Licence Professionnelle

Ingénierie des Systèmes Informatiques et Logiciels (ISIL)

ADMINISTRATION SYSTÈME ET RÉSEAUX

Pr. Said BENKIRANE

A.U: 2017/2018

Partie 1: Généralités sur les réseaux

- Introduction aux réseaux informatiques (topologie et classification des réseaux).
- Le modèle OSI & TCP/IP.
- Adressage, Routage, commutation dans les réseaux.

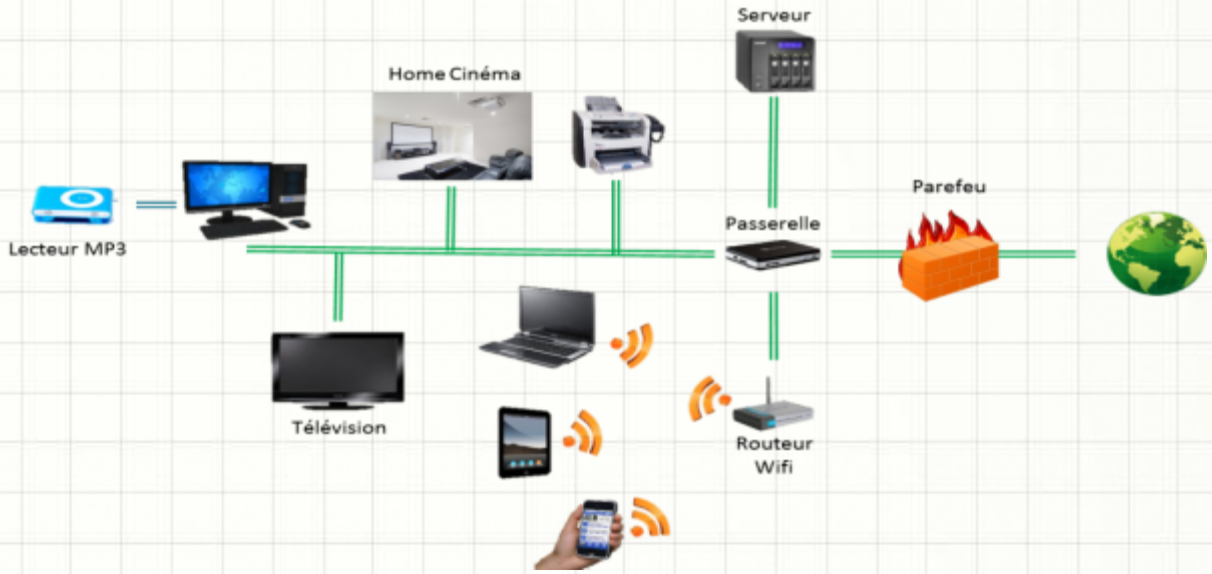
Partie 2: Administration des systèmes

- Environnement Windows Server
- Environnement Linux
- Configuration de services sous Windows et Linux

AD, Comptes (Utilisateurs, PC), GPO,
DNS, DHCP, IIS, Apache, HTTP,
Virtualisation,…

Partie 3: Introduction aux outils et méthodes de sécurisation

- Sécurité des réseaux (Firewall…)
- Notion de base de cryptologie : chiffrement symétrique, asymétrique, signature numérique, ...



Tâches de l'administrateur réseaux

Tâches de l'Administrateur Sys et Réseaux :

- Gestion du câblage réseau (connexion physique entre plusieurs machines).
- Gestion du routage (connexion logique entre l'intérieur et l'extérieur du réseau ou entre plusieurs sous-réseaux).
- Gestion de la sécurité (protection antivirale, pare-feu, prévention des intrusions etc.)
- Gestion des droits d'accès des utilisateurs (accès au réseau, etc.)
- Partage des ressources (dossiers, imprimantes…).

Tâches de l'Administrateur Sys et Réseaux :

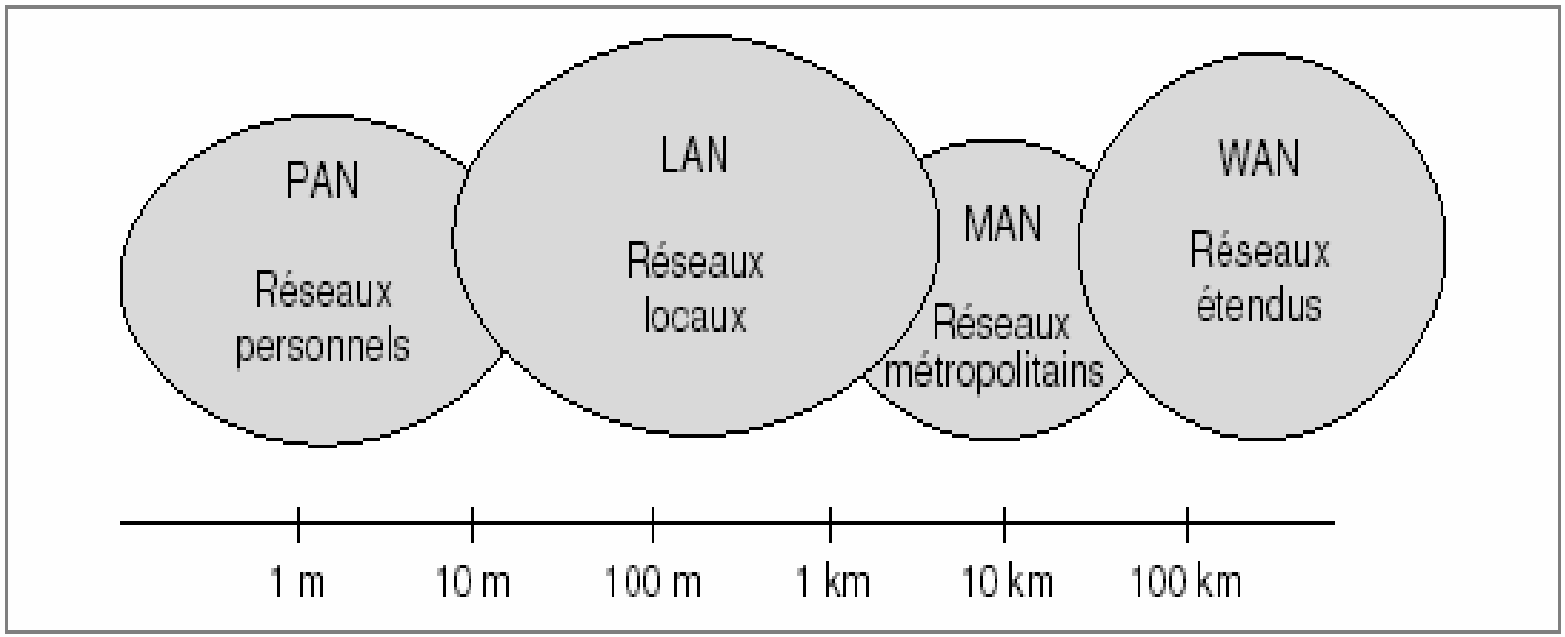
- Installation et paramétrage des équipements et logiciels réseaux et télécoms
- Supervision et dépannage des systèmes et applications réseaux
- Conduite et participation à des projets relevant de son périmètre
- Gestion de la sécurité en l'absence de RSSI ou d'ingénieur dédié
- Déploiement et gestion des terminaux mobiles

Les compétences requises sont :

- Connaissances matérielles (hardware)
- Couches du modèle OSI définissant les couches d'un réseau
- Protocoles de communication (TCP/IP étant le plus connu)
- Systèmes d'exploitation PC, serveurs et routeurs(IOS), (Windows, Linux, Unix…)
- Réseaux (protocoles, routage, virtualisation, Wi-Fi…)
- Sécurité (contrôle d'accès, pare-feu, supervision…)
- Téléphonie sur IP
- Stockage (SAN, NAS, réplication…)

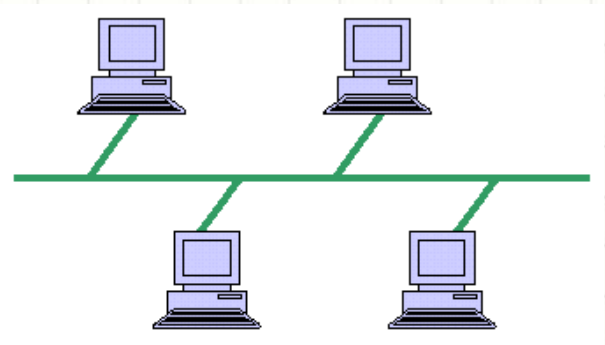
Partie 1
Généralités sur les réseaux

Classification des réseaux

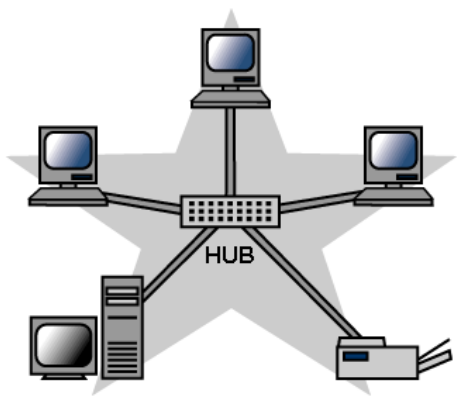


PAN : Personal Area Network
LAN : Local Area Network
MAN : Metropolitan Area Network
WAN : Wide Area Network

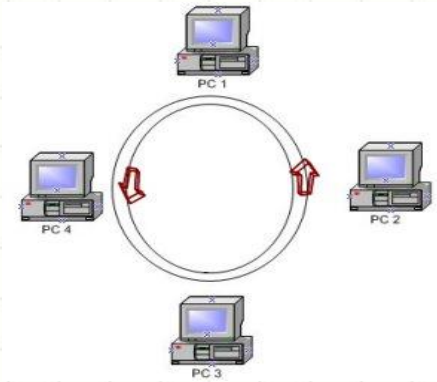
Topologie



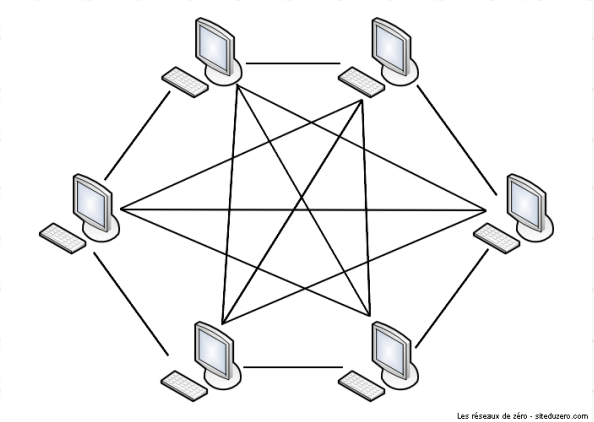
Topologie en bus



Topologie en étoile



Topologie en anneau



Topologie maillée

Les composants d'un réseau

- **Les équipements terminaux** (ordinateurs, stations, serveurs, téléphones, PDA, périphériques, machines hôtes, etc.)
- **Les supports de communication** (câbles, fibres, faisceaux, liaisons physiques, lignes de transmission, médium, etc.).
- **Les équipements d'interconnexion** (nœuds, routeurs, ponts, passerelles, etc.).

Les supports de communication:

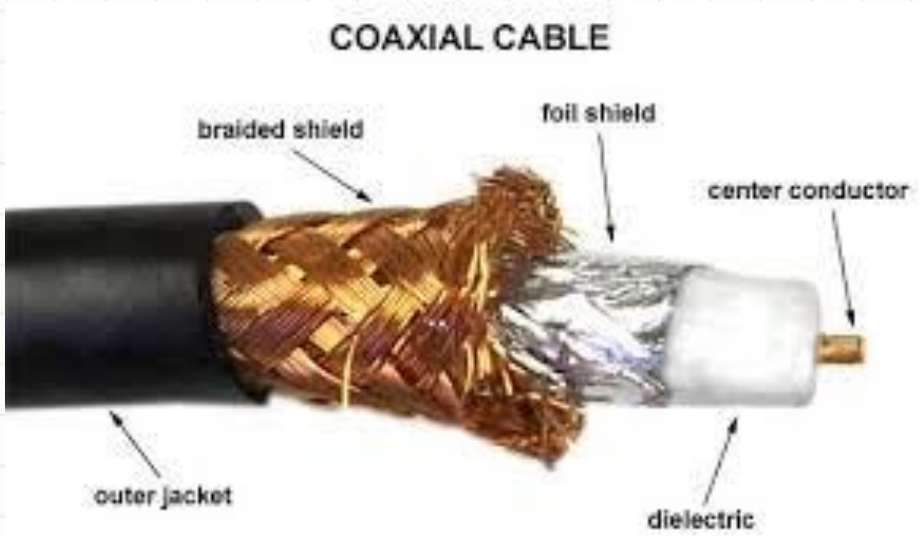
1) Paires torsadées

C’est le même câble utilisé pour les téléphones. Il existe des câbles à 2 ou 4 paires mais aussi des câbles blindés (STP) ou non blindés (UTP). Défini dans la norme **10 base T**, ce type de câbles est utilisé pour du câblage dit universel mais aussi pour les réseaux token ring (anneau à jeton) ou étoile.
C’est une solution économique mais limitée. La paire torsadée ne permet pas une grande vitesse de transmission de l’information et elle est en outre très sensible à l’environnement électromagnétique.

Les supports de communication:

2) Câble coaxial

Proche du câble qui relie le téléviseur à son antenne, le câble coaxial est composé d'un câble central entouré d'un isolant, lui-même recouvert d'une tresse métallique, elle-même recouverte d'un isolant. Il permet des vitesses de transmission bien plus élevées que la paire torsadée et des connexions à plus grande distance. Il reste néanmoins assez coûteux.



Les supports de communication:

3) Fibre optique

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données et de lumière. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peut servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longue distance et à des débits jusqu'alors impossibles,

Les supports de communication:

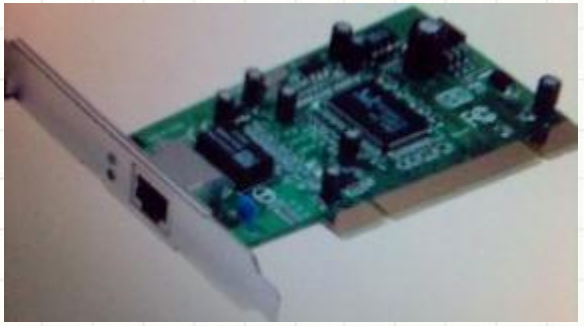
4) Les ondes électromagnétiques (faisceaux hertziennes)

Elles supportent de grande distance et de grandes capacités, pour une propagation en visibilité directe (entre 50 et 80 km). Elles prolongent et remplacent les câbles, pour une plus grande souplesse mais aussi une plus grande sensibilité au bruit.

Composants d'interconnexion des réseaux

1) La carte réseau

La carte réseau constitue l'interface physique entre l'ordinateur et le support de communication.
Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau (**NIC**).



2) Le concentrateur

Le concentrateur appelé **hub** en anglais est un équipement physique à plusieurs ports. Il sert à relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données reçues sur un port et les diffuser bêtement sur l'ensemble des ports.

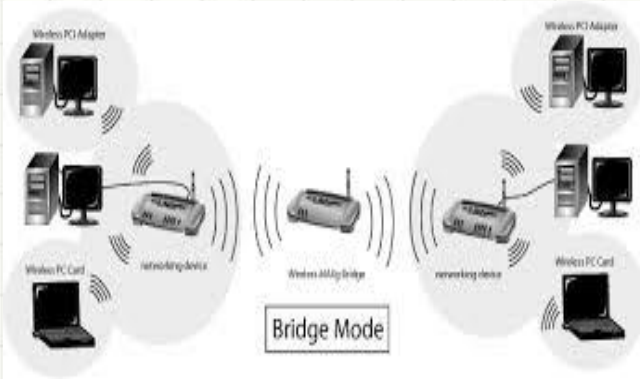
3) Le répéteur

Le répéteur appelé **repeater** en anglais, est un équipement qui sert à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de type différents.

Composants d'interconnexion des réseaux

4) Le pont

Le pont appelé **bridge** en anglais est un équipement qui sert à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est en mesure d'identifier l'émetteur et le récepteur ; comme ça il dirige la trame directement vers la machine destinataire.



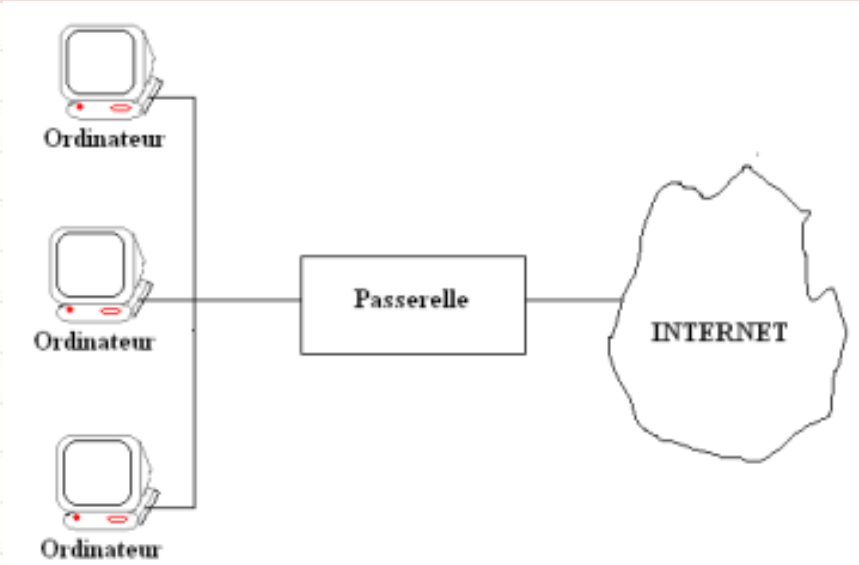
5) le commutateur

Le commutateur appelé **switch** en anglais, est un équipement multiport comme le concentrateur. Il sert à relier plusieurs équipements informatiques entre eux. Sa seule différence avec le hub, c'est sa capacité de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination.

Composants d'interconnexion des réseaux

6) La passerelle

La passerelle appelée **gateway** est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différents ; comme par exemple un réseau local et internet. Lorsque un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseaux a défini, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.



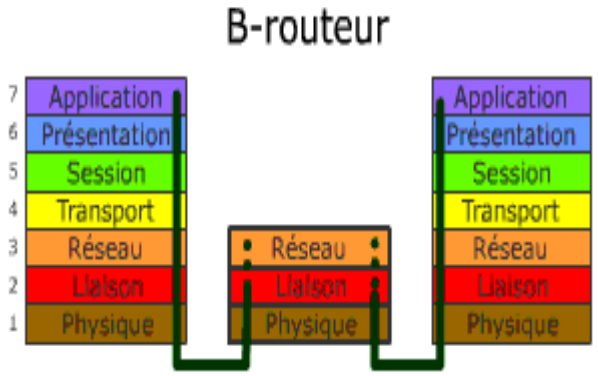
Composants d'interconnexion des réseaux

7) Le routeur

Le routeur (**Router**) est un matériel de communication de réseau informatique qui a pour rôle d'assurer l'acheminement des paquets, le filtrage et le control du trafic. Le terme router signifie emprunter une route.

8) Pont routeur ou B-routeur

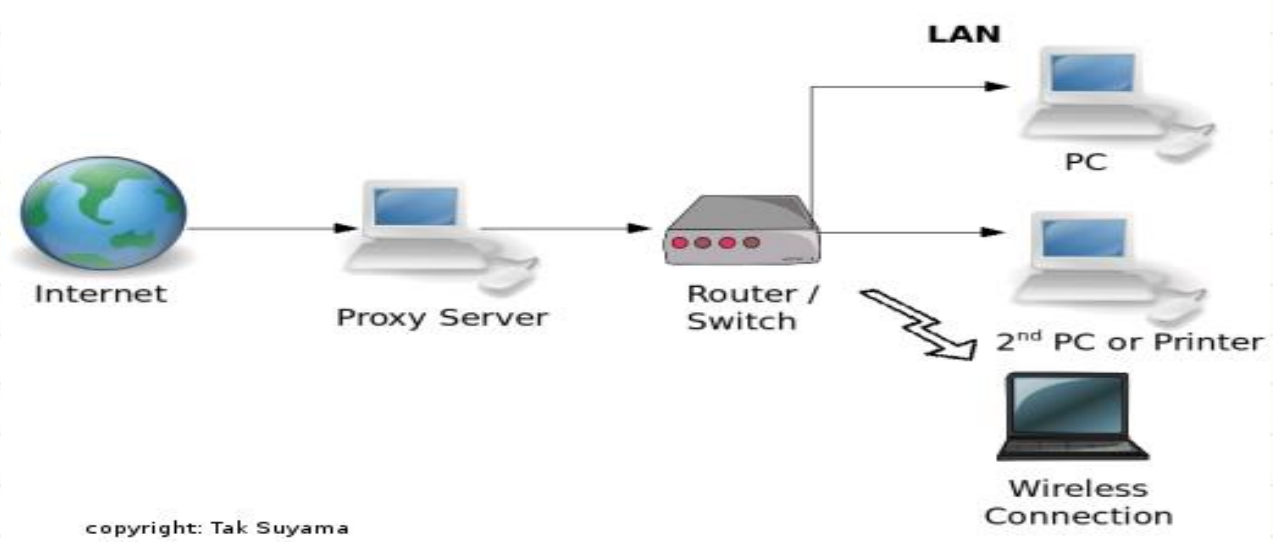
Le B-routeur se comporte à la fois comme un pont et un routeur. Si le protocole n'est pas routable, le B-routeur est capable de se replier vers un niveau inferieur et se comporter comme un pont. Dans le cas contraire, le B-routeur joue le rôle d'un routeur.



Composants d'interconnexion des réseaux

9) Proxy

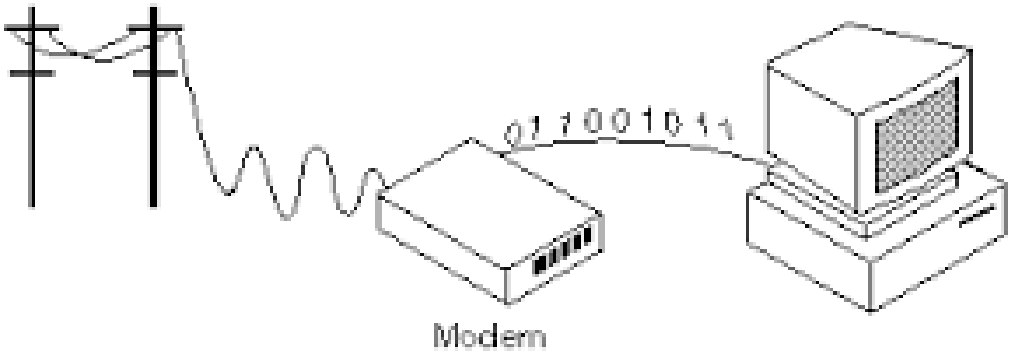
En réseau informatique, un proxy appelé serveur proxy ou serveur mandataire est souvent une machine et/ou logiciel servant de liaison entre une machine cliente et le serveur. La plupart des cas, le serveur proxy est utilisé entre un réseau local et internet. Le rôle principal d'un proxy est d'assurer l'accélération de la navigation, la journalisation des requêtes, la sécurité du réseau local, le filtrage et l'anonymat. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).



Composants d'interconnexion des réseaux

10) Le modem

Le modem (modulateur-démodulateur) est un équipement qui sert à lier le réseau téléphonique au réseau informatique. Souvent pour transmettre des données informatiques à distance, on utilise la ligne téléphonique comme support de transmission. Et comme nous savons que la ligne téléphonique ne transporte que des signaux analogiques et que les réseaux informatiques n'utilisent que des signaux numériques, le modem a pour rôle de convertir le signal numérique en signal analogique et vis versa. Le modem utilise donc les techniques de modulation et de démodulation.



Les modèles OSI et TCP/IP

Généralement, un modèle dans le sens de **“norme”** est une façon d’ordonner ou de classifier un ensemble d’élément. Dans notre cas, **les modèles OSI et TCP/IP** permettent de classifier et d’ordonner les protocoles et les standards de communication entre les machines. On parle parfois également de ***modèle en couche*** où chaque couche possède sa place et sa relation propre avec les couches adjacentes.

Le modèle OSI

Le modèle OSI (Open System Interconnexion) a été créé en 1977 afin d'éviter que chaque fournisseur de solution IT (réseaux et systèmes) ne fournisse sa propre implémentation du protocole lié à un service. **L'ISO** (International Standards Organisation) a donc décrit le modèle OSI pour qu'il corresponde à un grand panel d'implémentation sans favoriser un constructeur particulier.

Le modèle OSI

N°	Nom	Description
7	Application	Communication avec les logiciels
6	Présentation	Gestion de la syntaxe
5	Session	Contrôle du dialogue
4	Transport	Qualité de la transmission
3	Réseau	Sélection du chemin
2	Liaison de données	Préparation de l'envoi sur le média
1	Physique	Envoi sur le média physique

Figure 1- Les 7 couches du modèle OSI

Les 7 couches du modèle OSI

Couche 1 : Couche physique

La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

Couche 2 : Couche liaison de donnée

La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

- La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).
- La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

Couche 3 : Couche réseau

Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.

Les 7 couches du modèle OSI

Couche 4 : Couche transport

La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.

Couche 5 : Couche session

La couche session établit, gère et ferme les sessions de communications entre les applications.

Couche 6 : Couche présentation

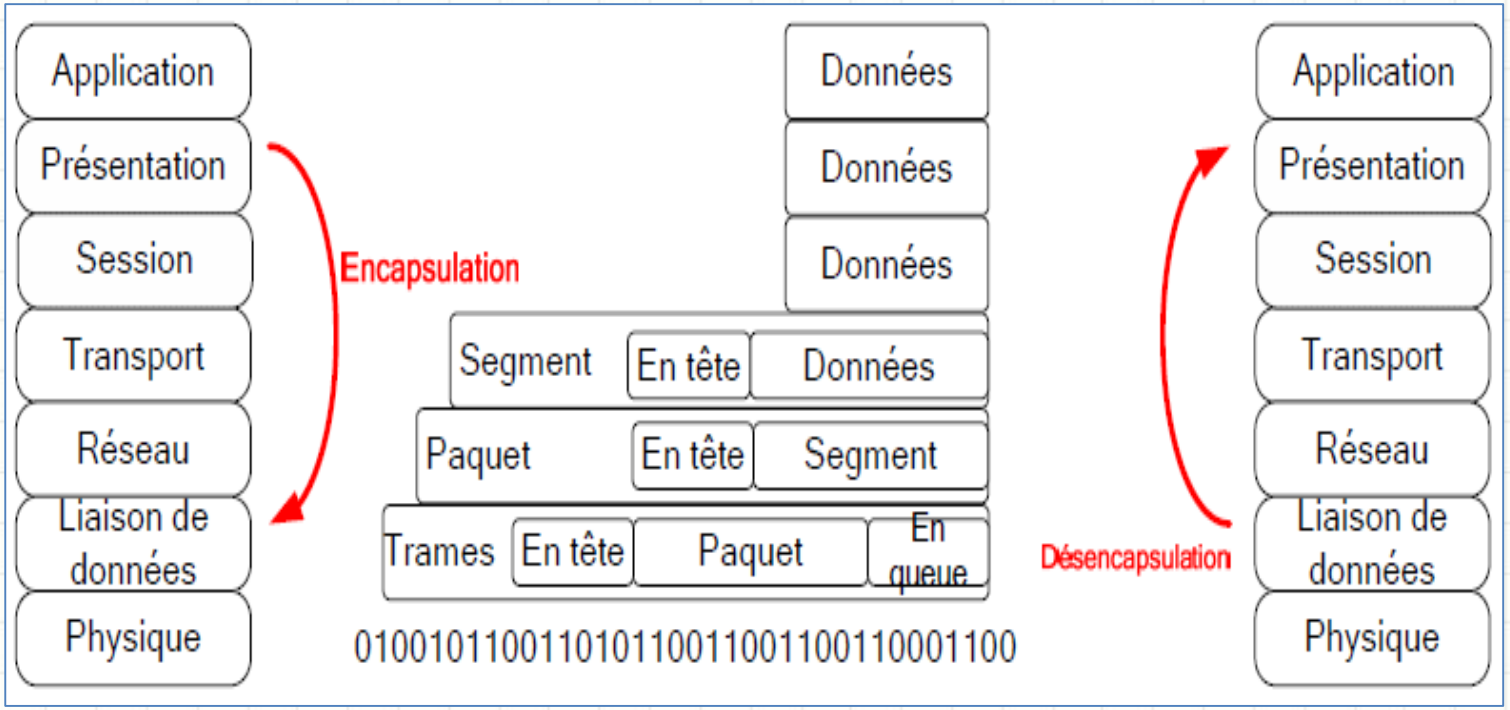
La couche présentation spécifie les formats des données des applications (Formatage, compression, cryptage).

Couche 7 : Couche application

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

Les 7 couches du modèle OSI

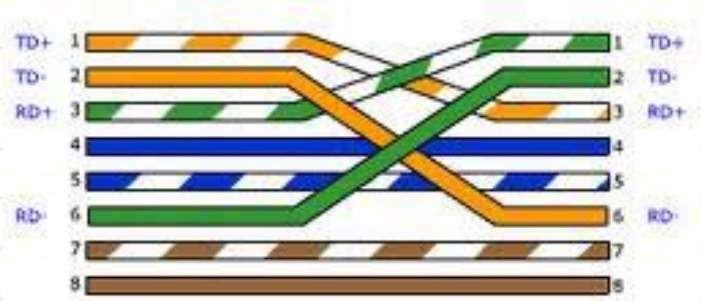
Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation



Encapsulation : processus de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.

Le modèle TCP/IP

Le modèle TCP/IP est nommé ainsi car les protocoles de communications TCP et IP y sont les éléments dominants. Il faut noter que les protocoles TCP et IP ont été inventés bien avant le modèle qui porte leur nom et également bien avant le modèle OSI. Le modèle TCP/IP a été construit suite aux travaux du département de la défense américaine (DoD) sur le réseau ARPANET, l'ancêtre d'internet, et sur le mode de communication numérique via des datagrammes.



Le modèle TCP/IP

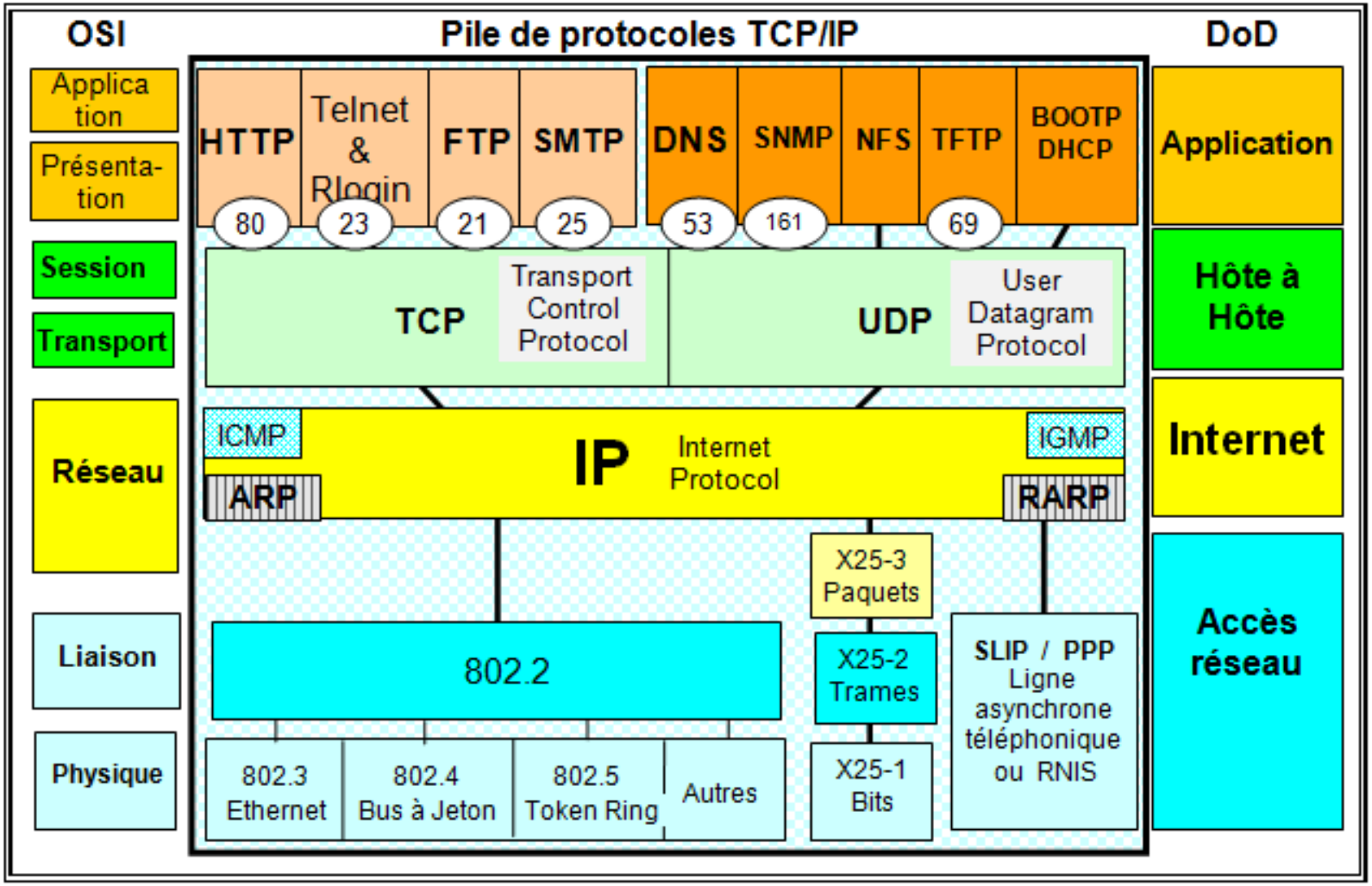
TCP/IP est conçue pour répondre à un certain nombre de critères parmi lesquels :

- **Masquer l'hétérogénéité matériel et logiciel**
- **Le fractionnement des messages en paquets ;**
- **L'utilisation d'un système d'adressage ;**
- **L'acheminement des données sur le réseau (routage) ;**
- **Le contrôle des erreurs de transmission de données.**

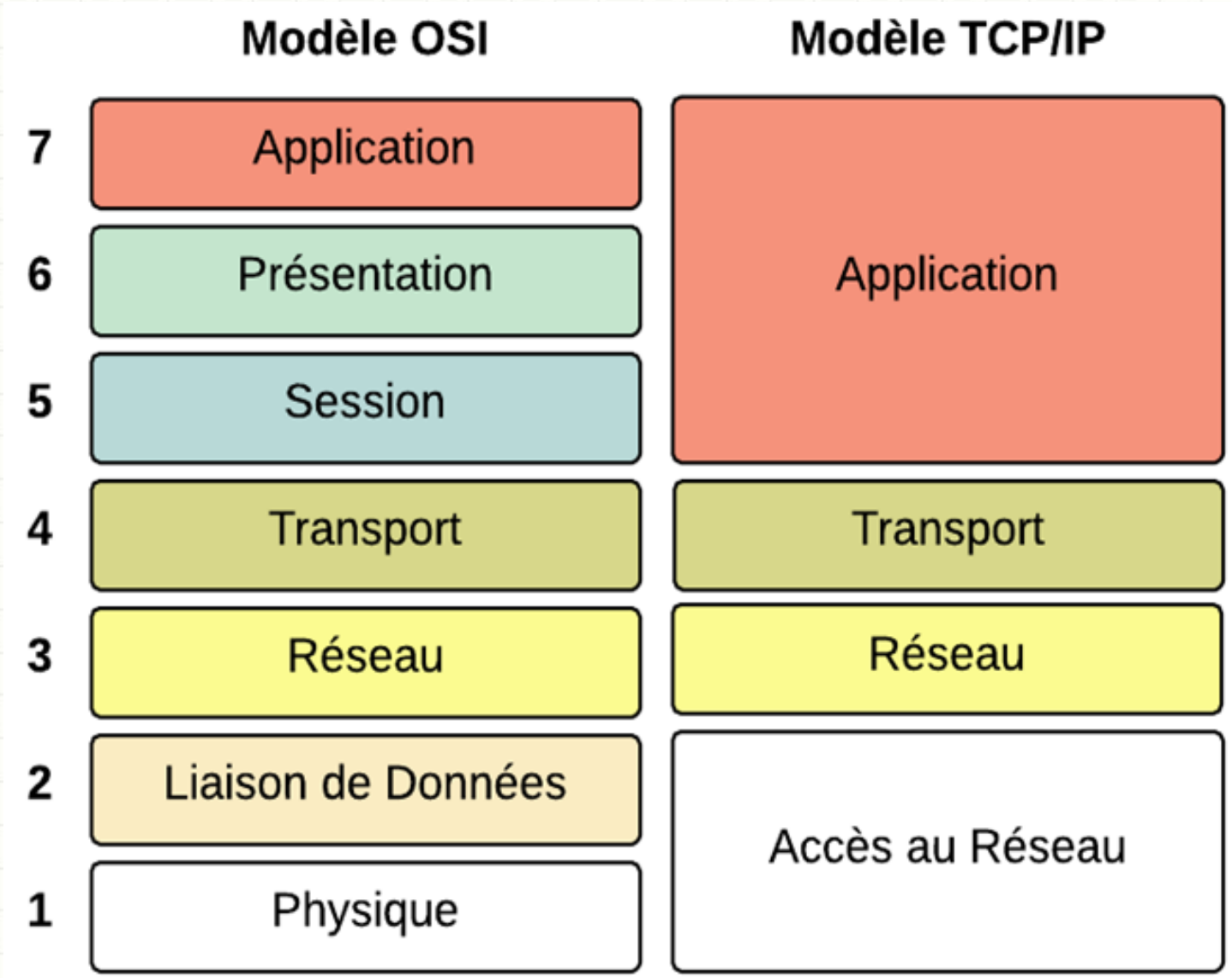
Le modèle TCP/IP

4	**Application** (data)	On trouve ici les protocoles « de haut niveau » qui sont associés à un service final comme le web (http/https), la messagerie (SMTP/POP/IMAP), le stockage de fichier (FTP/TFTP/…) ou le chiffrement (SSL) par exemple.
3	**Transport** (segment)	Responsable du bon acheminement des messages entre les machines et de l'optimisation des ressources réseaux.
2	**Réseau** (paquet)	La couche réseau s'occupe de déterminer le mode et la méthode d'acheminement entre plusieurs machines.
1	**Accès au réseau** (bits, trames)	Permet à un hôte d'envoyer des informations à un autre hôte, elle est la combinaison de la couche 1 et 2 du modèle OSI

Pile de Protocoles TCP/IP



Le modèle OSI & TCP/IP



Adressage IP V4

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (*Internet Protocol*), qui utilise des adresses numériques, appelées **adresses IP**, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, *194.153.205.26* est une adresse IP donnée sous une forme technique.

Une **adresse IP** est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :
une partie des nombres à gauche désigne le réseau est appelée **ID de réseau** (en anglais ***netID***),
Les nombres de droite désignent les ordinateurs de ce réseau est appelée **ID d'hôte** (en anglais ***host-ID***).

Adressage IP V4

Classes des adresses IP V4

Classe	Début en binaire	Valeurs	Identificateur de réseau	Identificateur d'hôte
A	0...	*1 à 126*	*a*	*b,c,d*
B	10...	*128 à 191*	*a,b*	*c,d*
C	110...	*192 à 223*	*a,b,c*	*d*
D	1110...	*224 à 239*	multicast	*a,b,c,d*
E	1111...	*240 à 255*	réservées	expérimental

Adressage IP V4

Espace d'adressage

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques

La répartition en pourcentages de l'espace total d'adressage IP est :

- Classes A - 50%
- Classes B - 25%
- Classes C - 12.5%
- Classes D - 6.25%
- Classes E - 6.25%

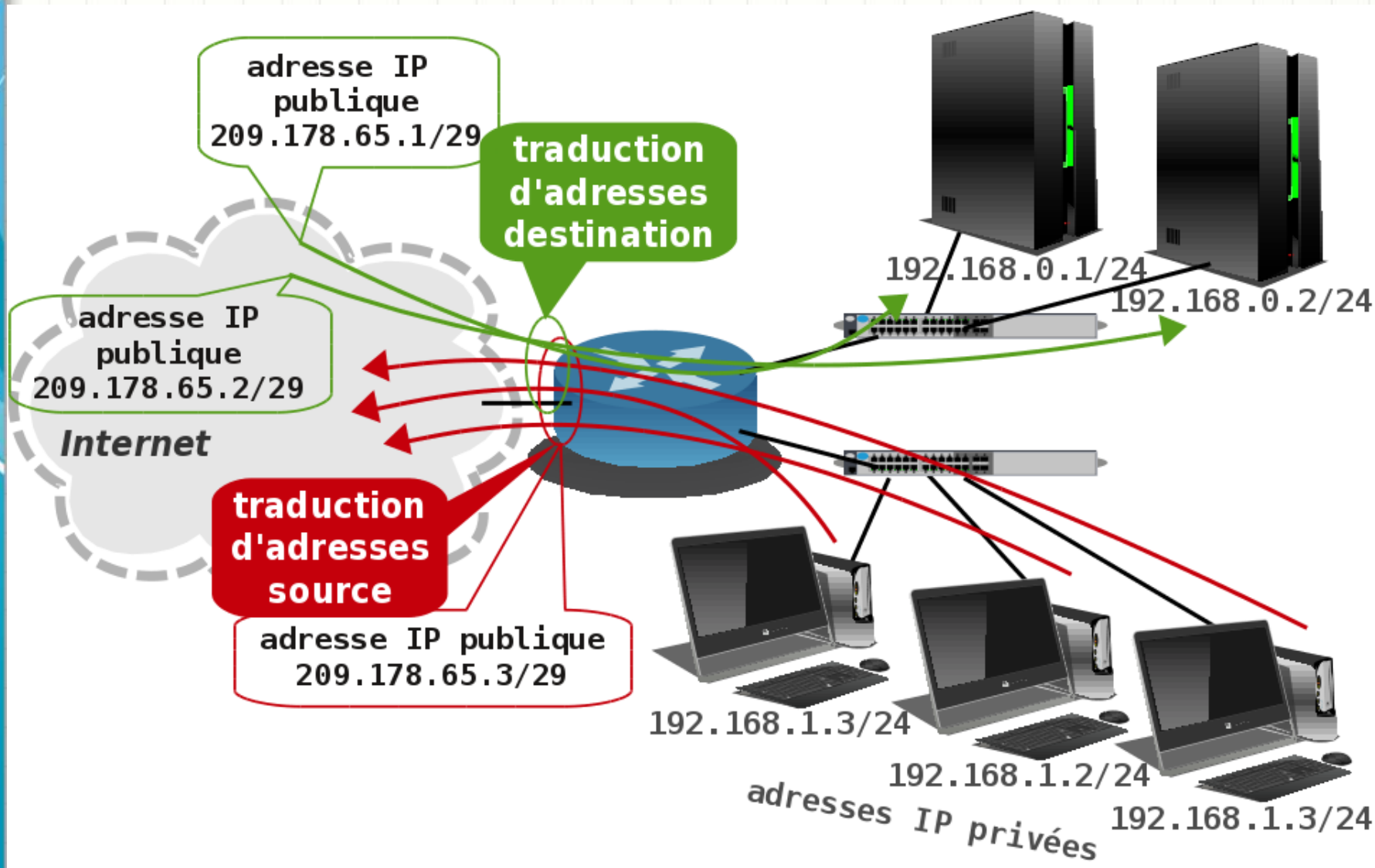
Adressage IP V4

Adresses IP V4 Réservées:

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	2^{24} = 16 777 216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	2^{20} = 1 048 576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	2^{16} = 65 536

L'administrateur est libre de diviser ces plages en sous-réseaux selon ses besoins.

Les réseaux privés & la traduction d'adresses (NAT)



Adresse MAC

Une **adresse MAC** (*Media Access Control*), parfois nommée **adresse physique**, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. A moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde.

Structure:

Une adresse MAC-48 est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret. Par exemple 5E:FF:56:A2:AF:15.

Adresses particulières

FF:FF:FF:FF:FF:FF	Adresse broadcast
01:00:0C:CC:CC:CC	Cisco Discovery Protocol
01:80:C2:00:00:00	Spanning Tree Protocol
33:33:xx:xx:xx:xx	Adresses multicast IPv6
01:00:5E:xx:xx:xx	Adresses multicast IPv4
00:00:0c:07:ac:xx	Adresses HSRP
00:00:5E:00:01:XX	Adresses VRRP

Sous-réseaux

Pourquoi créer des sous réseaux ?

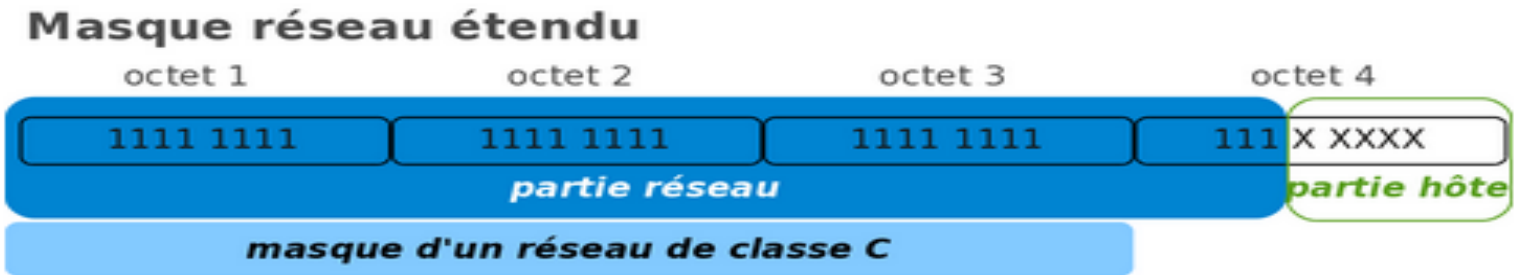
- **Utilisation de plusieurs media** (câbles, supports physiques).
- **Réduction de l'encombrement**.
- **Economise les temps de calcul**.
- **Isolation d'un réseau**.
- **Renforcement de la sécurité**.
- **Optimisation de l'espace réservé à une adresse IP**.

Masque de sous-réseau

Les masques de sous-réseaux (*subnet mask*) permettent de **segmenter un réseau en plusieurs sous-réseaux**. On utilise alors une partie des bits de l'adresse d'hôte pour identifier des sous-réseaux.

Le découpage d'une classe en sous-réseaux

la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0. Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254. Pour créer 8 sous réseaux: $8=2^3$, donc on fixe 3 bits de la partie host id,



Adresse réseau	192.168. 1. 0	Plage d'adresses utilisables	Adresse de diffusion
Masque de réseau	255.255.255.224		
Sous-réseau 0	192.168. 1. 0	192.168.1. 1 - 192.168.1. 30	192.168.1. 31
Sous-réseau 1	192.168. 1. 32	192.168.1. 33 - 192.168.1. 62	192.168.1. 63
Sous-réseau 2	192.168. 1. 64	192.168.1. 65 - 192.168.1. 94	192.168.1. 95
Sous-réseau 3	192.168. 1. 96	192.168.1. 97 - 192.168.1.126	192.168.1.127
Sous-réseau 4	192.168. 1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
Sous-réseau 5	192.168. 1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
Sous-réseau 6	192.168. 1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
Sous-réseau 7	192.168. 1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Adressage IP V4

Sous-réseaux:

Un administrateur gère un réseau 192.44.78.0/24. Il aimerait décomposer ce réseau en quatre sous-réseaux.

Pour cela, il réserve les deux premiers bits de l'identifiant machine pour identifier ses nouveaux sous-réseaux. Toute adresse IP d'un même sous-réseau aura donc 24 bits en commun ainsi que les deux bits identifiant le sous-réseau. Le masque de sous-réseau peut ainsi être codé de la façon suivante : 11111111.11111111.11111111.11000000 en binaire, ce qui correspondra à 255.255.255.192 en décimal. Les sous-réseaux seront :

192.44.78.0/26 (les adresses de 192.44.78.0 à 192.44.78.63)
192.44.78.64/26 (les adresses de 192.44.78.64 à 192.44.78.127)
192.44.78.128/26 (les adresses de 192.44.78.128 à 192.44.78.191)
192.44.78.192/26 (les adresses de 192.44.78.192 à 192.44.78.255)

62 adresses de chaque sous-réseau seront utilisables pour numéroter des interfaces.

Masque de sous-réseau variable (VLSM)

On parle de masque de sous-réseau variable (*variable-length subnet mask*, VLSM) quand un réseau est divisé en sous-réseaux dont la taille n'est pas identique, ceci permet une meilleure utilisation des adresses disponibles. Les protocoles de routage BGP, OSPF, IS-IS, EIGRP et RIPv2 supportent le VLSM car ils indiquent toujours un masque réseau associé à une route annoncée.

Par exemple, pour l'adresse 91.198.174.2/19 :

Le masque de sous-réseau (/19) est 255.255.224.0 ; l'adresse du sous-réseau est donc donnée par :
91.198.174.2 & 255.255.224.0 = 91.198.160.0

Soit en binaire :
01011011.11000110.10101110.00000010
& 11111111.11111111.11100000.00000000
= 01011011.11000110.10100000.00000000

Masque de sous-réseau variable (VLSM)

L'adresse de l'hôte au sein du sous-réseau est donnée par la partie restante (01110.00000010), ou par le calcul :
91.198.174.2 & 0.0.31.255 = 0.0.14.2
soit en binaire :

01011011.11000110.10101110.00000010
& 00000000.00000000.00011111.11111111
= 00000000.00000000.00001110.00000010

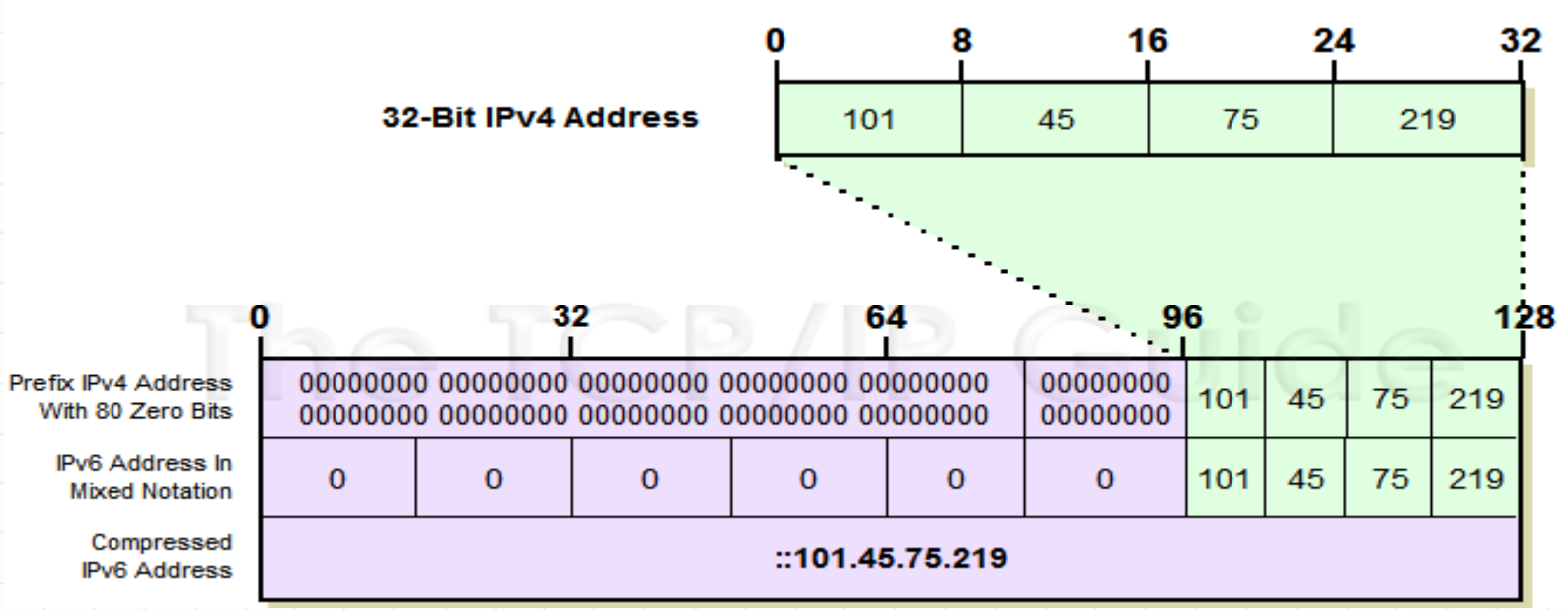
En résumé, pour cet exemple :

	Notation décimale	Notation binaire
Adresse IPv4	91.198.174.2	01011011.11000110.10101110.00000010
Masque de sous-réseau	255.255.224.0	11111111.11111111.11100000.00000000
Adresse du sous-réseau	91.198.160.0	01011011.11000110.10100000.00000000
Adresse de l'hôte	0.0.14.2	00000000.00000000.00001110.00000010

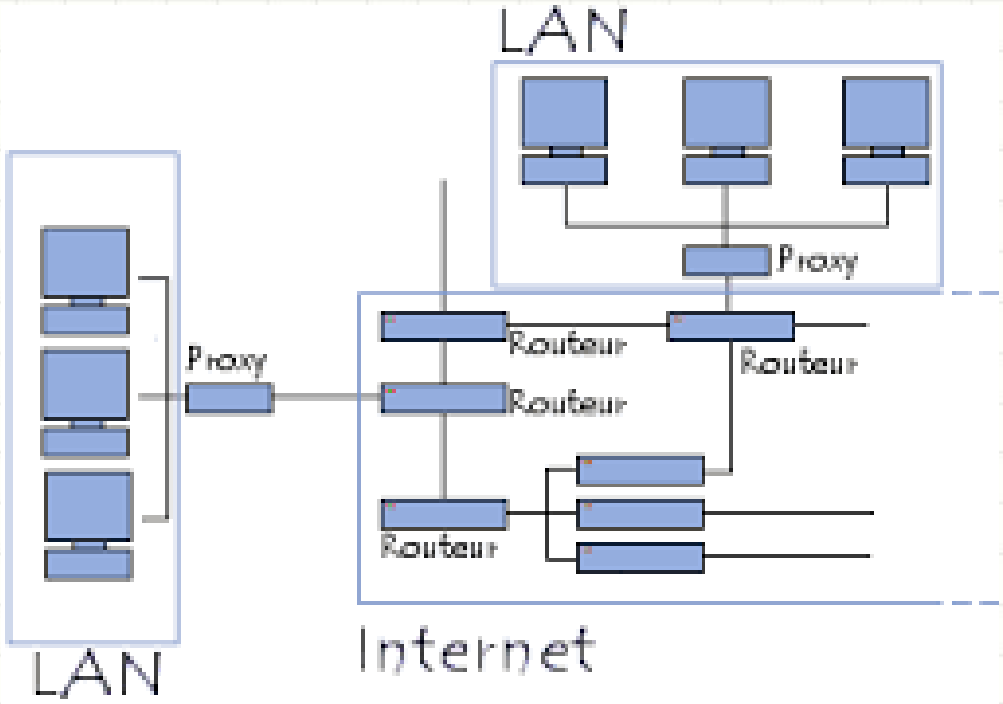
Adressage IP V6

L'**adresse IPv6** est une adresse IP, dans la version 6 du protocole IP (IPv6). Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4. On dispose ainsi d'environ $3,4 \times 10^{38}$ adresses.
IPv6 a été principalement développé en réponse à la demande d'adresses Internet qu'IPv4 ne permettait pas de contenter. En effet, le développement rapide d'Internet a conduit à la pénurie du nombre d'adresses IPv4 disponibles.

Structure des adresses IPv6



Configuration des routeurs et routage basique



Présentation d'un routeur Cisco

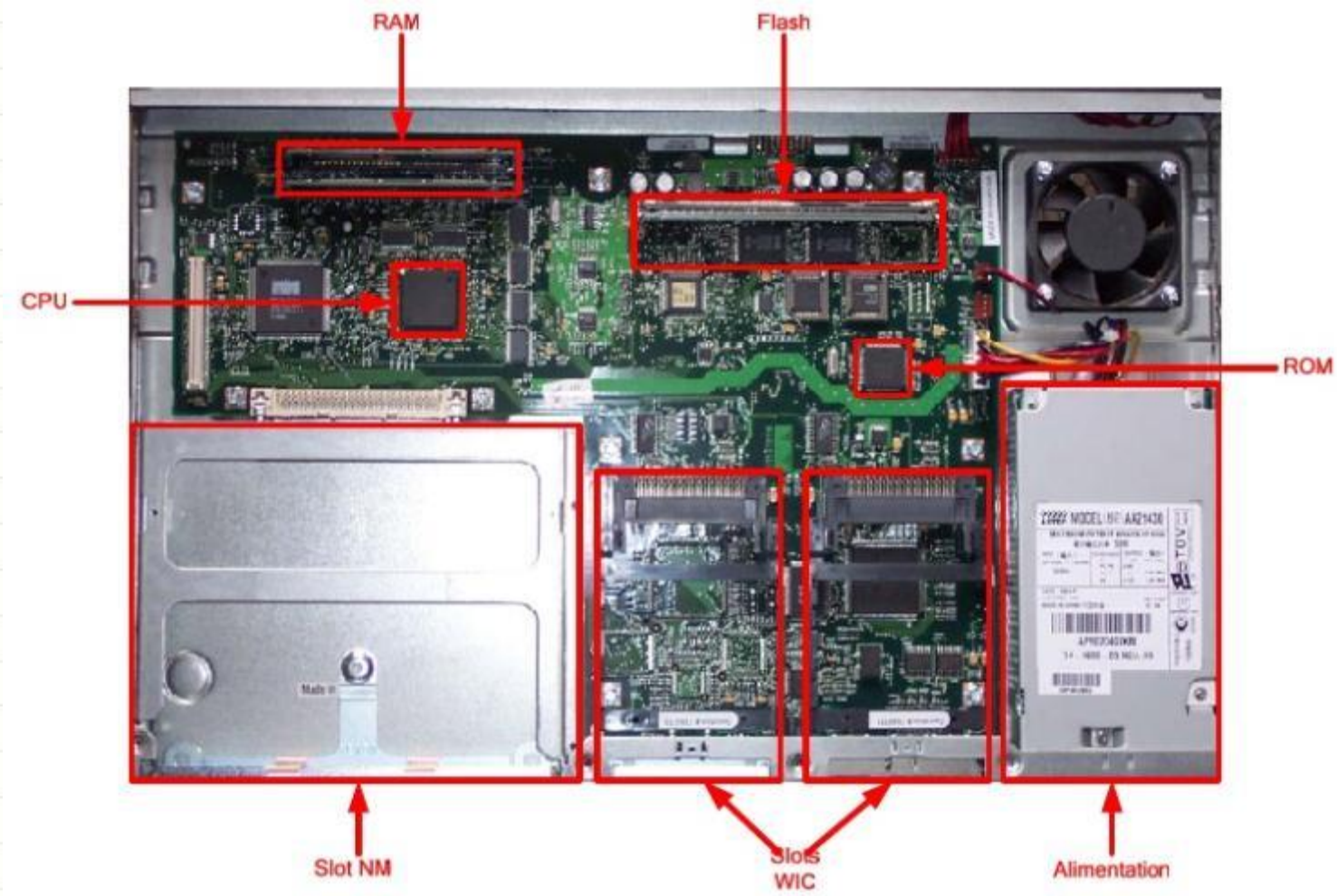
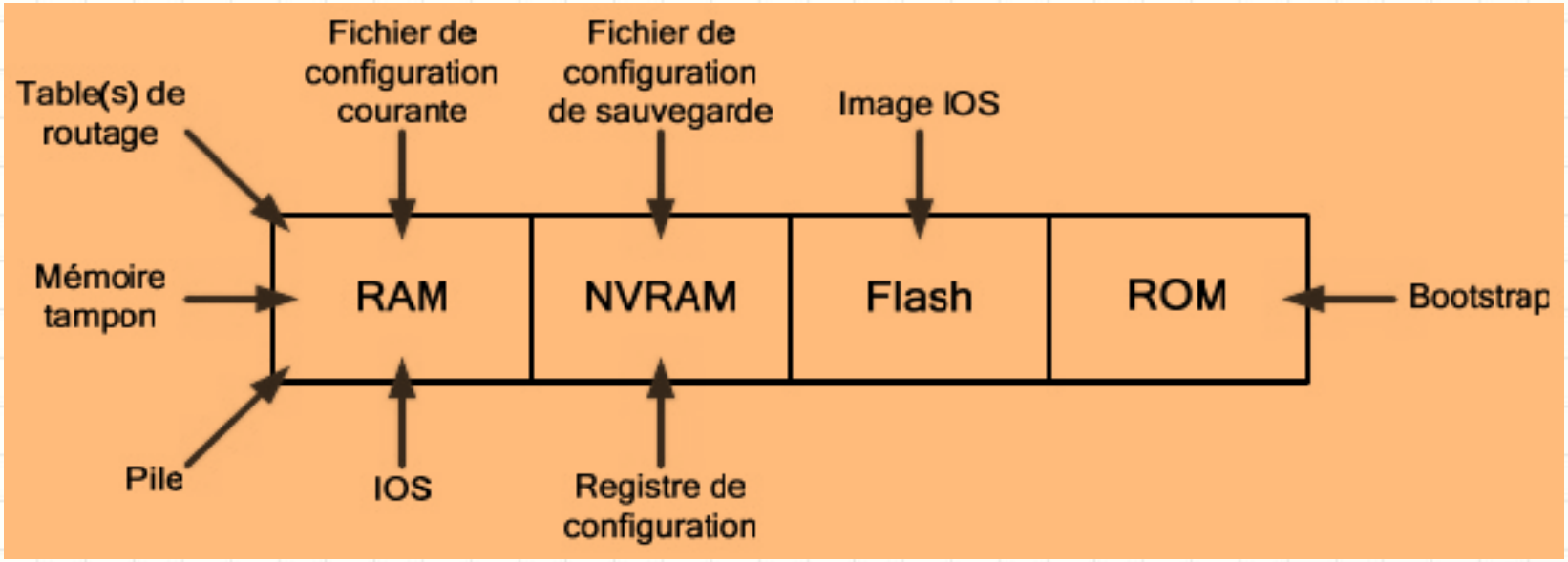
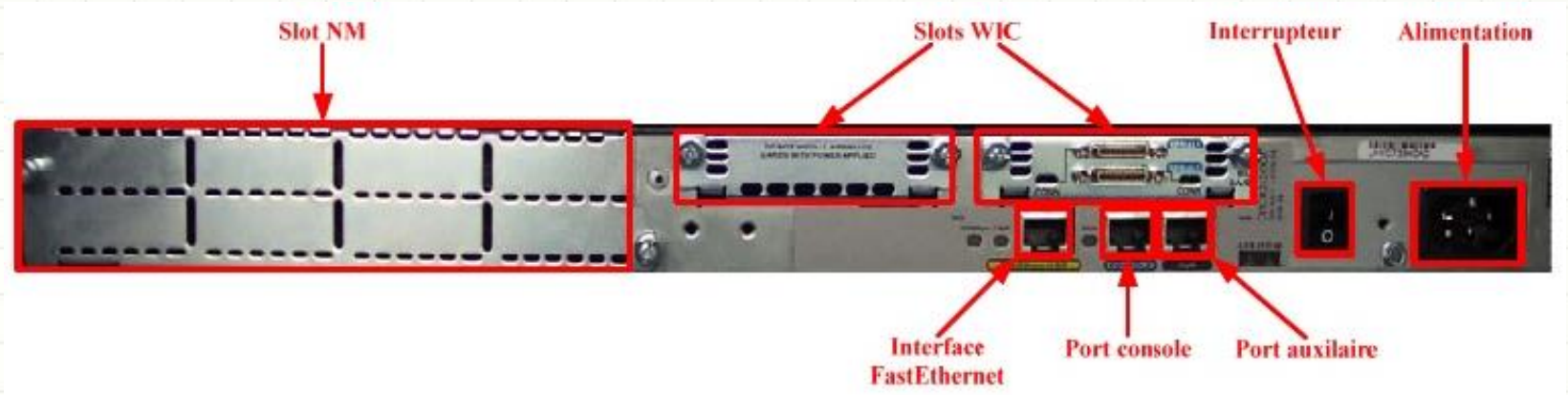


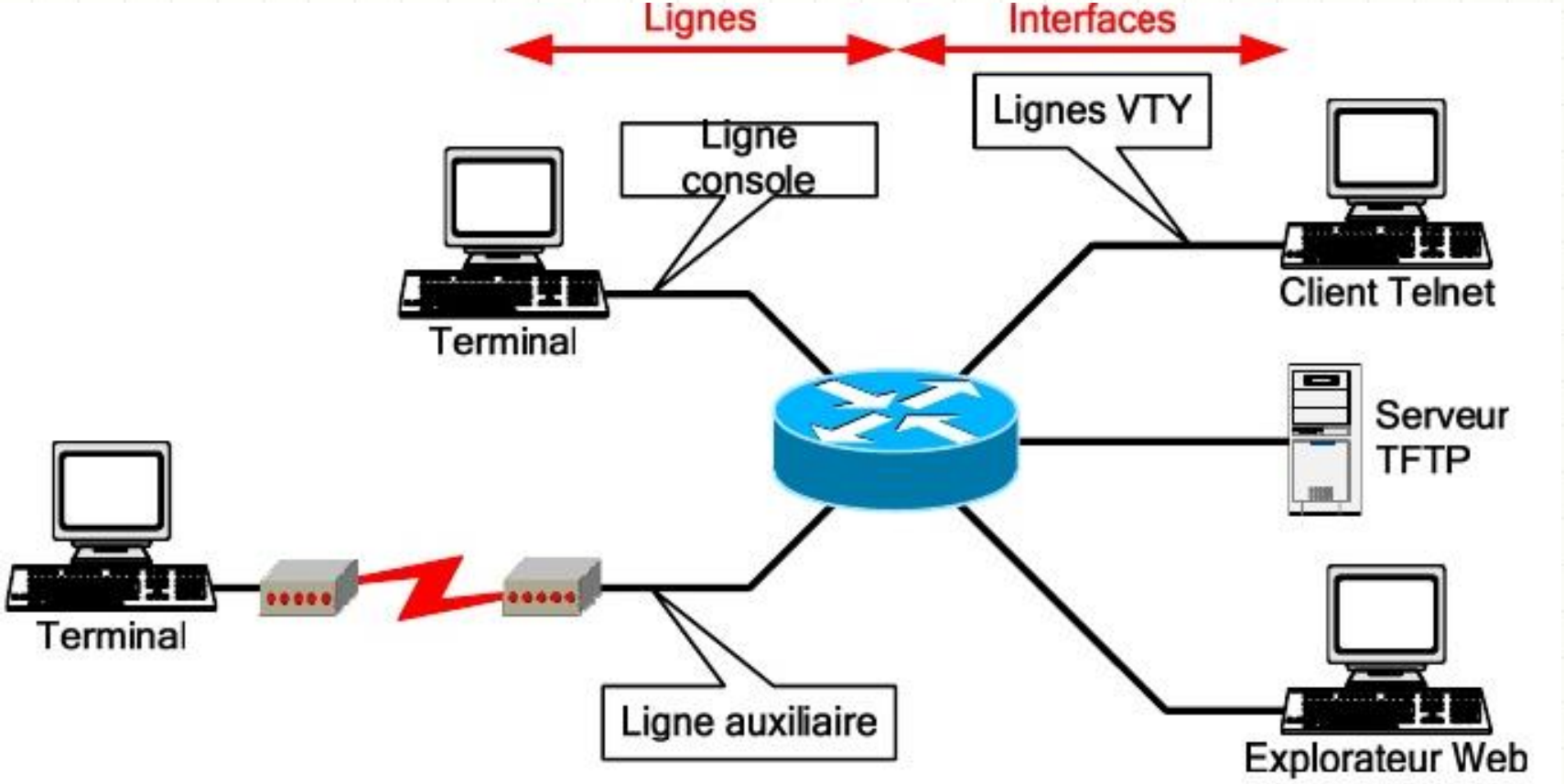
Schéma des mémoires d'un routeur Cisco



Composants externes



La configuration d'un routeur se fait par l'intermédiaire de lignes.



Modes de commandes

Mode utilisateur : Mode lecture qui permet à l'utilisateur de consulter des informations sur le routeur, mais ne lui permet pas d'effectuer des modifications. Dans ce mode, on ne dispose que de commandes de visualisation d'état sur le fonctionnement du routeur. C'est dans ce mode que l'on arrive lorsque l'on se connecte au routeur.

Mode privilégié : Mode lecture avec pouvoir. On dispose d'une panoplie complète de commandes pour visualiser l'état de fonctionnement du routeur, ainsi que pour importer/exporter et sauvegarder des fichiers de configurations et des images d'IOS.

Mode de configuration globale : Ce mode permet d'utiliser toutes les commandes de configuration ayant une portée globale à tout le routeur.

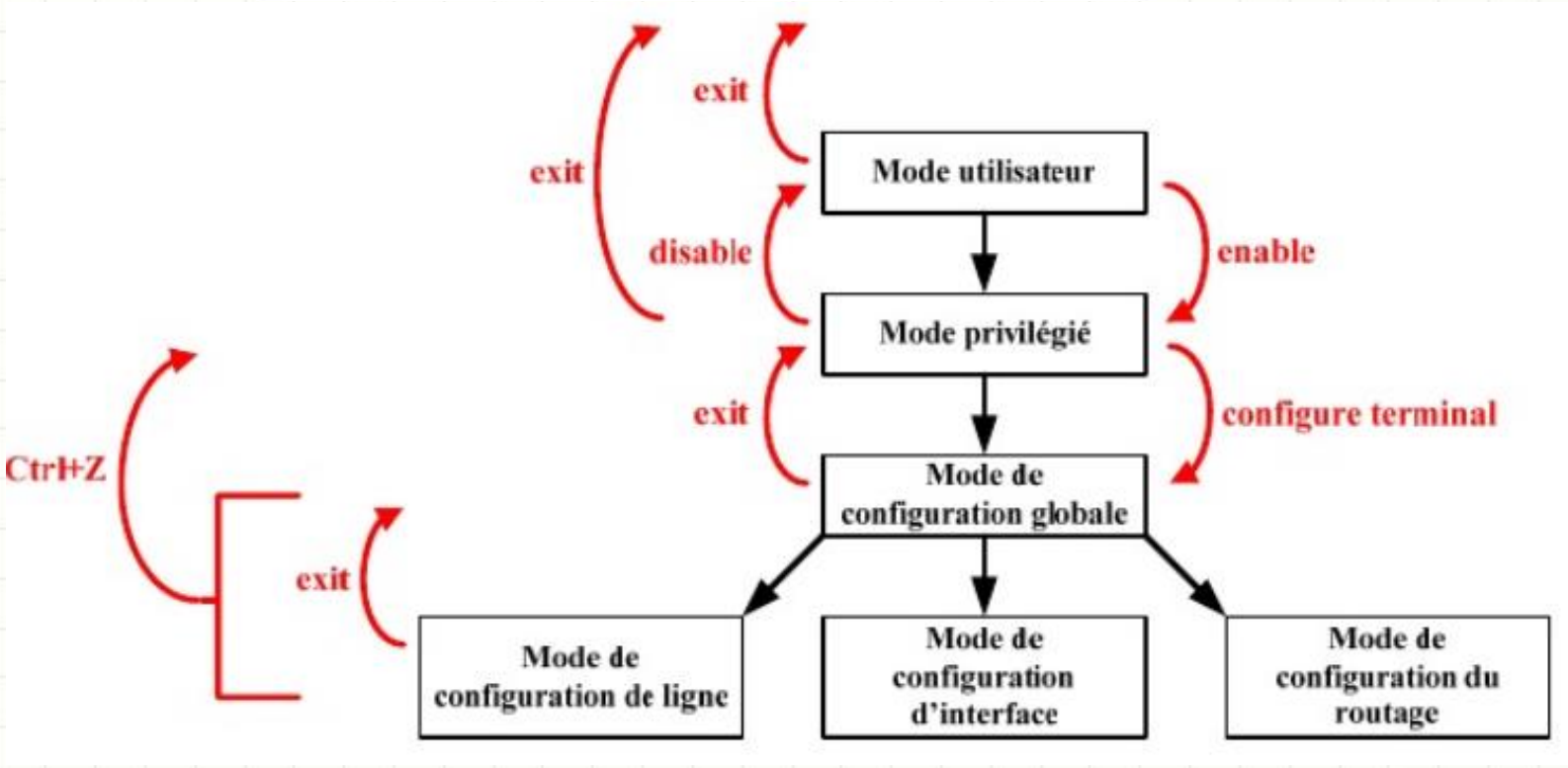
Modes de configuration spécifiques : On ne dispose que dans chaque mode spécifique des commandes ayant une portée localisée au composant du routeur spécifié par ce mode.

Mode SETUP : Mode affichant un dialogue interactif, grâce auquel l'utilisateur néophyte peut créer une configuration élémentaire initiale.

Mode RXBoot : Mode de maintenance permettant notamment de récupérer des mots de passe perdus.

Modes de commandes

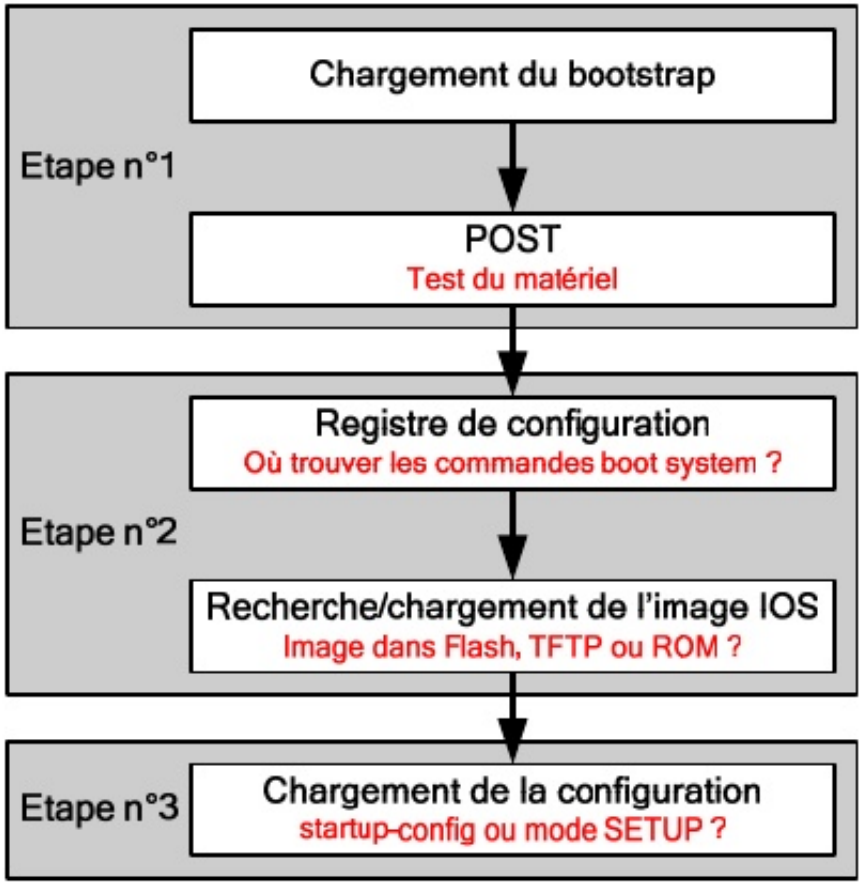
Mode	Invite de commande
Utilisateur	Router >
Privilégié	Router #
Configuration globale	Router (config) #
Interface	Router (config-if) #
Ligne	Router (config-line) #
Routage	Router (config-router) #



Gestion d'IOS et processus de démarrage

La séquence d'amorçage d'un routeur est découpée en 3 étapes :

- ❑ Etape n°1 : POST (Power On Self Test)
- ❑ Etape n°2 : Chargement d'IOS
- ❑ Etape n°3 : Chargement de la configuration



Le Routage:

La couche réseau fournit un acheminement de bout en bout et au mieux des paquets à travers les réseaux interconnectés. Ceci est effectué par 2 fonctions distinctes :

- **Fonction de routage**
- **Fonction de commutation**

La fonction de routage utilise la *table de routage* du protocole routé utilisé par le paquet à faire transiter pour déterminer le meilleur chemin à emprunter pour atteindre le réseau de destination. La métrique est utilisée pour offrir une mesure de qualité des différents chemins.

La fonction de commutation permet à un routeur d'accepter un paquet d'une file d'attente d'entrée et de le transmettre à une file d'attente de sortie. Le but de ces deux fonctions est donc complètement différent et entièrement complémentaire.

Routage statique et dynamique

Il existe deux types de routage :

- **Statique:** Tout est géré manuellement par un administrateur réseau qui enregistre toutes les informations dans la configuration d'un routeur. Il doit mettre à jour manuellement les entrées de route statique chaque fois qu'une modification de la topologie le nécessite.
- **Dynamique**: Une fois qu'un administrateur réseau a entré les commandes de configuration pour lancer le routage dynamique, les informations relatives aux routes sont mises à jour automatiquement, par un processus de routage.

Les protocoles de routage peuvent être classés selon l'algorithme qu'ils utilisent :

- Vecteur de distance (RIPv1 , RIPv2, IGRP)
- Etat de liens (OSPF, IS-IS)
- Hybride symétrique : EIGRP

Comparaison entre les protocoles à vecteur de distance et état de liens :

Vecteur de distance :

•Visualise la topologie du réseau du point de vue de leurs voisins.

•Ajoute des vecteurs de distance d'un routeur à l'autre.

•Mises à jour périodiques fréquentes et convergence lente.

•Passe des copies des tables de routage aux routeurs voisins.

Etat de lien :

•Dispose d'une vue commune de la topologie.

•Calcule le plus court chemin vers les autres routeurs.

•Mises à jour déclenchées par événement et convergence plus rapide.

•Passe les mises à jour du routage à état de liens aux autres routeurs.

Comparaison entre les protocoles à vecteur de distance et état de liens :

Vecteur de distance	Etat de lien
Algorithme Bellman-Ford (RIP)	Algorithme Dijkstra (OSPF)
Facile à configurer	Compétences requises
Partage des tables de routage	Partage des liaisons
Réseaux plats	Réseaux conçus (design) organisés en *areas*
Convergence plus lente	Convergence rapide, répartition de charge
Topologies limitées	Topologies complexes et larges
Gourmand en bande passante	Relativement discret
Peu consommateur en RAM et CPU	Gourmand en RAM et CPU
Mises à jour régulière en broadcast/muliscast	Mises à jour immédiate
Pas de signalisation	Signalisation fiable et en mode connecté
RIPv1 - UDP520 - 255.255.255.255 RIPv2 - UDP520 - 224.0.0.9 EIGRP - Cisco Systems (DUAL)	OSPFv2/v3 - IP89 - 224.0.0.5, 224.0.0.6, FF02::5, FF02::6 IS-IS

Systèmes autonomes

Un système autonome (AS) est, par définition, l'ensemble des dispositifs interconnectés régis par la même administration. Cela permet de délimiter la responsabilité du routage à un ensemble défini.

Cette notion de système autonome crée donc une nouvelle distinction entre les protocoles de routage :

- Protocoles de routage intérieurs (IGP) : Protocoles ayant pour mission principale le routage à l'intérieur d'un système autonome.
- Protocoles de routage extérieurs (EGP) : Protocoles permettant le routage entre les systèmes autonomes.

Classification	Protocoles
IGP	RIP, IGRP, EIGRP, OSPF et IS-IS
EGP	EGP et BGP

PROTOCOL	RIP 1	RIP 2	IGRP	EIGRP	OSPF	BGP
TYPE	DISTANCE VECTOR	DISTANCE VECTOR	DISTANCE VECTOR	BALANCED HYBRID/DV	LINK STATE	PATH VECTOR/DV
LOOP PREVENTION	HOLDDOWN, SPLIT HORIZ	HOLDDOWN, SPLIT HORIZ	HOLDDOWN, SPLIT HORIZ/DUAL	DUAL/FEASABLE SUCCESSOR ..	DIJHSTRA SPF ALGORITHUM + TOPOLOGY DATABASE	AS PATH
VLSM SUPPORT	NO	YES	NO	YES	YES	YES
ADMIN DIS	120	120	100	summary=5 internal=90 external=170	110	internal=200 external =20
UPDATE	30 sec	30 sec	90 sec	triggered	triggered and 30mins	config
METRIC	hops	hops	BW + DELAY	BW + DELAY	cost	med, local pref, weight, AS-Path .... etc. LOTS !
HOLDDOWN	180 sec	180 sec	280 sec	3 x hello	(max age = 1 hour)	config
FLASH UPDATES	NO	NO	YES	YES	YES	YES
HELLO	NO	NO	5 to 60 sec	5 to 60 sec	10 to 30 sec	keepalive
INFINITY	16 hops	16 hops	4M (+255 hops)	64M (+255 hops)	64k	config
AUTO SUMMARY	FIXED	FIXED	FIXED	default = auto	default = no auto	config
CONNECTION	broadcast UDP port 520	multicast 224.0.0.9 UDP port 520	broadcast IP protocol #9	multicast 224.0.0.10 (IP protocol #88)	multicast 224.0.0.5/6 (IP protocol #89)	TCP 179
RFC	1058	1723		Cisco	1247, 1583	1771
MAX PATHS	1-16 (default = 4)equal costs only1-16 (default = 4)	1-16 (default = 4)equal costs only1-16 (default = 4)	1-16 (default = 4) load balancing over non-equal paths also using VARIANCE 1-16 (default=4)	1-16 (default = 4) load balancing over non-equal paths also using VARIANCE1-16 (default=4)	1-16 (default = 4)equal costs only1-16 (default = 4)	config
AUTHENTICATION	NO	YES	NO	YES	YES	YES

Configuration d'un routeur cisco

Open-Source Network Simulators

- Cloonix
- CORE
- GNS3
- IMUNES
- Mininet
- Netkit
- Psimulator2
- Virtualsquare
- VNX and VNUML
- Dynamips
- Packet Tracer
- SemSim
- Boson NetSim
- CertExams
- RouterSim's CCNA Network Visualizer

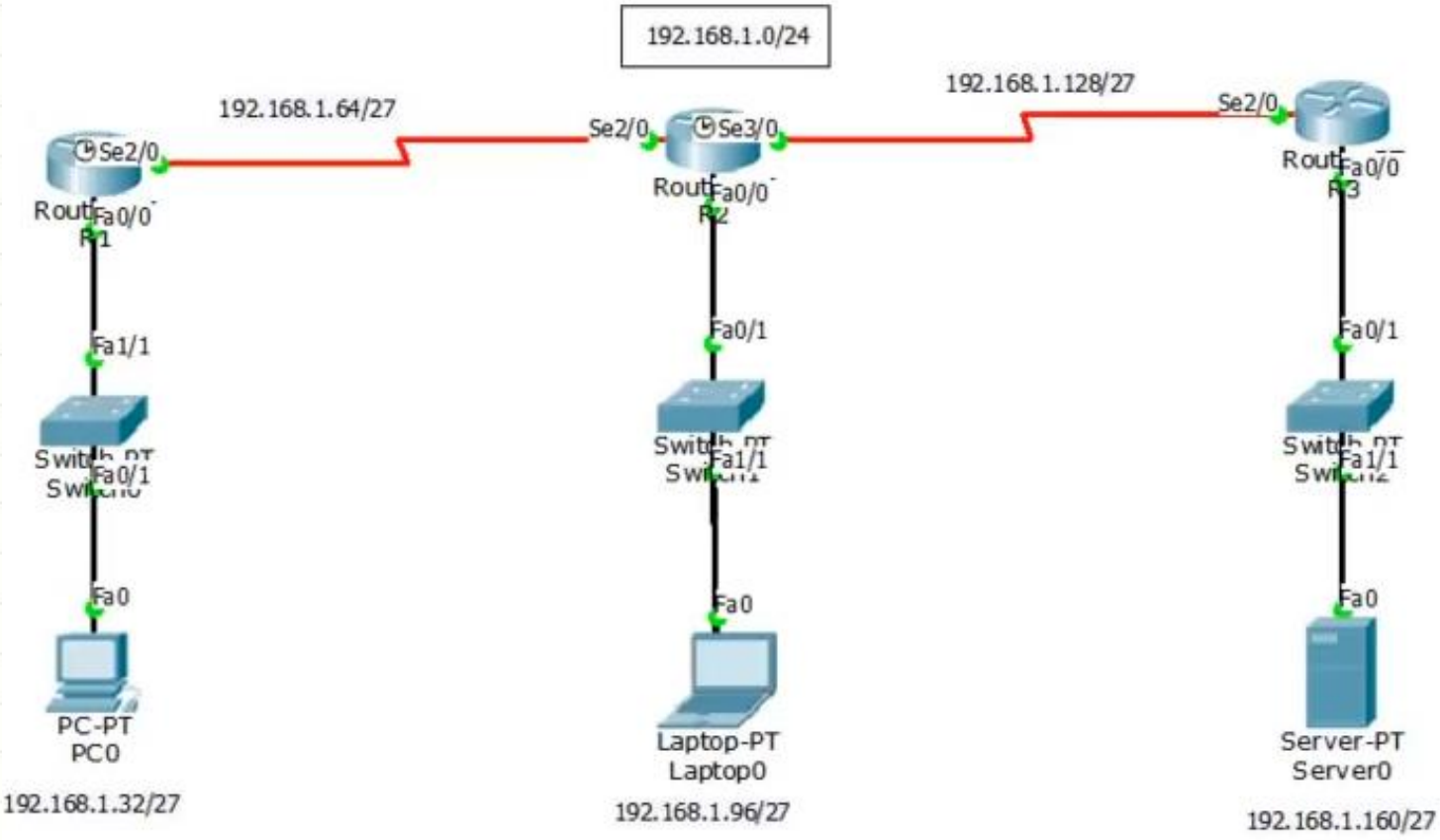
Travaux Pratiques

Mettre en place au sein de la topologie (ci-dessous) un routage basé sur les protocoles :

- ❑ Routage Statique
- ❑ RIP.
- ❑ EGIRP
- ❑ OSPF

http://routeur.clemanet.com/

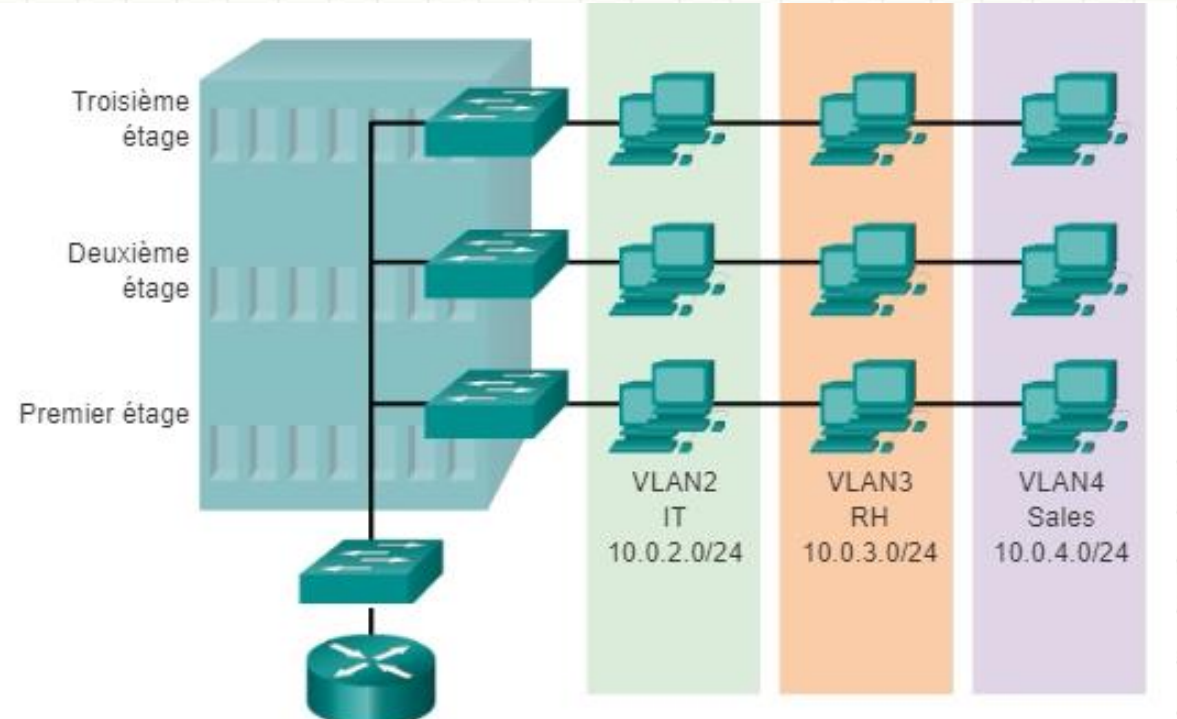
http://www.actualitix.com/commandes-routeurs-cisco.html#configuration-routeur



Introduction aux VLAN

Un **VLAN** (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*)

Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique. Les VLAN améliorent les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits.



Types de VLAN

- **VLAN niveau 1:** (aussi appelés **VLAN par port**, en anglais *Port-Based VLAN*)

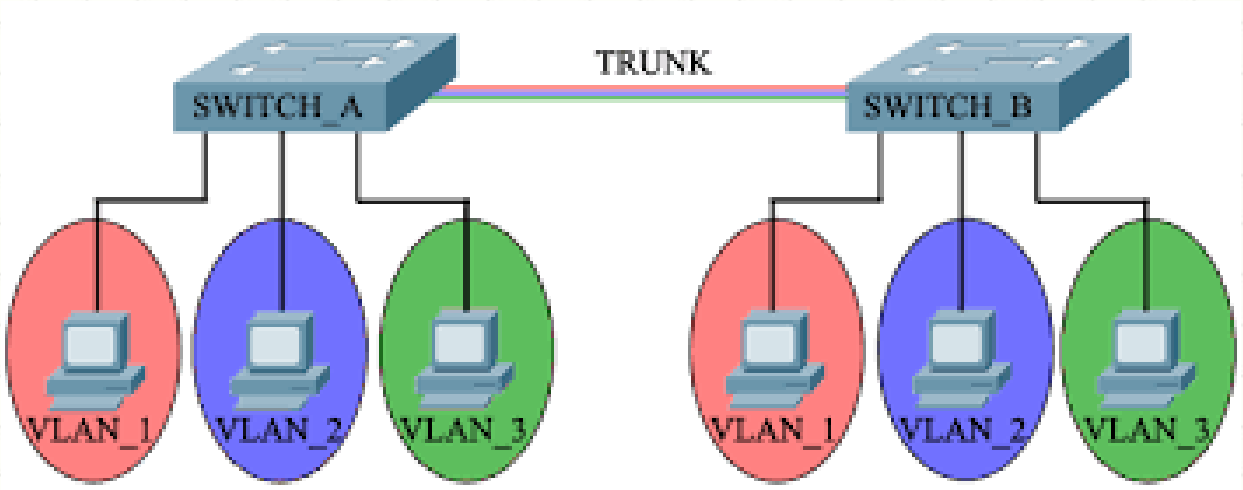
- **VLAN niveau 2:** (également appelé **VLAN MAC**, *VLAN par adresse IEEE* ou en anglais *MAC Address-Based VLAN*)

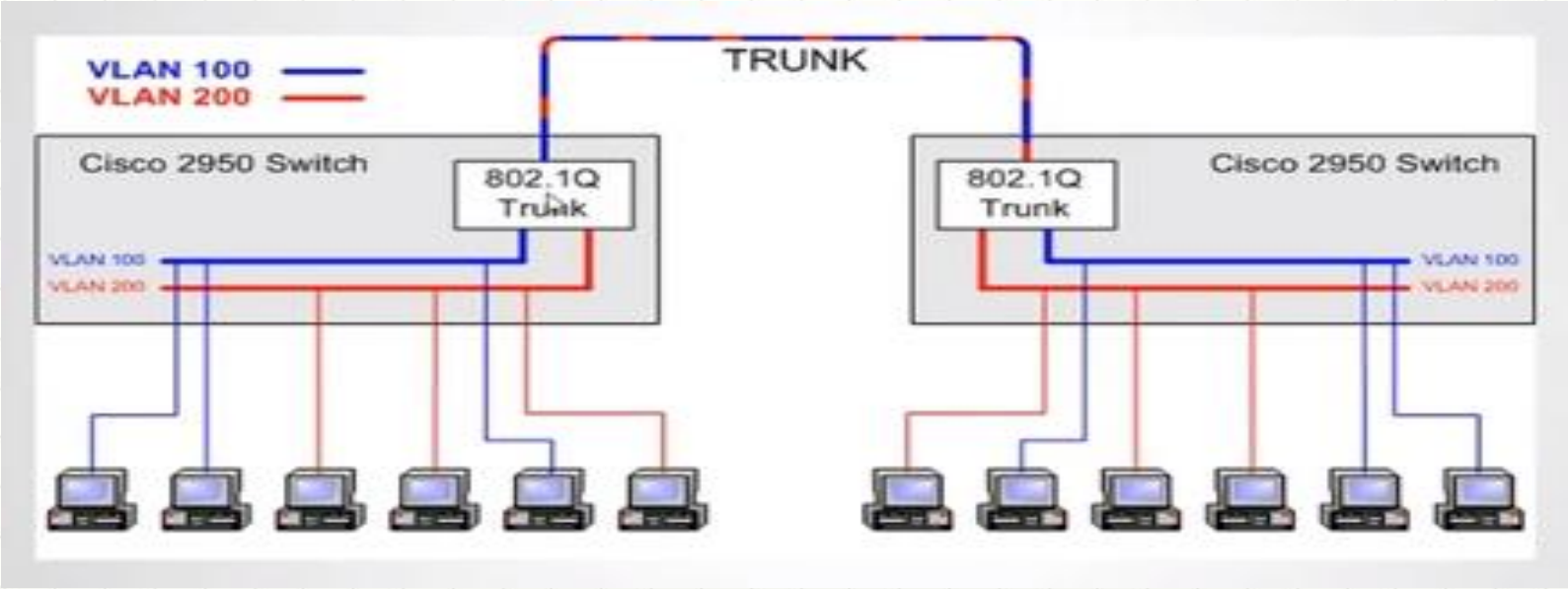
- **VLAN niveau 3** : on distingue plusieurs types de VLAN de niveau 3 :
  - Le **VLAN par sous-réseau** (en anglais *Network Address-Based VLAN*)
  - Le **VLAN par protocole** (en anglais *Protocol-Based VLAN*)

Les VLAN présentent les intérêts suivants:

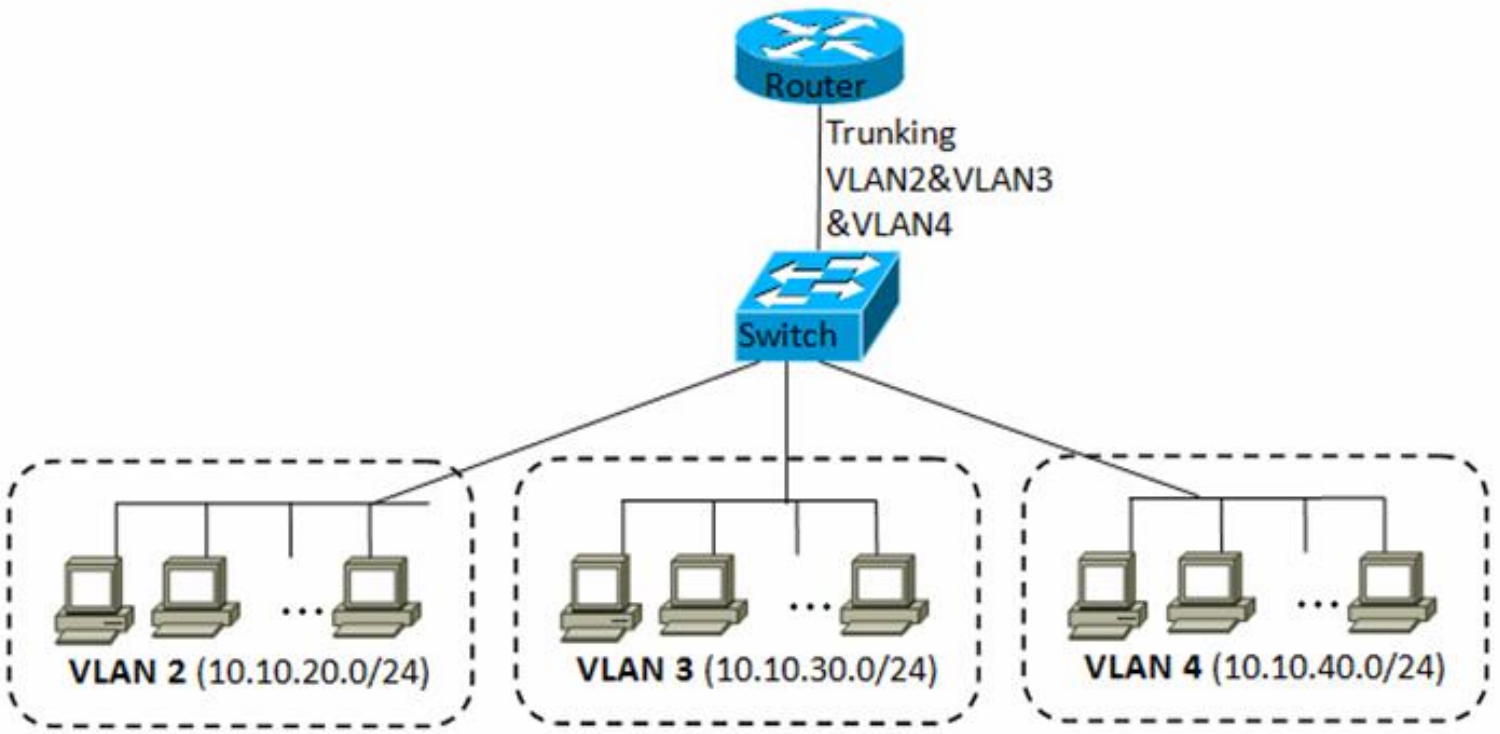
- Améliorer la gestion du réseau.
- Optimiser la bande passante.
- Séparer les flux.
- Segmentation : réduire la taille d'un domaine de broadcast,
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

Trunk (Agrégation de liens):





Routage Inter-Vlans:



- Interfaces Virtuelles
- Encapsulation
- Trunking

Travaux Pratiques sur les VLANs:

TP1: Création des Vlans

TP2: Création des liaisons Trunk

TP3: Routage Inter-Vlan

TP4: Protocole VTP

ACL – Access Control List

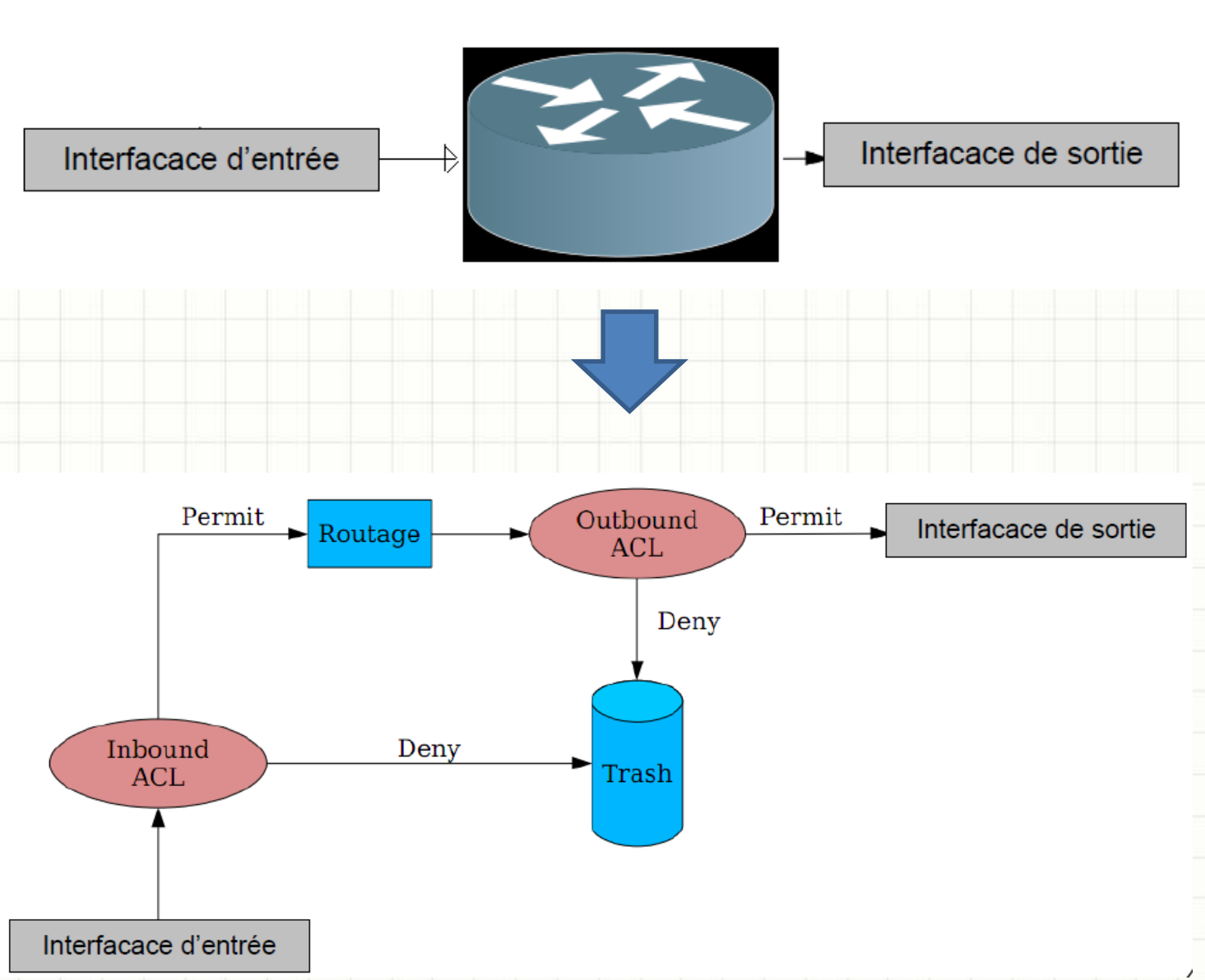
Une ACL (Access Control List) est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie.

Cette liste est parcourue de la première à la dernière instruction jusqu'à trouver une correspondance. Si le paquet répond aux critères d'une instruction, le reste des instructions est ignoré et le paquet est autorisé ou refusé. Si aucune correspondance n'est trouvée dans les critères explicités par l'administrateur, le paquet est implicitement
supprimé.

ACL – Access Control List

- Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, …).
- Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny).
- Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output).
- Une ACL est analysée par l'IOS de manière séquentielle.
- Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

ACL – Access Control List



ACL Standard

Permet d'analyser du trafic en fonction de:

- Adresse IP source

Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.

ACL Etendues

Permet d'analyser du trafic en fonction de:

- Adresse IP source
- Adresse IP destination
- Protocole (tcp, udp, icmp, …)
- Port source
- Port destination
- Etc.

Les ACLs étendues sont à appliquer le plus proche possible de la source.

Concevoir une ACL

- Lorsqu'une ACL contient plusieurs règles il faut placer les règles les plus précises en début de liste, et donc les plus génériques en fin de liste.

Conseils

- Concevoir une ACL dans un éditeur de texte et la configurer par copier/coller.
- Désactiver une ACL sur une interface avant de la modifier.

Configuration d'une ACL numérique standard

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 1 deny 192.168.0.0 0.0.3.255
R1(config)#access-list 1 permit any
```

Configuration d'une ACL nommée standard

```
R1(config)#ip access-list standard monACL
R1(config-std-nacl)#permit 192.168.0.0 0.0.0.255
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)#deny 192.168.0.0 0.0.3.255
R1(config-std-nacl)#permit any
R1(config-std-nacl)#exit
```

Vérification des ACLs

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Standard IP access list monACL
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#
```

ACL « numériques »

ACL identifées par un nombre.

1 à 99 :	ACL Standard
100 à 199 :	ACL Etendue
1300 à 1999 :	ACL Standard
2000 à 2699 :	ACL Etendue

ACL « nommées »

ACL identifiées par un nom sous la forme d'une chaîne de caractères alphanumériques.

Ces deux ACLs sont identiques.
Tout le trafic provenant du réseau 192.168.0.0/22 est bloqué à l'exception des deux subnets 192.168.0.0/24 et 192.168.1.0/24.

Configuration d'une ACL numérique étendue

```
R1(config)#access-list 100 permit tcp any host 192.168.1.100 eq 80
R1(config)#access-list 100 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
```

Configuration d'une ACL nommée étendue

```
R1(config)#ip access-list extended monACLextended
R1(config-ext-nacl)#permit tcp any host 192.168.1.100 eq 80
R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
R1(config-ext-nacl)#exit
```

Vérification des ACLs

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
R1#
```

Ces deux ACLs sont identiques.
- Tout trafic HTTP à destination de 192.168.1.100 est autorisé.
- Tout le traffic ICMP provenant de 192.168.0.0/24 à destination de 192.168.1.100 est autorisé.
- Tout autre trafic est rejeté.

Format général d'une règle étendue

```
<action> <protocole> <IP source> [port source] <IP dest> [port dest] [options]
```

- Permit / deny
- Tcp / udp , … Ip = tous les protocoles
- Adresse + wildcard mask. Ou Host 192.168.0.1 (adresse d'un hôte) Ou Any = n'importe quelle source.
- Adresse + wildcard mask. Ou Host 192.168.0.1 (adresse d'un hôte) Ou Any = n'importe quelle source.

Modifier une ACL

```
R1#show access-list 1
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#configure terminal
R1(config)#ip access-list standard 1
R1(config-std-nacl)#no 20
R1(config-std-nacl)#15 permit 192.168.1.0 0.0.0.127
R1(config-std-nacl)#^Z
R1#show access-list 1
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#
```

Entre en mode de configuration d'ACL

Supprime la règle portant le n° de séquence 20

Ajoute une règle avec le n° de séquence 15

Supprimer une ACL

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Standard IP access list monACL
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Extended IP access list 100
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list test
R1#configure terminal t
R1(config)#no access-list 100
R1(config)#no ip access-list standard monACL
R1(config)#^Z
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list test
R1#
```

Suppression d'une ACL numérotée

Suppression d'une ACL nommée

Appliquer une ACL sur une interface

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 1 in
              OU
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Applique l'ACL 1 pour le trafic entrant sur l'interface

Applique l'ACL 1 pour le trafic sortant de l'interface

Vérification des ACLs appliquées sur une interface

```
R1#show ip interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is 1
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  < … suite de l'affichage omis … >
R1#
```

ACL 1 appliquée en sortie

ACL 1 appliquée en entrée

Désactiver une ACL sur une interface

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no access-group 1 in
              OU
R1(config-if)#no access-group 1 out
R1(config-if)#
```

Appliquer une ACL sur les lignes VTY

```
R1(config)#line vty 0 4
R1(config-if)#access-class 1 in
R1(config-if)#
```

Désactiver une ACL sur les lignes VTY

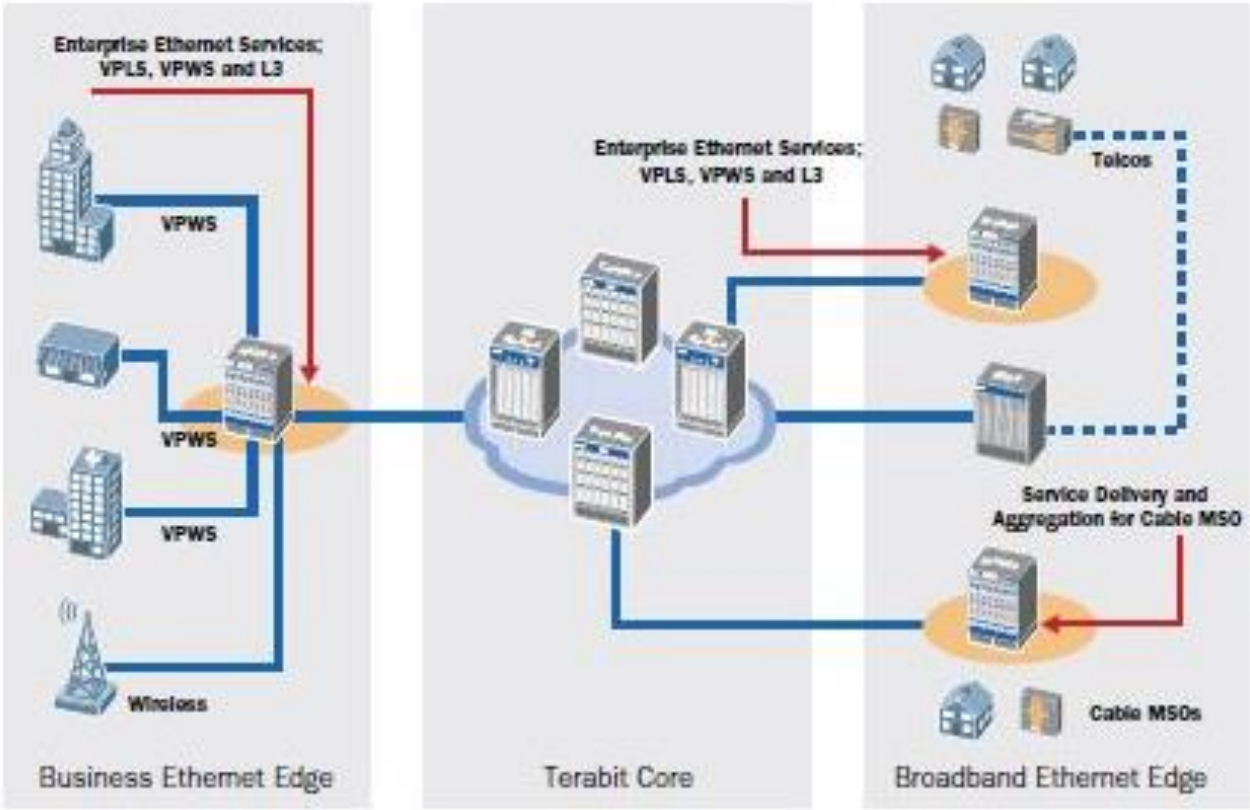
```
R1(config)#line vty 0 4
R1(config-if)#no access-class 1 in
R1(config-if)#
```

Vérifier le fonctionnement d'une ACL

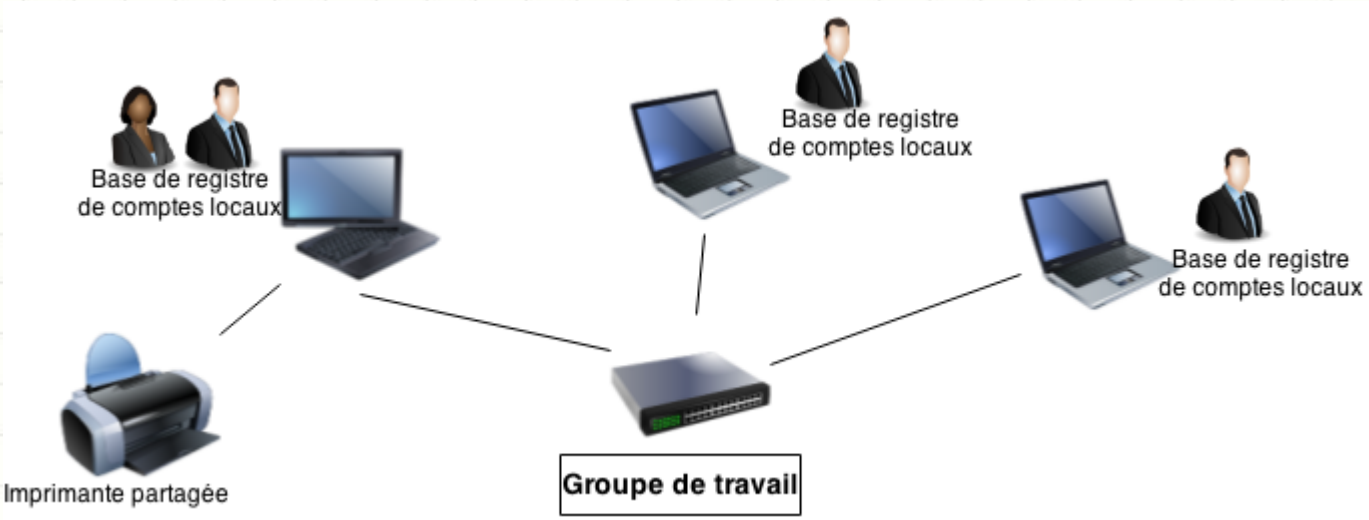
```
R1#show access-lists workingACL
Extended IP access list workingACL
    10 permit tcp any host 193.190.147.70 eq www (2 matches)
    20 permit icmp any host 193.190.147.70 (14 matches)
    30 deny ip any host 193.190.147.70 (4926 matches)
    40 permit ip any any (878382 matches)
R1#
```

Indique le nombre de fois où une règle de l'ACL a été appliquée

Partie 2: Administration des systèmes Windows Server & Linux

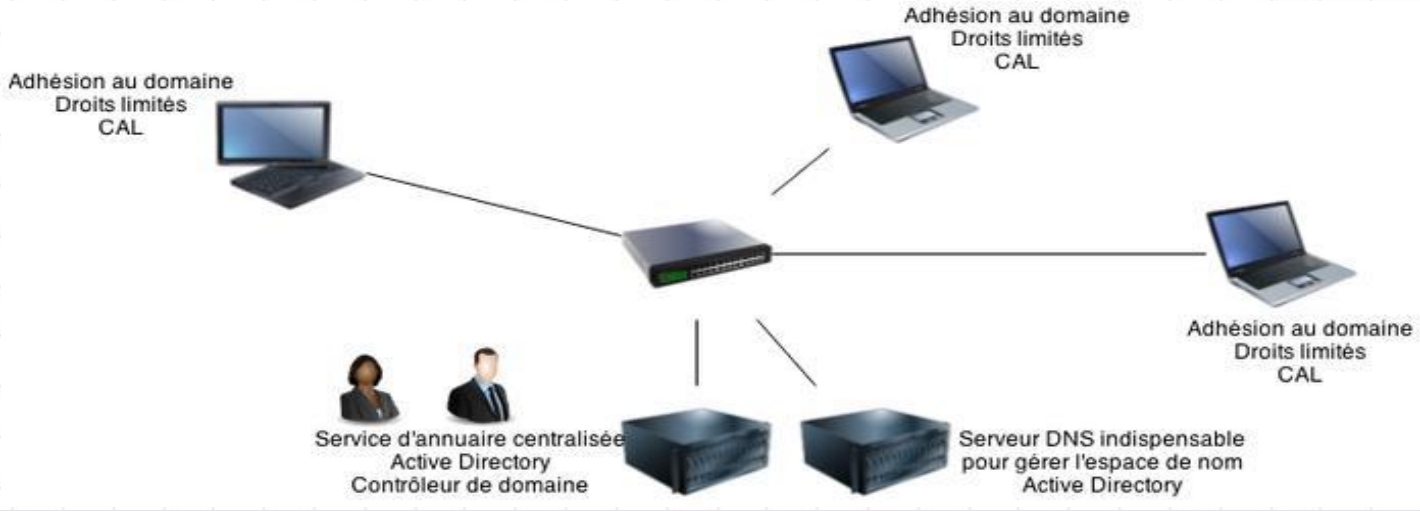


Groupe de travail (Workgroup) (peer to peer)



- Tous les ordinateurs sont des **homologues**, aucun ordinateur n'en contrôle d'autres.
- Chaque ordinateur a un ensemble de **comptes locaux** d'utilisateur.
- Pour ouvrir une session sur un ordinateur d'un groupe de travail, il faut disposer d'un compte sur cet ordinateur et donc sur chaque ordinateur sur lequel vous voulez travailler.
- Concerne de **petit réseau** où il y a moins de vingt ordinateurs.
- Un groupe de travail n'est pas protégé par un mot de passe.
- Tous les ordinateurs doivent se trouver sur le même réseau local ou le même sous-réseau.

Domaine Active Directory de Microsoft



- un ordinateur avec un système d'exploitation serveur est contrôleur de domaine;
- l'espace de noms est géré par un serveur DNS ;
- le service d'annuaire Active Directory contient les comptes de tous les utilisateurs;
- Les ordinateurs peuvent se trouver sur des réseaux locaux différents.

Avec un compte d'utilisateur créé sur le domaine (Active Directory) l'utilisateur :

- peut se connecter à tout ordinateur du domaine, sans nécessiter de compte local sur cet ordinateur ;
- ne peut apporter que des modifications limitées aux paramètres et à la configuration d'un ordinateur car les administrateurs réseau recherchent une cohérence de configuration sur l'ensemble des ordinateurs du réseau.

Windows Server 2008 R2

Date de sortie:

Mai 2010

Les éditions:

- Windows Serveur 2008 R2 Standard Edition
- **Windows Serveur 2008 R2 Enterprise Edition**
- Windows Serveur 2008 R2 Datacenter
- Windows Serveur 2008 R2 Web Edition

Windows Server 2012 R2 (date de sotie 2013)

- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Datacenter

Windows Serever 2016 Octobre 2016

Atelier 1.
Installation de Windows 2008 R2

Durée approximative de cet atelier : 1 heure

1. Vérifier les caractéristiques nécessaires
2. Créer au moins deux partitions
3. Installer **Windows Server R2 Entreprise Edition**

Active Directory (AD):

Active Directory est un service d'annuaire de Microsoft intégré aux versions serveur de Windows fonctionnant en TCP/IP. Il permet aux administrateurs réseaux de gérer centralement les ordinateurs interconnectés, de définir des stratégies pour un ensemble ou groupe d'utilisateurs, et de déployer centralement de nouvelles applications à une multitude d'ordinateurs.

Structure logique

- ✓ Forêts
- ✓ Arborescences
- ✓ Domaines
- ✓ Unités d'organisation
- ✓ Objets

Structure physique

- ✓ Sites
- ✓ Contrôleurs de domaines
- ✓ Liaisons entre sites

Objets d'Active Directory

Unité d'organisation:

Une unité d'organisation (OU, Organizational Unit) est un conteneur dans lequel on va pouvoir mettre des utilisateurs, des groupes, des ordinateurs ainsi que d'autres OU. Ainsi on peut appliquer des stratégies de groupe sur les OU.

Les Groupes:

Les groupes permettent de simplifier la gestion de l'accès des utilisateurs aux ressources du réseau. Les groupes permettent d'affecter en une seule action une ressource à un ensemble d'utilisateurs au lieu de répéter l'action pour chaque utilisateur. Un utilisateur peut être membre de plusieurs groupes. Les groupes se différencient de par leur type et de par leur étendue.

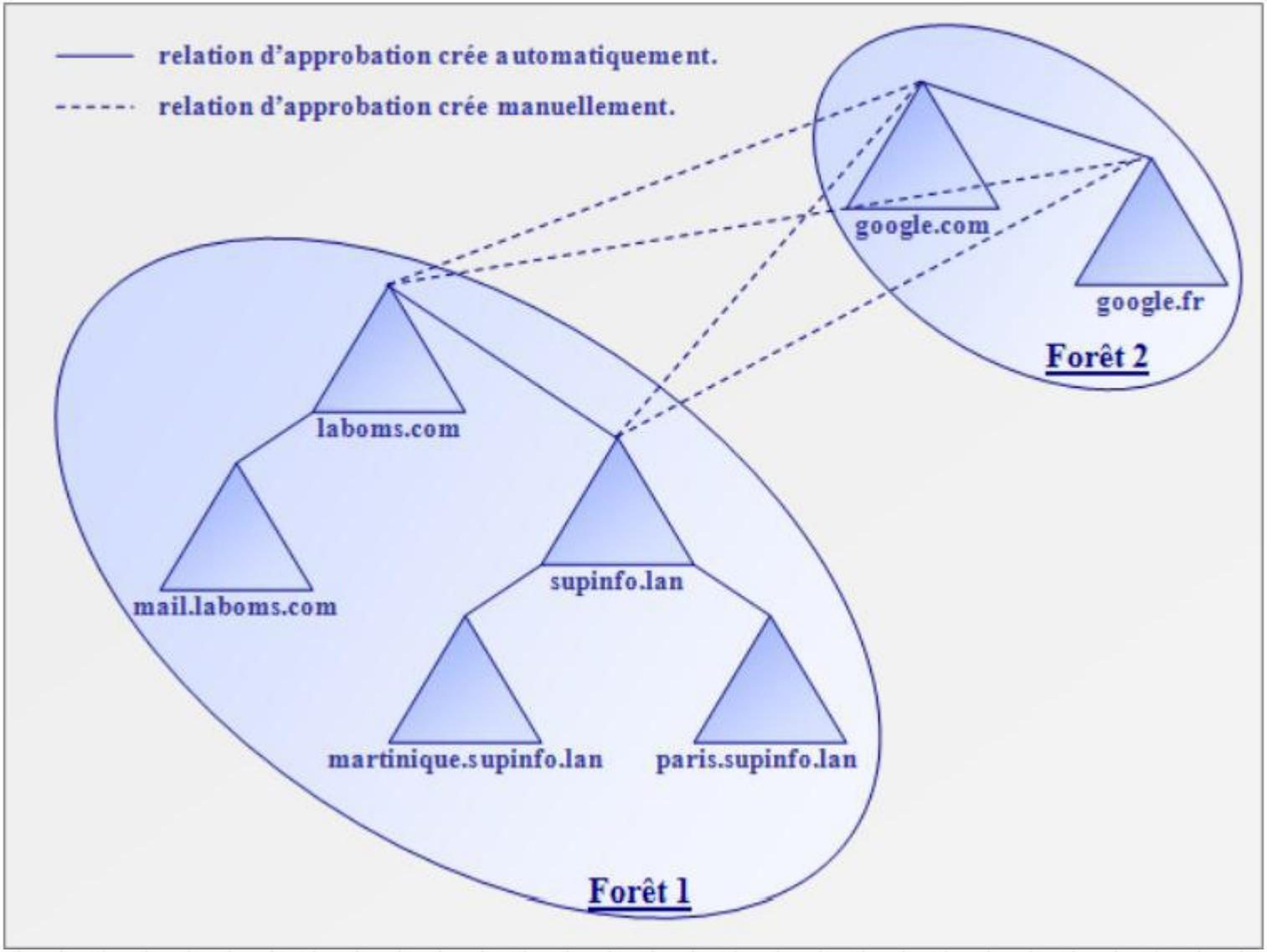
Il existe deux types de groupes dans Active Directory :

- **Les groupes de sécurité : permettent d'affecter des utilisateurs et des ordinateurs à des ressources.**
- **Les groupes de distribution : exploitables entre autres via un logiciel de messagerie.**

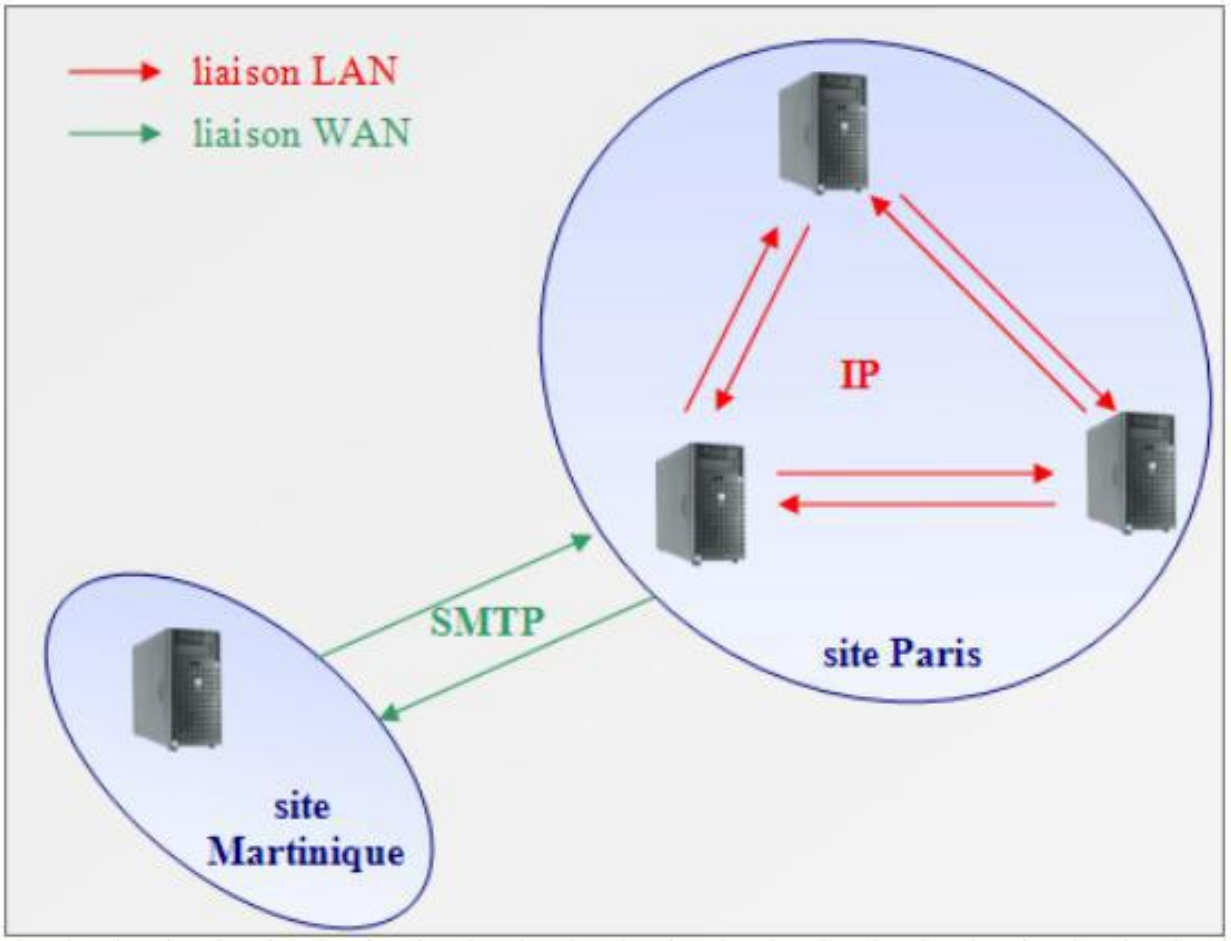
Les deux types de groupes gèrent chacun **trois niveaux d'étendue**:

- **Groupes globaux**
- **Groupes locaux**
- **Groupes universels**

Structure logique d'Active Directory:



Structure physique d'Active Directory:



La structure physique permet d'optimiser les échanges d'informations entre les différentes machines en fonction des débits assurés par les réseaux qui les connectent.

Atelier 2
Installation d’un domaine Windows 2008 R2

Durée approximative de cet atelier : 1 heure 30

Objectif

Installer les composants nécessaires et réaliser les configurations pour que notre serveur Windows 2008 R2 devienne contrôleur de domaine Windows.

Atelier 3
Gestion des utilisateurs du domaine

Durée approximative de cet atelier : 2 heures

Objectif

Comprendre et mettre en œuvre la gestion des utilisateurs avec Active Directory.

Atelier 4
Intégration d'une station au domaine

Durée approximative de cet atelier : 30 mn

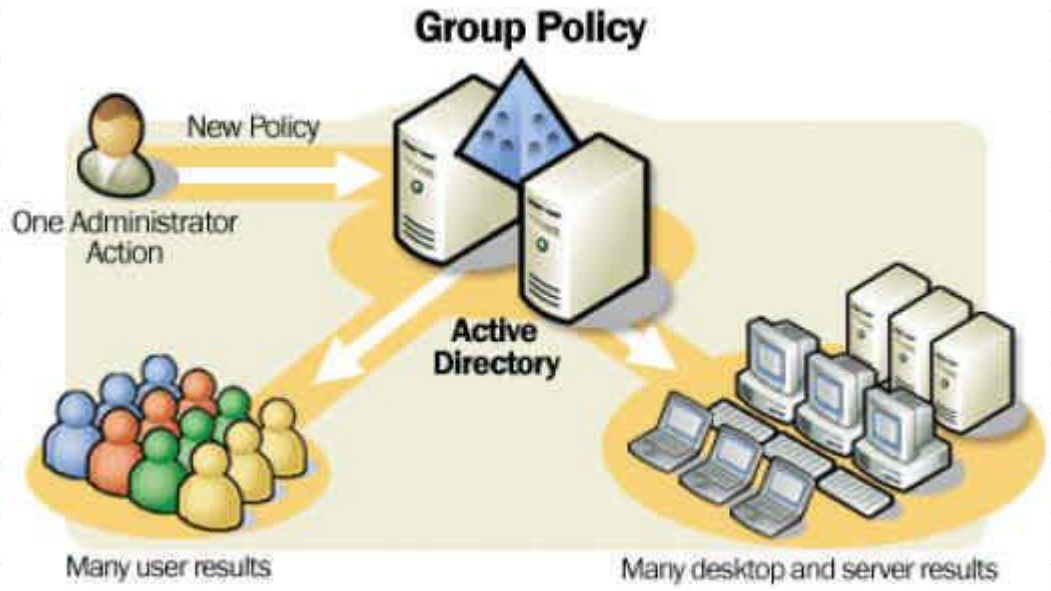
Objectif

Apprendre à intégrer une station Windows à un domaine Windows. Action indispensable pour profiter de toutes les possibilités offertes par Active Directory.

Stratégie de groupe (GPO)

Une Stratégie de groupe peut être définie comme: « des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement *Active Directory*.

Le principe étant qu'au démarrage d'une station, celle-ci va chercher sur le contrôleur de domaine la ou les stratégies à s'appliquer.



Atelier 5
Stratégies de groupe

Durée approximative de cet atelier : 1 heure

Objectif

Utilisation des GPO pour restreindre les actions et les risques potentiels comme par exemple le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc.

Atelier 6
Administration à distance Windows

Durée approximative de cet atelier : 1 heure

Objectif

Utiliser les outils de gestion à distance d’un serveur Windows.

Atelier 7
Serveur d'application web Windows

Durée approximative de cet atelier : 2 heures

Objectif

Installer le serveur Web Microsoft IIS (Internet Information Server) et l'environnement d'exécution des applications développées pour le framework.NET.

Atelier 8
SQL Server 2008 R2

Durée approximative de cet atelier : 3 heure

Objectif

Installer, configurer, mettre à disposition et sauvegarder un serveur SQL.

Atelier 10
Administration par Linux

Durée approximative de cet atelier : 8 heures

Objectifs

- ✓ Installation et configuration de système Linux (Redhat…)
- ✓ Se familiariser avec l'environnement Linux (commandes, réseau…)
- ✓ Configuration d'un contrôleur de domaine sous Linux
- ✓ Configuration des serveurs (DNS, DHCP, Apache, Tomcat…)
- ✓ Gestion des utilisateurs et groupes
- ✓ Droits d'accès et permissions
- ✓ Partage des ressources
- ✓ Sécurité.

FIN DE LA PARTIE II