l'acheminement par défaut

Les routes par défaut permettent de router des paquets dont les destinations ne correspondent à aucune autre route de la table de routage.

Router(config)#**ip route 0.0.0.0 0.0.0.0 {passerelle}**

Si le paquet ne correspond pas à une route plus spécifique de la table de routage, il sera acheminé vers le réseau 0.0.0.0.

Vérification de la configuration de route statique

Show running-config permet de vérifier que la route statique a été entrée correctement.
Show ip route permet de s'assurer que la route statique figure dans la table de routage.

Introduction aux protocoles de routage

Un protocole de routage est le *système de communication* utilisé *entre les routeurs*, il permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît (mises à jour des tables de routage).

Un protocole routé sert à diriger le trafic utilisateur. Il fournit suffisamment d'informations dans son adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre en fonction de la méthode d'adressage.

Systèmes autonomes

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune.

Les systèmes autonomes (AS) assurent la division de l'interréseau global en réseaux plus petits et plus faciles à gérer

L'InterNIC (*Internet Network Information Center*), un fournisseur de services ou encore un administrateur attribue un numéro d'identification à chaque système autonome. Ce numéro est un nombre à 16 bits (vitale pour la configuration d'IGRP).

Fonctionnement du routage dynamique :

Le protocole de routage prend connaissance de toutes les routes disponibles. Il insère les meilleures routes dans la table de routage et supprime celles qui ne sont plus valides.

Chaque fois que la topologie du réseau est modifiée (la croissance, reconfiguration ou une panne), la base de connaissances du réseau doit également être modifiée.

Lorsque tous les routeurs d'un interréseau reposent sur les mêmes connaissances, on dit de l'interréseau qu'il a **convergé**.

Une convergence rapide est préférable, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces.

Identification des classes des protocoles de routage

Il existe 2 grandes catégories :

- *vecteur de distance*
- *état de liens*

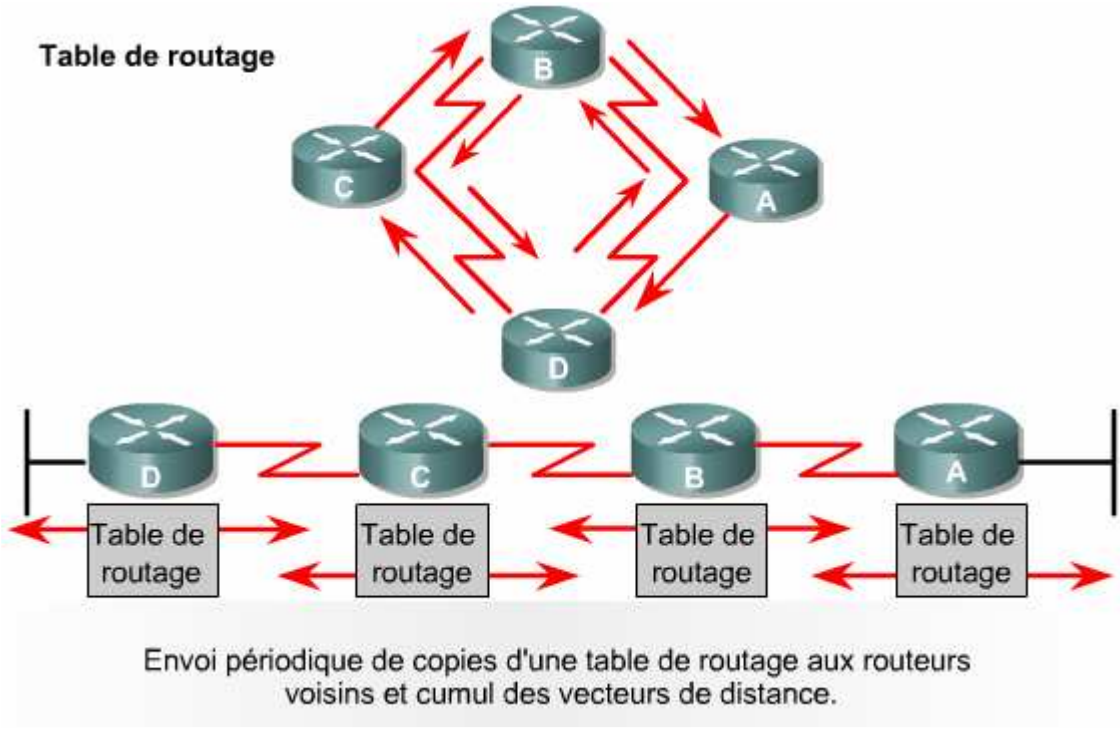
Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'interréseau.

L'approche à état de liens, également appelée routage par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau.

Fonctions du protocole de routage à vecteur de distance

Les algorithmes de routage à vecteur de distance (algorithmes Bellman-Ford) transmettent régulièrement des copies de table de routage d'un routeur à l'autre.

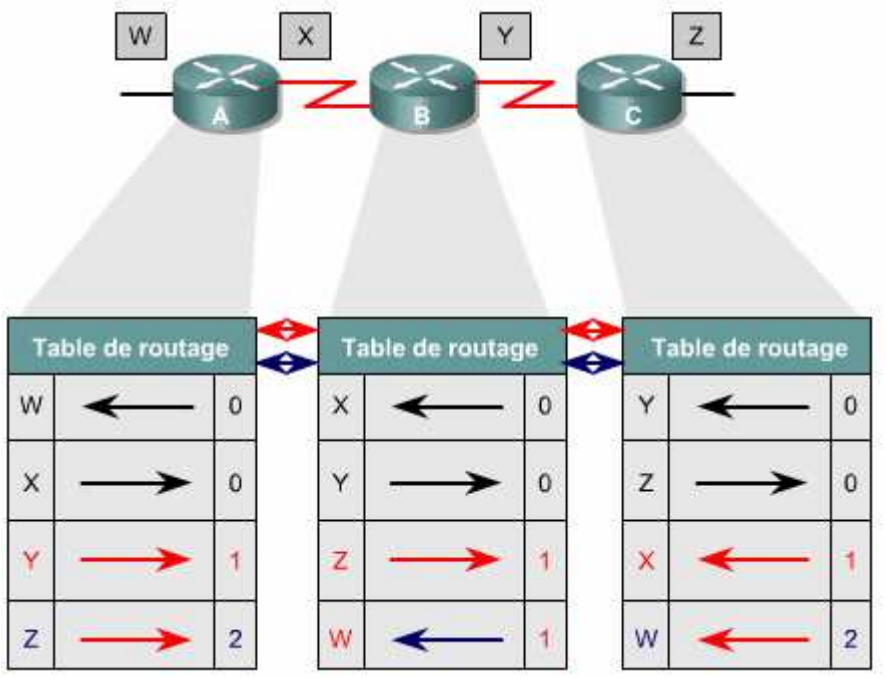
Chaque routeur reçoit l'intégralité des tables de routage des routeurs voisins auxquels il est directement connecté.



Envoi périodique de copies d'une table de routage aux routeurs voisins et cumul des vecteurs de distance.

L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau.

Chaque routeur voit uniquement ses voisins (ne connait pas la topologie exacte).
La distance entre l'interface et chaque réseau directement connecté est égale à **0**.



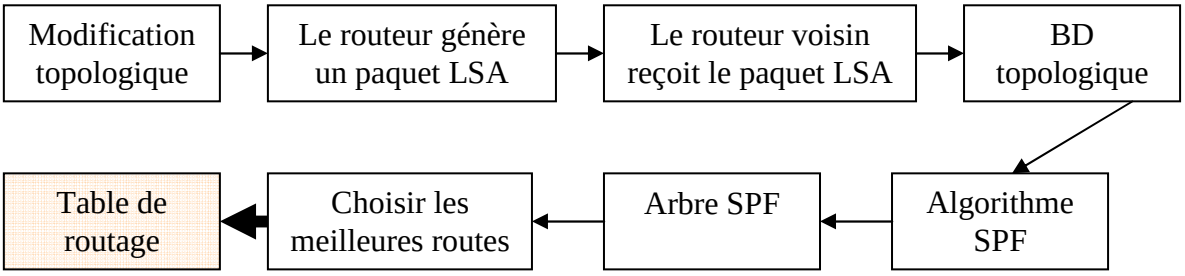
Fonctions du protocole de routage à état de liens

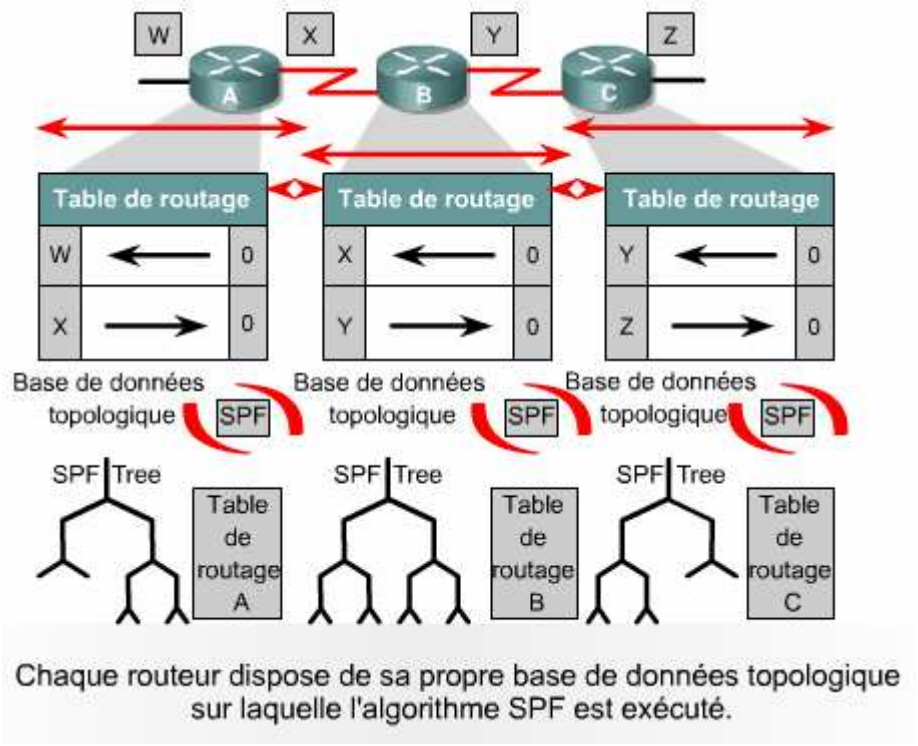
Les algorithmes à état de liens (algorithme de Dijkstra ou algorithme SPF) gèrent une base de données complexe d'informations topologiques (complète sur les routeurs distants et leurs interconnexions).

Le routage à état de liens utilise les éléments suivants :

- ***Mises à jour de routage à état de liens (LSA)* –** un petit paquet d'informations de routage qui est transmis entre les routeurs.
- ***Base de données topologique* –** un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liens.
- ***Algorithme SPF* –** L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.
- ***Tables de routage* –** Une liste des chemins et des interfaces connus.

Processus de découverte du réseau pour le routage à état de liens





Chaque routeur dispose de sa propre base de données topologique sur laquelle l'algorithme SPF est exécuté.

Considérations relatives au routage à état de liens:

- Surcharge du système (Processeurs)
- Mémoire requise.
- Consommation de bande passante

Vue d'ensemble des protocoles de routage

Un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes:

- la détermination du chemin,
- la commutation.

Le routeur se sert de la table de routage pour déterminer le meilleur chemin et transmet ensuite le paquet en utilisant la fonction de commutation. Il utilise la portion réseau de l'adresse pour sélectionner le chemin.

La commutation est le processus interne qu'utilise un routeur pour accepter un paquet sur une interface et le transmettre à une deuxième interface sur le même routeur.

Configuration de routage dynamique :

Router {protocole} {option}→ pour lancer le processus de routage (mode config globale)

Network **{adresse réseau directement connectée}**→ permet de déterminer les interfaces qui participeront à l'envoi et à la réception des mises à jour du routage.

Exemple :

```
Router(config)#router rip
Roouter(config-router)#network 172.16.0.0
```

Protocoles de routage:

Les protocoles suivants sont des exemples de protocoles de routage IP :

Le protocole RIP (Routing Internet Protocol) :

- un protocole de routage à vecteur de distance.
- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

Le protocole IGRP (Interior Gateway Routing Protocol)

- un protocole propriétaire développée par Cisco.
- un protocole de routage à vecteur de distance.
- La bande passante, la charge, le délai et la fiabilité (une métrique composite).
- Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes.

Le protocole OSPF (Open Shortest Path First)

- un protocole de routage à état de liens.
- C'est un protocole de routage de norme ouverte
- Il utilise l'algorithme SPF pour calculer le coût le plus bas vers une destination.
- Les mises à jour du routage sont diffusées à mesure des modifications de topologie.

Le protocole EIGRP (Enhanced IGRP)

- un protocole de routage à vecteur de distance amélioré (Cisco).
- Il utilise l'équilibrage de charge en coût différencié.
- Il utilise une combinaison de fonctions à vecteur de distance et à état de liens.
- Il utilise l'algorithme DUAL (Diffusing Update Algorithm) pour calculer le chemin.
- Les mises à jour du routage sont diffusées en mode multicast en utilisant l'adresse 224.0.0.10 et sont déclenchées par des modifications topologiques.

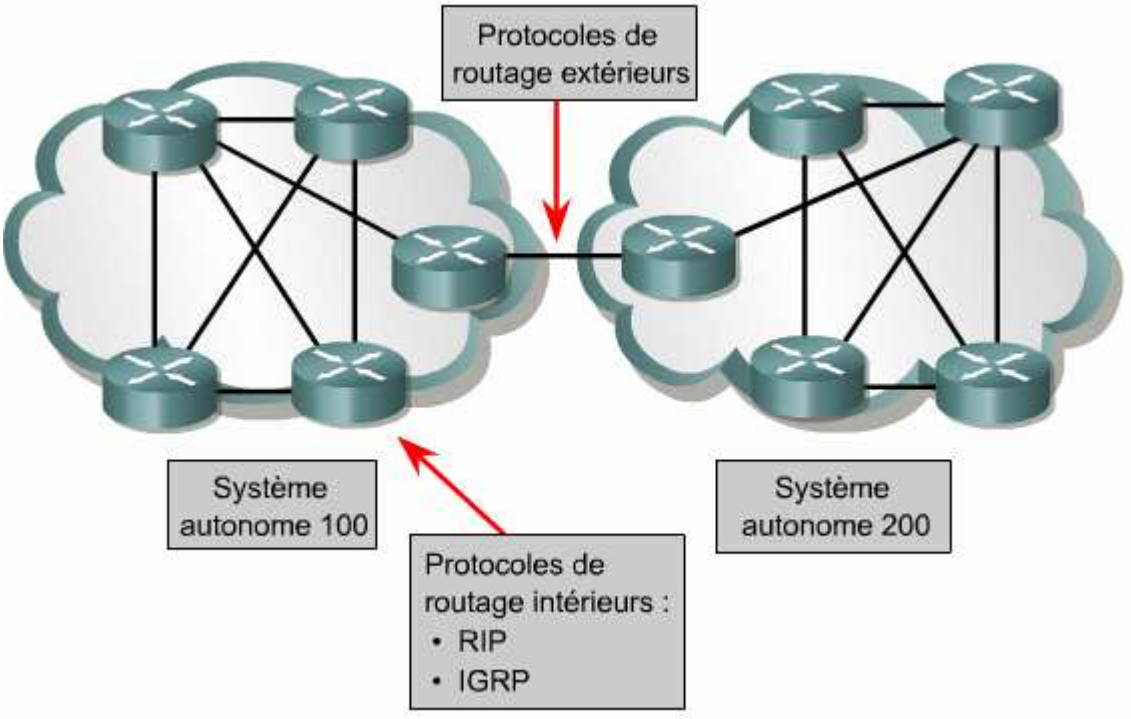
Le protocole BGP (Border Gateway Protocol)

- Il s'agit d'un protocole de routage extérieur à vecteur de distance.
- Il est utilisé pour la connexion entre les FAI ou entre les FAI et les clients.
- Il est utilisé pour acheminer le trafic Internet entre des systèmes autonomes.

Protocole IGP & EGP :

IGP → Protocoles utilisés à l'intérieur d'un Système autonome.

EGP → Protocoles utilisés entre les Systèmes autonomes.



Les protocoles de passerelle extérieurs IP nécessitent les trois ensembles d'informations suivants pour que le routage puisse commencer :

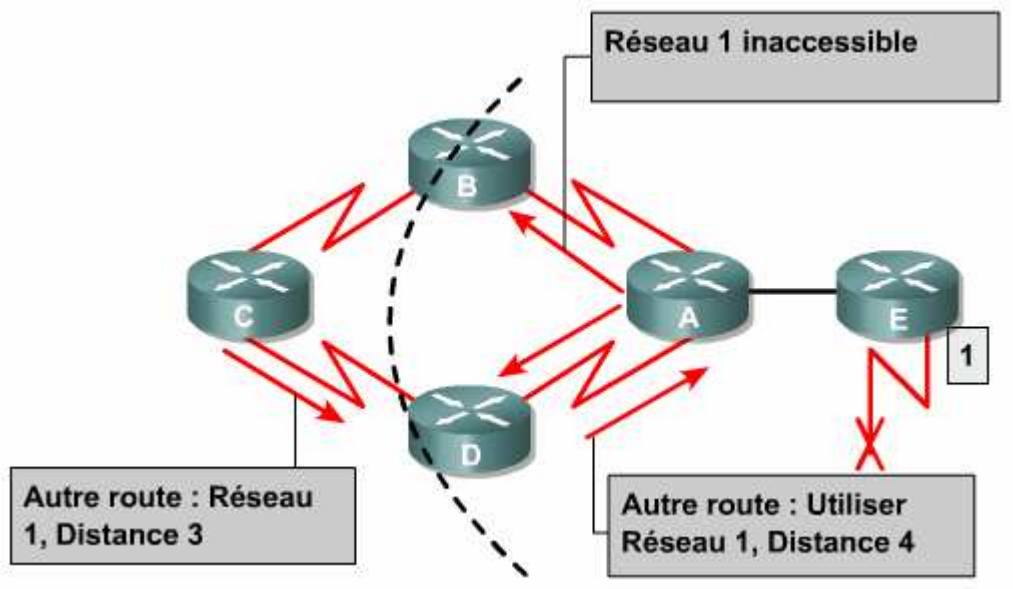
- *Une liste des routeurs voisins* avec lesquels échanger des informations de routage.
- *Une liste de réseaux à annoncer* comme étant directement accessibles.
- *Le numéro du système autonome* du routeur local.

Module 7

Protocoles de routage à vecteur de distance

Problèmes liés aux boucles de routage à vecteur de distance

Convergence lente → tables de routage incohérentes → Des boucles de routage.



1. Supposons que le meilleur chemin du routeur C vers le réseau 1 passe par le routeur B (distance=3).
2. Lorsque le réseau 1 tombe en panne, le routeur E envoie une mise à jour au routeur A. Ce dernier cesse d'acheminer des paquets vers le réseau 1, mais les routeurs B, C et D continuent de les acheminer car ils n'ont pas encore été informés de la panne. Lorsque le routeur A transmet sa mise à jour, les routeurs B et D cessent d'acheminer des paquets vers le réseau 1. Toutefois, le routeur C n'a toujours pas reçu de mise à jour. Pour lui, le réseau 1 est toujours accessible via le routeur B.
3. À présent, le routeur C envoie une mise à jour périodique au routeur D pour lui indiquer un chemin vers le réseau 1 passant par le routeur B. Le routeur D modifie sa table de routage pour refléter cette information erronée et la transmet au routeur A. Ce dernier la transmet à son tour aux routeurs B et E, et ainsi de suite.

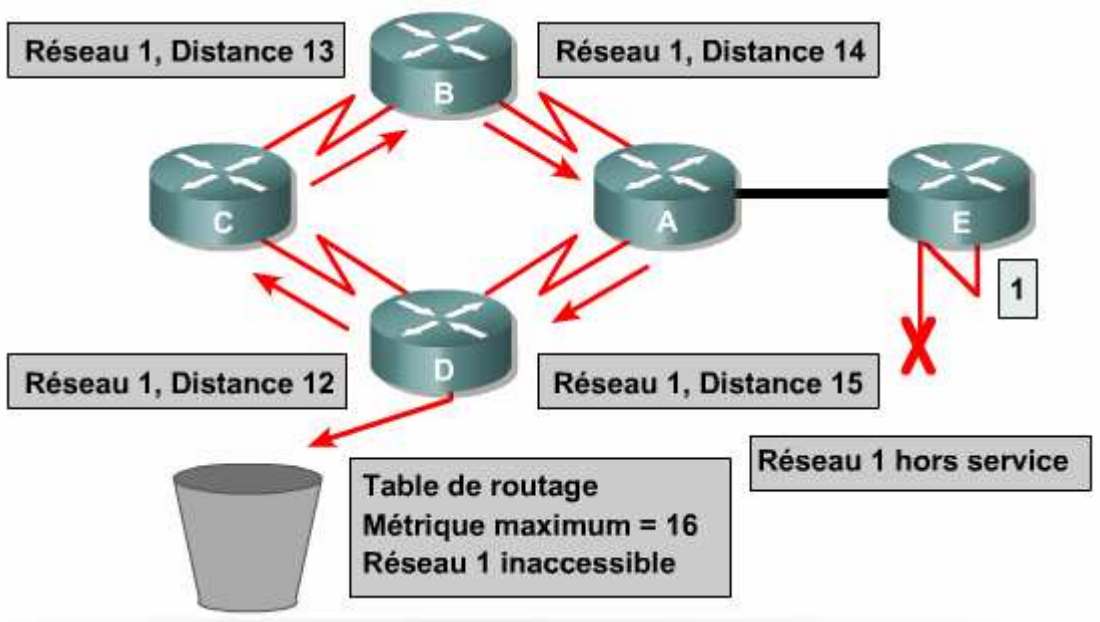
Tous les paquets destinés au réseau 1 génèrent alors ***une boucle*** à partir du routeur C vers les routeurs B, A et D, qui revient au routeur C.

Solutions pour éviter les boucles de routage :

Définition d'une valeur maximale

Le principe : définir une valeur de métrique maximale, le protocole de routage permet à la boucle de routage d'exister jusqu'à ce que la métrique dépasse la valeur maximale autorisée → réseau considéré inaccessible.

Exemple : le RIP (valeur maximale = 15) → la métrique 16 (inaccessible)



La fonction split horizon

Le principe : Si une mise à jour de routage relative au réseau 1 arrive du routeur A, le routeur B ou D n'est pas en mesure de renvoyer au routeur A les informations relatives au réseau 1.

→ Réduire les informations de routage erronées + réduire la charge de routage

Mode poison reverse

Le principe : le routeur détectant une panne, passe en mode poison reverse en créant une entrée de table de métrique supérieure à la métrique maximale autorisée (inaccessible) pour ce réseau.

Lorsque les voisins reçoivent un message poison reverse, ils renvoient au routeur d'origine une mise à jour poison reverse (s'assurer que toutes les routes du segment ont bien reçu les informations sur la route inaccessible).

Les mises à jour déclenchées

Le principe : Le routeur qui détecte une modification topologique envoie immédiatement un message de mise à jour aux routeurs adjacents qui, à leur tour, génèrent des mises à jour déclenchées pour signaler la modification à leurs routeurs voisins (sans attendre l'expiration du délai du compteur de mise à jour).

Compteurs de retenue

Le principe : Lorsqu'un routeur reçoit une mise à jour d'un routeur voisin lui indiquant qu'un réseau auparavant accessible est devenu inaccessible, il marque la route comme étant inaccessible et déclenche un compteur de retenue.

Si, avant l'expiration du délai de retenue (période de gel), une mise à jour provenant d'un autre routeur voisin indique une métrique inférieure, elle est ignorée.

→ Disposer de plus de temps pour transmettre à l'ensemble du réseau les informations relatives à une modification perturbatrice.

Le protocole RIP :

Introduction au RIP :

Le protocole RIP comprend 2 versions : RIP v1 et RIP v2

La version **RIP v2** présente les **améliorations** suivantes:

- Possibilité de transmettre des informations supplémentaires.
- Mécanisme d'authentification.
- Prise en charge des masques de sous-réseau de longueur variable (VLSM).

Les principales caractéristiques du protocole RIP sont les suivantes :

- Il s'agit d'un protocole de routage à vecteur de distance.
- Le nombre de sauts est la métrique utilisée pour sélectionner le chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

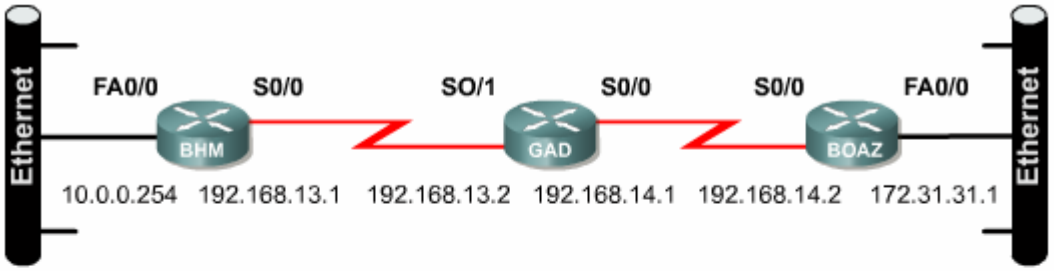
Configuration du protocole RIP :

La commande **router rip** permet de sélectionner le protocole RIP comme protocole de routage. La commande **network** permet d'indiquer au routeur les interfaces sur lesquelles exécuter RIP.

Le protocole RIP envoie des messages de mise à jour de routage à intervalles réguliers. Les routeurs RIP conservent uniquement la meilleure route vers une destination mais ils peuvent également gérer plusieurs chemins de coût égal vers une destination.

Router(config)#**router rip** → Active le processus de routage RIP
Router(config-router)#**network {numéro-réseau}** → Associe un réseau au processus RIP

Exemple :




```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

Utilisation de la commande ip classless

Absence de la commande ip classless :

Par défaut, un routeur suppose que tous les sous-réseaux d'un réseau directement connecté doivent se trouver dans la table de routage. Si un paquet reçu comporte une adresse de destination inconnue dans un sous-réseau inconnu d'un réseau directement attaché, le routeur suppose que le sous-réseau n'existe pas. Le routeur abandonnera donc le paquet même s'il existe une route par défaut.

Avec l'utilisation de la commande ip classless :

Le routeur ignore les frontières entre les classes de réseaux au sein de sa table de routage et acheminer tout simplement les données vers la route par défaut.

→ La commande **ip classless** est activée par défaut à partir de la version 11.3 de l'IOS.

Router(config)#**ip classless** → pour activer la fonction ip classless
Router(config)#**no ip classless** → pour désactiver la fonction ip classless

Problèmes de configuration RIP fréquents

«***Routage par rumeur***» → Les routeurs doivent se fier aux routeurs voisins pour obtenir les informations réseau dont ils n'ont pas connaissance directement (RIP).

→ On rencontre des problèmes de boucles de routage et de métrique de mesure infinie.

Router(config-if)#**no ip split-horizon** → Pour désactiver la fonction split horizon:

La valeur par défaut du compteur de retenue RIP est de 180 secondes. Il est possible de diminuer le compteur de retenue pour améliorer la convergence.

Dans l'idéal, il faudrait que la valeur du compteur corresponde au plus long temps de mise à jour possible pour l'interréseau.

→ Pour changer l'intervalle de mise à jour :

Router(config-router)#**timers basic** {**update**} {**invalid**} {**holddown**} {**flush**} [**sleeptime**]

→ Pour désactiver l'envoi des mises à jour de routage vers certaines interfaces.

Router(config-router)#**passive-interface** {**interface**}

Dans certains types de réseau (Frame Relay), le protocole RIP doit être informé sur les autres RIP voisins. Pour cela.

Router(config-router)#**neighbor** {**IP du routeur voisin**}

Configuration du routeur pour l'envoi et la réception des paquets :

Par défaut, la plate-forme logicielle Cisco IOS reçoit des paquets RIP Version 1 et 2 mais n'envoie que des paquets Version 1.

L'administrateur réseau peut configurer le routeur pour qu'il ne reçoive et n'envoie que des paquets Version 1 ou pour qu'il n'envoie que des paquets Version 2.

Globalement :

Commande	Usage
GAD(config-router)#**version {1|2}**	Configure le logiciel afin qu'il puisse recevoir et envoyer les paquets RIP Version 1 ou Version 2.
GAD(config-if)#**ip rip send version 1**	Configure une interface afin qu'elle n'envoie uniquement que des paquets RIP Version 2.
GAD(config-if)#**ip rip send version 2**	Configure une interface afin qu'elle n'envoie uniquement que des paquets RIP Version 2.
GAD(config-if)#**ip rip send version 1 2**	Configure une interface pour envoyer seulement des paquets RIP version 1 ou 2.

Sur une interface :

Commande	Usage
GAD(config-if)#ip rip receive version 1	Configure une interface afin qu'elle ne reçoive uniquement que des paquets RIP Version 1.
GAD(config-if)#ip rip receive version 2	Configure une interface afin qu'elle ne reçoive uniquement que des paquets RIP Version 2.
GAD(config-if)#ip rip receive version 1 2	Configure une interface afin qu'elle puisse recevoir des paquets RIP Version 1 ou Version 2.

Vérification de la configuration RIP

On utilise plusieurs commandes surtout : **show ip route** et **show ip protocols**

Show ip protocols → affiche les protocoles de routage utilisés pour l'acheminement du trafic

- Est-ce que RIP est configuré ?
- Est-ce que les interfaces appropriées envoient et reçoivent des mises à jour RIP ?
- Est-ce que le routeur annonce les réseaux appropriés ?

```
GAD#show ip protocols
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 5
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Outgoing update filter list for all interfaces is
    Incoming update filter list for all interfaces is
    Redistributing: Rip
    Default version control: send version 1, receive any
version
   Interface          Send    Recv      Triggered RIP   Key-chain
   FastEthernet0/0    1       1 2
   Serial0/0          1       1 2
Routing for Networks:
   192.168.1.0
   192.168.2.0
```

Vérifiez que RIP est configuré.

Vérifiez que les réseaux ont été déclarés.

Vérifiez l'interface RIP.

Show ip route → Examinez les routes RIP signalées par "R".

R 192.168.3.0/24 {120/1} via 192.168.2.2, 00 :00 :07, Serial0/0

Des commandes supplémentaires permettent de vérifier RIP, par exemple:

Show interface {interface}
Show ip interface {interface}
Show running-config

Dépannage des problèmes de mise à jour RIP

Debug ip rip → permet d'afficher les mises à jour RIP lors de leur envoi et de leur réception.

```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:33: RIP: received v1 update from 192.168.13.2
on Serial0/0
00:45:33:        192.168.14.0 in 1 hop
00:45:33:        172.31.0.0 in 2 hop
00:45:33:        172.29.0.0 15 hops
00:45:36: RIP: sending v1 update to 255.255.255.255
via Serial0/0 (192.168.13.1)
00:45:36:         network 10.0.0.0. metric 1
00:45:36: RIP: sending v1 update to 255.255.255.255
via FastEthernet0/0 (10.0.0.254)
00:45:36:          network 192.168.13.0. metric 1
00:45:36:          network 192.168.14.0. metric 2
00:45:36:          network 172.31.0.0. metric 3
00:45:36:          network 172.29.0.0. metric 16
```

Cette commande permet également de diagnostiquer des sous-réseaux contigus ou des réseaux en double

Des commandes supplémentaires permettent de résoudre les problèmes RIP :

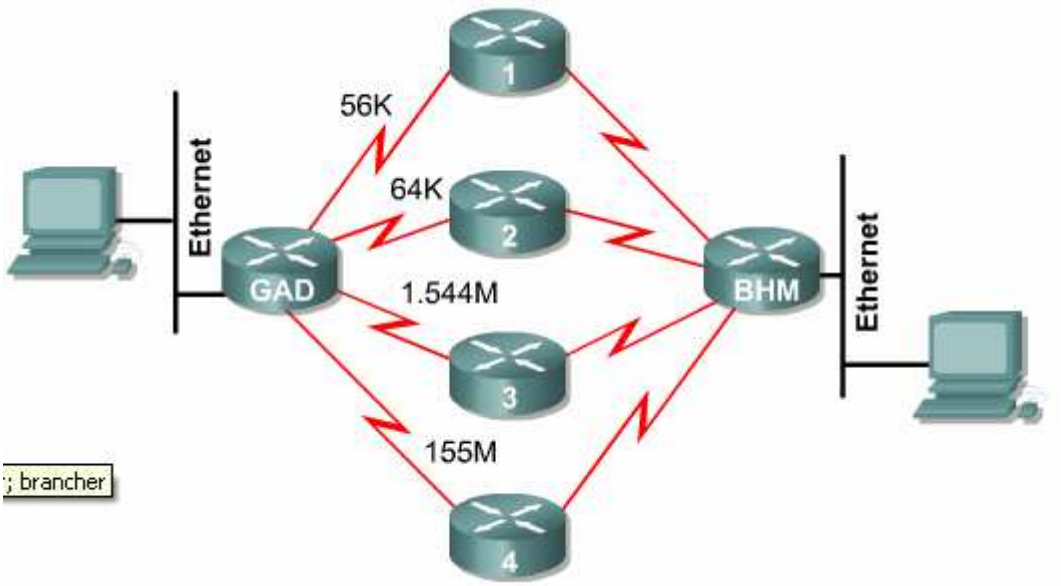
Show ip rip database
Show ip protocols {summary}
Show ip route
Debug ip rip {events}
Show ip interface brief

Équilibrage de charge RIP

L'équilibrage de charge est un concept permettant à un routeur de bénéficier de plusieurs « meilleurs chemins » vers une destination donnée.

RIP est capable de gérer un équilibrage de charge sur plus de six chemins de coût égal avec quatre chemins par défaut.

→ Par défaut, BGP n'autorise qu'un seul chemin vers une destination.



Show ip route → examiner les routes de coût égal.

```
Router#show ip route 10.0.0.0
  Routing entry for 10.0.0.0/8
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Advertised by rip (self originated)
  Last update from 192.168.75.7 on Serial1,
00:00:00 ago
  Routing Descriptor Blocks:
  * 192.168.57.7, from 192.168.57.7, 00:00:18 ago,
via Serial0
      Route metric is 1, traffic share count is 1
    192.168.75.7, from 192.168.75.7, 00:00:00 ago,
via Serial1
      Route metric is 1, traffic share count is 1
```

L'astérisque (*) signale la route active utilisée pour le nouveau trafic.

Remarque : Lorsqu'un routeur apprend plusieurs routes vers un réseau spécifique, c'est la route avec la distance administrative la plus courte qui est ajoutée à la table de routage.

Pour modifier le nombre maximum de chemins parallèles autorisés :

`Router(config-router)#`**maximum-paths** **[nombre de 0 jusqu'à 6]**

2 méthodes d'équilibrage de charge :

→ Équilibrage de charge par paquet

→ Équilibrage de charge par destination (par défaut)

Si le processus de commutation est activé, le routeur peut changer de chemin à chaque nouveau paquet.

Par défaut la commutation «Fast Switching» est activée → une seule des routes sera mise en mémoire cache pour l'adresse de destination et les paquets de la trame acheminés vers un hôte spécifique prendront tous le même chemin. Les paquets en route vers un hôte différent sur le même réseau peuvent utiliser une autre route.

No ip route-cache → pour désactiver la commutation «Fast Switching»

Intégration des routes statiques avec le protocole RIP

Un routeur RIP peut recevoir une route par défaut (passerelle de dernier recours) via une mise à jour envoyée par un autre routeur RIP. Le routeur peut aussi générer lui-même la route par défaut.

Il est possible d'indiquer qu'une route statique est moins recommandée qu'une route apprise de façon dynamique (***route statique flottante***) si la distance administrative pas défaut de la route statique est supérieure à celle de la route dynamique.

Remarque : Les routes statiques qui pointent vers une interface seront annoncées via le routeur RIP propriétaire de la route statique et ces routes seront propagées via l'interréseau.

Redistribute static → pour annoncer les routes statiques dans les mises à jour RIP.

→ Lorsqu'une interface tombe en panne, toutes les routes statiques pointant vers cette interface sont supprimées de la table de routage IP.

Le protocole IGRP :

Caractéristiques du protocole IGRP :

- Polyvalence : traiter automatiquement des topologies complexes.
- Flexibilité : la segmentation avec des caractéristiques en termes de BP et de délai
- Évolutivité : fonctionner sur des réseaux de très grande taille

Métriques du protocole IGRP :

→ Métriques utilisés : Bande passante, Délai, Charge, Fiabilité.

- Bande passante : Valeur de bande passante la plus faible sur le chemin
- Délai : Délai d'interface global le long du chemin
- Fiabilité : Fiabilité de la liaison vers la destination
- Charge : Charge d'une liaison vers la destination, en bits par seconde.

→ IGRP utilise par défaut la bande passante et le délai comme métriques.

Show ip protocols → pour afficher les métriques du protocole IGRP.

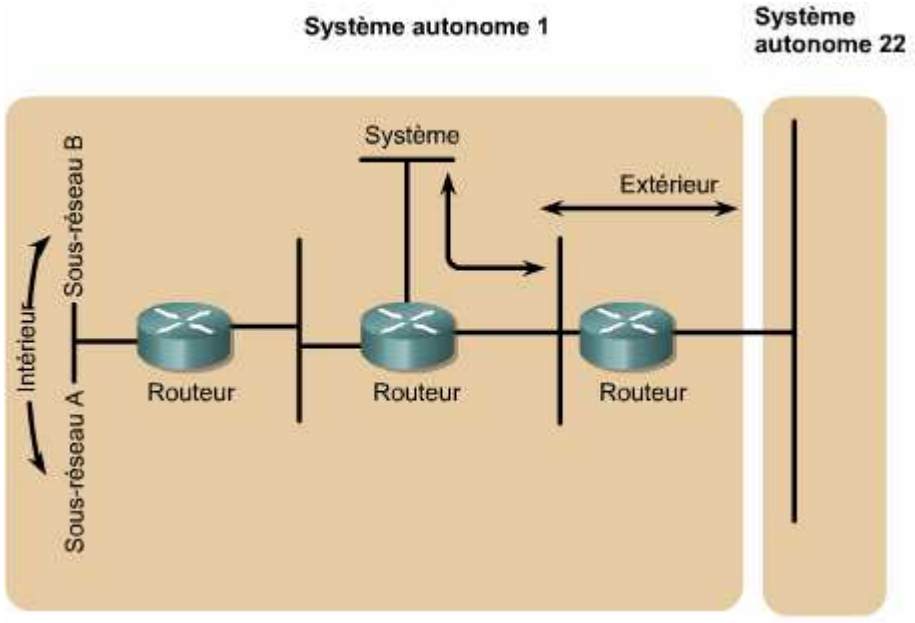
```
Router>show ip protocols
Routing Protocol is igrp 300
  Sending updates every 90 seconds, next due in 55
seconds
  Invalid after 270 seconds, hold down 280, flushed
after 360
  Outgoing update filter list for all interfaces is
not set
  Incoming update filter list for all interfaces is
not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igrp 300
  Routing for Networks:
    183.8.0.0
    144.253.0.0
```

Les coefficients K1 à K5 apparaissent sur le graphique. Ils sont utilisés par l'algorithme pour calculer la métrique de routage IGRP.

→ Par défaut, K1 = K3 = 1 K2 = K4 = K5 = 0.

Routes IGRP :

Le protocole IGRP annonce trois types de routes:



Intérieure : sont des routes situées entre les sous-réseaux d'un réseau relié à une interface de routeur. Si le réseau relié à un routeur n'est pas divisé en sous-réseaux, le protocole IGRP n'annonce pas les routes intérieures.

Système : sont les routes menant à d'autres réseaux au sein d'un système autonome. Elles ne contiennent pas d'information sur les sous-réseaux.

Extérieure : sont des routes menant à des réseaux extérieurs au système autonome, et qui sont utilisées lorsqu'une passerelle de dernier recours est envisagée

Caractéristiques de stabilité du protocole IGRP

Le protocole IGRP offre plusieurs fonctions conçues pour améliorer sa stabilité, notamment :

- ***les Gels*** : Lorsqu'un routeur tombe en panne, les routeurs voisins le détectent grâce à l'absence de messages de mise à jour périodiques.
- ***Split Horizon***.
- ***Poison reverse***.
- ***Gestion des compteurs***.

Les compteurs sont : un compteur de mise à jour, un compteur de temporisation, un compteur de retenue et un compteur d'annulation.

→ Le *compteur de mise à jour* indique la fréquence d'envoi des messages de mise à jour du routage (par défaut 90 secondes).

→ Le *compteur de temporisation* indique le laps de temps au bout duquel un routeur doit déclarer une route non valide en l'absence de messages de mise à jour la concernant (par défaut 270 secondes).

→ Le *compteur de retenue* indique le laps de temps pendant lequel les informations relatives aux routes non optimales sont ignorées (par défaut 280 secondes)

→ Le *compteur d'annulation* indique le laps de temps devant s'écouler avant la suppression d'une route dans la table de routage (par défaut 630 secondes)

```
RouterB#show ip protocols
Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 51
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
```

Configuration du protocole IGRP

```
Router(config)#router igrp {numéro de système autonome}
Router(config)#network {réseau directement connecté}
```

Exemple :

```
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0
```

Migration de RIP vers IGRP

1. show ip route pour vérifier le protocole RIP sur les routeurs à convertir.
2. Configurez le protocole IGRP sur les routeurs router rip
3. Entrez la commande show ip protocols sur les routeurs.
4. Entrez la commande show ip route sur les routeurs.

Vérification de la configuration IGRP

Show ip route → Pour vérifier les routes IGRP signalées par un "**I**"

I 192.168.3.0/24 {100/80135} via 192.168.2.2, 00 :00 :07, Serial0/0

Des commandes supplémentaires permettent de vérifier le protocole IGRP :

```
Show interface {interface}
Show running-config
Show running-config interface {interface}
Show running-config | begin interface {interface}
Show running-config | begin igrp
Show ip protocols
```

Dépannage du protocole IGRP

Debug ip igrp events

```
RouterA#debug ip igrp events
IGRP event debugging is on

00:21:38: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:21:38: IGRP: Update contains 0 interior, 2
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 1
```

Debug ip igrp transactions

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on

00:22:17: IGRP: received update from 192.168.2.2
on Serial0/0
00:22:17:    network 192.168.3.0, metric 80135
(neighbor 110)
00:23:07: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:23:07:    network 192.168.2.0, metric=80125
00:23:07:    network 192.168.3.0, metric=80135
00:23:07: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:23:07:    network 192.168.1.0, metric=110
```

Module 8

Messages de contrôle & d'erreur TC/IP suite

Présentation du protocole ICMP :

ICMP (Internet Control Message Protocol) est le composant de la pile de protocoles TCP/IP qui résout la limitation de base d'IP à garantir que les données sont acheminées dans l'éventualité de problèmes de communication réseau.

Signalement et correction des erreurs

→ L'ICMP est un protocole de signalement d'erreurs pour IP.

Un routeur qui n'arrive pas à router un paquet, il utilise ICMP «*destination inaccessible*» pour envoyer un message à la station de travail (l'origine de paquet) lui indiquant que le paquet n'a pas pu être acheminé.

Causes :

- L'équipement émetteur peut adresser le datagramme à une adresse IP inexistante ou à un équipement de destination qui est déconnecté de son réseau.
- une interface de connexion d'un routeur est arrêtée ou s'ils ne disposent pas des informations nécessaires pour trouver le réseau de destination.
- Détection de routes excessivement longues.

Remarque : L'ICMP ne signale l'état du paquet transmis qu'à l'équipement d'origine.

Acheminement de message ICMP

Les messages ICMP sont encapsulés dans des datagrammes de la même façon que toute autre donnée à l'aide d'IP. Voici un datagramme ICMP en capsulé dans un paquet IP :

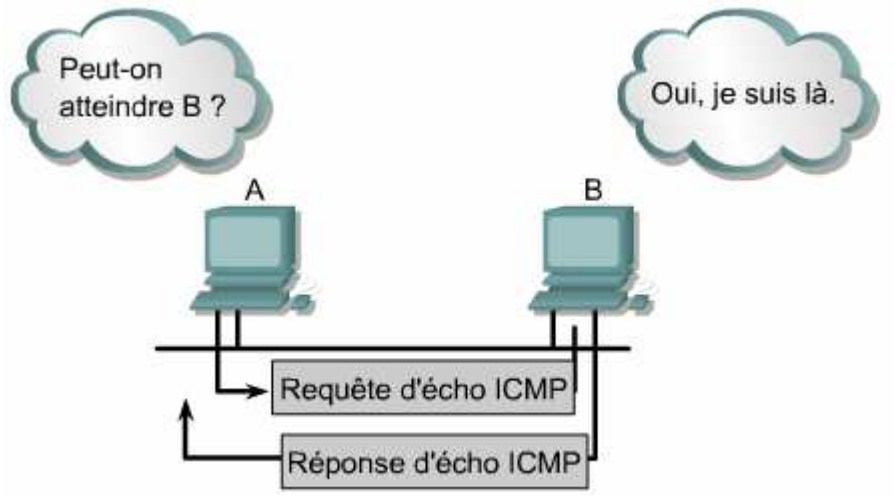
En-tête de trame	En-tête de datagramme	En-tête ICMP	Données ICMP
En-tête de trame	En-tête de datagramme	Zone de données du datagramme	
En-tête de trame	Zone de données de la trame		

Remarque : Les erreurs créées par les messages ICMP ne génèrent pas leurs propres messages ICMP. Il est ainsi possible qu'une erreur de transmission de datagramme ne soit jamais signalée à l'émetteur des données.

Utilisation de requêtes ping pour tester l'accessibilité de la destination

Le protocole ICMP peut être utilisé pour tester la disponibilité d'une destination particulière.

→ La réponse d'écho, confirme l'accessibilité de la destination.



La demande d'écho comprend une valeur de durée de vie (*TTL*). La durée de vie est un champ contenu dans l'en tête du paquet IP qui permet de limiter la transmission des paquets.

A chaque fois qu'un routeur transmet un paquet il décrémente la valeur TTL de un. Quand un routeur reçoit un paquet avec un TTL égal à 1, il ne transmet pas le paquet.

Messages ICMP :

Format de message :

Tous les formats de messages ICMP commencent par ces trois champs:

- ***Type*** : indique le type de message ICMP envoyé
- ***Code*** : inclut des informations supplémentaires spécifiques au type de message
- ***Checksum*** (somme de contrôle) : vérifier l'intégrité des données

0	8	16	31
Type (0 ou 8)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Données facultatives			
...			

Types de messages ICMP :

Types de message ICMP	
0	Réponse d'écho
3	Destination inaccessible
4	Épuisement de la source
5	Requête de redirection/modification
8	Requête d'écho
9	Annonce de routeur
10	Sélection de routeur
11	Dépassement du délai
12	Problème de paramètre
13	Demande d'horodatage
14	Réponse d'horodatage
15	Demande d'informations
16	Réponse à la demande d'informations
17	Demande de masque d'adresse
18	Réponse à la demande de masque d'adresse

Message Destination inaccessible

0	8	16	31
Type (3)	Code (0-12)	Somme de contrôle	
Inutilisé (doit être zéro)			
En-tête Internet + 64 premiers bits du datagramme			

Codes d'un message Destination inaccessible :

La valeur du code indique la raison de la non transmission du paquet.

0 = réseau inaccessible
1 = hôte inaccessible
2 = protocole inaccessible
3 = port inaccessible
4 = fragmentation nécessaire et DF défini
5 = échec de route source
6 = réseau de destination inconnu
7 = hôte de destination inconnu
8 = hôte source isolé
9 = communication avec le réseau de destination administrativement interdite
10 = communication avec l'hôte de destination administrativement interdite
11 = réseau inaccessible pour le type d'unité
12 = hôte inaccessible pour le type de service

Un message destination inaccessible peut également être envoyé lorsqu'il est nécessaire de fragmenter un paquet. C'est le cas en principe lorsqu'un datagramme est transmis d'un réseau Token-Ring à un réseau Ethernet.

Des messages destination inaccessible peuvent également être générés si les services liés à l'IP tels que les services FTP ou les services Web ne sont pas disponibles.

Erreurs diverses :

Certains types d'erreurs au niveau de l'en-tête peuvent empêcher les équipements qui traitent les datagrammes de les transmettre.

0	8	16	31
Type (12)	Code (0-2)	Somme de contrôle	
Pointeur		Inutilisé (doit être zéro)	
En-tête Internet + 64 premiers bits du datagramme			

Remarque : Lorsque la valeur de code est 0, le champ pointeur indique l'octet du datagramme qui a produit l'erreur.

Messages de contrôle TCP/IP Suite

Présentation :

Contrairement aux messages d'erreur, les messages de contrôle ne résultent pas de paquets perdus ou de conditions d'erreurs qui se produisent lors de la transmission de paquets. À la place, ils sont utilisés pour informer les hôtes de conditions telles que la congestion du réseau ou de l'existence d'une meilleure passerelle jusqu'à un réseau distant.

Demandes de redirection/modification ICMP

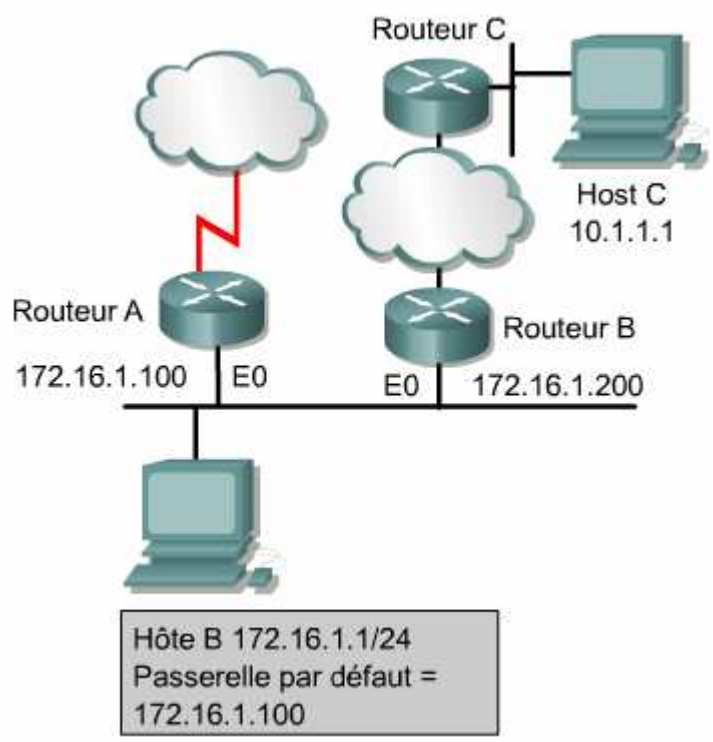
Ce type de message ne peut être émis que par une passerelle.

Les situations forceront l'envoi des messages ICMP « redirect/change »

- L'interface via laquelle le paquet entre dans le routeur est la même que celle par laquelle il ressort
- Le sous-réseau/réseau de l'adresse IP origine est identique à celui de l'adresse IP du saut suivant du paquet routé.
- Le datagramme n'est pas acheminé à l'origine.
- Le datagramme n'est pas acheminé à l'origine.
- La route de redirection n'est pas une autre redirection ICMP ou une route par défaut.

Exemple :

L'hôte B envoie un paquet à l'hôte C sur le réseau 10.0.0.0/8. Puisque l'hôte B n'est pas directement connecté au même réseau, il transmet le paquet à sa passerelle par défaut, le routeur A. Le routeur A trouve la route appropriée vers le réseau 10.0.0.0/8 en consultant sa table de routage. Il détermine que le chemin vers le réseau emprunte la même interface d'où provient la demande de transmission du paquet. Il transmet le paquet et envoie une demande de redirection/modification à l'hôte B, lui indiquant d'utiliser le routeur B comme passerelle pour acheminer toutes les futures demandes au réseau 10.0.0.0/8.



Paquet « redirect/change » :

0	8	16	31
Type (5)	Code (0-3)	Somme de contrôle	
Adresse Internet du routeur			
En-tête Internet + 64 premiers bits du datagramme			

Valeur de code	Action requise
0	Datagrammes redirigés pour le réseau.
1	Datagrammes redirigés pour l'hôte.
2	Datagrammes redirigés pour le type de service et les réseaux.
3	Datagrammes redirigés pour le type de service et l'hôte.

Le champ *Router Internet Address* de la redirection ICMP est l'adresse IP qui serait utilisée comme passerelle par défaut pour un réseau particulier.

Synchronisation d'horloge et estimation du temps de transit

Les hôtes de différents réseaux qui essaient de communiquer à l'aide de logiciels qui requièrent une synchronisation peuvent de ce fait rencontrer des problèmes. Le type de message d'horodatage ICMP est conçu pour éviter ce problème.

Le ***message de demande d'horodatage ICMP*** permet à un hôte de demander l'heure courante de l'hôte distant. L'hôte distant utilise un message de ***réponse d'horodatage ICMP*** pour répondre à la demande.

0	8	16	31
Type (13 ou 14)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Horodatage d'origine			
Horodatage de réception			
Horodatage de transmission			

Le champ type d'un message d'horodatage peut avoir la valeur

- 13 (demande d'horodatage)
- 14 (réponse d'horodatage).

→ Horodatage de départ est l'heure à laquelle l'hôte demandeur a envoyé la demande.
→ Horodatage de réception est l'heure à laquelle l'hôte de destination reçoit la demande.
→ Horodatage de transmission est renseigné juste avant que la réponse ne soit retournée.

Les horodatages sont calculés en nombres de millisecondes écoulées depuis zéro heure, temps universel (UT).

Remarque : des protocoles plus robustes tels que le NTP (Network Time Protocol), au niveau des couches supérieures, effectuent la synchronisation d'horloge de façon bien plus fiable.

Format de messages de demande d'information

Les messages de demandes et de réponse d'informations ICMP étaient initialement conçus pour permettre à l'hôte de déterminer son numéro de réseau.

0	8	16	31
Type (15 ou 16)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	

- Le type 15 correspond à un message de demande d'information
- Le type 16 correspond à un message de réponse d'information.

Remarque : Ce type de message ICMP est aujourd'hui considéré comme obsolète. D'autres protocoles tels que BOOTP, RARP et DHCP utilisés pour obtenir les numéros de réseau.

Requêtes de masque d'adresse

Si un hôte ne connaît pas le masque de sous-réseau, il peut envoyer une demande de masque d'adresse au routeur local.

0	8	16	31
Type (17 ou 18)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Masque d'adresse			

- Le type 17 correspond à un message demande de masque d'adresse
- Le type 18 correspond à un message de réponse de masque d'adresse.

Message de détection de routeur

Lorsqu'un hôte démarre sur le réseau et qu'il n'a pas été configuré manuellement avec une passerelle par défaut, il peut prendre connaissance des routeurs disponibles au travers du processus de détection de routeur un message de sollicitation de routeur, en utilisant l'adresse multicast 224.0.0.2 comme adresse de destination.

Lorsqu'un routeur qui prend en charge le processus de détection reçoit le message de détection de routeur, il retourne une annonce de routeur.

0	8	16	31
Type (9)	Code (0)	Somme de contrôle	
Nombre d'adresses	Taille d'entrée d'adresse	Durée de vie	
Adresse du routeur 1			
Niveau de préférences 1			
Adresse du routeur 2			
Niveau de préférences 2			

Champs IP	
Adresse source	Adresse IP appartenant à l'interface à partir de laquelle ce message est envoyé.
Adresse de destination	Adresse d'annonce configurée ou adresse IP d'un hôte voisin.
Durée de vie	1 si l'adresse de destination est une adresse multicast IP ; sinon, au moins 1.

Messages de congestion et de contrôle de flux

Si plusieurs ordinateurs tentent d'accéder simultanément à la même destination, l'ordinateur de destination risque d'être submergé → La congestion peut se produire

→ Entraîne un abandon de paquets

Ce message demande à l'émetteur de réduire le débit de transmission des paquets. Dans la plupart des cas, la congestion s'atténue en peu de temps, et l'origine peut augmenter le débit tant qu'elle ne reçoit pas d'autres messages d'épuisement de la source.

La plupart des routeurs Cisco n'envoient pas ce type de message par défaut, car il peut lui-même contribuer à la congestion du réseau.

Module 9

Dépannage de base d'un routeur

Examen de la table de routage

Commande show ip route

Show ip route → affiche le contenu de la table de routage IP.

Show ip route connected → afficher les routes directement connectés « C »
Show ip route {address} → affiche les entrée routant cers une destination particulier.
Show ip route rip → afficher les routes RIP « R »
Show ip route igrp → afficher les routes IGRP « I »
Show ip route static → afficher les routes manuellement configurés.

Détermination de la passerelle de dernier recours

Les routes par défaut sont utilisées lorsque le routeur est incapable d'associer un réseau de destination à une entrée spécifique de la table de routage.

Avantage → Les tables de routage ne sont pas encombrées.

→ Un administrateur doit configurer au moins un routeur avec une route par défaut.

Ip route 0.0.0.0 0.0.0.0 {adresse passerelle / interface de sortie}
Ou
Ip default-network {adresse passerelle}

La commande **`ip default-network`** s'utilise dans le système d'adressage avec classes (*classful*), ce qui signifie que si le routeur a une route vers un sous-réseau entré par cette commande, il n'installera en fait que la route vers le réseau principal non segmenté.

La commande show ip route affiche ce qui suit :

```
Gateway of last resort is 172.16.1.2 to network 0.0.0.0
```

Détermination des adresses de couche 2 et 3

L'adresse de couche 3 est utilisée pour acheminer le paquet du réseau source au réseau de destination. Les adresses IP d'origine et de destination restent identiques. L'adresse MAC change à chaque saut ou routeur.

Détermination de la distance administrative de la route

La distance administrative est un nombre qui mesure la fiabilité de la source des informations de route. Plus la distance administrative est petite, plus la source est fiable.

Détermination de la métrique de la route

La métrique est une valeur qui mesure les avantages d'une route. Plus cette valeur est petite, meilleur est le chemin.

IGRP calcule la métrique comme suite :

Métrique = [K1 * bande passante + (K2 * bande passante)/(256-charge) + K3*délai] * [K5/(fiabilité + K4)]

Les valeurs par défaut des constantes sont K1 = K3 = 1 et K2 = K4 = K5 = 0.

Métrique = bande passante + délai

Détermination de la dernière mise à jour de routage

Show ip route

```
Gateway of last resort is not set

R   200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14,
Serial0/0
C   192.168.10.0/24 is directly connected, Serial0/0
C   192.168.0.0/24 is directly connected, Loopback0
```

Show ip protocols

```
rt1#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 9
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 1, receive
any version
   Interface    Send Recv Triggered RIP Key-chain
   Serial0/0    1   1 2
   Loopback0    1   1 2
 Routing for Networks:
  192.168.0.0
  192.168.10.0
```

Show ip rip database

```
rt1#show ip rip database
192.168.0.0/24    auto-summary
192.168.0.0/24    directly connected, Loopback0
192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, Serial0/0
200.200.200.0/24    auto-summary
200.200.200.0/24
[1] via 192.168.10.2, 00:00:20, Serial0/0
```

Observation de chemins multiples vers une destination

IGRP supporte l'équilibrage de charge de coût différent qui est mieux connu sous le nom de *variance*.

Variance {n} → Pour demander au routeur d'inclure aussi les routes avec une métrique inférieure à n fois la métrique minimum pour la meilleure route pour cette destination

n est une valeur entre 1 et 128

```
rt1#show ip route
----output omitted----
Gateway of last resort is not set
I   192.168.30.0/24 [100/8986] via 192.168.0.2,
 00:00:22, FastEthernet0/0 [100/10976] via
 192.168.10.2, 00:00:22, Serial0/0

----output omitted----
```

Tests réseau :

Test sur la base des couches OSI

Les erreurs peuvent être identifiées au niveau de la couche 1 :

- Câbles rompus
- Câbles déconnectés
- Câbles raccordés à des ports inappropriés
- Connexions instables
- Câbles inappropriés (câbles console, croisés et droits)
- Problèmes d'émetteur-récepteur
- Problèmes de câblage ETCD
- Problèmes de câblage ETTD
- Unités hors tension

Les erreurs peuvent être identifiées au niveau de la couche 2 :

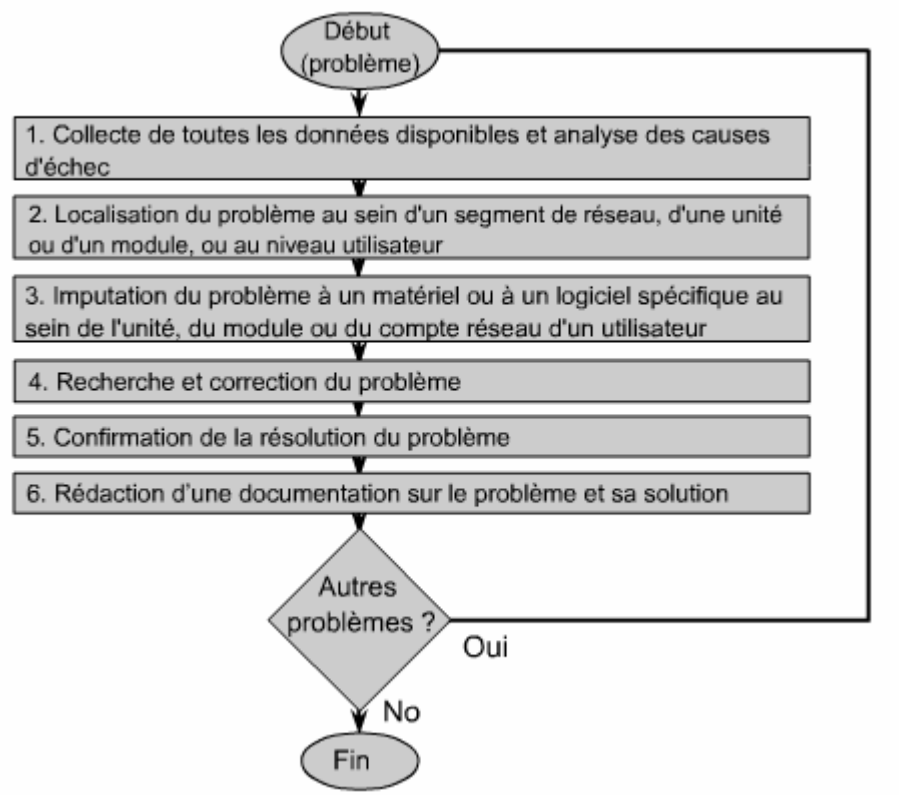
- Interfaces série configurées de façon incorrecte
- Interfaces Ethernet configurées de façon incorrecte
- Ensemble d'encapsulation inapproprié
- Fréquence d'horloge inappropriée pour les interfaces série
- Problèmes de carte réseau (NIC)

Les erreurs peuvent être identifiées au niveau de la couche 3 :

- Protocole de routage non activé
- Protocole de routage incorrect activé
- Adresses IP incorrectes
- Masques de sous-réseau incorrects

Il est préférable de commencer les tests par la couche 1, jusqu'à la couche 7 si nécessaire.

Utilisation d'une approche structurée du dépannage



Dépannage de la couche 1 à l'aide des témoins lumineux

Les témoins lumineux sont des voyants qui signalent l'état d'une interface (indiquer si le trafic est en cours de transmission (TX) ou reçu (RX) + une connexion n'est pas valide)
Solution → Mettez l'unité hors tension et replacez la carte d'interface.

→ Vérifiez que tous les câbles appropriés sont connectés aux ports appropriés.
→ Vérifiez que tous les ports de concentrateur et de commutateur sont associés au réseau VLAN ou au domaine de collision approprié, et que les options de Spanning Tree correspondantes, entre autres, sont définies correctement.
→ Remplacer l'émetteur-récepteur ci nécessaire.
→ Assurez-vous également que l'unité est bien sous tension.

Dépannage de la couche 3 à l'aide de la commande ping

La commande **ping** envoie un paquet à l'hôte de destination et attend un paquet de réponse de celui-ci. Les résultats du protocole d'écho peuvent aider à évaluer la fiabilité chemin-hôte et les délais sur le chemin.

Les informations affichées par la requête **ping** indiquent les temps minimum, moyen et maximum que prend un paquet de requêtes ping pour trouver un système donné et revenir.

```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Ping [protocole] {hôte | adresse} → (mode privilégié et en mode utilisateur)

L'utilisation d'une commande **ping** étendue indique au routeur d'exécuter une gamme plus étendue d'options de test.

Ping → **Entrée** (sans saisir d'adresse IP).

Dépannage de la couche 7 à l'aide de la commande Telnet

Telnet est un protocole de terminal virtuel qui permet de vérifier le logiciel de la couche application entre les stations d'origine et de destination.

Une connexion Telnet réussie indique que l'application de couche supérieure, ainsi que les services des couches inférieures, fonctionnent correctement.

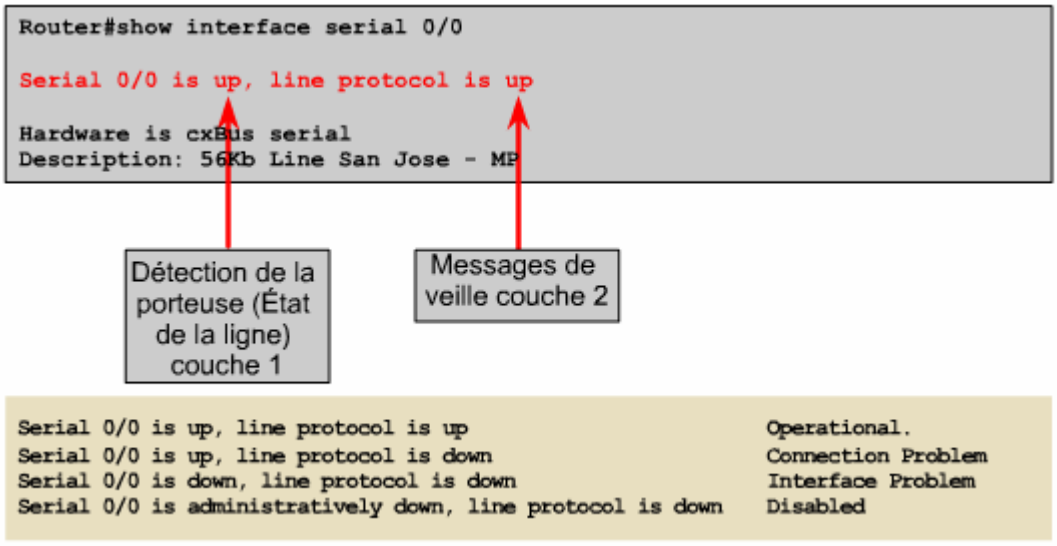
Lors la connexion via Telnet échoue, vérifiez ce qui suit :

- Une recherche DNS inverse sur l'adresse du client peut-elle être trouvée ?
- Telnet ne puisse pas négocier les options appropriées **debug telnet**
- Telnet désactivé ou été déplacé vers un port autre que 23 sur le serveur de destination.

Dépannage des problèmes de routeur

Dépannage de la couche 1 à l'aide de la commande show interfaces :

Show interfaces → Pour vérifier l'état et les statistiques des interfaces.



Un extrait de la commande show interfaces Serial 0/0 :

```
Last clearing of "show interface" counters never
Input queue: 8/75/0 (size/max/drops): Total output
drops: 0
Queing strategy: weighted fair
Output queue: 0/1000/0 (size/max total/drops)
  Conversations 0/2/64 (allocated/max allocated)
5 minute input rate 797000 bits/sec, 85 packets/sec
5 minute output rate 796000 bits/sec, 85 packets/sec
  32363 packets input, 44680841 bytes, 0 no buffer
Received 132 broadcasts, 0 units, 0 giants, 0 threttles,
0 input errors, 0 frame, 0 overrun, 0 ignored, 0 abort
32370 packets output, 44681225 bytes, 0 underruns, 0
output errors, 0 colitions, 95 interface resets, 0
output buffer failures, 0 put buffers swapped out
13 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Indicateurs de la couche 1

Si un nombre croissant d'erreurs d'entrée apparaît dans ces informations, plusieurs facteurs peuvent être à l'origine de ces erreurs. Certains problèmes sont liés à la couche 1:

- Équipement téléphonique défectueux
- Ligne série parasitée
- Câble inapproprié ou longueur de câble incorrecte
- Câble ou connexion endommagé(e)

- Unité CSU/DSU défectueuse
- Matériel de routeur défectueux

Le nombre de réinitialisations d'interface résultent d'un trop grand nombre de messages de test d'activité. Les problèmes de couche 1 suivants peuvent être à l'origine :

- Une ligne incorrecte entraînant des transitions de porteuse
- Un problème matériel au niveau d'une unité CSU/DSU ou d'un commutateur

Remarque : Les statistiques reflètent le fonctionnement du routeur depuis son démarrage ou depuis la dernière remise à zéro des compteurs.

Show version → pour rechercher depuis quand le routeur est en service.

GAD uptime is 6 hours, 21 minutes

Clear counters → pour remettre les compteurs à zéro.

Ces compteurs devraient toujours être effacés après résolution d'un problème d'interface.

Dépannage de la couche 2 à l'aide de la commande show interfaces

Les messages de test d'activité sont des messages envoyés par une unité du réseau à une autre pour lui indiquer que le circuit virtuel existant entre les deux est toujours actif.

Si l'interface manque trois messages de test d'activité consécutifs, le protocole de ligne est considéré comme inactif.

Si l'interface est active et que le protocole de ligne est désactivé, un problème de couche 2 existe. Les causes possibles sont les suivantes:

- Aucun message de test d'activité (keepalives)
- Aucune fréquence d'horloge (clock rate)
- Aucune correspondance au niveau du type d'encapsulation

Dépannage à l'aide de la commande show cdp

Show cdp neighbors detail → afficher des infos sur les unités directement connectées

Si la couche physique fonctionne correctement, toutes les autres unités Cisco directement connectées doivent être affichées. L'absence d'unité connue reflète probablement un problème au niveau de la couche 1.

Remarque : Pour des raisons de sécurité, CDP doit être configuré uniquement sur des liaisons entre des unités Cisco, et désactivé sur les liaisons utilisateur qui ne sont pas gérés localement

```
GAD#show cdp neighbors detail
-------------------------
Device ID: 33 50- srvs
Entry address(es): IP address: 192.168.119.245
Platform: cisco WS-C3550-24, Capabilities: Router Switch IGMP
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 179 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(8) EA1c, RELEASE
   SOFTWARE
(fc1)
Copyright (c) 1986_2002 by cisco Systems, Inc.
Compiled Fri 15-Feb-02 10:50 by antonino
```

Dépannage à l'aide de la commande traceroute

Les informations affichées par la commande **traceroute** indiquent le saut au niveau duquel le problème est survenu (*****)

Traceroute fournit également des informations indiquant les performances relatives des liaisons. Le temps de parcours aller-retour (**RTT**) est le temps nécessaire pour envoyer un paquet et obtenir une réponse.

L'échec d'une réponse n'est pas toujours synonyme de problème, car les messages ICMP ont pu être limités en débit ou filtrés au niveau du site hôte (sur Internet).

Traceroute envoie une séquence de datagrammes UDP à partir du routeur vers une adresse de port non valide sur l'hôte distant. Pour la première séquence de trois datagrammes envoyée, la valeur du champ Durée de vie est définie sur **un**. Avec cette valeur, le datagramme est temporisé au niveau du premier routeur sur le chemin. Ce routeur répond ensuite en envoyant un message ICMP de dépassement du délai indiquant que le datagramme a expiré.

Trois autres messages UDP sont à présent envoyés, avec cette fois une valeur de durée de vie réglée sur **2**. En conséquence, le deuxième routeur renvoie des messages ICMP de dépassement du délai. Ce processus se poursuit jusqu'à ce que les paquets atteignent réellement leur destination ou que le TTL maximum ait été atteint. La valeur maximale par défaut de TTL pour traceroute est 30.

```
Arab#traceroute 192.168.6.1

Type escape sequence to abort.
Trace the route to Eva (192.168.6.1)

1 Boaz (192.168.10.1)        72 msec  72 msec 88 msec
2 Centre (192.168.12.1)      80 msec 128 msec 80
3 Decatur (192.168.75.1)     540 msec 88 msec 84 msec
4 Eva (192.168.6.1)          96 msec     *    96 msec
```

Dépannage des problèmes de routage

Show ip route → pour vérifier que le routeur dispose d'une route pour un réseau.

Show ip protocols → pour rechercher une erreur de configuration du protocole de routage.

La commande **Show ip protocols** permet d'identifier les protocoles configurés, les réseaux annoncés, les interfaces envoyant des mises à jour et les sources des mises à jour.

```
Gadsden#show ip protocols
Routing Protocol is "igrp 12"
   Sending updates every 90 seconds, next due in 49
seconds
   Invalid after 270 seconds, hold down 280, flushed
after 630
    Outgoing update filter list for all interfaces is
not set
    Incoming update filter list for all interfaces is
not set
------output omitted-----
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 15
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Outgoing update filter list for all interfaces is
```

Dépannage à l'aide de la commande show controllers

Show controllers → pour déterminer le type de câble connecté sans avoir à l'inspecter.

Intérêt → Repérer un type de câble incorrect ou un câble défectueux

Exemple :

Show controllers serial o/o → interroge le circuit intégré, ou puce de contrôleur, qui contrôle les interfaces série et affiche des informations sur l'interface physique série 0/0.

→ Le résultat varie d'une puce de contrôleur à une autre.

```
GAD#show controllers serial 0/0

QUICC Serial unit 0
idb at 0x20A31A3A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]= 0x2: 0x00000030, Protocol-specific
[PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x0006
Transmit on Demand [T0DR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
----output omitted----
DTE V.35 serial cable attached.
```

Présentation des commandes debug

Debug → pour afficher des événements et des données dynamiques (en cours).

→ Ces événements peuvent concerner le trafic sur une interface, les messages d'erreur générés par des nœuds sur le réseau, les paquets de diagnostic propres à un protocole et d'autres données utiles pour le dépannage.

Remarque : Le résultat de la commande **debug** peut nuire aux performances, car il crée des surcharges sur le processeur susceptibles d'interrompre le fonctionnement normal du routeur.

Debug all → activer tous les événements debug (utilisée avec modération).
No debug all ou **Undebug all** → désactiver tous les événements debug.

Terminal monitor → afficher les événements debug au sein de la session telnet.

Timestamps → permet de placer un horodatage sur un message de déboguage (l'heure de l'événement de déboguage et le temps écoulé entre plusieurs événements).

Router(config)#**service timestamps debug uptime**

Show version → pour déterminer l'intervalle de temps écoulé depuis la dernière occurrence de l'événement de déboguage.

Show debugging → afficher les événements debug activés.

```
GAD#debug ip eigrp
IP-EIGRP Route Events debugging is on
GAD#show debug
IP route IP_EIGRP Route debugging is on
```

Router#clock set 15:46:00 3 May 2004 → exemple pour régler la date et l'heure

→ Activer l'affichage de l'heure et la date d'arrivée d'un événement.

Router(config)#service timestamps debug datetime localtime

→ Régler l'horloge du routeur après chaque rechargement ou panne d'alimentation électrique

Router(config)#service timestamps debug uptime

Exemple :

```
GAD#debug ip rip events
RIP event debugging is on
GAD#
00:24:16: RIP: sending v1 update to 255.255.255.255 via
Ethernet0/0 (1.0.0.1)
00:24:16:RIP: Update contains 3 routes
00:24:16:RIP: Update queued
00:24:16:RIP: Update sent via Ethernet0/0
00:24:16:RIP: sending v1 update to 255.255.255.255 via
Serial0/0 (2.0.0.1)
00:24:16:RIP: Update contains 1 routes
00:24:16:RIP: Update queued
00:24:16:RIP: Update sent via Serial0/0
00:24:16:RIP: received v1 update from 2.0.0.2 on
Serial0/0
00:24:16:RIP: Update contains 2 routes
GAD#undebug all
```

Module 10

TCP/IP (niveau intermédiaire)

Fonctionnement du protocole TCP

La couche transport assure avec fiabilité le transport et la régulation du flux de données depuis la source jusqu'à la destination. Pour cela, des fenêtres glissantes et des numéros de séquence sont utilisés, parallèlement à un processus de synchronisation qui garantit que chaque hôte est prêt à communiquer

Synchronisation ou échange en trois étapes

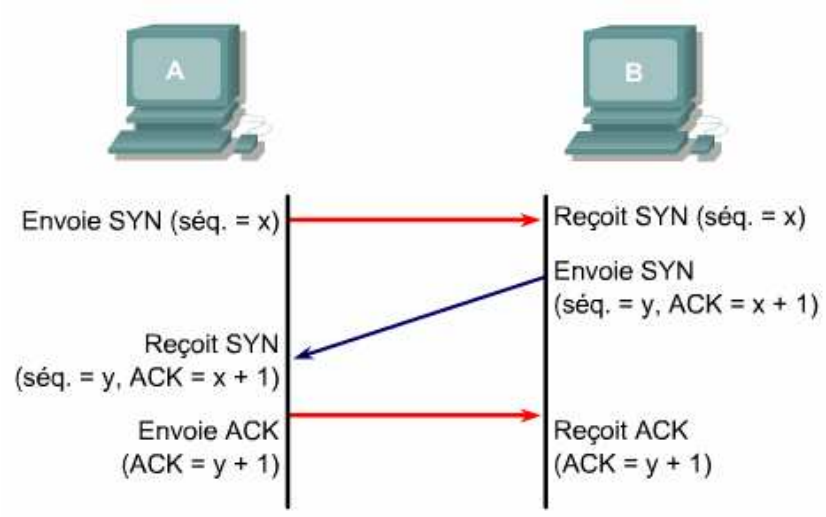
Le protocole TCP est orienté connexion. Avant de transmettre des données, les deux hôtes exécutent un processus de synchronisation pour établir une connexion virtuelle pour chaque session entre les hôtes.

→ Pour établir une session TCP, l'hôte client va utiliser le numéro de port bien connu du service qu'il désire contacter et qui est fourni par l'hôte serveur.

Pour établir une connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (**ISN** – Initial Sequence Number).

La séquence de la synchronisation :

1. L'hôte émetteur (A) initie une connexion *en envoyant un paquet SYN* à l'hôte récepteur (B) indiquant que son numéro de séquence initial ISN = X.
2. B reçoit le paquet, enregistre que la séquence de A = X, répond par un accusé de réception de X + 1 et indique que son numéro de séquence ISN = Y. L'accusé X + 1 signifie que l'hôte B a reçu tous les octets jusqu'à X inclus et qu'il attend l'arrivée de X + 1.
3. L'hôte A reçoit le paquet de B, apprend que la séquence de B est Y et répond par un accusé de Y + 1, qui met fin au processus de connexion:



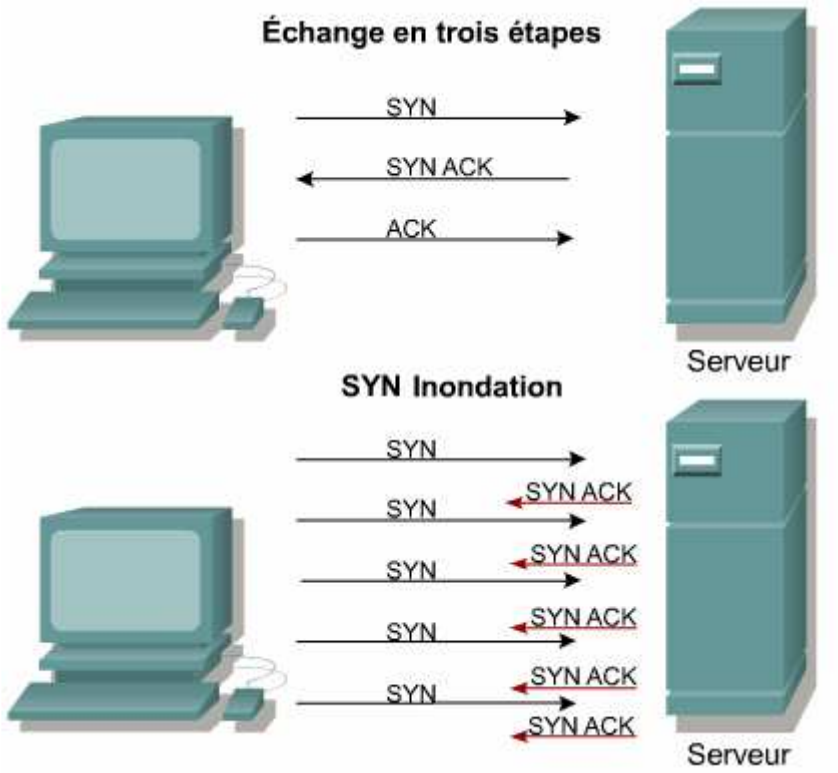
Structure d'un segment TCP

0	4	10	16	24	31
Port source			Port de destination		
Numéro de séquence					
Numéro d'accusé de réception					
HLEN	Réservé	Bits de code	Fenêtre		
Somme de contrôle			Pointeur d'urgence		
Options (le cas échéant)				Remplissage	
Données					
...					

Attaques par déni de service

Les attaques par déni de service sont destinées à refuser des services à des hôtes légitimes qui tentent d'établir des connexions.

L'inondation SYN est un type d'attaque par déni de service → Elle exploite le processus normal d'échange en trois étapes et oblige les unités cible à envoyer un accusé de réception à des adresses source, qui ne complètent pas l'échange en trois étapes.



Le pirate lance une synchronisation mais « usurpe » l'adresse IP source. On parle de « ***spoofing*** » lorsque l'unité réceptrice répond à une adresse IP inexistante et inaccessible, puis est placée dans un état d'attente (mémoire) jusqu'à recevoir l'accusé de réception final de l'unité émettrice → consommer des ressources système.

Pour se protéger : diminuer le délai d'attente de connexion + augmenter la taille de la file d'attente de connexion + utiliser un logiciel spécial.

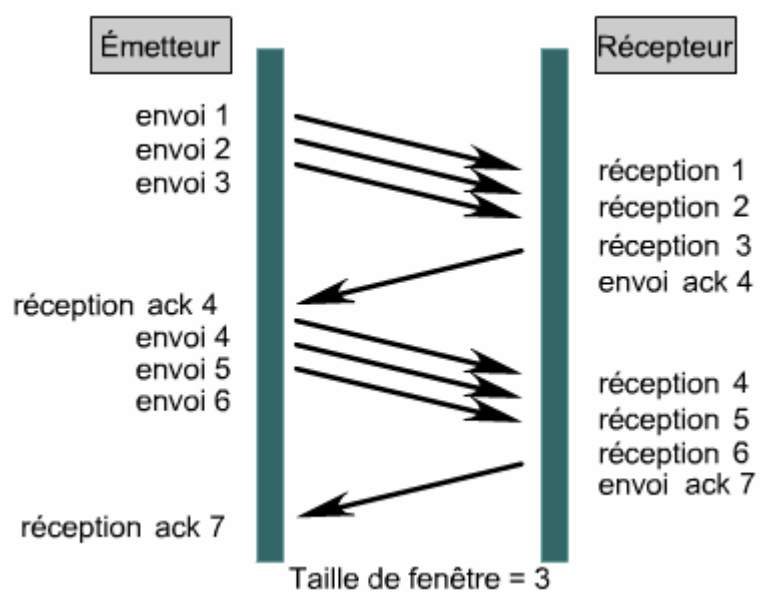
Fenêtrage et taille de fenêtre

Les données doivent être divisées en segments plus petits pour permettre une meilleure transmission. TCP est responsable de la répartition de ces données en segments.

La taille de fenêtre définie la quantité de données qui peut être transmise à la fois avant que la destination ne réponde par un accusé de réception.

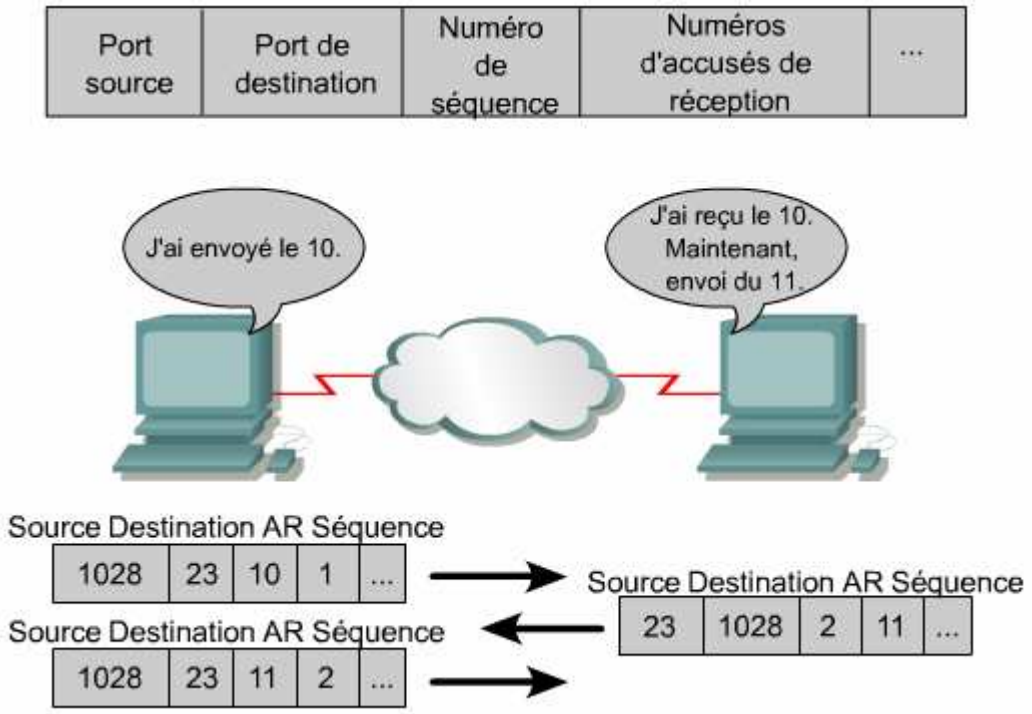
TCP utilise le fenêtrage pour ajuster de façon dynamique la taille des transmissions. Les équipements négocient une taille de fenêtre.

Remarque : La taille de la fenêtre peut être modulée en fonction des accusés de réception.



Numéros de séquence

TCP applique des numéros de séquence aux segments de données transmis, de sorte que le récepteur soit capable d'assembler correctement les octets dans leur ordre d'origine.
+ Le récepteur s'assure qu'il a reçu la totalité des données.



Accusés de réception positifs

Dans un segment TCP, le champ du numéro de séquence est suivi du champ du numéro d'accusé de réception (lieu où s'effectue le suivi des octets transmis et reçus).

TCP utilise une technique de retransmission et d'accusé de réception pour contrôler le flux de données et confirmer l'arrivée des données.

Selon la technique PAR (Processus Accusé de Réception), la source envoie un paquet, démarre un compteur et attend un accusé de réception avant d'envoyer le paquet suivant, dans la même session.

→ Si le compteur arrive à expiration avant que la source n'ait reçu un accusé de réception, celle-ci retransmet le paquet (avec un débit plus lent) et redémarre le compteur.

Remarque : Le protocole TCP utilise des accusés de réception prévisionnels dans lesquels le numéro de l'accusé de réception indique le prochain octet attendu dans la session TCP.

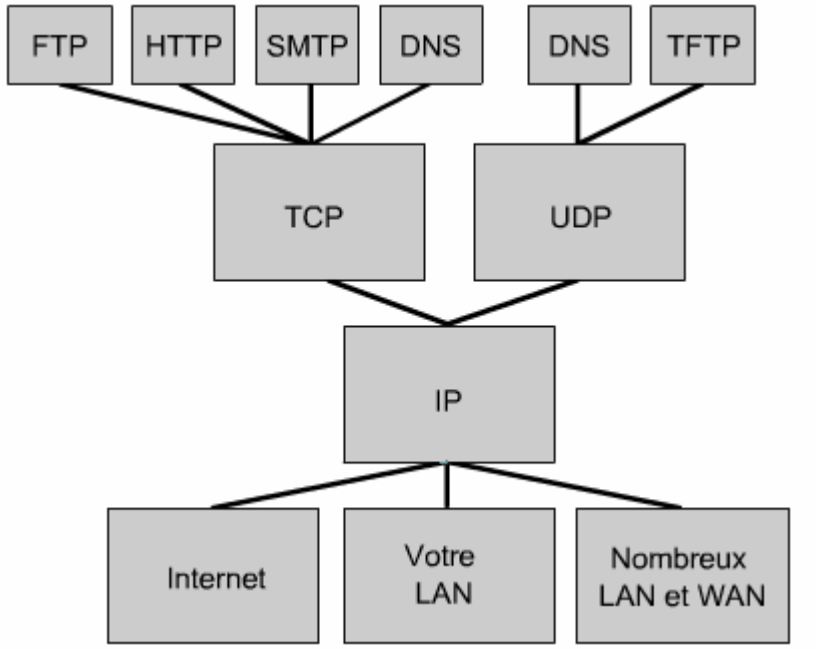
Exemple : l'unité de destination ne reçoit pas les trois octets (un dépassement de capacité des tampons), elle n'envoie pas d'accusé de réception → l'unité source sait que les octets doivent être transmis de nouveau, à un débit plus lent.

→ Réduction de la vitesse de transmission entre les hôtes + Fiabilité de la communication.

Fonctionnement du protocole UDP

Le protocole ***UDP*** permet une transmission de paquets non orientée connexion et sans garantie de remise conforme au niveau de la couche 4 du modèle OSI.

Le protocole UDP n'utilise ni fenêtrage, ni accusé de réception. Par conséquent, les protocoles de couche application doivent assurer la détection des erreurs.



Structure d'un segment UDP

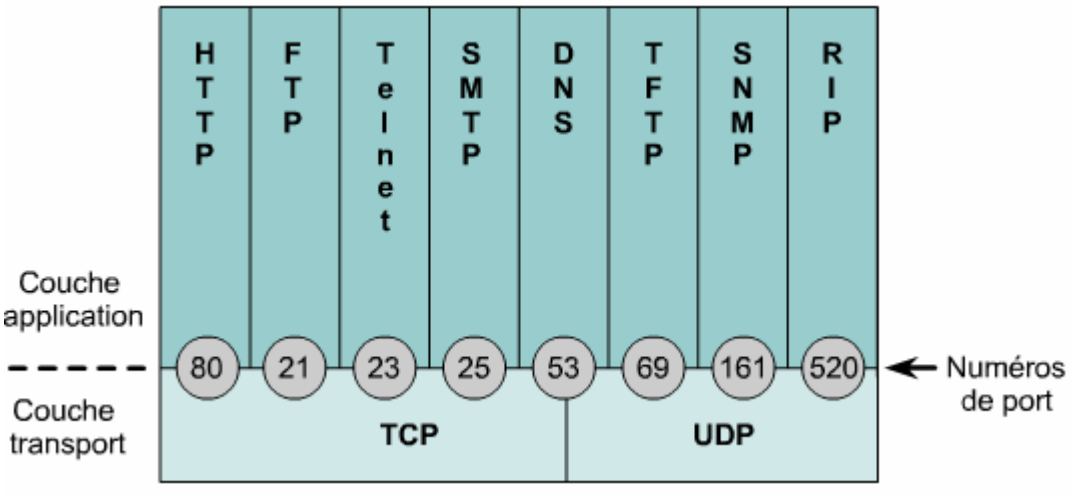
Nombre de bits	16	16	16	16	16
	Port source	Port de destination	Longueur	Somme de contrôle	Données...

→ Port source : facultatif
→ Port de destination détermine l'application à laquelle un segment UDP est destiné.
→ Longueur : identifie le nombre d'octets dans le segment UDP
→ Somme de contrôle : facultatif mais peut être utilisé pour garantir que les données n'ont pas été endommagées pendant la transmission.

Ports de la couche transport

Conversations multiples entre hôtes

Un ***numéro de port*** doit être associé à la conversation entre les hôtes pour garantir que le paquet atteint le service approprié sur le serveur (un serveur qui joue plusieurs rôles par exemple).



Les plages attribuées aux numéros de port sont les suivantes:

- Les 1023 premiers ports sont des ports bien connus (définis par l'IANA)
- Les ports enregistrés sont compris entre 1024 et 49151.
- Les ports compris entre 49152 et 65535 sont des ports dits dynamiques ou privés.

Ports de services

Un numéro de port doit être associé aux services exécutés sur les hôtes pour que la communication soit possible.

Exemple : ***FTP*** transmet des connexions TCP via les ***ports 20*** et ***21***.

Ports de clients

Les ports source définis par le client sont déterminés de manière dynamique.

En règle générale, un client détermine le port source en affectant de manière aléatoire un numéro supérieur à 1023.

Exemple : un client qui tente de communiquer avec un serveur Web

Source → Il utilise TCP et règle le port de destination sur 80 et le port source sur 1045.
Destination → le paquet est transmis à la couche transport, puis au service HTTP (80) + répond à la requête par un segment (port 80 comme source et port 1045 comme destination).

Exemple de sessions multiples entre des hôtes

Un hôte peut établir une connexion telnet sur le port 23 tout en surfant sur Internet via le port 80.

→ Les adresses IP et MAC sont identiques car les paquets proviennent du même hôte.
→ Chaque conversation côté source a besoin de son propre numéro de port.

Comparaison des adresses MAC, des adresses IP et des numéros de port

Les *numéros de port* sont situés au niveau de la *couche transport* et sont desservis par la couche réseau. La couche réseau affecte l'adresse logique (adresse IP) et est ensuite desservie par la couche liaison de données qui affecte l'adresse physique (adresse MAC).

Numéro de port, adresse IP, adresse MAC, numéro de port

Analogie : Le processus s'apparente à l'envoi d'une lettre normale.

Sur une lettre, l'adresse est composée d'un **nom**, de la **rue** et de la **ville**. Ces éléments sont comparables au **numéro de port**, à **l'adresse MAC** et à **l'adresse IP** utilisés pour les données de réseau.

Module 11

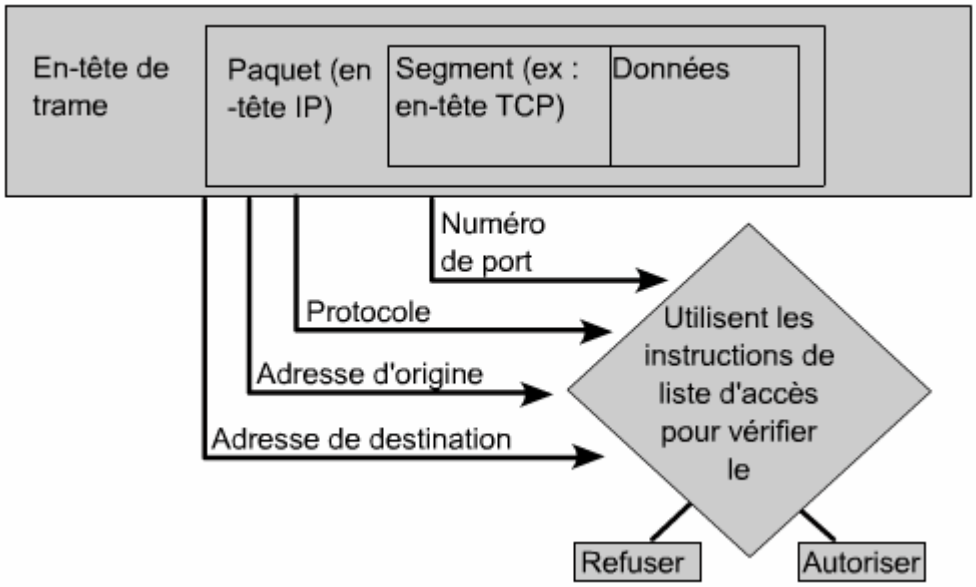
Listes de contrôle d'accès (ACL)

Notions de base sur les ACL :

Définition des listes de contrôle d'accès

Les ***listes de contrôle d'accès*** sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter.

Certaines conditions dans une ACL sont des adresses source et de destination, des protocoles et des numéros de port de couche supérieure.



→ Gérer le trafic + sécuriser l'accès d'un réseau en entrée comme en sortie.

→ Des ACL peuvent être créées pour tous les protocoles routés, tels qu'IP et IPX.
→ Une ACL séparée doit être créée pour chaque direction : une pour le trafic entrant et une pour le trafic sortant.

Exemple : Si le routeur a deux interfaces configurées pour IP, AppleTalk et IPX, 12 listes d'accès distinctes sont nécessaires : une liste pour chaque protocole, fois deux pour la direction (entrée et sortie), fois deux pour le nombre d'interfaces.

Les principales raisons pour créer des listes de contrôle d'accès :

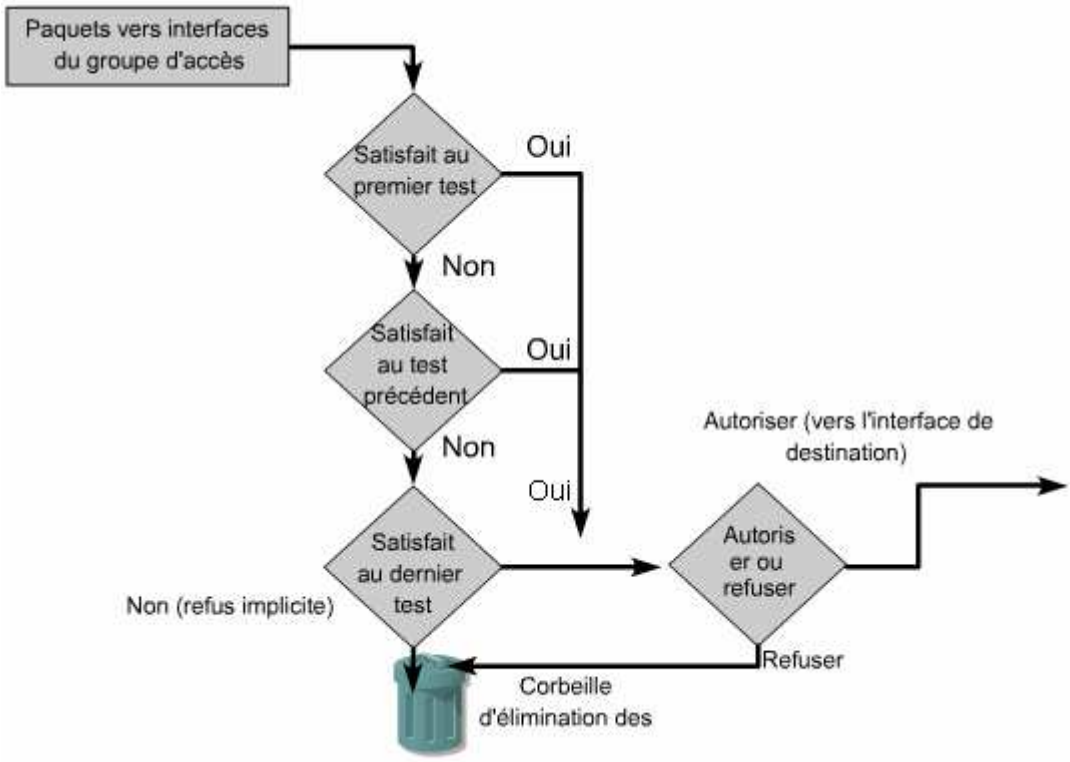
- Limiter le trafic réseau et accroître les performances (limitant le trafic vidéo)
- Contrôler le flux de trafic. (limiter l'arrivée des mises à jour de routage)
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section.

- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur. (autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet).
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

Fonctionnement des listes de contrôle d'accès

L'ordre des instructions ACL est important. Cisco IOS teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin.

Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées.



Remarque : Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est rejeté. Ceci est le résultat de l'instruction implicite deny any à la fin de chaque ACL.

Processus de routage dans un routeur

→ Vérifier la correspondance (@ MAC)
→ Rechercher une ACL sur l'interface d'entrée → Vérifier → accepter ou rejeter le paquet
→ Déterminer l'interface de destination (table de routage)
→ Si le paquet est accepté → router le paquet vers l'interface de partance.
→ Vérifier l'ACL sur l'interface de destination → accepter ou rejeter le paquet
→ Vérifier l'autorisation du paquet.
→ Encapsuler le paquet (en trame) et l'Envoi à l'unité suivante.

Création de listes de contrôle d'accès

Il existe différents types de listes de contrôle d'accès : standard, étendues, IPX et AppleTalk.
Sur un routeur, vous devez identifier chaque liste en lui attribuant un numéro unique.

Protocole	Plage
IP standard	1-99, 1300-1999
IP étendu	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX étendu	900-999
Protocole IPX Service Advertising	1000-1099

Access-list → Pour créer et paramétrer les conditions d'une ACL.
Access-group → Pour assigner une ACL à l'interface qui convient

Router(config)#**access-list {n° ACL} {permit | deny} {conditions}**

{n° ACL} → indique le type d'ACL
{permit | deny} → accepter ou refuser
{conditions} → liste des conditions de test

Router(config-if)#**{protocole}access-group {n° ACL} {in | out}**

{in | out} → indique s'il s'agit d'un trafic entrant ou sortant d'un routeur

Remarque : Une liste de contrôle d'accès contenant des instructions numérotées ne peut pas être modifiée. Elle doit être supprimée à l'aide des instructions de l'ACL en utilisant la commande **no access-list {n° ACL}** pour être ensuite recréée.

Exemple :

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Règles doivent être respectées lors de la création et de l'application des listes d'accès :

- Une liste d'accès par direction et par protocole.
- Les listes d'accès standard doivent être appliquées le plus près possible de la destination.
- Les listes d'accès étendues doivent être appliquées le plus près possible de la source.

- Pour faire référence à une interface d'entrée ou de sortie, placez-vous à l'intérieur du routeur en regardant l'interface en question.
- Les instructions sont traitées dans l'ordre depuis le début de la liste jusqu'à la fin jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est détectée, le paquet est refusé.
- Il existe un refus implicite **deny any** à la fin de toutes les listes de contrôle d'accès.
- Les hôtes spécifiques doivent être rejetés en premier, tandis que les groupes ou les filtres généraux viennent en dernier.
- La condition de correspondance est examinée en premier. L'acceptation ou le refus est examiné UNIQUEMENT si la condition est vraie.
- Ne travaillez jamais avec une liste d'accès qui est appliquée de manière active.
- Utilisez un éditeur de texte pour créer des commentaires indiquant la logique, puis ajoutez les instructions correspondantes.
- Il n'est pas possible d'ajouter et de supprimer des lignes spécifiques dans des listes d'accès numérotées.
- Une liste d'accès IP envoie un message ICMP d'hôte inaccessible à l'émetteur du paquet rejeté et élimine le paquet dans la corbeille prévue à cet effet.
- Soyez particulièrement attentif lorsque vous supprimez une liste d'accès (une instruction **deny any** peut être appliquée par défaut à l'interface et tout le trafic peut être arrêté).
- Les filtres de sortie ne concernent pas le trafic généré par le routeur local.

Rôle du masque générique

Un masque générique est une quantité de 32 bits divisés en quatre octets.

Les masques génériques utilisent les uns et les zéros binaires pour filtrer des adresses IP individuelles ou de groupes pour autoriser ou refuser un accès à des ressources à l'aide d'une adresse IP précise. Le (0) implique que la valeur soit comparée (correspondance parfaite exigée), tandis que le (1) implique de bloquer la comparaison (correspondance exacte non exigée).

Deux mots-clés spéciaux sont utilisés dans les listes de contrôle d'accès : **any** et **host**.

Any remplace 0.0.0.0 dans l'adresse IP et 255.255.255.255 dans le masque générique. Cette option établit une correspondance avec toute adresse avec laquelle elle est comparée.
Host remplace le masque 0.0.0.0. Ce masque nécessite une correspondance parfaite entre tous les bits de l'adresse ACL et ceux de l'adresse du paquet. Avec cette option, une seule adresse concorde.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Peut être écrit comme suit :

```
Router(config)#access-list 1 permit any
```

```
Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0
```

Peut être écrit comme suit :

Remarque : Le masque de sous-réseaux et le masque générique représentent deux choses différentes même s'ils sont tous les deux appliqués à des adresses IP

Exemple de calcul des masques génériques et prise des décisions :

L'ACL configurée → *Access-list 1 permit 172.16.0.0 0.0.255.255*
→ Supposons qu'un paquet entrant de la source 172.17.1.1

@ IP (172.16.0.0) : 10101100.00010000.00000000.00000000
Masque générique (0.0.255.255) : 00000000.00000000.xxxxxxxx.xxxxxxxx
Valeur de correspondance 1 : 10101100.00010000.xxxxxxxx.xxxxxxxx

@ IP (172.17.1.1) : 10101100.00010001.00000001.00000001
Masque générique (0.0.255.255) : 00000000.00000000.xxxxxxxx.xxxxxxxx
Valeur de correspondance 2 : 10101100.00010001.xxxxxxxx.xxxxxxxx

➔ Pas de correspondance → paquet refusé.

Vérification des listes de contrôle d'accès

Show ip interface → affiche les informations relatives à l'interface IP et indique si des listes de contrôle d'accès sont configurées.

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
```

Show access-lists → affiche le contenu de toutes les listes de contrôle d'accès sur le routeur.

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
```

Show running-config → permet également d'afficher les listes d'accès d'un routeur, ainsi que les informations d'affectation aux interfaces.

```
!
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny   172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq telnet
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq ftp
!
line con 0
 transport input none
```

Listes de contrôle d'accès (ACL)

Listes de contrôle d'accès standard

Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés.

- Les plages de numéros de liste d'accès 1 - 99 et 1300 - 1999
- Filtrage uniquement sur l'adresse IP d'origine
- Masques génériques
- Application à l'interface la plus proche de la destination

→ La plage additionnelle (1300 à 1999) « ACL IP expansées » utilisée afin de procurer un maximum de 798 nouvelles ACL standards (version 12.0)

Syntaxe complète de la commande ACL standard :

```
Router(config)#access-list {n° ACL} {deny | permit | remark} {source} {masque générique} [log]
```

{n° ACL} → indique le numéro d'ACL (entre les plages « 1 et 99 » et « 1300 et 1999 »)
{permit | deny} → accepter ou refuser
remark → ajouter un commentaire pour la compréhension (facultatif)
{conditions} → liste des conditions de test
{source} → adresse réseau ou l'hôte d'où provient le paquet.
{masque générique} → pour indiquer les bits à comparer (facultatif)
[log]→ Provoque un message de journalisation informatif au sujet du paquet correspondant à l'ACL à envoyer au port console.

Exemples :

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

Remarque : Notez que la première instruction ACL ne contient aucun masque générique. Dans le cas où aucune liste n'apparaît, le masque par défaut (0.0.0.0) est utilisé.

Listes de contrôle d'accès étendues

→ Elles fournissent une plus grande gamme de contrôle.
→ Elles vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port.

Exemple : Une liste de contrôle d'accès étendue peut autoriser le trafic de messagerie issu de l'interface Fa0/0 vers des destinations S0/0 données tout en refusant des transferts de fichiers et des navigations sur le Web.

- Les plages de numéros de liste d'accès 100-199 et 2000 - 2699
- Adresse IP de destination source
- Numéro de protocole de couche 4
- Application au port le plus proche de l'hôte source

→ Pour une même liste de contrôle d'accès, plusieurs instructions peuvent être configurées. (Vous pouvez définir autant d'instructions que vous le souhaitez, la seule limite étant la mémoire disponible sur le routeur).

Syntaxe complète de la commande ACL étendue :

```
access-list access-list-number [dynamic dynamic-name [timeout
minutes]] {deny | permit | remark} protocol source source-
wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log | log-input] [time-range time-
range-name] icmp-type icmp-code icmp-message igmp-type
[operator operand] [port port number or name] [established]
[fragments]
```

Opérateurs : eq = égale gt = supérieur lt = inférieur neq = non égale

Exemples :

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

Listes de contrôle d'accès nommées

Les listes de contrôle d'accès nommées IP ont été introduites (version 11.2), afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

Avantages :

- Identifier de manière intuitive une liste d'accès à l'aide d'un nom alphanumérique.
- L'IOS ne limite pas le nombre d'ACL nommées qui peuvent être configurées.
- Les ACL nommées permettent de modifier des listes de contrôle d'accès sans avoir à les supprimer, puis à les reconfigurer.

Remarque : Un même nom ne peut pas être utilisé pour plusieurs listes de contrôle d'accès.

Syntaxe de la création :

Ip access-list **{extended | standard} {nom de l'ACL}**

```
router(config-ext-nacl)#permit|deny protocol source
source-wildcard [operator [port]] destination
destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log] [time-range time-
range-name]
```

Exemple :

```
Rt1(config-ext-nacl)#remark (Liste d'accès pour permettre l'accès au
courriel et au serveur DNS.)
Rt1(config-ext-nacl)#permit tcp any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit udp any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#exit

Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

Emplacement des listes de contrôle d'accès

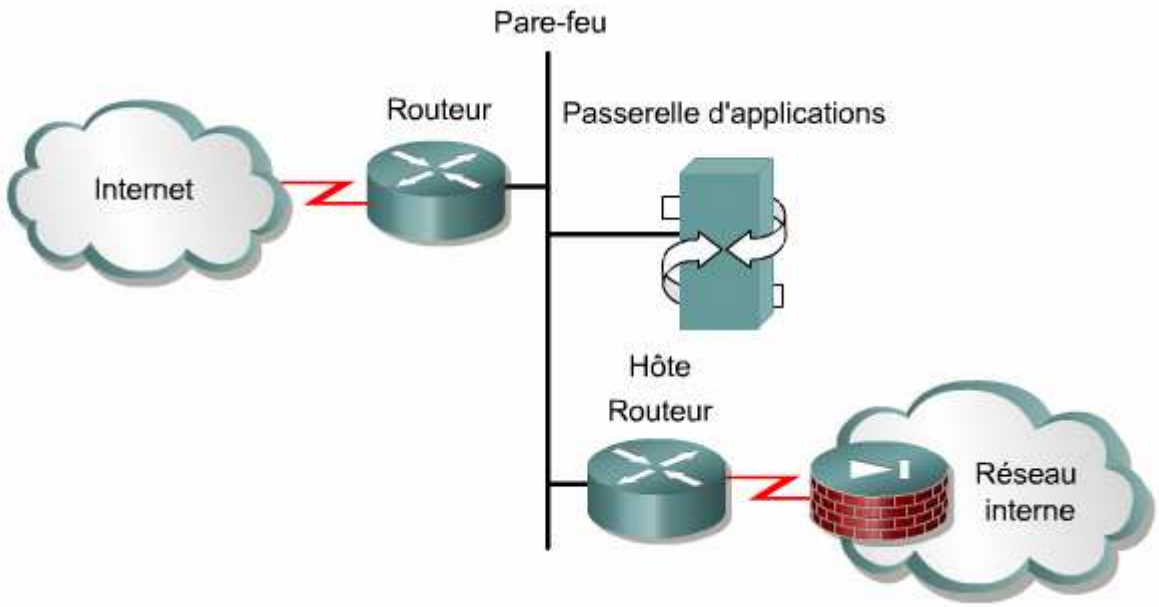
Si le trafic est filtré, la liste de contrôle d'accès doit être placée à l'endroit où elle aura le plus grand impact sur les performances.

La règle générale est de placer les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé.

Pare-feu

Un ***pare-feu*** est une structure située entre l'utilisateur et le monde extérieur afin de protéger le réseau interne des intrus.

Exemple :



Dans l'architecture présentée, le routeur connecté au réseau Internet, appelé routeur externe, oblige tout le trafic entrant à passer par la passerelle d'application. Le routeur connecté au réseau interne, appelé routeur hôte, accepte uniquement les paquets de la passerelle d'application. En fait, la passerelle gère la livraison des services réseau vers le réseau interne et à partir de celui-ci.

→ Les listes de contrôle d'accès doivent être utilisées dans les routeurs pare-feu, lesquels sont souvent placés entre le réseau interne et un réseau externe
→ Les listes de contrôle d'accès sont utilisées sur un routeur situé entre deux sections du réseau pour contrôler le trafic entrant ou sortant d'une section particulière du réseau interne.

Restriction de l'accès au terminal virtuel

Par défaut, une liste d'accès étendue pour le trafic Telnet sortant n'empêche pas le routeur de lancer des sessions Telnet.

L'objectif de l'accès limité au terminal virtuel est d'augmenter la sécurité du réseau.

Exemple : Processus de création de la liste de contrôle d'accès au terminal virtuel :

```
Creating the standard list:

Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Rt1(config)#access-list 2 permit 172.16.2.0 0.0.0.255
Rt1(config)#access-list 2 deny any

Applying the access list:

Rt1(config)#line vty 0 4
Rt1(config-line)#login
Rt1(config-line)#password secret
Rt1(config-line)#access-class 2 in
```

Vous devez prendre en compte les éléments suivants lors de la configuration :

- Lors du contrôle de l'accès à une interface, un nom ou un numéro peut être utilisé.
- Seules les listes d'accès numérotées peuvent être appliquées à des lignes virtuelles.
- Définissez des restrictions identiques sur toutes les lignes de terminal virtuel.

Module 11+

les ACL (cours supplément)

Création des ACL - Généralités

Pour créer une liste de contrôle d'accès, il faut :

→ Créer la liste de contrôle d'accès (**access-list**).
→ Assigner cette ACL à une interface (**access-group**)

Structure générale d'une ACL :

Router(config)#**access-list** ***n° ACL*** {permit|deny} *instructions*

Router(config-if)#protocole **access-group** ***n° ACL*** *{in|out}*

Les différents types d'ACL

Il existe 3 types de liste de contrôle d'accès :

Les ACLs standards utilisent des spécifications d'adresses simplifiées (origine seulement)
Les ACLs étendues utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis.
Les ACLs nommées peuvent être soit standards, soit étendues (faciliter la compréhension)

Une seule liste de contrôle d'accès est permise par port, par protocole et par direction, c'est-à-dire qu'on ne peut pas par exemple définir deux ACLs sur l'interface E0 pour le trafic IP sortant. Par contre, on peut définir deux ACLs pour le trafic IP mais, une pour le trafic entrant et l'autre pour le trafic sortant…

Numéro des ACLs

Au moment de configurer les listes de contrôle d'accès il faut identifier chaque liste de protocole en lui attribuant un numéro unique.

Plage	Protocole
1-99	IP standard
100-199	IP étendue
600-699	AppleTalk
800-899	IPX standard
900-999	IPX étendue
1000-1099	IPX Service Advertising Protocol

Par exemple, si l'on affecte le numéro 30 à une ACL, cela induit le fait que cette ACL sera de type standard et concernera le trafic IP.

Le masque générique

Un masque générique est jumelé à une adresse IP. Les chiffres 1 et 0 sont utilisés pour indiquer la façon de traiter les bits de l'adresse IP correspondante.

0 pour vérifier et 1 pour ne pas vérifier

Exemple :

→ On veut vérifier (autoriser ou refuser) les sous réseaux 172.30.16.0 à 172.30.31.0

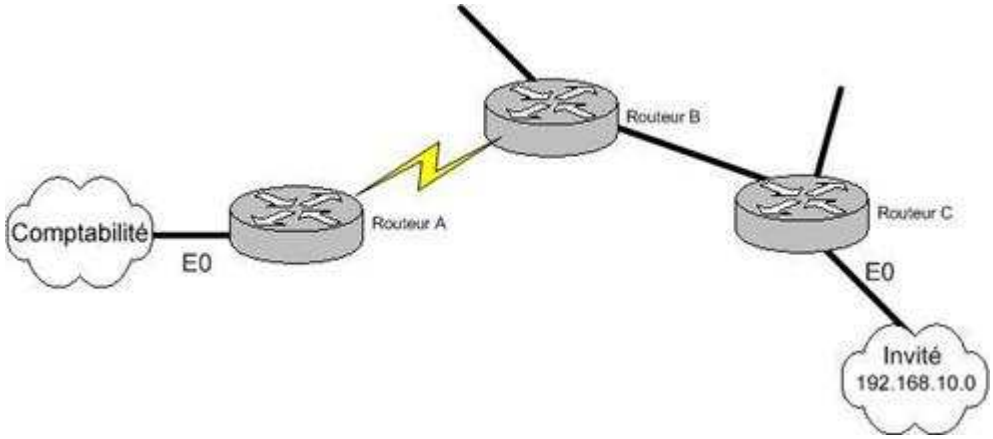
Les deux premiers octets de l'adresse IP sont identiques
16 en notation binaire: 0001 0000
31 en notation binaire: 0001 1111
Les bits commencent à être différents à partir du 4ème bit de ce 3ème octet.
A partir de là on met tous les bits à 1

→ Le masque générique est alors **0.0.15.255**

Création d'une ACL standard

Router(config)#**access-list** n°_ACL {deny | permit} **adresse d'origine** masque générique

Exemple :



On veut interdire au réseau « Invité » d'accéder au réseau « Comptabilité ».

```
Routeur_A(config)#access-list 1 deny 192.168.10.0 0.0.0.255
Routeur_A(config)#access-list 1 permit any
Routeur_A(config)#
```

02:18:17 connecté | Détec. auto | 9600 8-N-1 | DÉFIL | Maj | Num | Capturer | Écho

→ Le numéro de l'ACL est 1 : il s'agit donc d'une ACL ip standard
→ L'adresse d'origine est 192.168.0 et le masque est 0.0.0.255
On note que les trois premiers octets du masque ne sont constitués que de 0 et que le dernier octet n'est constitué que de 1. On vérifie donc exactement les trois premiers octets de l'adresse d'origine, mais on ne s'occupe pas du dernier octet.
→ On a donc bien interdit (deny) tous les postes du réseau 192.168.0.0
→ La deuxième ligne indique d'autoriser (permit) tout le reste (any)

Car n'oublions pas qu'il y a toujours une commande implicite « deny any » à la fin des ACLs.
La deuxième étape est d'affecter cette ACL à une interface du routeur.

```
Routeur_A(config)#int e0
Routeur_A(config-if)#ip access
Routeur_A(config-if)#ip access-group 1 out
Routeur_A(config-if)#
```

01:46:46 connecté | Détec. auto | 9600 8-N-1 | DÉFIL | Maj | Num

→ On s'aperçoit que le routeur qui a été choisi est Routeur_A.
En effet avec les ACLs standards, comme on ne peut définir que l'adresse d'origine, on place ces ACLs au plus près de la destination.
Si on avait mis cette ACL sur le routeur B on aurait interdit l'accès à partir de ce routeur, alors qu'on ne veut interdire que l'accès au réseau « Comptabilité ».
→ L'ACL est définie en « out » : on interdit donc le trafic (requête) provenant du réseau « Invité » à **sortir** sur l'interface du réseau « Comptabilité ».

Si on ne définit ni «in» ni «out», la valeur «out» est prise par défaut.

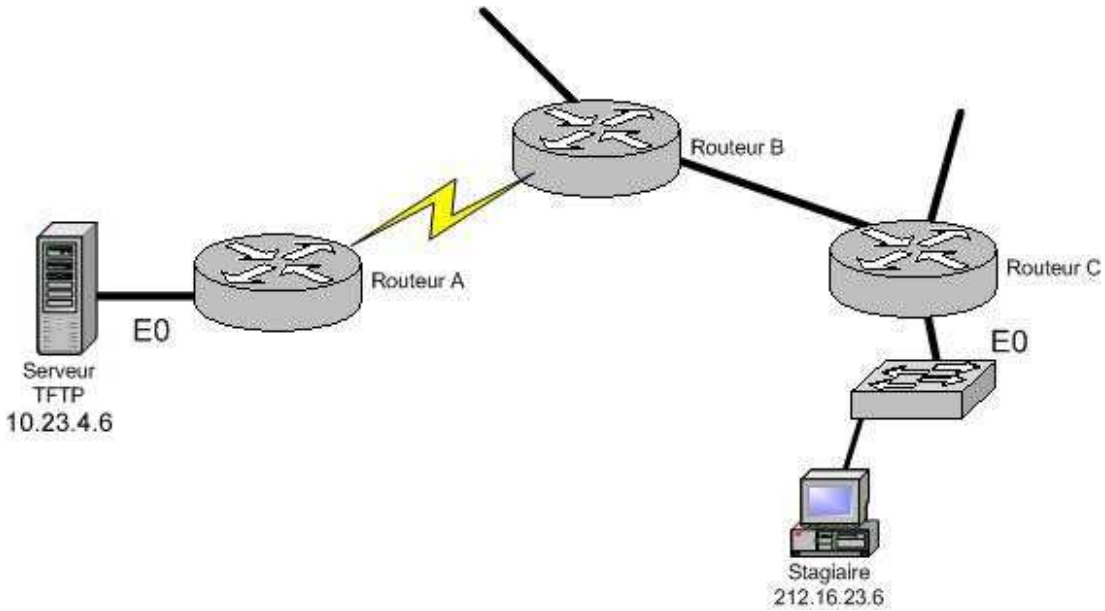
Création d'une ACL étendue

Router(config)# **access-list** *n° ACL* {**permit** | **deny**} *protocol* **adresse d'origine** *masque générique* **adresse destination** *masque générique operateur operande*

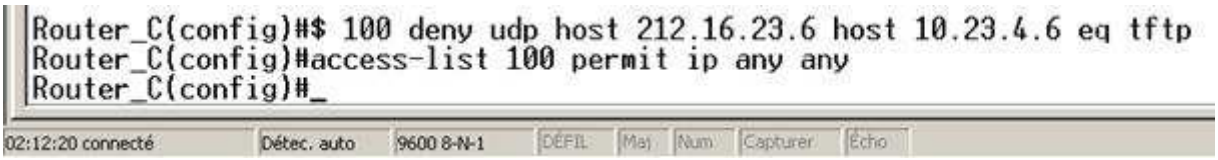
Operateur operande : *lt*, *gt*, *eq* ou *neq* suivi d'un numéro de port

Lt pour lower than (plus petit que)
Gt pour greater than (plus grand que)
Eq pour equal (égal à)
Neq pour non equal (différent de)

Exemple :

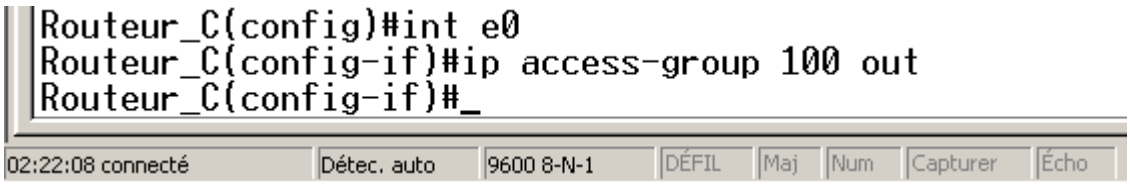


On veut refuser au stagiaire d'accéder au serveur TFTP.



→ On remarque que le mot host a été tapé avant les adresses IP.
Ce mot permet d'éviter de devoir taper le masque générique 0.0.0.0 après l'adresse IP.
→ eq tftp indique qu'il faut interdire le trafic tftp uniquement.
→ Le protocole indiqué est UDP : UDP est le protocole qui supporte le service TFTP.
→ La deuxième ligne indique qu'il faut autoriser tout le reste du trafic (IP) pour n'importe quelle source (any) vers n'importe quelle destination (le deuxième any).

Assignons désormais cette ACL :



→ On remarque que l'ACL a été placée sur le routeur C, au plus proche de la source.
Les ACLs étendues nous permettent de spécifier l'adresse de destination, il est donc possible de bloquer au plus vite les paquets non désirés, et d'éviter qu'ils atteignent le routeur A, et donc de polluer la bande passante pour des paquets qui seront refusés.

Les ACL nommées.

Router(config)#**access-list** {standard | extended} ***nom_ACL***

Router_C(config-ext-nacl)# *instructions*

Vous ne pouvez pas utiliser le même nom dans le cas de listes de contrôle d'accès multiples.

Reprenons l'exemple précédent, on peut nommer cette ACL « stagiaire » :

Router_C(config)# access-list extended Stagiaire
Router_C(config-ext-nacl)#deny udp host 212.16.23.6 host 10.23.4.6 eq tftp
Router_C(config-ext-nacl)#permit ip any any

Router_C(config-if)# ip access-group Stagiaire out

Vérifier les ACLs configurées :

Show access-lists → pour afficher le contenu de toutes les listes de contrôle d'accès.
Show access-lists {n° ACL} → afficher le contenue d'une liste bien précise.