



FORMATION CISCO
Base documentaire

SOMMAIRE

1^{ère} partie : Prise en main du matériel Cisco

1. PRESENTATION GENERALE.	5
1.1. CONFIGURATION LOCALE.	5
1.2. CONFIGURATION DISTANTE.	5
2. IOS.	6
3. MEMOIRES.	6
3.1. INITIALISATION.	6
3.2. SAUVEGARDE DE LA CONFIGURATION.	7
3.2.1. <i>Startup-config</i> .	7
3.2.2. <i>Running-config</i> .	7
4. MODES DE CONFIGURATION.	8
4.1. PRESENTATION.	8
4.2. INVITE DE COMMANDE.	8
4.3. PASSAGE D'UN MODE A L'AUTRE.	9
4.4. AIDE CONTEXTUELLE.	10
4.5. MESSAGES D'ERREUR.	10
4.6. COMMANDES ABREGEES.	10
5. ANNEXE : CONFIGURATION HYPETERMINAL / PUTTY.	11
6. ANNEXE : CONFIGURATION DE BASE.	12
7. ANNEXE : SAUVEGARDE-CONFIGURATION.	13
7.1. COPIER-COLLER.	13
7.2. UTILISATION D'UN SERVEUR TFTP.	13
8. ANNEXE : PERTE DE MOT DE PASSE ET/OU D'IOS	ERREUR ! SIGNET NON DEFINI.



2^{nde} partie : La commutation

1. ROLE DU COMMUTATEUR	14
2. VLANS.....	15
2.1. MISE EN SITUATION.	15
2.2. PRINCIPE DE FONCTIONNEMENT..	16
2.3. DIFFERENTS TYPES DE VLAN.	17
2.3.1. VLAN par port.	17
2.3.2. VLAN par adresse MAC.	17
2.3.3. VLAN par sous-réseau.	17
2.3.4. Autres. Types de VLAN.....	17
2.4. ETIQUETAGE DES TRAMES (802.1Q).....	18
3. SPANNING-TREE.	19
3.1. MISE EN SITUATION	19
3.1.1. Tempête de broadcast.	19
3.1.2. Trames reçues en double	19
3.1.3. Tables d'adresses MAC imparfaites.	19
3.2. PRESENTATION DU SPANNING-TREE	20
3.3. FONCTIONNEMENT DU PROTOCOLE STP (802.1D).	20
3.3.1. 1 ^{ère} étape : Sélection du Root bridge.....	20
3.3.2. 2 ^{ème} étape : Sélection du meilleur chemin.....	21
3.3.3. 3 ^{ème} étape : Activation des ports.	21
3.3.4. Nom des ports.	21
3.4. TRAME BPDU.....	22
4. VTP	23
5. ANNEXE : CONFIGURATION DES VLAN SUR UN SWITCH CISCO	23
6. ANNEXE : CONFIGURATION SPANNING-TREE SUR UN SWITCH CISCO	24
7. ANNEXE : CONFIGURATION VTP SUR UN SWITCH CISCO.....	ERREUR ! SIGNET NON DEFINI.



3^{ème} partie : Le routage

1. UN ROUTEUR, POUR QUOI FAIRE ?	26
2. PRINCIPE DE FONCTIONNEMENT DU ROUTAGE.	26
3. INTERFACES DU ROUTEUR.....	27
3.1. COTE LAN.....	27
3.2. COTE WAN.....	27
4. TABLE DE ROUTAGE.....	28
4.1. ADRESSE DE DESTINATION.	28
4.2. TABLE DE ROUTAGE.....	28
4.3. TYPES DE ROUTES.	29
5. MECANISME DE DECISION.....	29
6. ROUTAGE STATIQUE	30
6.1. QUAND UTILISER LES ROUTES STATIQUES ?	30
7. ROUTAGE DYNAMIQUE.....	31
7.1. DETECTION AUTOMATIQUE DE RESEAUX	31
7.2. MAINTENANCE DES TABLES DE ROUTAGE.....	ERREUR ! SIGNET NON DEFINI.
7.3. PROTOCOLES DE ROUTAGE IP.....	ERREUR ! SIGNET NON DEFINI.
7.4. MEILLEUR CHEMIN ET MÉTRIQUE.....	ERREUR ! SIGNET NON DEFINI.
8. FONCTION DE COMMUTATION.....	ERREUR ! SIGNET NON DEFINI.
9. ANNEXE : COMMANDES DE BASES POUR LE ROUTAGE.....	ERREUR ! SIGNET NON DEFINI.
9.1. ROUTAGE STATIQUE.	ERREUR ! SIGNET NON DEFINI.
9.1.1. Configuration d'une route par défaut.....	Erreur ! Signet non défini.
9.1.2. Configuration d'une route statique.	Erreur ! Signet non défini.
9.1.3. Activation du routage.	Erreur ! Signet non défini.
9.1.4. Vérifier la table de routage.....	Erreur ! Signet non défini.
9.2. ROUTAGE RIP.	ERREUR ! SIGNET NON DEFINI.
9.2.1. Configuration de base.....	Erreur ! Signet non défini.
9.2.2. Vérifications.....	Erreur ! Signet non défini.
9.2.3. Exemple	Erreur ! Signet non défini.
9.3. ROUTAGE OSPF.....	ERREUR ! SIGNET NON DEFINI.
9.3.1. Activation du routage.	Erreur ! Signet non défini.
9.3.2. Vérifications.....	Erreur ! Signet non défini.

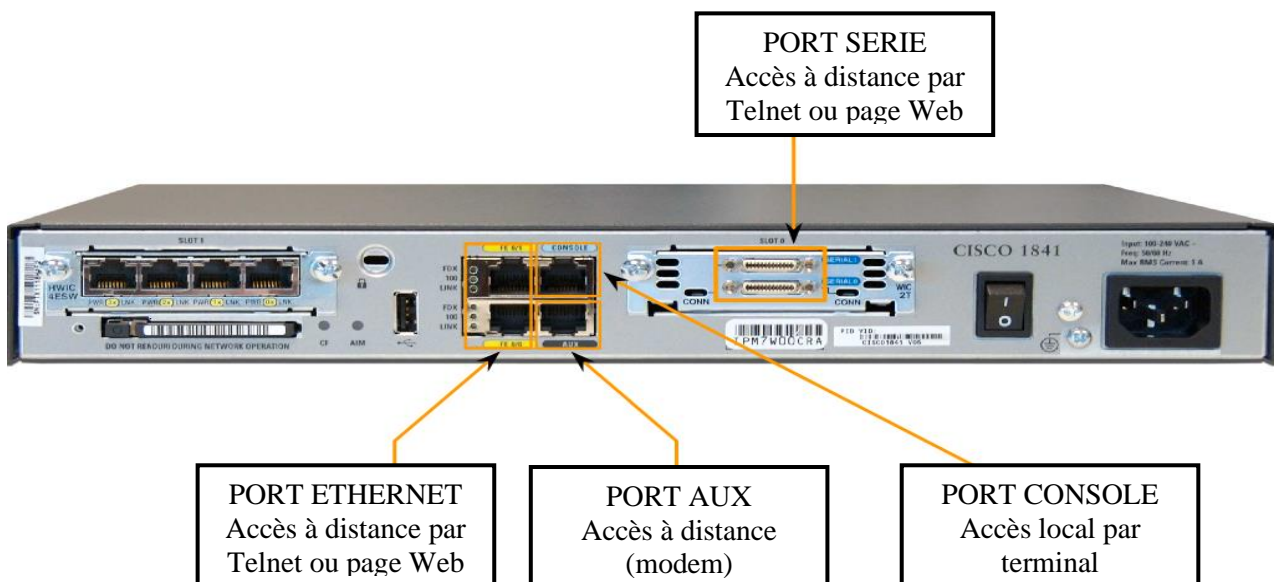
1^{ère} partie : Prise en main du matériel Cisco

Cette première partie a pour objectif de découvrir les matériels Cisco et d'effectuer les opérations élémentaires : accès, configuration de base, sauvegarde/mémorisation.

1. Présentation générale.

Un routeur (ou un commutateur) Cisco peut être administré/paramétré de différentes façons :

- Localement ou à distance.
- Par page web ou en ligne de commande(CLI).



1.1. Configuration locale.

Le port Console: Il est utilisé pour relier directement un PC avec HyperTerminal ou Putty (par exemple) en utilisant un câble série. Cisco fournit pour cela des câbles plats bleu pâle. **Le port console est indispensable si le routeur n'a pas d'adresse IP de configurée.**

1.2. Configuration distante.

Dès qu'une adresse IP a été configurée sur le routeur, il est possible de configurer ce dernier à distance, à partir d'un ordinateur. La communication utilise alors l'une des interfaces de réseau du routeur (Ethernet, adsl, série ...).

Les différentes sources de configuration peuvent être :

- *Un navigateur web* : `http://@IP_du_routeur`
- *Une fenêtre de commande* : `Telnet @IP_du_routeur`
- *Un serveur TFTP* qui permettra de télécharger un fichier de configuration sur le routeur.

2. IOS.

À l'instar d'un ordinateur personnel, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation. Sans système d'exploitation, le matériel est inopérant. Cisco IOS est le logiciel système des périphériques Cisco. IOS signifie Internetworking Operating System.



Il existe différentes versions d'IOS, en fonction de l'appareil, des fonctionnalités voulues et de la mémoire du routeur (ou commutateur).

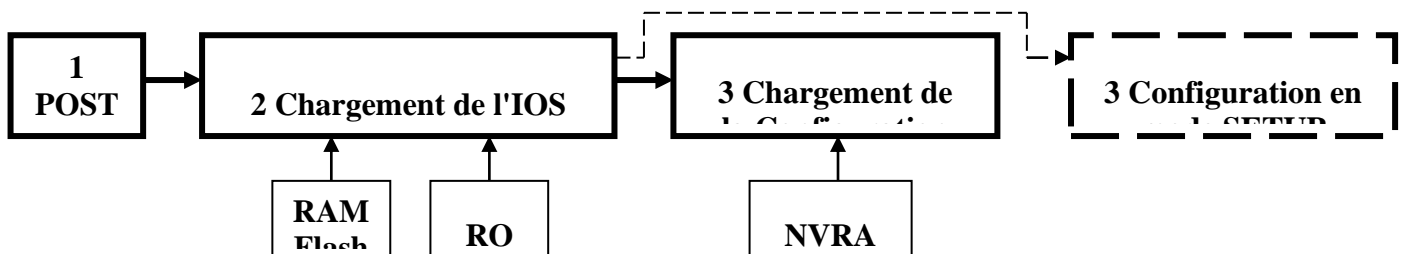
3. Mémoires.

Un routeur (ou un commutateur) dispose de plusieurs types de mémoires :

- **ROM :** *Le programme auto-test de mise sous tension (**POST** = Power-On Self-Test), le programme d'amorçage du routeur, tout ou partie du système d'exploitation appelé **IOS** (Internetworking **O**perating **S**ystem).*
- **NVRAM :** *Le fichier de configuration du routeur tel qu'il sera au démarrage (configuration de démarrage, aussi appelée **Start-Up Configuration** ou **START**).*
- **RAM Flash :** *Une ou plusieurs versions d'IOS. (La RAM Flash est couramment appelée la **FLASH**).*
- **RAM :** *La configuration active du routeur (configuration en cours aussi appelée **Running Configuration** ou **RUN**), la table de routage, les adresses IP, ...*

3.1. Initialisation.

La figure suivante image la séquence d'initialisation d'un routeur CISCO :



Lors de l'étape N°3, si aucun fichier de configuration n'est trouvé, le routeur se met en mode SETUP (mode de configuration à l'aide d'une suite de questions).

```

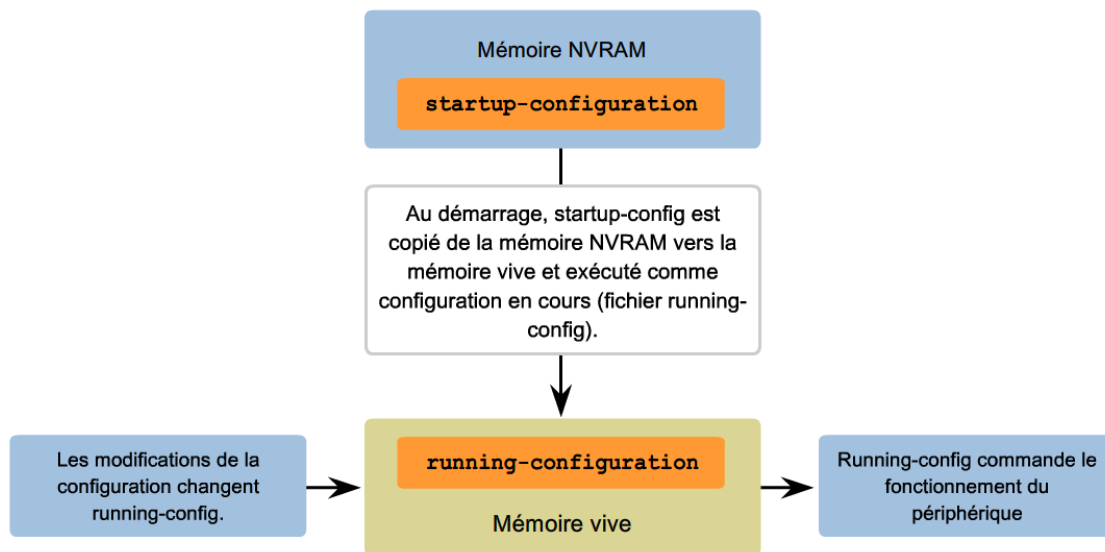
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
  
```

3.2. Sauvegarde de la configuration.

Un routeur (ou un commutateur) contient deux fichiers de configuration.

3.2.1. Startup-config.

Le fichier de configuration initiale (**startup-config**) est utilisé au démarrage du système pour configurer le périphérique. Le fichier de configuration initiale, appelé startup-config, est stocké en mémoire vive non volatile (NVRAM).



3.2.2. Running-config.

Le fichier de configuration **running-config** représente la configuration en cours de fonctionnement. Si on modifie un paramètre, on modifie ce fichier.

☞ Pour sauvegarder la configuration en cours avant extinction du routeur, il faut la taper la commande suivante:

Router# copy running-config startup-config

Ainsi, lors du prochain redémarrage, on récupérera la configuration sauvegardée.

☞ Pour récupérer la configuration initiale du routeur, il faut la taper la commande suivante:

Router# copy startup-config running-config

☞ Pour effacer la configuration initiale du routeur, il faut la taper la commande suivante:

Router# wr erase

☞ Pour recharger la config startup, il faut taper:

Router# reload

4. Modes de configuration.

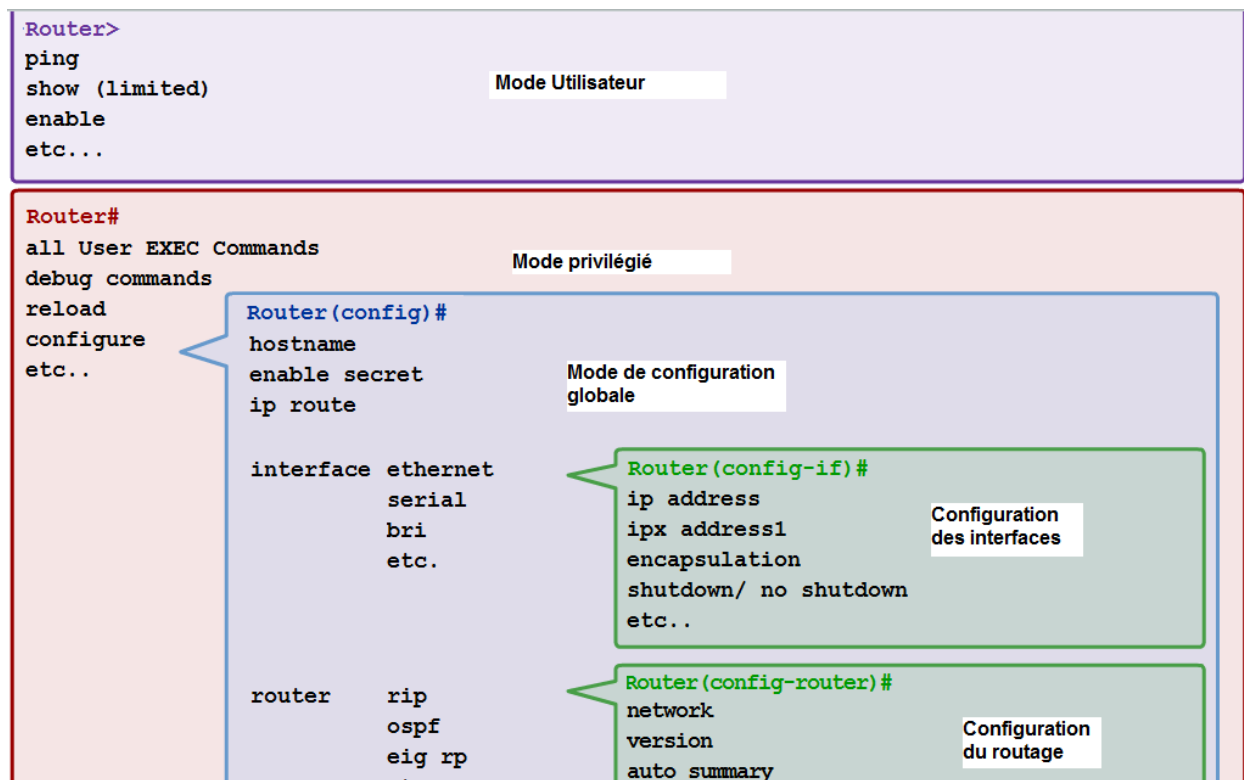
4.1. Présentation.

Les appareils Cisco proposent plusieurs modes de configuration. Chaque mode permet d'effectuer des tâches particulières et possède un jeu de commandes spécifiques qui sont disponibles lorsque le mode est en vigueur.

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

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

La figure ci-dessous montre la structure hiérarchique des modes IOS avec des invites et des fonctionnalités classiques.



4.2. Invite de commande.

Par exemple, pour configurer une interface réseau, il faudra passer par les modes "utilisateur", "privilégié" puis "config globale". L'invite change en fonction du mode dans lequel on se trouve :

```
Router>ping 192.168.10.5

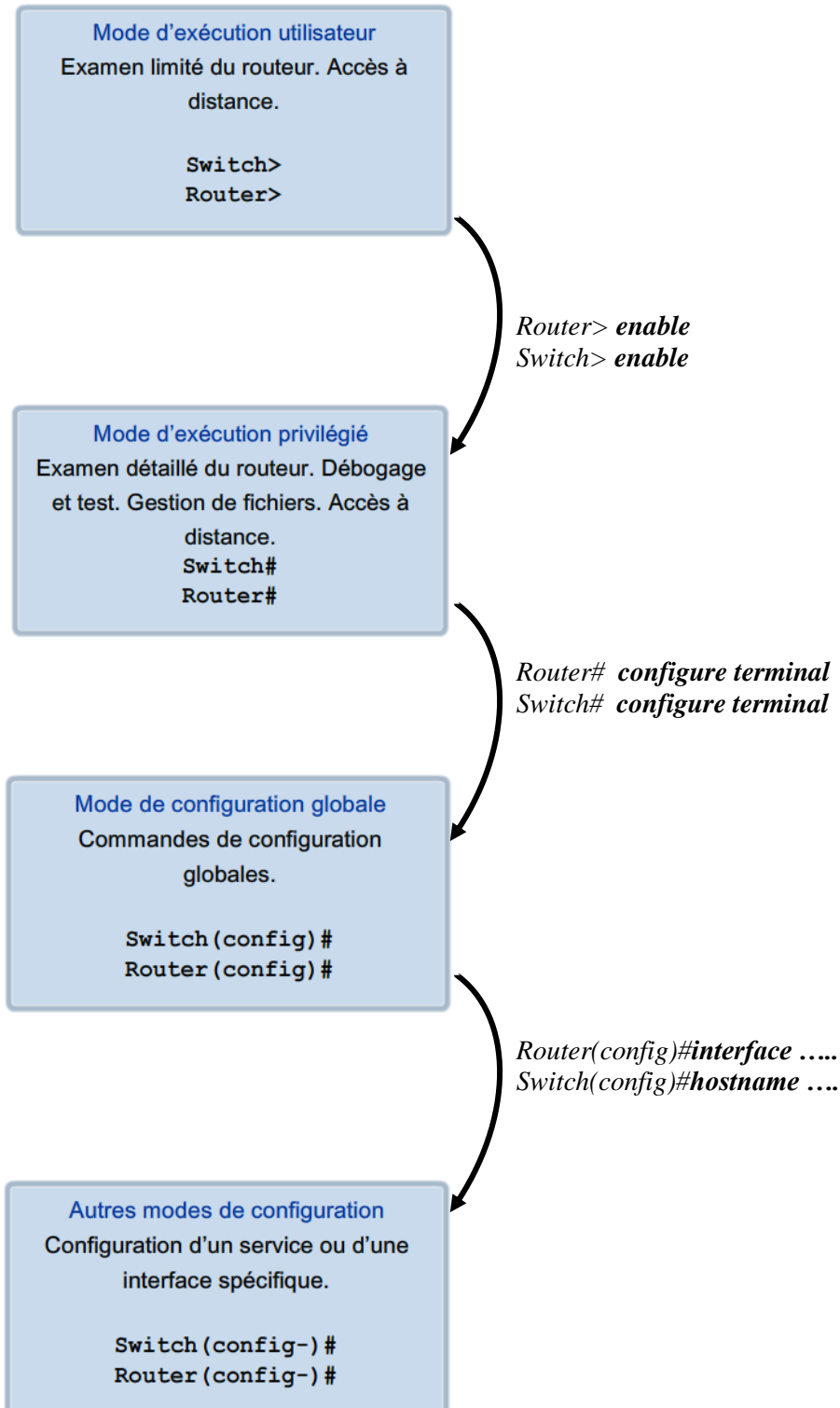
Router#show running-config

Router (config) #Interface FastEthernet 0/0

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


4.3. Passage d'un mode à l'autre.

La figure ci-dessous présente quelques exemples de commandes à taper pour passer d'un mode à l'autre.



Pour revenir en arrière, il suffit de taper **exit** ou **Ctrl-Z**

4.4. Aide contextuelle.

Cisco IOS propose une aide dans l'utilisation de ses commandes. On utilise pour cela le ?

Quelques exemples:

<i>Router# ?</i>	Affiche la liste des commandes possibles
<i>Router# cl?</i>	Affiche la liste des commandes possibles commençant par "cl".
<i>Router# clock ?</i>	Affiche la liste des commandes possibles associées à "clock".
<i>Router# clock set ?</i>	Affiche la liste des commandes possibles associées à "clock set".

4.5. Messages d'erreur.

Lorsque la commande n'est pas valide ou incomplète, un message ou un symbole apparaît.

Quelques exemples:

IOS renvoie un message d'aide indiquant que des mots clés ou des arguments obligatoires manquent à la fin de la commande :

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

IOS renvoie un message d'aide indiquant que vous n'avez pas entré assez de caractères pour permettre à l'interpréteur de commandes de reconnaître la commande :

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

IOS renvoie un accent circonflexe (^) pour indiquer l'emplacement où l'interpréteur de commandes ne parvient pas à déchiffrer la commande :

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

4.6. Commandes abrégées.

Il n'est pas utile de taper toute la commande. On peut ainsi abréger certaines commandes.

Quelques exemples:

<i>Router# sh ip int br</i>	à la place de	<i>Router# show ip interface brief</i>
<i>Router# copy run start</i>	à la place de	<i>Router# copy running-config startup-config</i>

Dans le même ordre d'idée, on peut rappeler les commandes précédemment entrées en utilisant les flèches Haut et Bas.

5. ANNEXE : Configuration Putty

1. Putty est un simple logiciel exécutable : il ne nécessite pas d'installation.

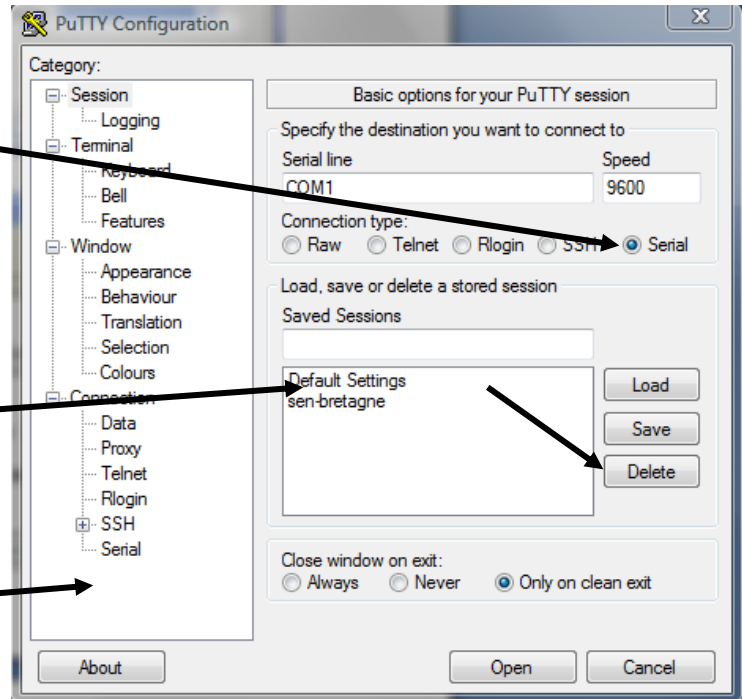
2. Lancer Putty : l'écran ci-contre s'affiche :

3. Cocher le type de connexion

4. Préciser si nécessaire le port COM utilisé et la vitesse correspondante (9600 par défaut).

5. On peut sauvegarder les paramètres de connexion.

5. Il est possible d'ajuster les paramètres de la connexion bien que cela soit rarement nécessaire pour une liaison série.

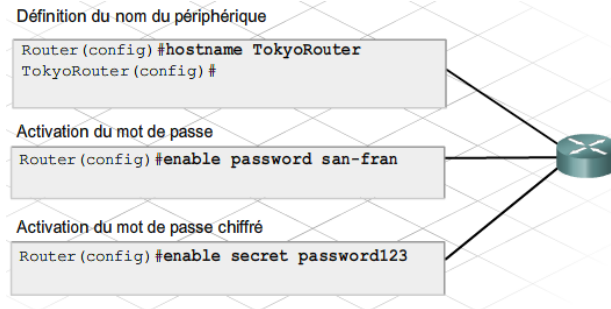


6. Lancer la connexion... Une fenêtre noire apparaît, dans laquelle vous tapez les commandes

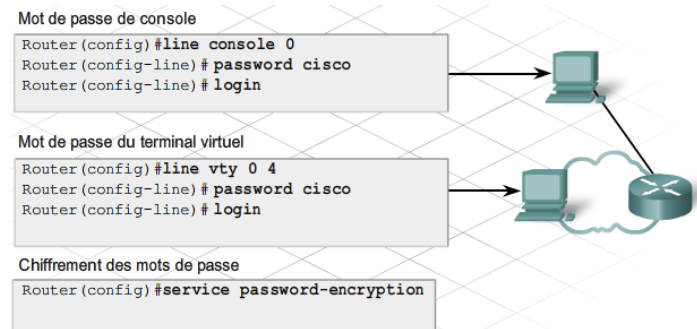
6. ANNEXE : Configuration de base.

1. Configuration du nom et du mot de passe.

La configuration initiale d'un périphérique Cisco IOS requiert la configuration du nom du périphérique, puis des mots de passe utilisés pour contrôler l'accès aux diverses fonctions du périphérique.



2. Autres mots de passe.



3. Configuration d'une interface (routeur).

Les étapes de configuration d'une interface sont les suivantes :

Étape 1. Spécification du type d'interface et du numéro de port de l'interface

Étape 2. Spécification d'une description de l'interface

Étape 3. Configuration de l'adresse IP et du masque de sous-réseau de l'interface

Étape 4. Définition de la fréquence d'horloge si vous configurez une interface série en tant que DCE

Étape 5. Activation de l'interface

```
Router(config)#interface fastethernet 0/0
Router(config-if)#description connection to Admin LAN
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#description connection to Router2
Router(config-if)#ip address 192.168.1.125 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```



4. Configuration d'une interface (switch).

Si on veut pouvoir administrer un commutateur à partir d'un client Telnet sur un PC, ou par l'une des interfaces LAN ou WAN, il faut affecter une adresse IP au vlan d'administration qui est souvent le vlan par défaut. La configuration de l'interface se fait à partir du mode de **configuration globale**.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address ip-address ip-mask
Switch(config-if)#no shutdown
```

5. Vérifications :

```
Router# show running-config
Router# show ip interfaces brief
```

7. ANNEXE : Sauvegarde-configuration

7.1. Copier-Coller

Il est possible de faire un Copier-Coller depuis ou vers Hyperterminal. Cela permet de sauvegarder une configuration dans un fichier texte.

Pour restaurer une configuration, il faut d'abord se placer en mode de configuration globale

```
Router> enable
Router# configure terminal
Router(config)# A cet endroit, « collez » votre fichier texte
```

7.2. Utilisation d'un serveur tftp

Le serveur TFTP permet de sauvegarder/restaurer un fichier de configuration mais aussi (et surtout !) un IOS complet pour une mise à jour ou suite à un crash.

L'utilisation de TFTP n'est possible que si le routeur communique avec l'ordinateur par IP.

1. Télécharger et installer Solarwinds TFTP
2. Dans TFTP Server, configurer le répertoire de travail du serveur.
3. Relever l'adresse IP de votre ordinateur.
4. Sauvegarder la configuration courante :

```
Router# copy run tftp
```

5. Et répondre aux questions (adresse du serveur TFTP et nom du fichier)

Le principe est le même depuis le serveur TFTP vers le routeur (ou commutateur).

2nde partie : La commutation

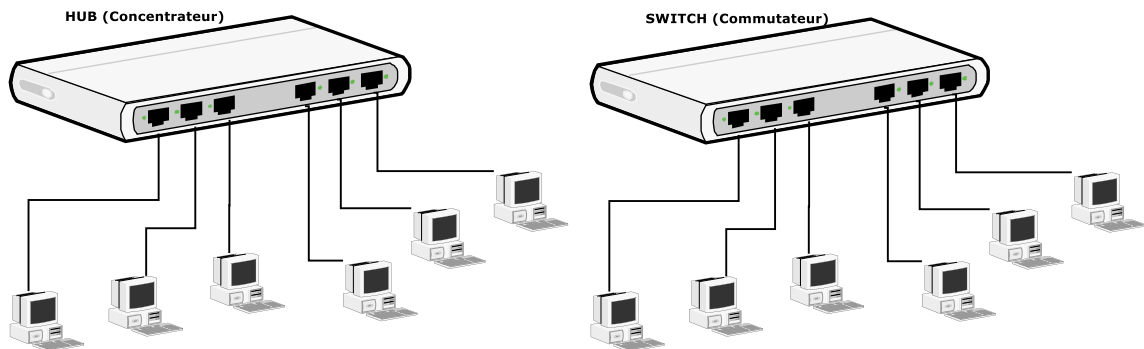
Cette seconde partie vise l'installation et la configuration des commutateurs.

1. Rôle du commutateur

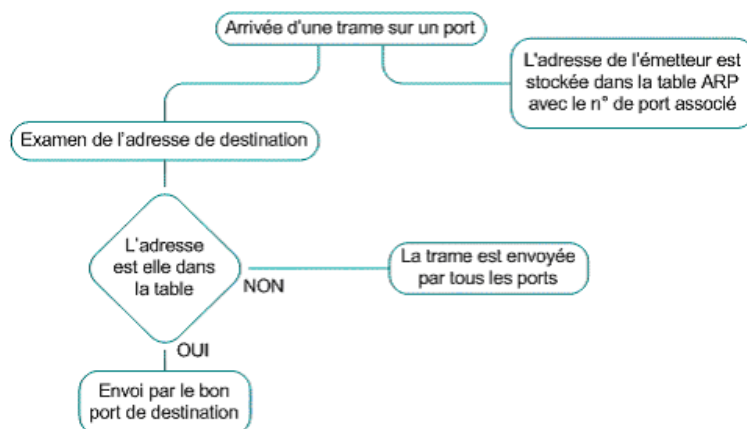
Le commutateur (switch) assure la connexion entre les ordinateurs du réseau, au même titre qu'un hub, mais en plus performant :

Lorsqu'un hub reçoit une trame, il la réémet sur tous les ports. Cela signifie qu'un seul ordinateur peut émettre à un moment donné.

Lorsqu'un switch reçoit une trame, il la réémet uniquement sur le port auquel est connecté le destinataire. Cela signifie qu'il peut y avoir plusieurs « communications » simultanées, comme l'illustre le schéma ci-dessous :



Afin d'orienter correctement les communications, le switch mémorise dans une table l'adresse MAC, les machines et le port auquel elles sont connectées.

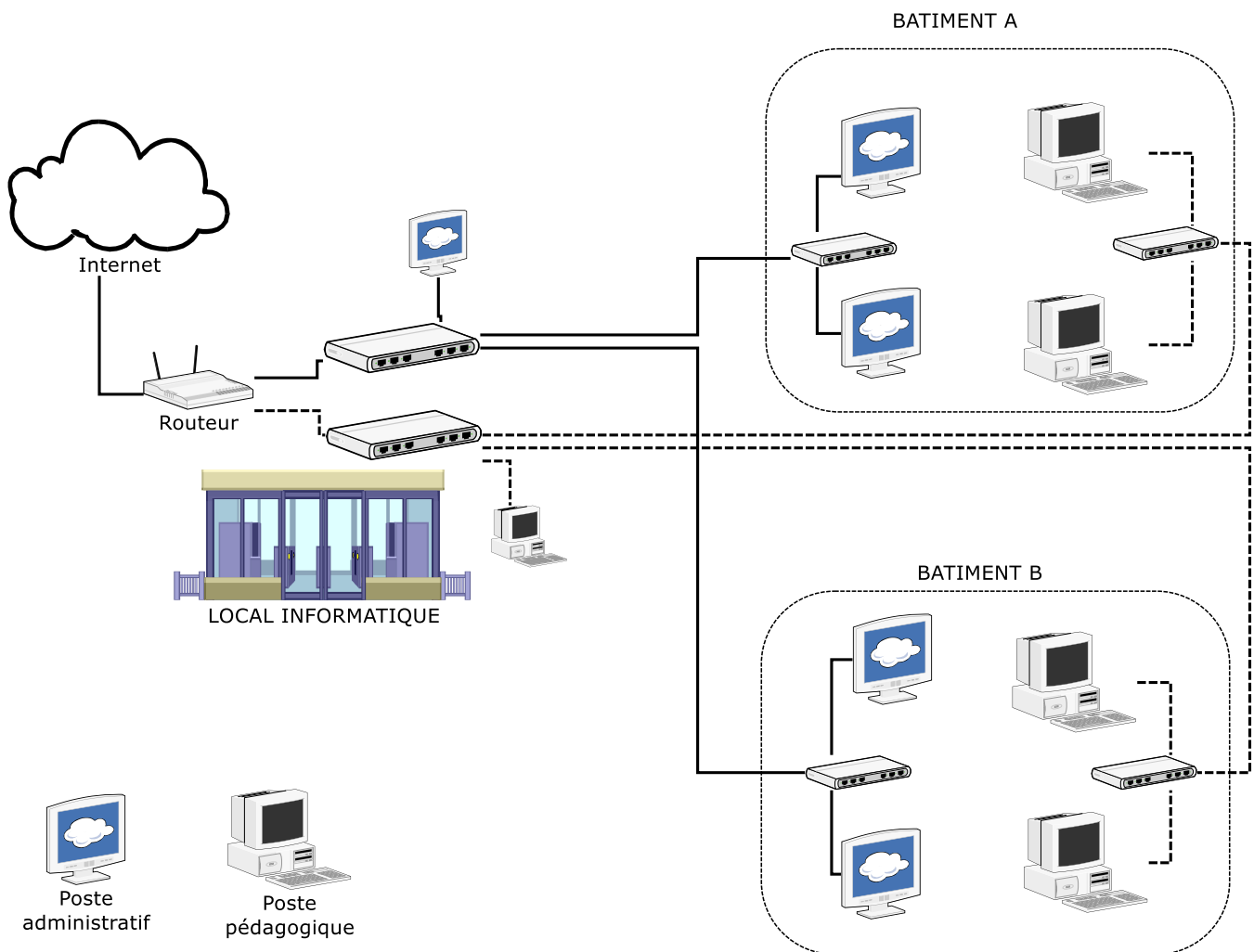


2. VLANs

2.1. Mise en situation.

Dans une entreprise ou une organisation administrative, il n'est pas rare que des machines géographiquement voisines ne fassent pas partie du même service / réseau. Par exemple, dans la salle des professeurs d'un lycée, on pourra trouver un ordinateur connectés au réseau pédagogique (pour la préparation des cours) et un ordinateur connecté au réseau administratif (pour la saisie des notes).

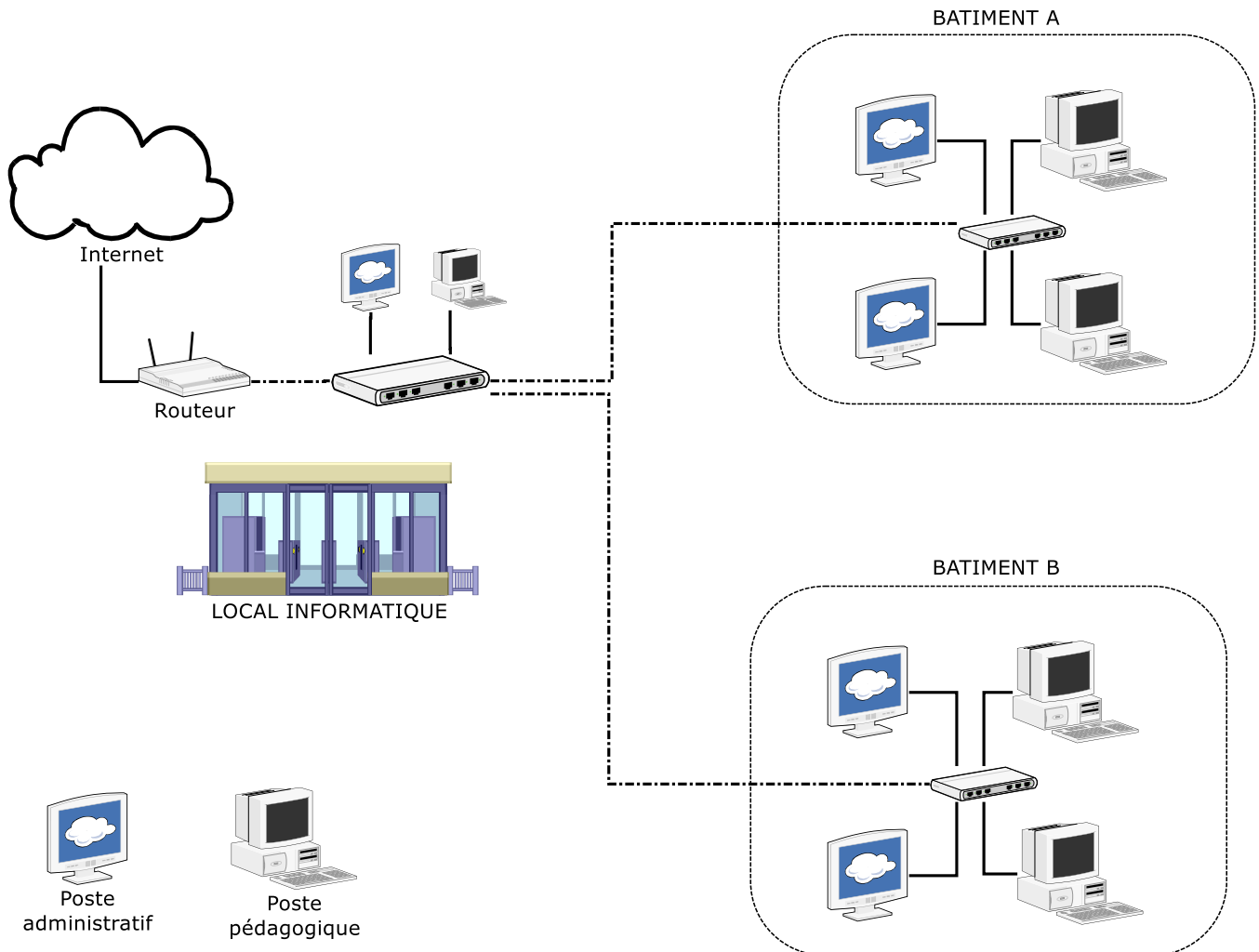
Ces ordinateurs ne doivent pas communiquer pour des questions de sécurité. Pour ce faire, il faut utiliser des matériels distincts : switches, câbles, fibres. Bref, il faut tout en double, comme l'illustre le schéma ci-dessous.



Remarque : Le routeur représente le point potentiel d'interconnexion entre les deux réseaux. Cependant, les interfaces réseau étant différentes, la communication entre les deux sera impossible, sauf paramétrage spécifique.

Sur ce second schéma, tous les ordinateurs sont reliés aux mêmes équipements et utilisent les mêmes voies de transmissions entre bâtiments. Pourtant, les ordinateurs pédagogiques et administratifs ne peuvent communiquer, malgré le fait qu'ils possèdent des IP compatibles.

Ceci est dû au fait que ce réseau utilise les VLAN ou réseaux virtuels.



2.2. Principe de fonctionnement..

Un VLAN ou réseau virtuel est un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elle était sur le même segment. **Un VLAN est identifié par son VID** (numéro).

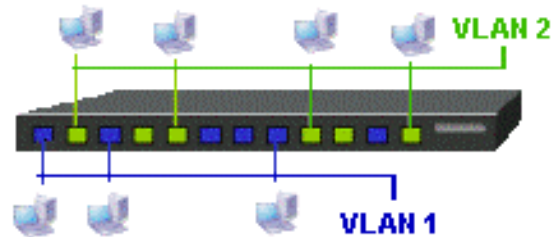
Dans le schéma ci-dessus, les postes du réseau administratif font partie d'un VLAN, les postes du réseau pédagogique font partie d'un autre VLAN, lesquels ne peuvent communiquer, sauf par le biais du routeur, s'il est programmé pour cela.

2.3. Différents types de VLAN.

2.3.1. VLAN par port.

Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur à un VLAN particulier. C'est une solution simple, qui a été rapidement mise en œuvre par les constructeurs.

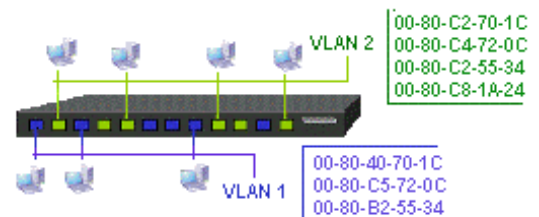
Les VLAN par port manquent de souplesse, tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN.



2.3.2. VLAN par adresse MAC.

Un VLAN par adresse MAC, ou VLAN de niveau 2 est constitué en associant les adresses MAC des stations à chaque VLAN.

L'intérêt de ce type de VLAN est surtout l'indépendance de la localisation. La station peut être déplacée, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN. Les VLAN configurables avec l'adresse MAC sont bien adaptés à l'utilisation de stations portables.



Cependant, la configuration peut s'avérer fastidieuse car elle nécessite de renseigner une table de correspondance avec toutes les adresses MAC et elle doit être partagée par tous les commutateurs.

2.3.3. VLAN par sous-réseau.

Également appelé VLAN de niveau 3, un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas, les commutateurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN. Cette solution est l'une des plus intéressantes, malgré une petite dégradation des performances de la commutation due à l'analyse des informations.

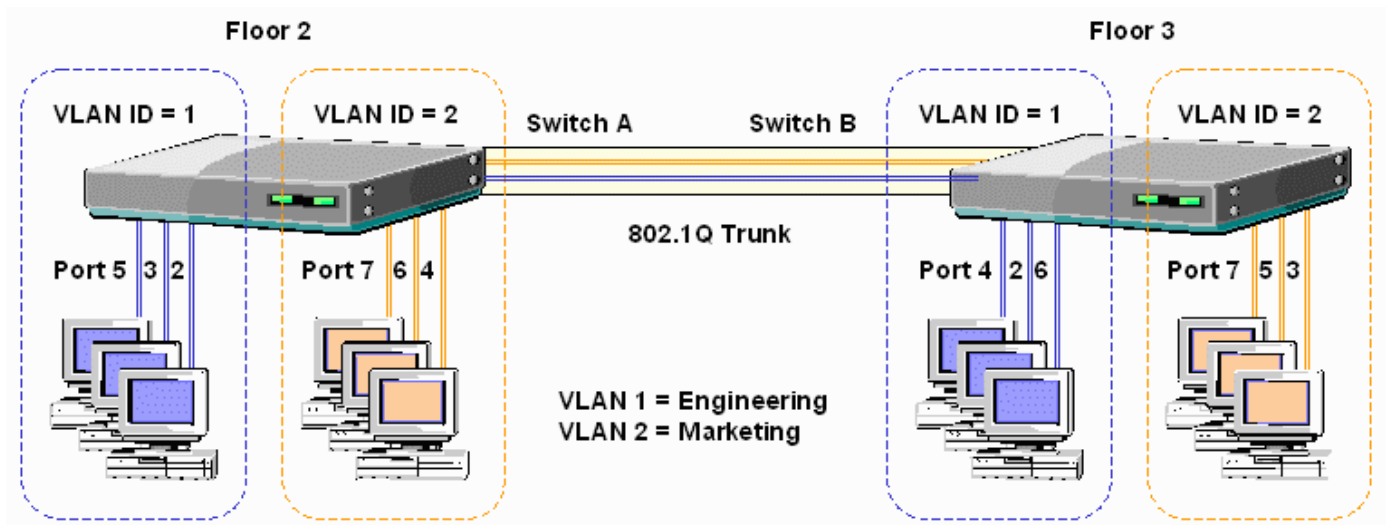
2.3.4. Autres. Types de VLAN

On trouve dans la littérature des références au Vlan par protocoles. C'est à dire qu'on associe une trame à un Vlan en fonction du protocole qu'elle transporte. Ce protocole peut être un protocole de niveau 3 pour isoler les flux IP, IPX, Appletalk .etc...

Mais on peut trouver aussi des Vlan construits à partir de protocole supérieur (notamment H320). On parle quelquefois de Vlan par règles ou par types de service.

Enfin l'apparition du Wi-fi pose des problèmes de sécurité que les Vlan peuvent résoudre. Ainsi une solution basée sur des Vlan par SSID est envisageable.

2.4. Etiquetage des trames (802.1Q).



Comment le commutateur de gauche recevant une trame du commutateur de droite peut-il savoir à quel VLAN elle appartient ?

On utilise pour cela le **marquage (tag)** des trames. Concrètement, on ajoute un en-tête supplémentaire contenant notamment le n° de VLAN (VID) auquel appartient la trame. La norme 802.1Q définit trois sortes de trames :

- Les trames non étiquetées (untagged frame).
- Les trames étiquetées (tagged frame).
- Les trames étiquetées par une priorité (priority-tagged frame).

Dans le langage Cisco, un port taggué est appelé « trunk ».

Remarque importante : Les switches doivent être configurés de la même manière, c'est-à-dire utiliser les mêmes numéros de VLAN.

Voir Annexe pour configuration-type

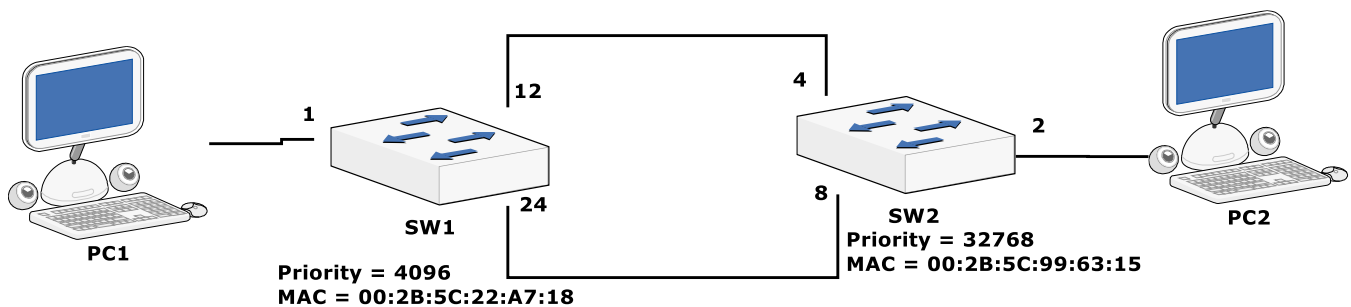
3. Spanning-Tree.

3.1. Mise en situation

Dans une architecture informatique, il arrive que le réseau comporte des boucles : plusieurs chemins possibles pour aller d'un point à un autre. Ce système présente un avantage certain : la redondance permet de pallier une éventuelle coupure d'un lien.

Mais cette redondance, si elle est mal gérée, peut entraîner des problèmes très importants.

3.1.1. Tempête de broadcast.



1. PC1 envoie une requête ARP (en broadcast).
2. SW1 reçoit sur le port 1 et diffuse sur les ports 12 et 24
- 3a. SW2 reçoit sur le port 4 et diffuse vers 2 et 8
- 3b. En même temps, SW2 reçoit sur le port 8 et diffuse vers 4 et 2.
- 4a. SW1 reçoit sur le port 24 et diffuse vers 1 et 12.
- 4b. En même temps, SW1 reçoit sur le port 12 et diffuse sur 1 et 24
5. Répétition de 3a et 3b.
6. Répétition de 4a et 4b

Ce phénomène, appelé *tempête de broadcast* (broadcast storm) génère un trafic (inutile) très important.

3.1.2. Trames reçues en double

1. PC1 envoie un ping vers PC2.
2. SW1 reçoit sur le port 1 et diffuse (ports 12 et 24) car il ne connaît pas la position de PC2
- 3a. SW2 reçoit sur la demande ping sur le port 4 et envoie PC2.
- 3b. En même temps, SW2 reçoit sur la demande sur le port 8 et envoie vers PC2.

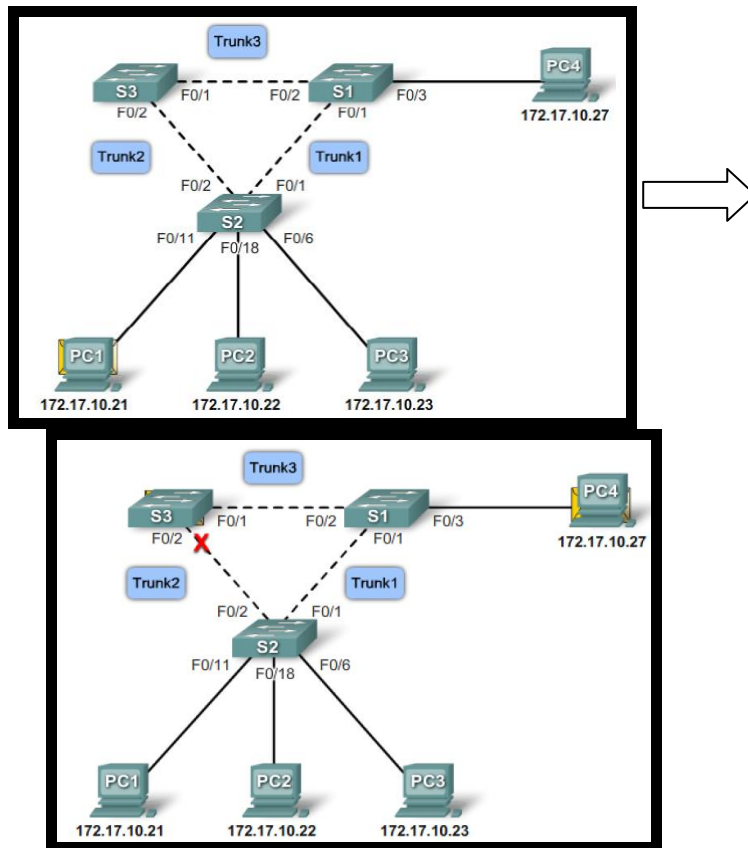
PC2 aura donc reçu deux demandes identiques.

3.1.3. Tables d'adresses MAC imparfaites.

Du fait des diffusions en double, les tables des switchs se remplissent de manière imparfaites ou erronnées. Par exemple, SW2 "pensera" que PC1 est connecté sur son port 4 ou 8 ?. Avec des architectures plus complexes, une trame pourrait ainsi emprunter un chemin plus long que nécessaire.

3.2. Présentation du Spanning-Tree

Afin d'éviter les problèmes cités plus haut, on utilise un système chargé de détecter les boucles et de désactiver les liens redondants. C'est le protocole *Spanning-Tree*, ou *Arbre de Recouvrement*.



Avant

Après : le lien S2-S3 est désactivé

Il existe plusieurs protocoles de Spanning-Tree. Le plus connu est le STP ou 802.1D

3.3. Fonctionnement du protocole STP (802.1D).

3.3.1. 1^{ère} étape : Sélection du Root bridge.

Le Root Bridge, ou switch racine, est celui qui a la plus petite Bridge Identity (BID). Il s'agit d'un nombre composé de :

- Une *priorité*, comprise entre 1 et 655356 (par défaut à 32768).
- L'*adresse MAC* du switch, pour départager en cas d'égalité sur la priorité.

3.3.2. 2^{ème} étape : Sélection du meilleur chemin.

L'étape suivante consiste à sélectionner le meilleur chemin depuis les switchs vers le Root Bridge. Chaque liaison à un "coût". Le coût le plus faible l'emporte.

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

En cas d'égalité parfaite (coût, puis @MAC), c'est le numéro de port le plus faible qui détermine le "gagnant".

3.3.3. 3^{ème} étape : Activation des ports.

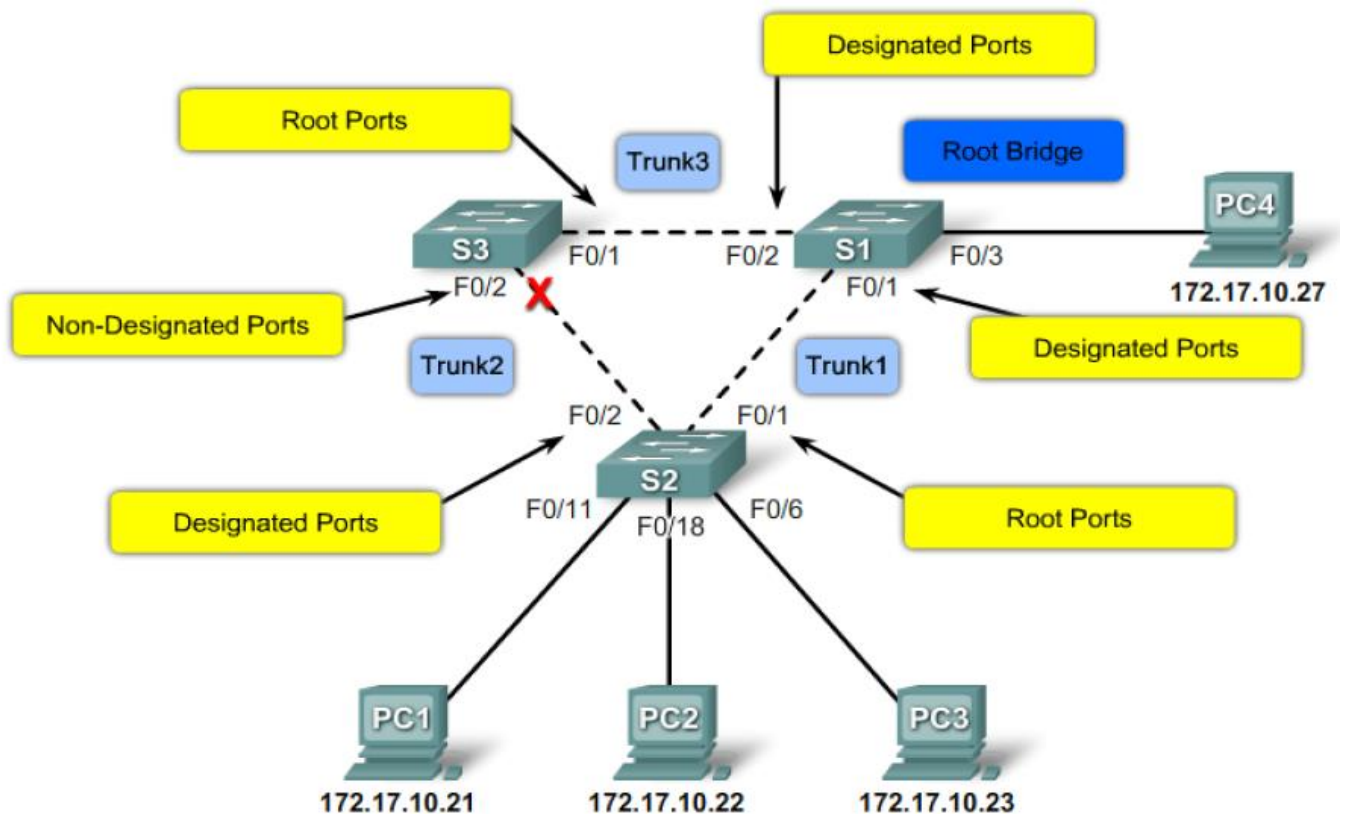
En fonction des deux étapes précédentes, les ports sont activés ou désactivés. On dit qu'ils sont :

- **Actif**, ou **Forwarding** : C'est le fonctionnement habituel d'un port de commutateur.
- **Inactif** ou **Blocking** : Le port est désactivé mais lit/transmet les trames STP pour être informé en cas de défaillance.

3.3.4. Nom des ports.

Chaque port faisant partie de la topologie STP est nommé :

- **Root Port** : Ce sont les ports qui mènent au Root Bridge. Le Root Port reçoit les messages émis par le Root Bridge.
- **Designated Ports** : Ce sont les ports qui émettent les trames 802.1D à destination des différents commutateurs.
- **Non désigné Port** : Ou Blocking Port, représente les ports qui n'émettent pas de données. Ces ports lisent quand même les messages 802.1D



3.4. Trame BPDU.

Chaque "Designated Port" émet une trame BPDU (Bridge Protocol Data Unit) en Multicast. Tous les switches prenant en charge le protocole STP en sont les destinataires. Cette trame contient les informations suivantes.

Protocole	Version	Type Msg	Flags	Root ID	Coût	ID Pont	ID Port	Age Msg	Age Max	Hello T	Forward Delay
2	1	1	1	8	4	8	2	2	2	2	2

- Protocole, Version : Valeur toujours à 0
- Type Message (1 octet) :
 - 0 pour un message de configuration,
 - 128 pour un message de changement de topologie
- Flags : (1 octet) mais seulement 2 bits utilisés
 - TC : Topology-Change
 - TCA : Topology-Change Acknowledgment, Acquiescement en réception d'un message de configuration avec le bit TC à 1.
- Root ID et Port ID : 2 octets pour la priorité et 6 pour l'@ Mac
- Coût du port : alloue un coût à un port, pour privilégier un port par rapport à un autre et la transmission de trame (1 à 65535)
- Age Max: temps maximum d'attente pour qu'un pont considère la topologie caduque (recalcul de la topologie) (6 à 40 s, 20 s recommandé)
- Hello Time : intervalle entre chaque envoi de trames (hello) par le pont maître (1 à 10s, 2 s recommandé)

- Forward Delay : durée de l'état écoute et de l'état apprentissage (4 à 30 s, 15 s recommandé)

Suite à la détection d'une panne, la nouvelle configuration met environ 50 secondes à se mettre en place (Age Max + 2 x Forward Delay)

Voir Annexe pour configuration-type

4. VTP

Le protocole VTP (Vlan Trunking Protocol) est un protocole propriétaire qui permet de configurer les Vlan sur un seul commutateur. Cette configuration, ainsi que les éventuelles modifications/mises à jour sont ensuite transmises automatiquement aux autres commutateurs, via les ports taggués.

Il y a donc un serveur et des clients, faisant tous partie du même domaine VTP.

La configuration des Vlan est transmise via les ports taggués (trunk). Si un commutateur non configuré reçoit une trame VTP sur un port, celui-ci est automatiquement mis en mode trunk.

La limite de ce système est qu'il est quand même nécessaire d'affecter manuellement les ports sur chaque commutateur.

Voir Annexe pour configuration-type

5. ANNEXE : Configuration des VLAN sur un switch Cisco

1. Création des Vlan.

Switch> enable	Passer en mode privilégié
Switch# vlan database	
Switch(vlan)# vlan 2 name peda	Crée le VLAN nommé peda avec le numéro (VID) 2.
Switch(vlan)# vlan 3 name admin	Crée le VLAN nommé admin avec le numéro (VID) 3.
Switch(vlan)# exit	

2. Affectation des ports (ports 1 à 4 : VLAN 2 - ports 9 à 12 VLAN 2).

Switch# configure terminal	
Switch(config)# interface fastEthernet 0/1	paramétrage du port n°1
Switch(config-if)# switchport mode access	pas de tag sur ce port (access)
Switch(config-if)# switchport access vlan 2	affectation du port au vlan 2
Switch(config-if)# exit	
Switch(config)# interface fastEthernet 0/9	paramétrage du port n°9
Switch(config-if)# switchport mode access	pas de tag sur ce port (access)
Switch(config-if)# switchport access vlan 3	affectation du port au vlan 3
Switch(config-if)# exit	

Remarque : Pour configurer plusieurs interfaces en même temps:

Switch(config)# interface range fastEthernet 0/1 - 4	configure les ports 1 à 4
	Ne fonctionne pas avec tous les IOS

3. Création du lien taggué ou trunk (port 24 -> Routeur)

Switch(config)# interface fastEthernet 0/24	paramétrage du port n°24
--	--------------------------



```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# exit
```

ce lien sera taggé (trunk)...
...au format 802.1Q (Commande
inutile sur Cisco 2950 et +)

Remarque : Selon les IOS, la fonction trunk est automatique ou à paramétrer manuellement

4. Quelques commandes utiles.

En mode utilisateur privilégié (enable) :

Switch# show vlan	Voir la configuration des VLAN.
Switch# show conf	Voir la configuration de démarrage.
Switch# show run	Voir la configuration en cours
Switch# show ip int brief	Voir le statut des ports
Switch# show interface trunk	Voir les ports taggués (ne fonctionne pas sur tous les IOS)

Switch# erase flash :vlan.dat Supprime tous les vlans.

En mode de configuration vlan (vlan database) :

Switch(vlan)#no vlan id Supprimer le VLAN de numéro id.

Pour quitter un mode : **Ctrl Z**

6. ANNEXE : Configuration Spanning-Tree sur un switch Cisco

Par défaut, le spanning-tree est activé sur les commutateurs Cisco sur le Vlan 1 (qui contient tous les ports).

Pour le diagnostic :

#show spanning-tree [?]

Désactivation de STP :

(config)#no spanning-tree vlan *vlan-id*

Priorité du switch :

(config)#spanning-tree [vlan *vlan-id*] priority *priority*

R209

Ethernet



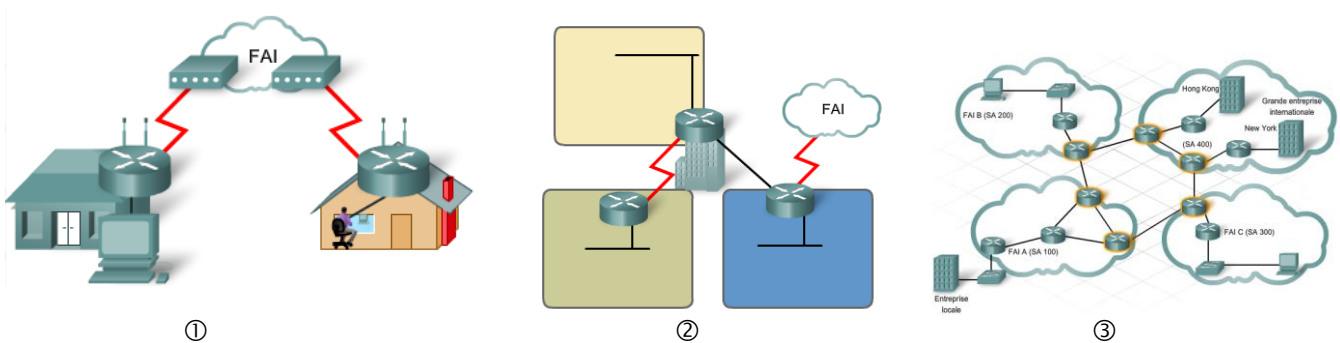
3^{ème} partie : le routage

1. Un routeur, pour quoi faire ?

Dans un petit réseau d'entreprise ou chez les particuliers, tous les ordinateurs sont reliés directement et accèdent à Internet en passant par un routeur. ①

Lorsque l'entreprise est importante, établie sur différents sites, elle dispose de plusieurs réseaux, reliés entre eux par des routeurs. ②

Internet, réseau des réseaux, est constitué de milliers de routeurs, capables d'acheminer l'information d'un ordinateur à un autre. ③

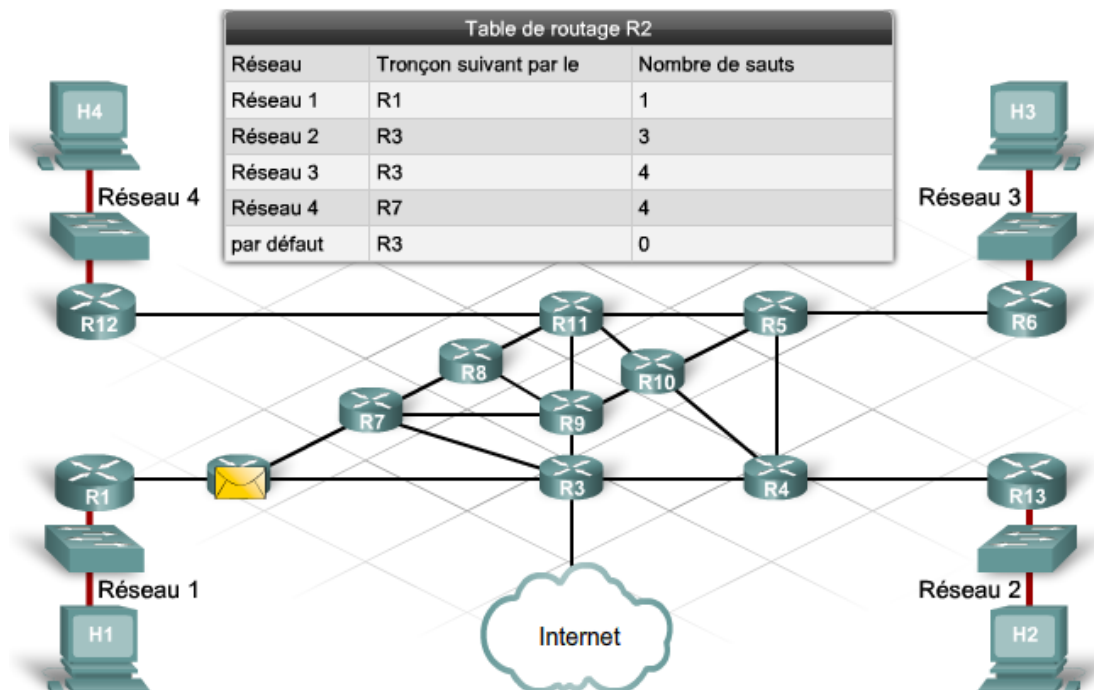


2. Principe de fonctionnement du routage.

Lorsqu'un ordinateur émet un message vers un autre, hors de son réseau, ce message est transmis au routeur. Ce routeur effectue les actions suivantes :

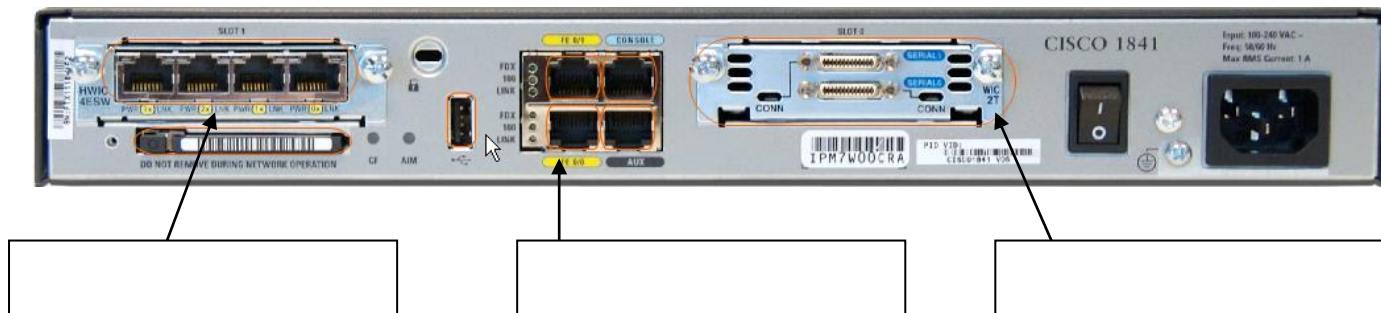
- Lire l'adresse du destinataire.
- Consulte sa table de routage pour déterminer la route à suivre pour atteindre cette destination.
- Transmet le message au routeur suivant (ou au destinataire s'il est à côté).

Dans l'illustration ci-dessous, le poste H1 veut envoyer un message au poste H3. Plusieurs routeurs ont déjà été traversés. Le message est arrivé au niveau de R2.



3. Interfaces du routeur.

Un routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces, chacune appartenant à un réseau IP différent. Ces interfaces peuvent être connectées à des réseaux locaux (LAN) ou à des réseaux étendus (WAN). Les connecteurs et les supports de transmission sont donc spécifiques. Néanmoins, toutes les interfaces possèdent leur propre adresse IP.

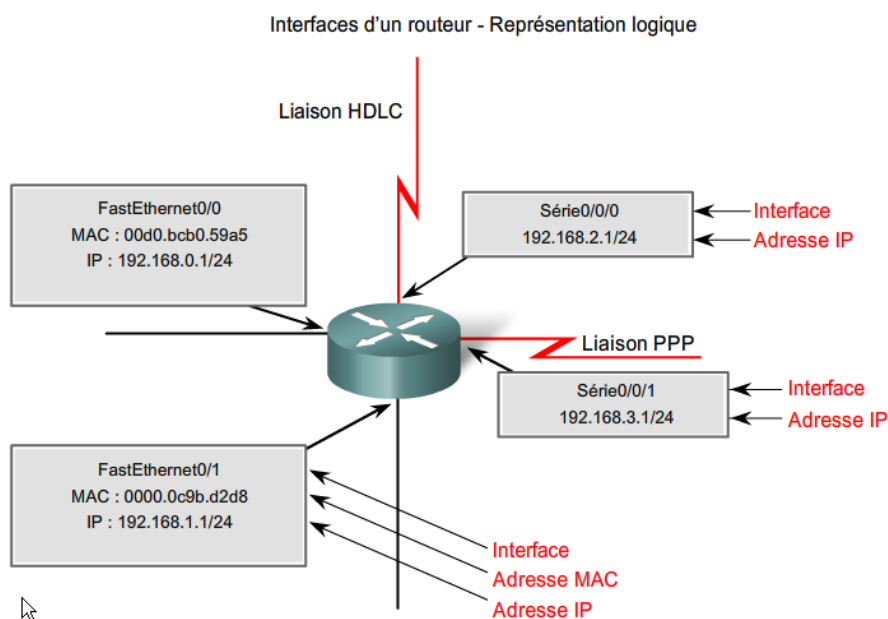


3.1. Côté LAN.

Côté LAN, le routeur possède généralement une interface Ethernet. Le connecteur est de type RJ45. Comme une carte réseau Ethernet de PC, une interface Ethernet de routeur possède également une adresse MAC de couche 2 et participe au réseau local Ethernet de la même manière que tous les autres hôtes de ce réseau. Il fait généralement office de passerelle par défaut pour les machines connectées sur cette interface.

3.2. Côté WAN.

Les interfaces WAN servent à connecter les routeurs à des réseaux externes, généralement sur une distance géographique importante. L'encapsulation de couche 2 peut être de différents types, notamment PPP, Frame Relay et HDLC (High-Level Data Link Control). À l'instar des interfaces LAN, chaque interface WAN a sa propre adresse IP et son propre masque de sous-réseau



4. Table de routage.

4.1. Adresse de destination.

Lorsqu'un routeur reçoit un paquet, il examine l'adresse IP de destination pour savoir où le transférer. L'adresse de destination est composée d'une partie réseau et d'une partie hôte. Le routeur s'intéresse à la partie réseau. Pour cela, il effectue un ET logique entre l'adresse et le masque correspondant.

Exemple :

Adresse de destination	194	.	51	.	3	.	49
Masque correspondant	255	.	255	.	255	.	0

Adresse réseau de destination . . .

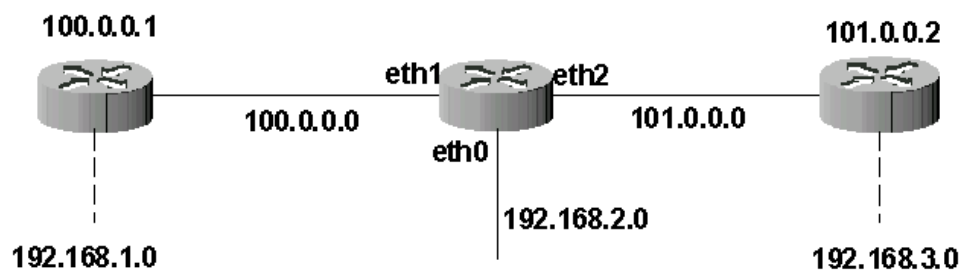
4.2. Table de routage.

Un routeur utilise une table de routage pour déterminer le lieu d'expédition des paquets. La table de routage contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné. Une route possède quatre composants principaux :

- le réseau de destination ;
- le masque de sous-réseau ;
- l'adresse de passerelle ou d'interface ;
- le coût de la route ou la mesure.

Réseau	Masque	Moyen de l'atteindre	Métrique
192.168.2.0	255.255.255.0	eth0	0
100.0.0.0	255.0.0.0	eth1	0
101.0.0.0	255.0.0.0	eth2	0
192.168.1.0	255.255.255.0	100.0.0.1	1
192.168.3.0	255.255.255.0	101.0.0.2	1

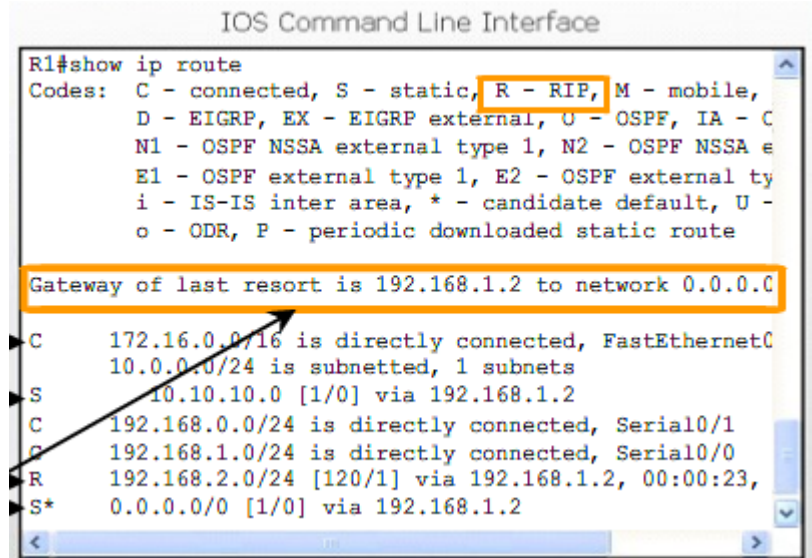
Cette table de routage correspond au routeur du milieu dans le réseau ci-dessous.



Par exemple, pour atteindre le réseau 192.168.1.0, le routeur central devra transmettre le message à l'adresse 100.0.0.1 via l'interface Eth1 et devra franchir 1 autre routeur avant d'arriver à destination.

4.3. Types de routes.

Une table de routage peut contenir différents types de routes. Elles sont classées en 4 grandes catégories. La table de routage ci-dessous présente ces catégories.



```

IOS Command Line Interface
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile,
       D - EIGRP, EX - EIGRP external, U - OSPF, IA - C
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA e
       E1 - OSPF external type 1, E2 - OSPF external ty
       i - IS-IS inter area, * - candidate default, U -
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/
    10.0.0.0/24 is subnetted, 1 subnets
S    10.10.10.0 [1/0] via 192.168.1.2
C    192.168.0.0/24 is directly connected, Serial0/1
C    192.168.1.0/24 is directly connected, Serial0/0
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:23,
S*   0.0.0.0/0 [1/0] via 192.168.1.2
  
```

Routes directement connectées (C) : Il s'agit des réseaux directement reliés au routeur.

Routes statiques (S) : Ce sont des routes programmées manuellement, en indiquant l'adresse et le masque de destination, ainsi que la passerelle correspondant.

Routes dynamiques (R) ou (O) ou (D) : Ces routes ont été envoyées au routeur par les routeurs voisins. Il peut ainsi apprendre la configuration du réseau en échangeant avec ses voisins. Il existe différents protocoles dynamique, parmi lesquels on peut citer RIP, OSPF, BGP.

Route par défaut (S*) : La route par défaut est un type de route statique qui spécifie une passerelle à utiliser lorsque la table de routage ne contient pas de chemin vers le réseau de destination.

Si le routeur ne trouve pas de route correspondant à l'adresse de destination et qu'il ne possède pas de route par défaut, le message est tout simplement détruit. L'expéditeur est alors informé par un message icmp.

Un routeur contient la plupart du temps ces 4 types de routes simultanément.

5. Mécanisme de décision.

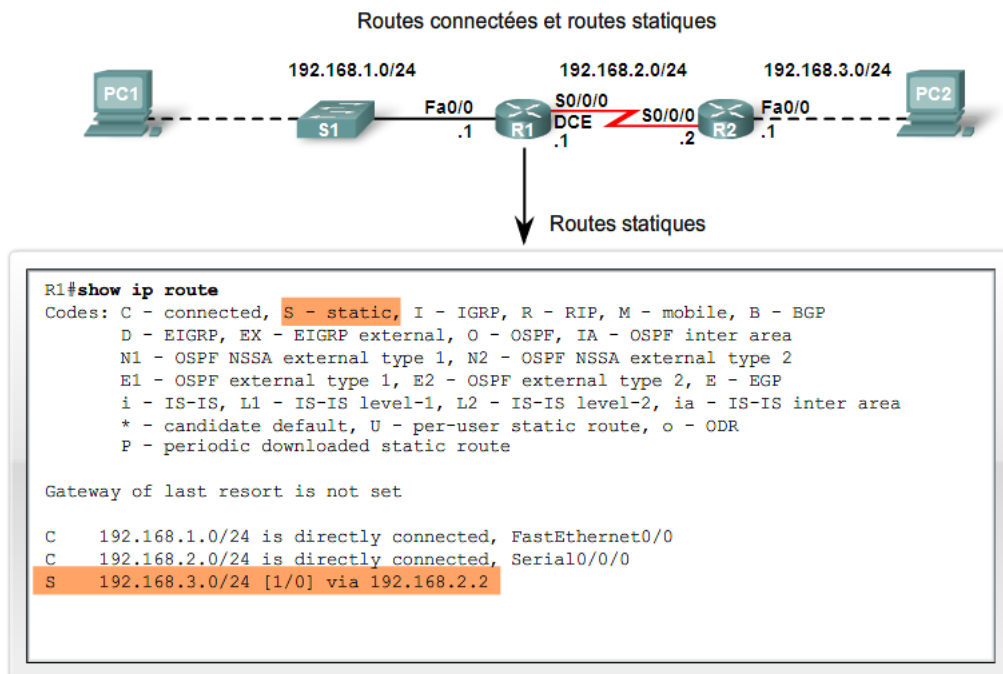
1. Chaque routeur prend sa décision tout seul, en fonction des informations disponibles dans sa table de routage.
2. Le fait qu'un routeur dispose de certaines informations dans sa table de routage ne signifie pas que les autres routeurs ont les mêmes informations.
3. Les informations de routage concernant un chemin menant d'un réseau à un autre ne fournissent aucune information sur le chemin inverse ou le chemin de retour.

6. Routage statique

6.1. Quand utiliser les routes statiques ?

Les routes statiques doivent être utilisées dans les cas suivants :

- **Un réseau ne comporte que quelques routeurs.** Dans ce cas, l'utilisation d'un protocole de routage dynamique ne présente aucun bénéfice substantiel. Au contraire, le routage dynamique risque d'accroître la charge administrative.
- **Un réseau est connecté à Internet par le biais d'un seul FAI.** Il n'est pas nécessaire d'utiliser un protocole de routage dynamique sur ce lien car le FAI représente le seul point de sortie vers Internet.
- **Un réseau de grande taille est configuré dans une topologie Hub and Spoke.** Une topologie Hub and Spoke est constituée d'un emplacement central (le concentrateur ou « Hub ») et de multiples terminaisons (les rayons ou « spokes »), chaque rayon ayant une seule connexion au concentrateur.



Remarque importante :

Si une route est défectueuse, le routeur continue à vouloir l'utiliser. C'est une des limites du routage statique.



7. Routage dynamique.

Dès que le réseau atteint une certaine taille (avec plusieurs routeurs), il est nécessaire de mettre en œuvre un routage dynamique. Les protocoles de routage dynamique sont utilisés par les routeurs pour partager des informations sur l'accessibilité et l'état des réseaux distants. Les protocoles de routage dynamique effectuent plusieurs tâches, notamment :

- détection de réseaux.
- mise à jour et maintenance des tables de routage.

7.1. Détection automatique de réseaux

Concrètement, les routeurs s'échangent leurs tables et établissent un « meilleur chemin » s'il en existe plusieurs. Ce meilleur chemin dépend du protocole utilisé (voir plus loin).

7.2. Maintenance des tables de routage

Après la découverte initiale des réseaux, les protocoles de routage dynamique les mettent à jour et les gèrent dans leurs tables de routage. Les protocoles de routage dynamique déterminent également un nouveau meilleur chemin si le chemin initial devient inutilisable (ou si la topologie change).

7.3. Protocoles de routage IP

Il existe plusieurs protocoles de routage dynamique IP. Voici quelques-uns des protocoles de routage dynamiques les plus répandus en matière de routage des paquets IP :

- protocole RIP (Routing Information Protocol)
- protocole IGRP (Interior Gateway Routing Protocol)
- protocole EIGRP (Enhanced Interior Gateway Routing Protocol)
- protocole OSPF (Open Shortest Path First)
- protocole IS-IS (Intermediate System-to-Intermediate System)
- protocole BGP (Border Gateway Protocol)

7.4. Meilleur chemin et métrique.

La détermination du meilleur chemin d'un routeur implique d'évaluer plusieurs chemins menant au même réseau de destination et de choisir le chemin optimal ou « le plus court » pour atteindre ce réseau.

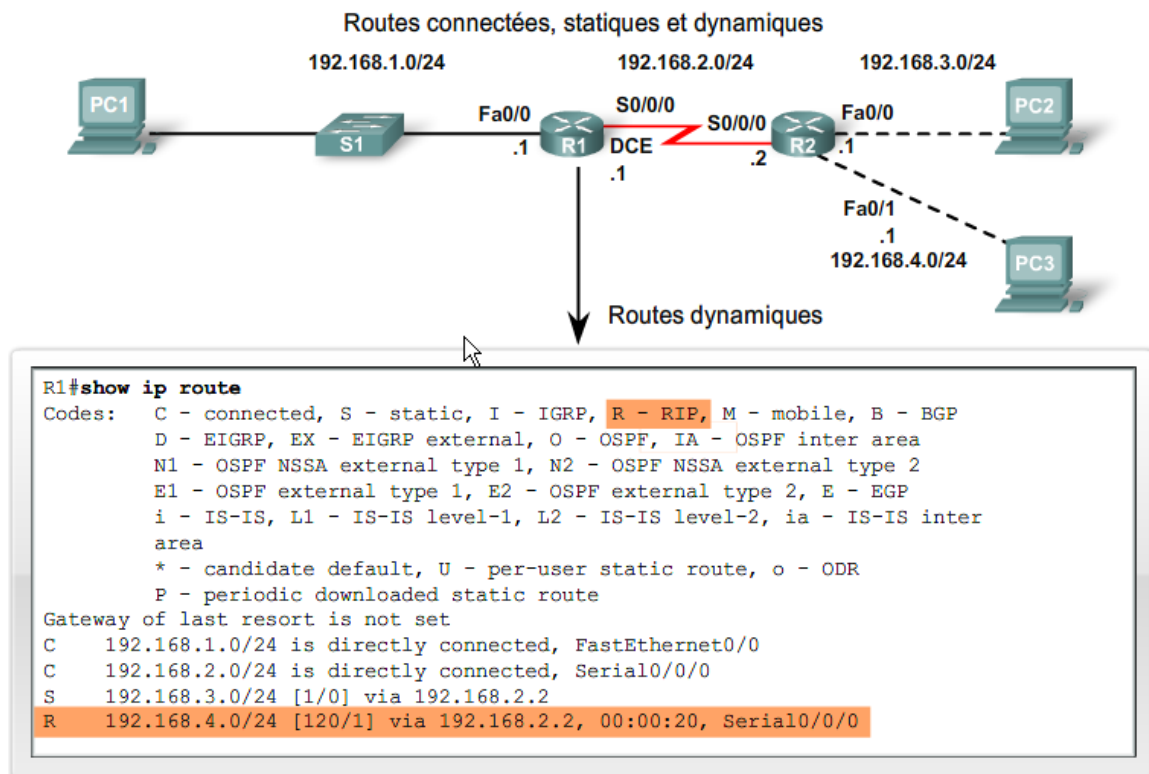
Le meilleur chemin est sélectionné par un protocole de routage, qui utilise une valeur ou une métrique pour déterminer la distance à parcourir pour atteindre un réseau.

Protocoles à vecteur de distance.

Certains protocoles de routage, tels que le protocole RIP, se basent sur le nombre de sauts simples, qui représente le nombre de routeurs entre un routeur et le réseau de destination.

Protocoles à état de liens.

Pour relier un routeur au réseau de destination, d'autres protocoles de routage, tels que le protocole OSPF, déterminent le chemin le plus court en examinant la bande passante des liens et en utilisant ceux dont la bande passante est la meilleure.



Dans l'illustration ci-dessous la route dynamique déclarée utilise le protocole RIP. L'indication entre crochets [120/1] est décomposée comme suit :

Le premier nombre représente la Distance Administrative ou fiabilité du protocole utilisé (120 pour RIP).

Le second chiffre est la métrique. Ici, 1 seul routeur sépare R1 de PC3.

Les tableaux ci-dessous présentent les distances administratives et le coût (métrique) de chaque liaison.

Origine de la route	Distance administrative	Mesure(s) par défaut
Connecté	0	0
Statique	1	0
Résumé du routage EIGRP	5	
Protocole BGP externe	20	Valeur attribuée par l'administrateur
Protocole EIGRP interne	90	Bande passante, délai
Protocole IGRP	100	Bande passante, délai
Protocole OSPF	110	Coût de la liaison (bande passante)
Protocole de routage IS-IS	115	Coût de la liaison (valeur attribuée par l'administrateur)
Protocole RIP	120	Nombre de sauts
Protocole EIGRP externe	170	
Protocole BGP interne	200	Valeur attribuée par l'administrateur

Tableau des distances administratives

Medium	Coût
Ligne série 56kbps	1785
T1 (ligne série 1544kbps)	64
E1 (ligne série 2048kbps)	48
Token Ring 4 Mbps	25
Ethernet	10
Token Ring 16Mbps	6
Fast Ethernet 100Mbps, FDDI	1

Tableau des coûts OSPF

Pour simplifier, l'algorithme SPF fait la somme des coûts à partir de lui-même vers tous les réseaux de destination. S'il y a plusieurs chemins possibles vers une destination, celle qui a le coût le plus faible est choisie. Par défaut, OSPF inscrit quatre routes équivalentes dans sa table de routage pour permettre la répartition de charge (*Load Balancing*).

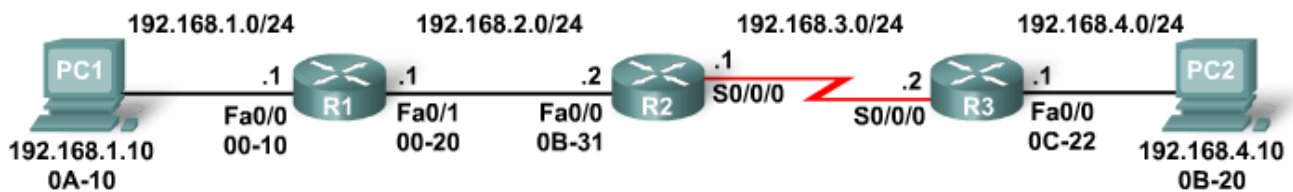
8. Fonction de commutation.

Que fait un routeur d'un paquet qu'il a reçu d'un réseau et qui est destiné à un autre réseau ? Le routeur effectue les trois étapes principales suivantes :

1. Il décapsule le paquet de couche 3 en supprimant l'en-tête et la queue de bande de la trame de couche 2.
2. Il examine l'adresse IP de destination du paquet IP pour trouver le meilleur chemin dans la table de routage.
3. Il encapsule le paquet de couche 3 dans une nouvelle trame de couche 2 et transfère la trame à l'interface de sortie.

Il est fort possible que le paquet soit encapsulé dans un type de trame de couche 2 différent de celui dans lequel il a été reçu. Par exemple, le paquet peut être reçu par le routeur sur une interface FastEthernet, encapsulé dans une trame Ethernet et transféré d'une interface série encapsulé dans une trame PPP.

L'illustration ci-dessous présente un chemin qui utilisera des liaisons Ethernet et Série.



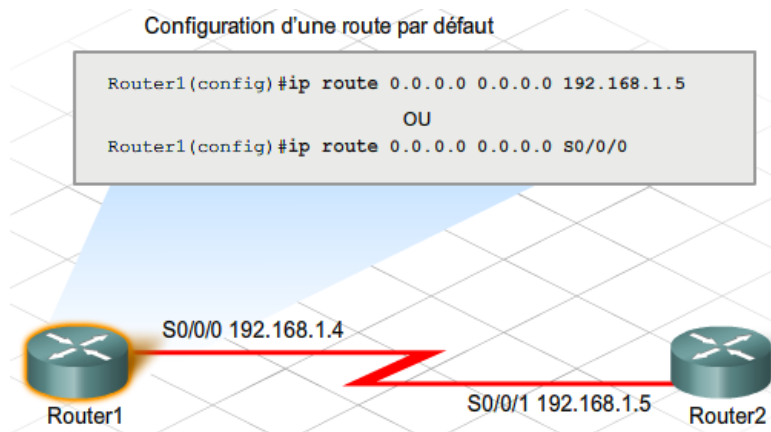
Dans tous les cas, les adresses IP Source et Destination ne changent pas.

9. ANNEXE : Commandes de bases pour le routage

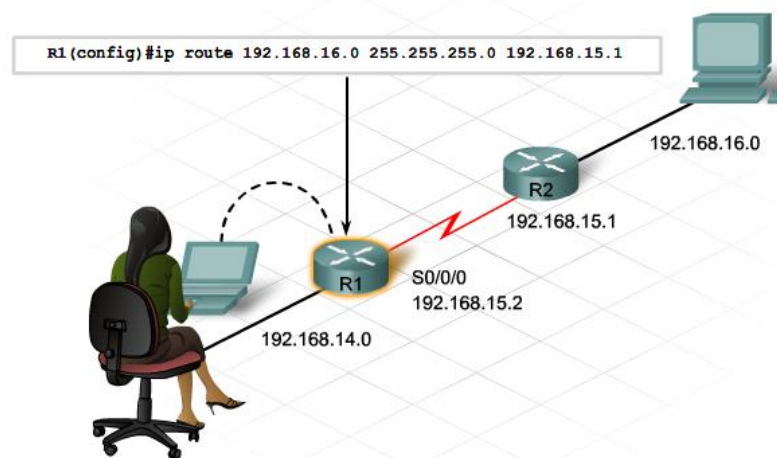
On considère que les interfaces sont correctement configurées et fonctionnelles.

9.1. Routage statique.

9.1.1. Configuration d'une route par défaut.



9.1.2. Configuration d'une route statique.



9.1.3. Activation du routage.

```
Router(config)#iprouting
```

9.1.4. Vérifier la table de routage.

```
Router# show ip route
```

La lettre C devant une route indique un réseau directement connecté.

La lettre S indique une route statique.

Le symbole * indique la route par défaut (si elle est déclarée).

9.2. Routage RIP.

9.2.1. Configuration de base.

RIP est un protocole à vecteur de distance courant, pris en charge par la plupart des routeurs. Il s'agit d'un choix approprié pour les petits réseaux dotés de plusieurs routeurs.

Pour la configuration la plus basique du protocole RIPv2, trois commandes sont à retenir :

<code>Router(config)# router rip</code>	Active le routage RIP
<code>Router (config-router)# version 2</code>	Spécifie la version (1 ou 2)
<code>Router(config-router)# network [numéro_réseau]</code>	Déclare les réseaux qui seront transmis
<code>Router(config)# ip default-network [numéro_réseau]</code>	Permet de faire propager une destination par défaut

9.2.2. Vérifications.

`Router# show ip route`

Affiche la table de routage

La lettre C devant une route indique un réseau directement connecté.

La lettre S indique une route statique.

La lettre R indique une route découverte grâce au protocole RIP.

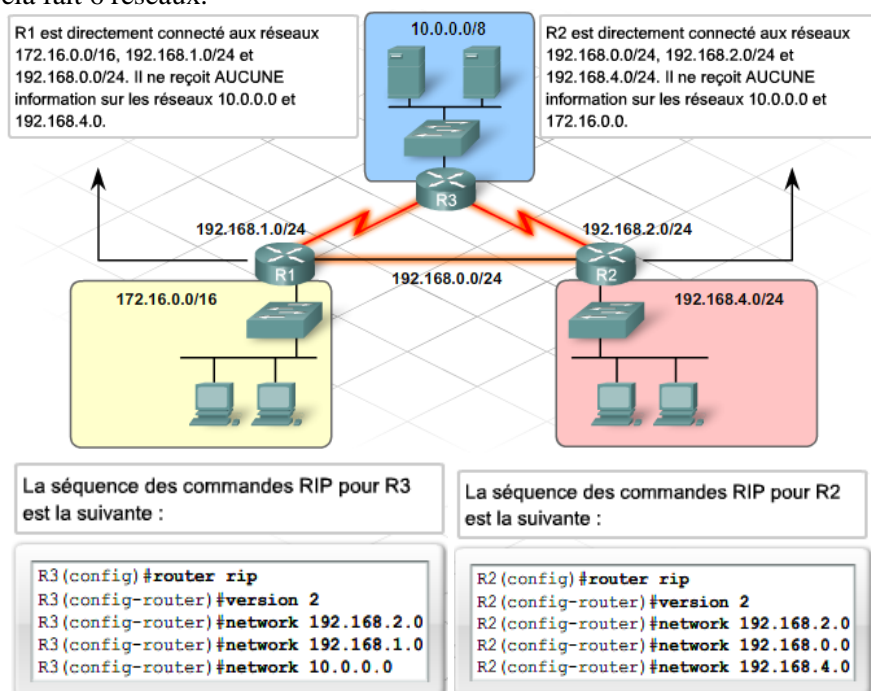
Le symbole * indique la route par défaut (si elle est déclarée).

La commande **show ip protocols** vérifie que le routage RIP est configuré, que les interfaces correctes envoient et reçoivent des mises à jour RIP et que le routeur annonce les réseaux appropriés.

La commande **debug ip rip** peut être utilisée pour observer les réseaux annoncés dans les mises à jour de routage à mesure que celles-ci sont envoyées et reçues. A utiliser avec parcimonie...

9.2.3. Exemple

Dans cette configuration, chaque routeur est connecté à un réseau local. En plus des réseaux inter-routeurs, cela fait 6 réseaux.



9.3. Routage OSPF.

9.3.1. Activation du routage.

OSPF est activé à l'aide de la commande de configuration globale **router ospf process-id**. Le process-id (id de processus) est un nombre compris entre 1 et 65535 choisi par l'administrateur réseau. Le **process-id** n'a qu'une signification locale, ce qui veut dire qu'il n'a pas à correspondre à celui des autres routeurs OSPF.

```
R1(config)#router ospf 1
R1(config-router)#
```

Il faut ensuite déclarer les réseaux participants par la commande

Router(config-router)# network réseau masque-generique area

Vous noterez que le masque est différent de ceux habituellement utilisés : il s'agit du **masque générique**. Pour simplifier, c'est l'inverse du masque normal.

Le champ **area** fait référence à la zone OSPF. Une zone OSPF est un groupe de routeurs qui partagent les informations d'état de liens.

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

Pour que l'OSPF fonctionne de manière appropriée, il est essentiel de définir la bande passante des interfaces séries.

Exemple: La bande passante d'une liaison série à 64kbits/s

```
Router(config)# interface serial 0/0
Router(config-if)# bandwidth 64
```

L'instruction de configuration suivante propagera la route par défaut à tous les routeurs situés dans la zone OSPF :

Router(config-router)# default-information originate

9.3.2. Vérifications.

Router# show ip route

Affiche la table de routage

La lettre C devant une route indique un réseau directement connecté.

La lettre S indique une route statique.

La lettre O indique une route découverte grâce au protocole OSPF.

Le symbole * indique la route par défaut (si elle est déclarée).

La commande **show ip ospf neighbor** peut être utilisée pour vérifier et réparer les relations de voisinage OSPF.