Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Avertissement sur les Droits d'Auteur et Licence

- Ce cours est un projet open source publié sous la licence Creative Commons Attribution (CC BY).
- Certaines images et textes utilisés dans ce cours proviennent de sources diverses.
- Bien que nous ayons essayé de créditer les auteurs lorsque possible, il est possible que certaines attributions aient été omises.
- Si vous êtes l'auteur d'un contenu utilisé et que vous souhaitez que votre contribution soit correctement citée, veuillez nous contacter à tanguykabore@yahoo.fr
- Licence : Vous êtes libre de partager, modifier et redistribuer ce cours sous réserve de citer la source originale et de respecter les termes de la licence.
- Contact : Pour toute question ou correction, veuillez nous contacter à tanguykabore@yahoo.fr

Planning

- **Partie 1: Fondamentaux des réseaux**
- **Partie 2: Adressage IPv4**
- **Partie 3: Routage**
- **Partie 4: Réseaux LAN**
- **Partie 5: Commutation avancée**
- **Partie 6: ACL**
- **Partie 7: IPv6**

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 1: Fondamentaux des réseaux

1.1. Qu'est-ce qu'un réseau ?

Un réseau est un ensemble d'ordinateurs et de dispositifs interconnectés pour partager des ressources et des informations.

1.2. Types de Réseaux

- **PAN** (Personal Area Network) : Réseau personnel utilisé pour la communication entre des dispositifs proches.
- **LAN** (Local Area Network) : Réseau local limité à une petite zone géographique.
- **MAN** (Metropolitan Area Network) : Réseau couvrant une ville ou une grande zone métropolitaine.
- **WAN** (Wide Area Network) : Réseau couvrant de grandes distances géographiques.

1.3. Topologies de Réseaux (1/2)

La topologie réseau décrit la disposition physique ou logique des dispositifs.

- **Topologie en Bus** : Un câble principal unique avec tous les dispositifs connectés.
- **Topologie en Étoile** : Tous les dispositifs connectés à un point central (commutateur ou hub).
- **Topologie en Anneau** : Chaque dispositif connecté à deux autres formant un cercle.

1.3. Topologies de Réseaux (2/2)

La topologie réseau décrit la disposition physique ou logique des dispositifs.

- **Topologie Maillée** : Chaque dispositif est directement connecté à plusieurs autres.
- **Topologie Hybride** : Combinaison de deux ou plusieurs types de topologies.

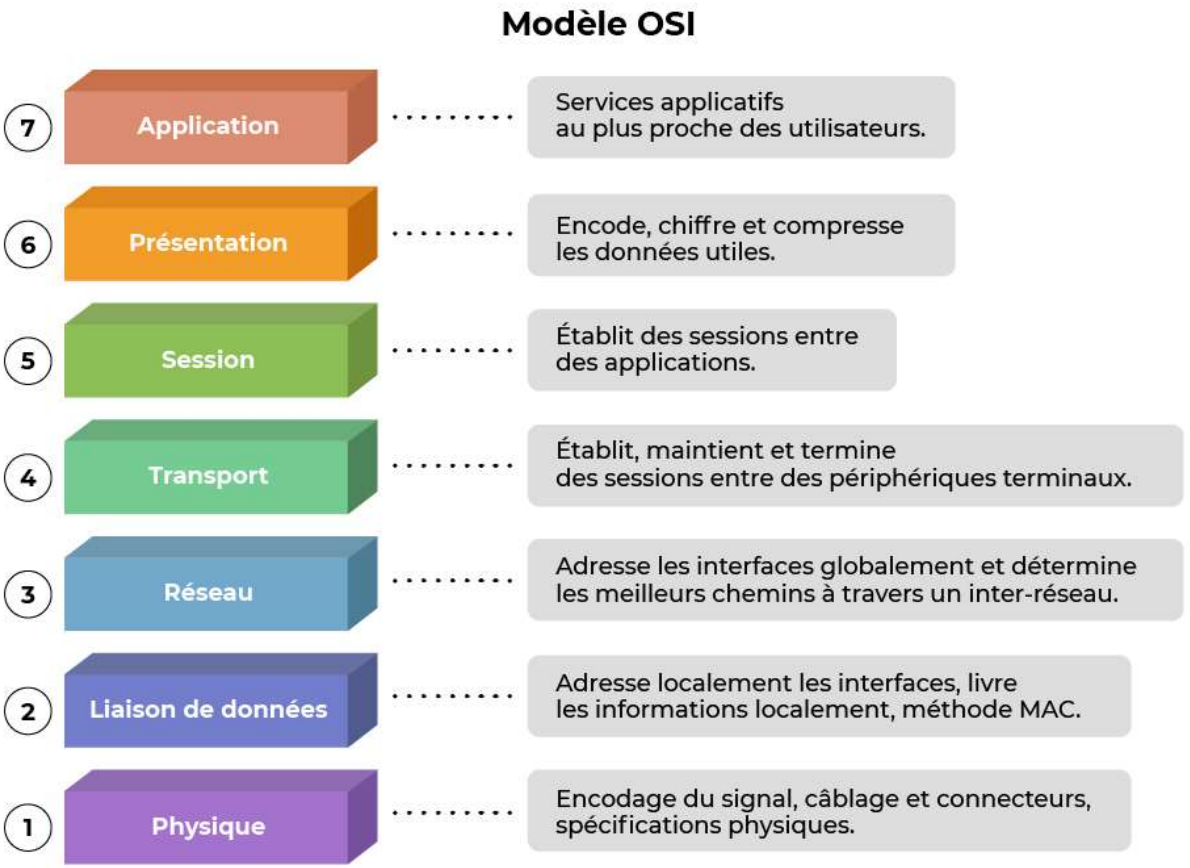
1.4. Modèle OSI (Open Systems Interconnection): Utilité

- **Cadre Théorique** : Le modèle OSI est principalement un outil pédagogique et conceptuel. Il n'est pas directement utilisé dans les implémentations réseau, mais il aide à comprendre comment les différents aspects de la communication réseau s'articulent.
- **Standardisation** : Fournit une base pour la création de standards et de protocoles qui permettent l'interopérabilité entre les produits et technologies de différents fabricants.
- **Dépannage** : Aide à isoler les problèmes de réseau en identifiant la couche où se situe le problème.

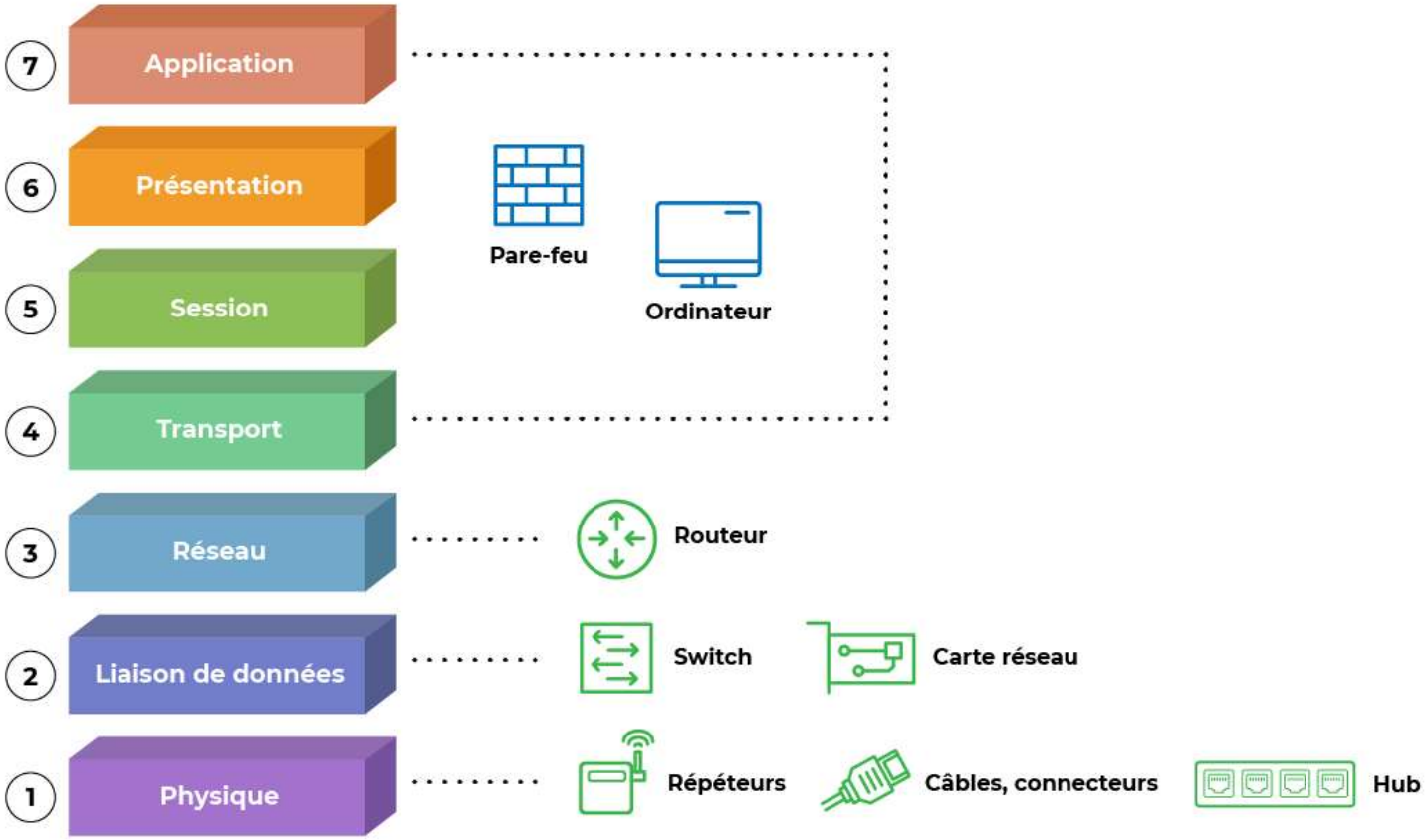
1.5. Modèle OSI : Cas d'Utilisation

- **Éducation** : Utilisé dans les cours et formations pour enseigner les principes de base des réseaux.
- **Documentation** : Fournit un cadre pour documenter et expliquer les technologies et les protocoles réseau.
- **Analyse et Dépannage** : Utilisé pour structurer l'analyse et le dépannage des problèmes réseau en se concentrant sur des couches spécifiques.

1.6. Modèle OSI : Couches (1/2)



1.6. Modèle OSI : Couches (2/2)



1.7. Adresses Réseaux : Adresse IP

- **Définition** : Adresse logique attribuée à chaque dispositif sur un réseau pour permettre leur identification et communication.
- **Format** :
  - IPv4 : 32 bits, représentée en quatre nombres décimaux séparés par des points (ex : 192.168.1.1)
  - IPv6 : 128 bits, représentée en huit groupes de quatre chiffres hexadécimaux séparés par des deux-points (ex : 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
- **Rôle** : Permet l'identification et le routage des paquets de données à travers les réseaux.

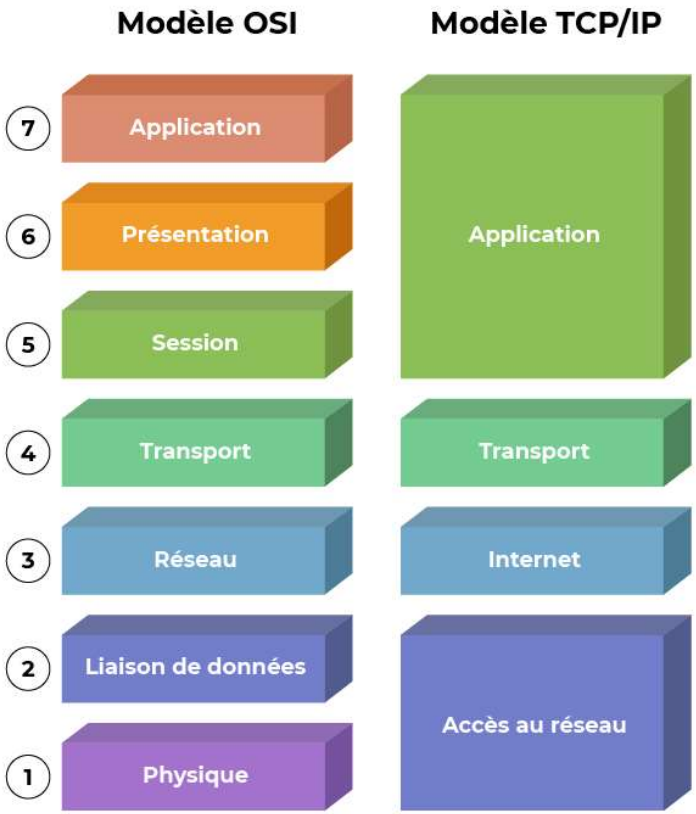
1.8. Adresses Réseaux : Adresse MAC

- **Définition** : Adresse matérielle unique attribuée à une interface réseau pour la communication au sein d'un réseau.
- **Format** : 48 bits, généralement représentés en hexadécimal (ex : 00:1A:2B:3C:4D:5E)
- **Utilisation** : Utilisée pour l'identification des dispositifs sur un réseau local.

1.9. Modèle TCP/IP: Utilité

- **Implémentation Pratique** : Le modèle TCP/IP est utilisé pour la conception et l'implémentation des réseaux, notamment l'Internet. Il est plus pratique et directement applicable que le modèle OSI.
- **Interopérabilité** : Assure que les différentes technologies et protocoles peuvent fonctionner ensemble pour fournir des services réseau.
- **Standardisation de l'Internet** : TCP/IP est la base des protocoles utilisés sur Internet, garantissant une communication fiable et standardisée à travers des réseaux diversifiés.

1.10. Modèle TCP/IP: Cas d'Utilisation



1.11. Unités de Données de Protocole (PDU)

- **Définition** : Blocs de données échangés entre les entités homologues de chaque couche des modèles.
- **Rôle** :Assure la structure et le format des données pour leur transmission efficace et correcte à travers le réseau.

1.12. PDU selon le Modèle OSI et TCP/IP

<table>
<tr><th>OSI Model</th><th>PDU</th><th>TCP/IP Stack</th></tr>
<tr><td>Application</td><td rowspan="3">Data</td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Segment</td><td>Transport</td></tr>
<tr><td>Network</td><td>Packet</td><td>Internet</td></tr>
<tr><td>Data Link</td><td>Frame</td><td rowspan="2">Network Access/Link</td></tr>
<tr><td>Physical</td><td>Bits</td></tr>
</table>

1.13. Commutateurs et Routeurs

- **Commutateur** (Switch) : Dispositif qui filtre et transfère les trames entre des segments de réseau en utilisant des adresses MAC.
- **Routeur** : Dispositif qui achemine les paquets de données entre différents réseaux en utilisant des adresses IP.

1.14. Différences entre Commutation et Routage

- **Commutation** :
  - Niveau de la couche : 2 (Liaison de Données)
  - Utilise les adresses MAC
  - Gère la communication au sein d'un même réseau
- **Routage** :
  - Niveau de la couche : 3 (Réseau)
  - Utilise les adresses IP
  - Gère la communication entre différents réseaux

1.15. Définition des Protocoles

- **Définition** : Règles et conventions pour la communication entre les dispositifs réseau.
- **Importance** : Standardisent la communication, garantissent l'interopérabilité et facilitent la gestion des réseaux.

1.16. RFC (Request for Comments)

- **Définition** : Documents publiés par l'IETF (Internet Engineering Task Force) qui décrivent les normes, protocoles, procédures et politiques pour Internet et les réseaux.
- **Rôle** : Facilite la standardisation et l'évolution des technologies de communication.

1.17. Protocole ARP (Address Resolution Protocol)

Un protocole utilisé pour mapper une adresse IP (couche 3) à une adresse MAC (couche 2) sur un réseau local.

1.18. Protocole ARP: Fonctionnement

- **Étape 1** : Un dispositif envoie une requête ARP à l'adresse MAC FF:FF:FF:FF:FF pour connaître l'adresse MAC associée à une adresse IP.
- **Étape 2** : Le dispositif cible répond avec son adresse MAC.
- **Table ARP** : Une table de correspondance stockant les paires d'adresses IP et MAC pour réduire le nombre de requêtes ARP.
- **Cache ARP** : Stocke temporairement les correspondances IP-MAC pour améliorer les performances réseau.

1.19. Protocole ICMP (Internet Control Message Protocol)

- **Définition:** Protocole de messagerie utilisé pour le diagnostic et la gestion des réseaux.
- **Rôle Principal:**
  - Signaler les erreurs de communication.
  - Échanger des informations de diagnostic.
- **Exemples d'utilisation:**
  - **Ping:** Teste la connectivité entre deux dispositifs.
  - **Traceroute:** Détermine le chemin emprunté par les paquets pour atteindre une destination.

1.20. Protocole DNS (Domain Name System)

- **Définition:** Système de résolution de noms de domaine en adresses IP.
- **Rôle Principal:** Traduire les noms de domaine lisibles par l'humain en adresses IP compréhensibles par les machines.
- **Fonctionnement:** Reçoit une requête pour un nom de domaine et renvoie l'adresse IP correspondante.

1.21. Protocole DHCP (Dynamic Host Configuration Protocol)

- **Définition:** Protocole réseau qui permet d'attribuer dynamiquement des adresses IP aux dispositifs sur un réseau.
- **Rôle Principal:** Simplifier la gestion des adresses IP en les attribuant automatiquement.

1.22. Protocole NAT (Network Address Translation)

- **Définition:** est un protocole utilisé pour modifier les adresses IP dans les paquets réseau.
- **Rôle Principal:** Permettre à plusieurs dispositifs sur un réseau local d'utiliser une seule adresse IP publique pour accéder à Internet.

Etude de cas 1

Envoi de Données dans un Même Réseau (1/3)

- **Situation**: Dispositif A (PC1) envoie des données à Dispositif B (PC2) sur le même réseau local (LAN).
- **Adresse des Dispositifs :**
  - PC1: IP = 192.168.1.2, MAC = 00:1A:2B:3C:4D:5E
  - PC2: IP = 192.168.1.3, MAC = 00:1A:2B:3C:4D:5F

Envoi de Données dans un Même Réseau (2/3)

❑Requête ARP

- PC1 vérifie son cache ARP pour l'adresse MAC associée à l'IP 192.168.1.3. Si elle n'est pas trouvée, PC1 envoie une requête ARP.
- PC2 répond avec son adresse MAC : 00:1A:2B:3C:4D:5F.

❑Envoi de la Trame

- PC1 encapsule les données dans une trame Ethernet avec :
  - Adresse MAC source : 00:1A:2B:3C:4D:5E
  - Adresse MAC destination : 00:1A:2B:3C:4D:5F
- La trame est transmise via le commutateur.

Envoi de Données dans un Même Réseau (3/3)

❑Transmission via Commutateur

- Le commutateur utilise l'adresse MAC destination pour transférer la trame à PC2.

❑Réception de la Trame

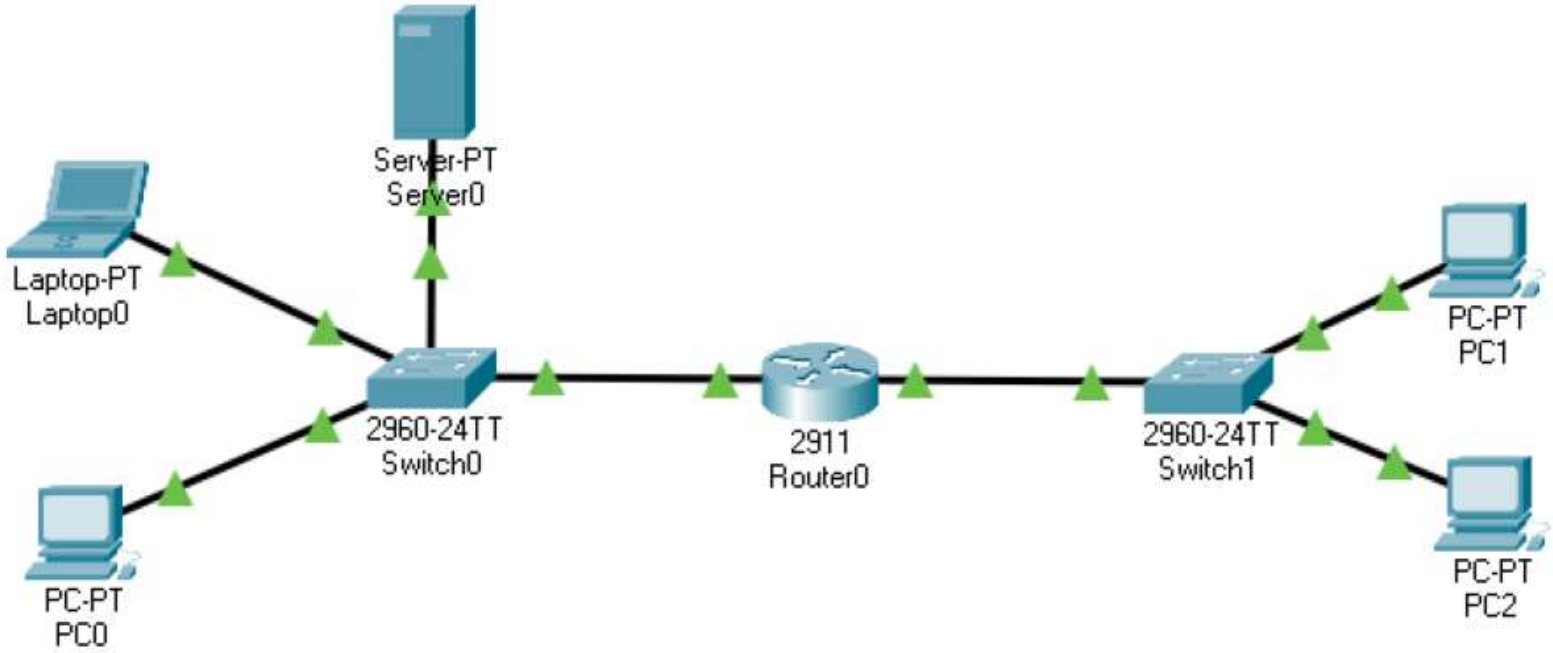
- PC2 reçoit la trame, extrait les données et les traite.

Envoi de Données entre Réseaux Différents

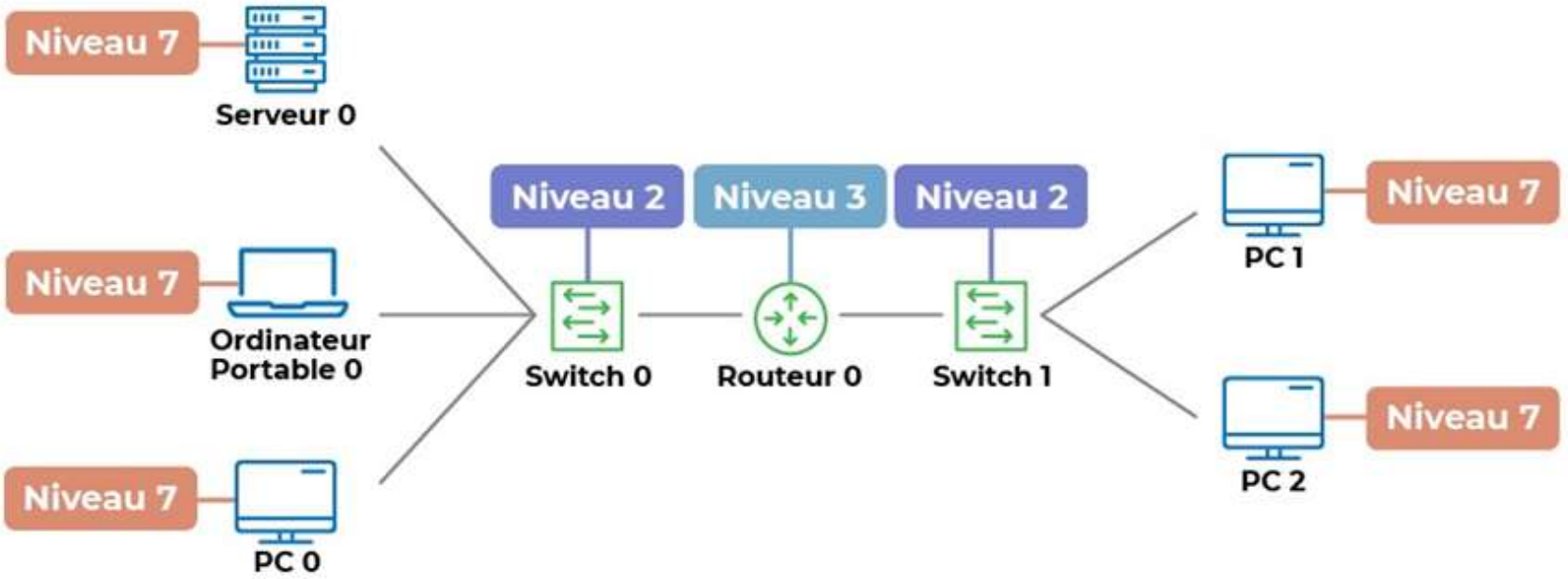
- **Situation:** Dispositif A (PC1) envoie des données à Dispositif B (PC2) situé dans un réseau différent.
- **Réseau 1** : 192.168.1.0/24
  - **PC1** : IP = 192.168.1.2, MAC = 00:1A:2B:3C:4D:5E
  - **Routeur1 (R1)** : IP = 192.168.1.1, MAC = 00:1A:2B:3C:4D:60
- **Réseau 2** : 10.0.0.0/24
  - **PC2** : IP = 10.0.0.2, MAC = 00:1A:2B:3C:4D:5F
  - **Routeur2 (R2)** : IP = 10.0.0.1, MAC = 00:1A:2B:3C:4D:61
- **Réseau intermédiaire (entre R1 et R2)** : 192.168.2.0/24
  - **R1** : IP = 192.168.2.1, MAC = 00:1A:2B:3C:4D:62
  - **R2** : IP = 192.168.2.2, MAC = 00:1A:2B:3C:4D:63

Exercice 1

Identifiez sur l'architecture réseau à quelle couche du modèle OSI est associé chacun des équipements qui le composent.



Correction: Exercice 1 (1/2)



Correction: Exercice 1 (2/2)

- Les switchs sont des équipements de niveau 2 qui comprennent les adresses MAC.
- Les routeurs sont des équipements de niveau 3 qui comprennent les adresses IP.
- Tous les équipements terminaux sont des équipements de niveau 7, car ils hébergent des applications capables de comprendre des protocoles de niveau 7.

LAB 1: Configuration Réseau et Commandes DOS

Adresse MAC

- **Objectif**: Découvrir l'adresse MAC de la carte réseau.
- **Commande**: getmac /v /fo table
- **Explication:** Cette commande affiche la liste des interfaces réseau et leurs adresses MAC.

Adresse IP

- **Objectif**: Vérifier l'adresse IP assignée à la carte réseau.
- **Commande**: ipconfig
- **Explication**: La commande ipconfig affiche la configuration IP de toutes les interfaces réseau.

Table ARP

- **Objectif:** Examiner la table ARP pour voir les adresses IP et MAC correspondantes sur votre réseau.
- **Commande:** arp -a
- **Explication:** La commande arp -a affiche les entrées de la table ARP.

DNS

- **Objectif**: Effectuer une requête DNS pour résoudre un nom de domaine en adresse IP.
- **Commande**: nslookup istburkina.com
- **Explication**: La commande nslookup permet de vérifier la résolution DNS pour un domaine donné.

DHCP

- **Objectif:** Renouveler l'adresse IP obtenue par DHCP.
- **Commande:**
  - ipconfig /release
  - ipconfig /renew
- **Explication**: La commande ipconfig /release libère l'adresse IP actuelle, et ipconfig /renew demande une nouvelle adresse IP au serveur DHCP.

Trace Route

- **Objectif**: Tracer le chemin emprunté par les paquets pour atteindre une destination.
- **Commande**: tracert istburkina.com
- **Explication**: La commande tracert affiche chaque saut (routeur) parcouru pour atteindre la destination.

Ping

- **Objectif:** Tester la connectivité réseau avec un autre dispositif.
- **Commande**: ping istburkina.com
- **Explication:** La commande ping envoie des paquets ICMP Echo Request à une destination pour vérifier la connectivité.

Netstat

- **Objectif:** Afficher les connexions réseau actives et les ports d'écoute.
- **Commande**: netstat -an
- **Explication:** La commande netstat -an affiche toutes les connexions et les ports d'écoute sous forme numérique.

ROUTE PRINT

- **Objectif:** Afficher la table de routage de l'ordinateur pour examiner les routes réseau et les chemins de destination.
- **Commande**: route print
- **Explication:** Fournit une liste des routes actuellement configurées sur l'ordinateur, incluant les réseaux disponibles, les routes par défaut, et les métriques associées à chaque chemin.

PATHPRINT

- **Objectif:** Analyser le chemin réseau et les performances de chaque nœud intermédiaire entre l'ordinateur et une destination spécifique.
- **Commande**: pathping [adresse IP ou nom d'hôte]
- **Explication:** Combine les fonctionnalités de ping et tracert, fournissant des informations détaillées sur les temps de réponse et la perte de paquets le long du chemin réseau vers une destination donnée.

Câbles Droit et Croisé

- **Objectif:** Comprendre les différences entre les câbles droits et croisés.
- **Explication:**
  - **Câble Droit:** Utilisé pour connecter des dispositifs de types différents (ex. PC à switch).
  - **Câble Croisé:** Utilisé pour connecter des dispositifs de même type (ex. PC à PC).

Rapport du LAB 1 : Exploration des Commandes Réseau

Rédigez un rapport avec des captures d'écran des différentes commandes du Lab1. Travail individuel. À rendre à l'adresse tanguykabore@yahoo.fr avant la prochaine séance avec pour objet et le nom du document PDF : « nom_prénom_RIM_2024 ». Tout mail qui ne respectera pas les consignes de nommage sera ignoré.

TEl: +226 75643226

Master 1 Réseaux Informatiques

Architecture des réseaux

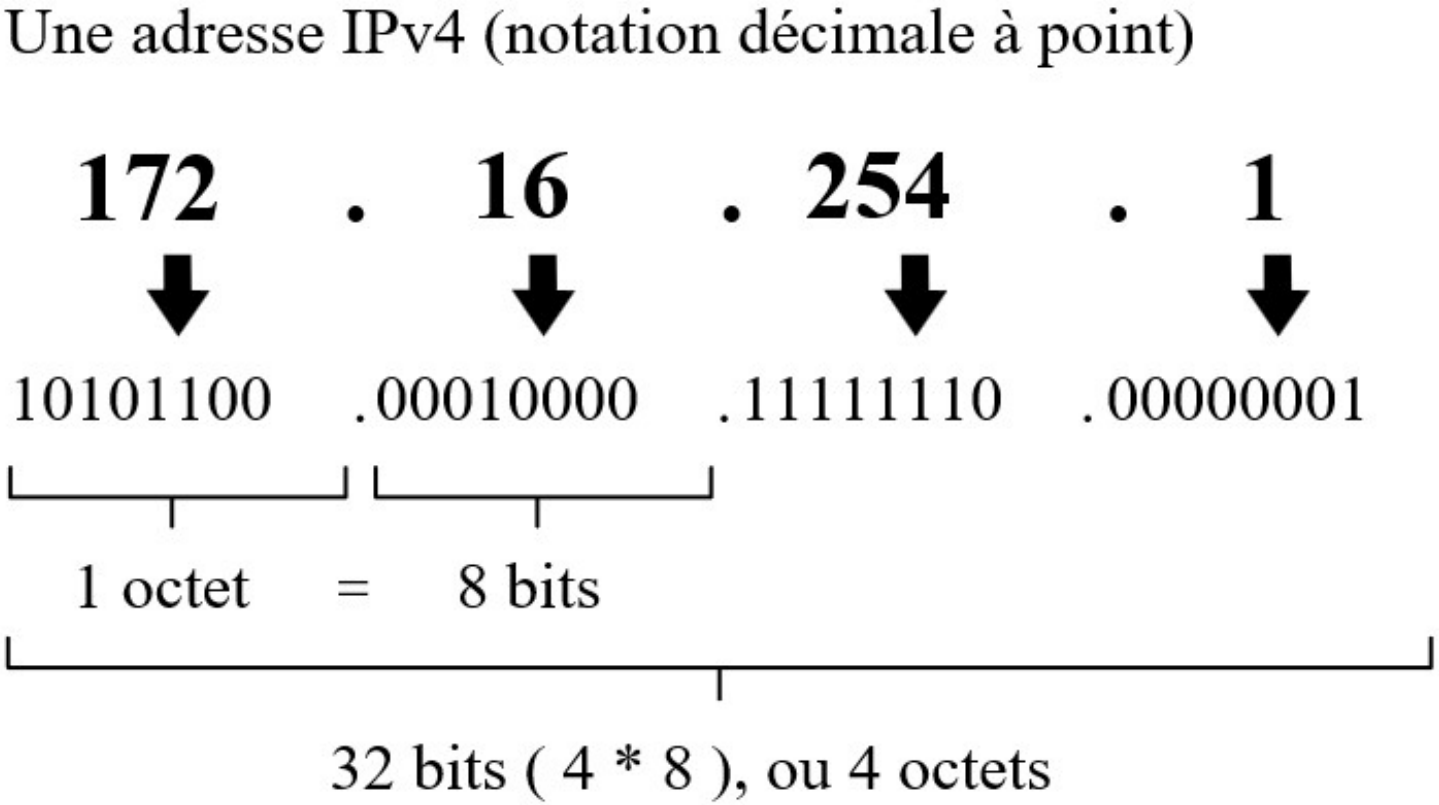
B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 2: Adressage IPv4

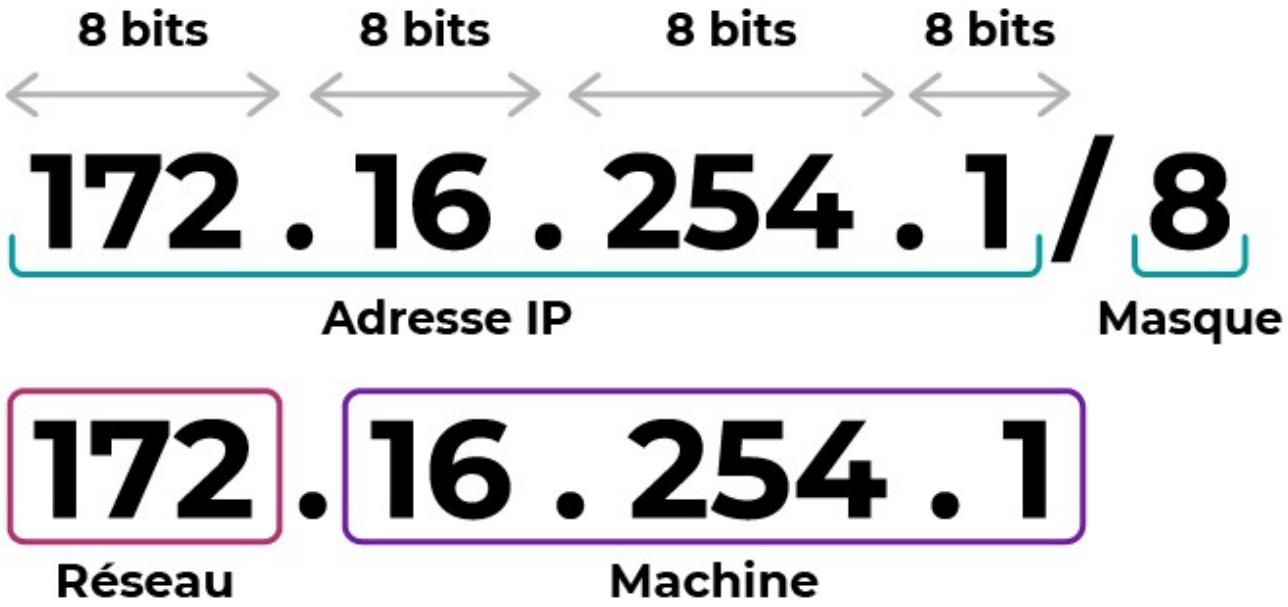
1.1. Adresse IPv4



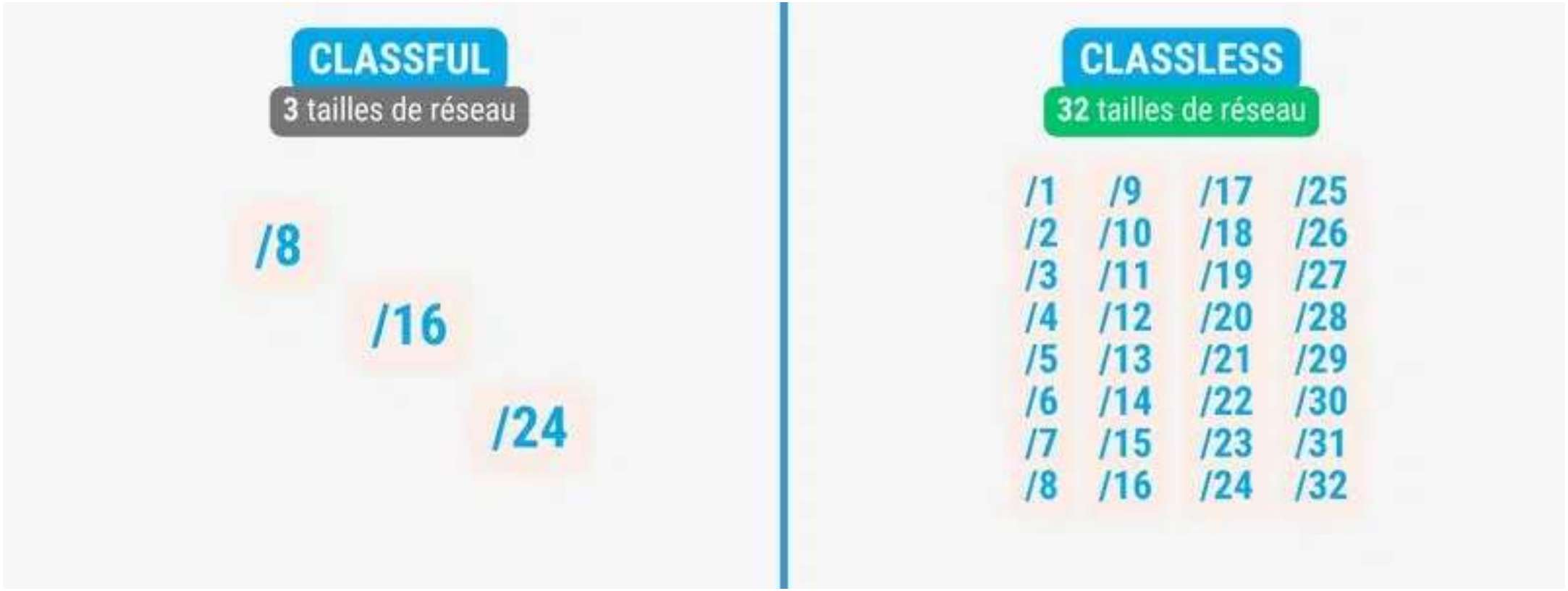
1.2. Masque de réseau

C'est une suite de 32 bits dont la partie des bits qui fixent l'adresse de réseau est une série continue de 1 (partie gauche) et la partie qui correspond aux hôtes est une série continue de 0 (partie droite).

1.3. Notation CIDR (Classless Inter-Domain Routing)



1.4. Type d’adressage



1.5. Classe d'adresse

1.6. Calcul de l'adresse réseau

Elle est calculée par application en binaire du masque sur l'adresse IP en utilisant la fonction ET (AND logique).

Seul 1 ET 1 = 1, toutes les autres combinaisons produisent un 0.

1.7. Calcul de l'adresse de diffusion

L’adresse de diffusion d'un réseau est la dernière adresse du réseau. Elle est donc constituée en positionnant tous les bits de l'hôte à 1. Elle s’obtient en faisant un OU logique entre l’adresse de réseau et l’inverse du masque.

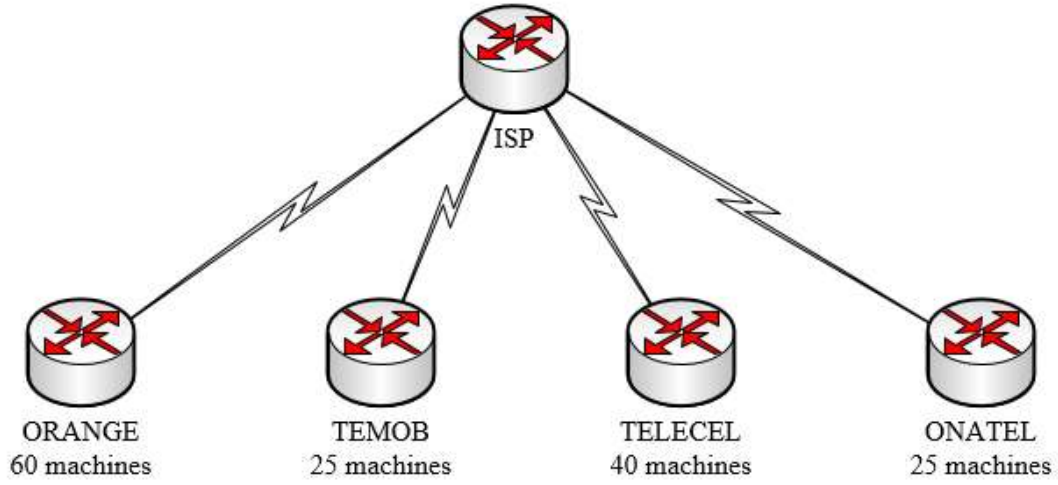
1.8. Calcul de la plage adressable

La plage adressable est l'ensemble des adresses que peut prendre un hôte sur le réseau. La première adresse de la plage est donc celle qui suit l'adresse réseau. La dernière adresse de la plage est donc celle qui précède l'adresse de diffusion.

1.9. VLSM (Variable Length Subnet Masking)

- **Définition**: Technique d'adressage IP qui permet d'utiliser des sous-réseaux de tailles différentes au sein d'un même réseau.
- **Avantages**:
  - Utilisation efficace de l'espace d'adressage IP.
  - Réduction du gaspillage d'adresses IP.

Exercice 2 : (Adressage IP VLSM)



Soit le réseau étendu avec l'adresse réseau suivante : 192.128.16.0/21. Déterminer les identifiants réseaux des LAN et WAN.

LAB 2: VLSM

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 3: Routage

1.1. Concept de Routage

- **Définition** : Le routage est le processus de sélection des chemins dans un réseau pour envoyer des données de la source à la destination.
- **Importance** :
  - **Optimisation** : Assure l'utilisation efficace des chemins disponibles.
  - **Fiabilité** : Permet la redondance et la tolérance aux pannes.
  - **Scalabilité** : Facilite la gestion des grands réseaux.

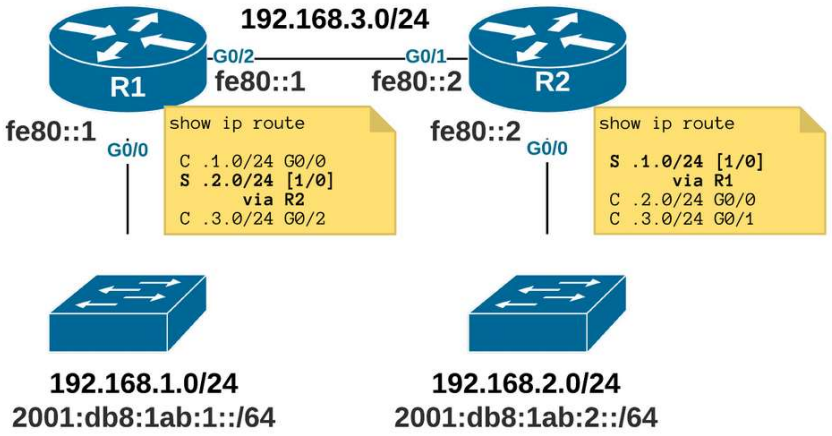
1.2. Protocoles de routage

Pour les réseaux, un protocole constitue un ensemble de règles normalisées de formatage des données conçu pour permettre à n'importe quel ordinateur connecté de comprendre les données. Un protocole de routage est un protocole utilisé pour identifier ou annoncer les chemins réseau.

1.3. Types de Routage: Route statique

- **Définition** : Configuration manuelle des routes par l'administrateur réseau.
- **Avantages** : Simplicité, contrôle total.
- **Inconvénients** : Maintenance lourde, absence de redondance automatique.

1.4. Table de route

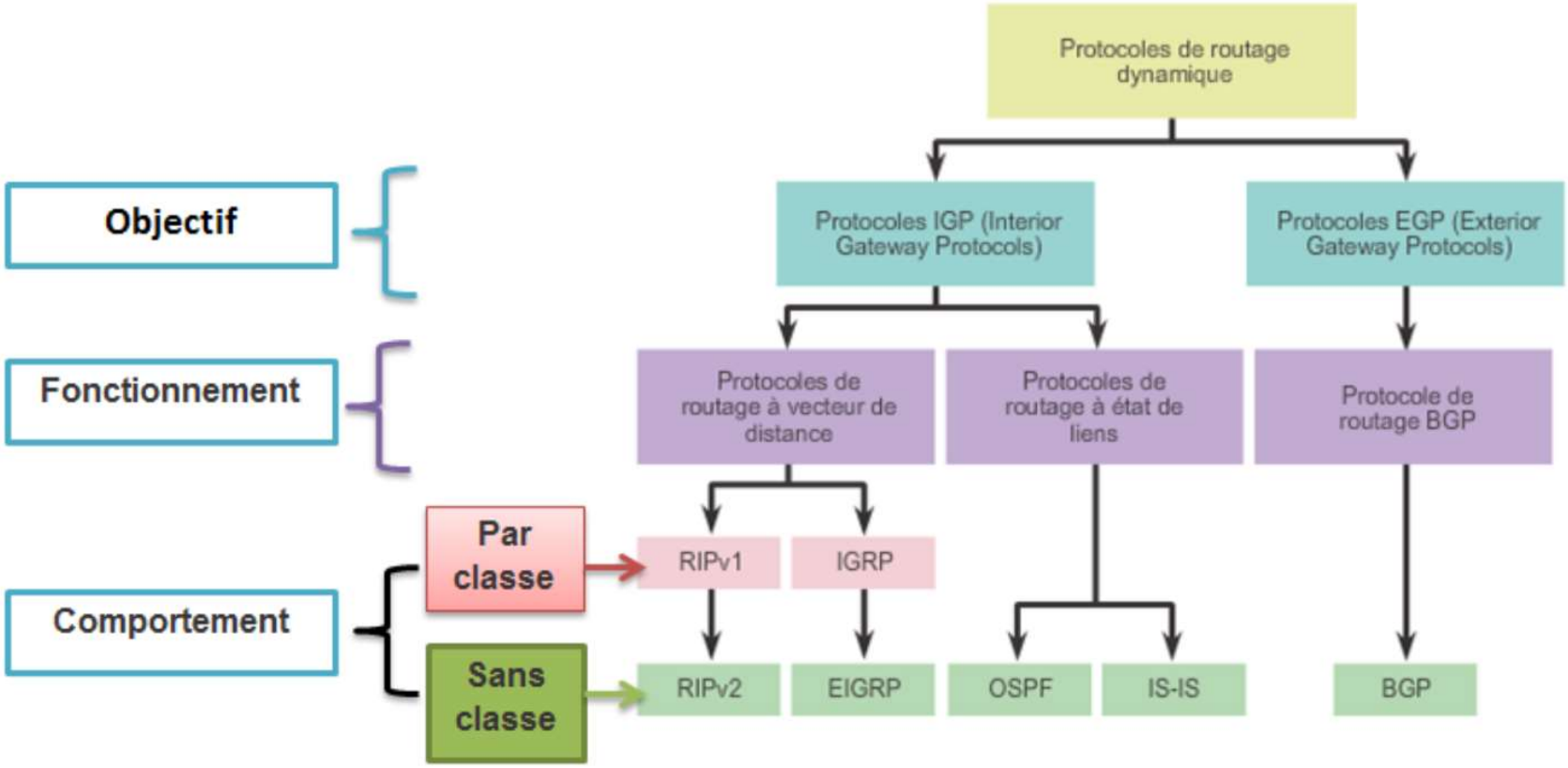


Routeur	Adresse de sous réseau de destination	Masque de sous réseau	Passerelle

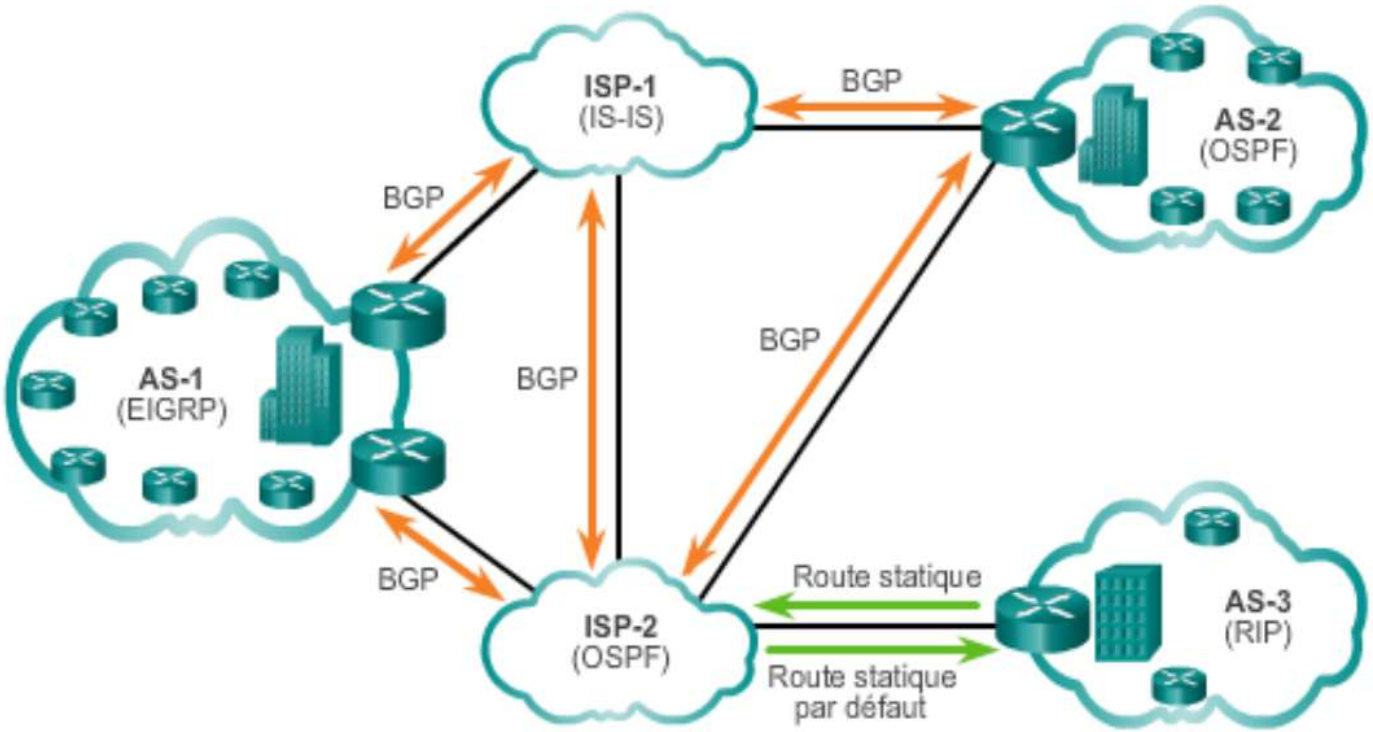
1.5. Types de Routage : Route dynamique

- **Définition** : Utilisation de protocoles de routage pour découvrir et maintenir automatiquement les routes.
- **Exemples de Protocoles** :
  - **RIP (Routing Information Protocol)**
  - **OSPF (Open Shortest Path First)**
  - **EIGRP (Enhanced Interior Gateway Routing Protocol)**
  - **BGP (Border Gateway Protocol)**
- **Avantages** : Adaptabilité, gestion automatique des routes.
- **Inconvénients** : Complexité, utilisation des ressources.

1.6. Classification des protocoles de routage



1.7. Comparaison IGP et EGP



1.8. Comparaison des protocoles de routage

	Vecteur de distance				État des liens	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Vitesse de convergence	Lente	Lente	Lente	Rapide	Rapide	Rapide
Évolutivité: taille du réseau	Faible	Faible	Faible	Élevée	Élevée	Élevée
Utilisation de VLSM	Non	Oui	Non	Oui	Oui	Oui
Utilisation des ressources	Faible	Faible	Faible	Moyenne	Élevée	Élevée
Implémentation et maintenance	Simple	Simple	Simple	Complexe	Complexe	Complexe

LAB 3: Configuration des équipements CISCO

Mode de Configuration Globale

Accéder au mode de configuration globale pour commencer la configuration :

Commandes:

- Router>enable
- Router#configure terminal

Changement du Nom d'Hôte

Commande pour changer le nom du routeur :

Commandes:

- Router(config)#hostname nouveau-nom

Configuration du Mot de Passe: Enable/Secret

Pour configurer le mot de passe enable (en clair) :

Commandes:

- Router(config)#enable password votre-mot-de-passe

Pour configurer le mot de passe secret (crypté) :

Commandes:

- Router(config)#enable secret votre-mot-de-passe

Configuration du Mot de Passe Console

Pour configurer le mot de passe console :

Commandes:

- Router(config)#line console 0
- Router(config-line)#password mot-de-passe-console
- Router(config-line)#login

Commande de Synchronisation des Logs

Pour empêcher les messages d'état d'interrompre les commandes :

Commandes:

- Router(config-line)#logging synchronous

Configuration du Mot de Passe Telnet

Pour configurer le mot de passe Telnet :

Commandes:

- Router(config)#line vty 0 4
- Router(config-line)#password mot-de-passe-telnet
- Router(config-line)#login

Remarques: Utilisez line vty 0 15 pour plus de sessions simultanées

Configuration de SSH (1/2)

Routeur# conf t

Routeur(config)# ip domain-name [domaine]

Routeur(config)# crypto key generate rsa

Routeur(config)# ip ssh version 2

Routeur(config)# username [utilisateur] privilege 15 secret [mot_de_passe]

Configuration de SSH (2/2)

Routeur(config)# line vty 0 4

Routeur(config-line)# transport input ssh

Routeur(config-line)# login local

Routeur(config-line)# exit

Configuration du DHCP (1/2)

Routeur# configure terminal

Routeur(config)# ip dhcp excluded-address <adresse-IP-début> <adresse-IP-fin>

Routeur(config)# ip dhcp pool <nom-du-pool>

Routeur(dhcp-config)# network <réseau> <masque-sous-réseau>

Routeur(dhcp-config)# default-router <adresse-IP-passerelle>

Routeur(dhcp-config)# dns-server <adresse-IP-DNS>

Routeur(dhcp-config)# lease <durée-en-jours>

Configuration du DHCP (2/2)

Si le serveur DHCP se trouve sur un réseau différent de celui du client, on doit configurer l'interface sur le routeur pour relayer les requêtes DHCP. Cela se fait en ajoutant l'adresse IP du serveur DHCP avec la commande ip helper-address.

Routeur(config)# interface <interface>

Routeur(config-if)# ip helper-address <adresse-IP-serveur-DHCP>

Sauvegarde de la Configuration

Sauvegarder la configuration en RAM vers la NVRAM :

Commandes:

- Router#copy running-configuration startup-configuration

Commandes abrégées :

- Router#copy run start

Sauvegarde de la Configuration sur TFTP

Routeur> show file systems

Routeur> dir flash:

Routeur> dir nvram:

Routeur# copy running-config tftp

Routeur# copy tftp running-config

Configuration des Adresses IPv4

Attribuer une adresse IPv4 à une interface :

Commandes:

- Router(config)#interface type-interface numéro-interface
- Router(config-if)#ip address adresse-ip-interface masque-sous-réseau

Activer l'interface :

- Router(config-if)#no shutdown

Ajouter une Description d'Interface

Ajouter une description informative à une interface :

Commandes:

- Router(config-if)#description Votre Description

Configurer la Valeur de Bande Passante

Modifier la bande passante pour les calculs de routage.
Bande passante de l'interface en kilobits par seconde :

Commandes:

- Router(config-if)#bandwidth valeur-bande-passante

Régler la Vitesse et le Mode Duplex

Régler la Vitesse et le Mode Duplex

- **Régler le mode duplex** :
  - Router(config-if)#duplex mode-duplex
- **Régler la vitesse du port** :
  - Router(config-if)#speed vitesse-port
- **mode-duplex** : auto, half, full
- **vitesse-port** : 10, 100, 1000, auto

Configuration d'une Bannière de Connexion

Définir une bannière à afficher lors de la connexion au routeur :

Commandes:

- Router(config)#banner motd #Votre Message Ici#

Encryption des Mots de Passe

- Chiffrement des mots de passe pour les rendre incompréhensibles dans la configuration en cours d'exécution
- Le mot de passe secret est déjà chiffré, mais les autres mots de passe (vty, console, auxiliaire) ne le sont pas

Activer le Service de Chiffrement

Commande pour chiffrer les mots de passe. Utiliser cette commande avant de définir les mots de passe:

Commandes:

- Router(config)#service password-encryption

Désactiver le Service de Chiffrement

Désactiver le service de chiffrement après avoir configuré les mots de passe :

Commandes:

- Router(config)#no service password-encryption

Afficher la configuration en cours

Commandes:

- Router#show running-config

LAB 4: Configuration des routes

Configuration du Routage Statique

Commande pour configurer une route statique :

Commandes:

- Router(config)#ip route [adresse-réseau-destination] [masque-sous-réseau] [adresse-next-hop]

Ou

- Router(config)#ip route [adresse-réseau-destination] [masque-sous-réseau] [interface-de-sortie]

Configuration des Routes par Défaut

Utilisée pour les réseaux en impasse ou pour acheminer tout le trafic via un chemin spécifique. Commande pour configurer une route par défaut :

Commandes:

- Router(config)#ip route 0.0.0.0 0.0.0.0 [adresse-next-hop]

Ou

- Router(config)#ip route 0.0.0.0 0.0.0.0 [interface-de-sortie]

Configuration du Réseau par Défaut

Configuration d'une passerelle de dernier recours. Nécessite une autre route statique pour indiquer l'interface de sortie ou l'adresse next-hop:

Commandes:

- Router(config)#ip default-network [adresse-réseau-par-défaut]

Distance Administrative

Ce tableau présente les valeurs par défaut de la distance administrative pour différentes sources d'information de routage. Plus le nombre est petit, plus la confiance accordée à cette source est élevée.

Source d'information de routage	Distance administrative par défaut
Réseau directement connecté	0
Route statique	1
EIGRP interne	90
IGRP	100
OSPF	110
Système intermédiaire à système intermédiaire (IS-IS)	115
Protocole d'information de routage (RIP)	120

Distance Administrative des Routes Statiques

La distance administrative définit la confiance accordée à une information de routage. Commande pour configurer une distance administrative pour les routes par défaut :

Commandes:

- Router(config)#ip route 0.0.0.0 0.0.0.0 [adresse-next-hop] [distance-administrative]

Ou

- Router(config)#ip route 0.0.0.0 0.0.0.0 [interface-de-sortie] [distance-administrative]

Configuration de RIPv2 (1/2)

Activer le protocole RIP sur le routeur

Commandes:

- Router(config)#router rip

Identifier les réseaux à annoncer avec la commande network :

Commandes:

- Router(config-router)#network network-id

Configuration de RIPv2 (2/2)

Configurer le routeur pour recevoir et envoyer uniquement les paquets Version 2 :

Commandes:

- Router(config-router)#version 2

Empêcher les mises à jour d'être diffusées sur Internet :

Commandes:

- Router(config-router)#passive-interface interface-type interface-number

Vérification de la Configuration RIP

Vérifier la configuration RIP avec les commandes :

Commandes:

- Router#show ip route
- Router#show ip protocols
- Router#debug ip rip

Configuration de OSPF

Activer le processus OSPF :

Commandes:

- Router(config)#router ospf process-number

Annoncer les réseaux directement connectés à la Zone 0 :

Commandes:

- Router(config-router)#network network-address wildcard-mask area 0

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 4: Réseaux LAN

1.1. Norme IEEE 802.3

- La norme IEEE 802.3 définit l'Ethernet.
- Elle spécifie les caractéristiques physiques et les méthodes d'accès au média.
- Utilisée pour les réseaux locaux (LAN).

1.2. Standards Ethernet

- Ethernet 10BASE-T : 10 Mbps, câbles UTP Cat5;
- Fast Ethernet (100BASE-TX) : 100 Mbps, câbles UTP Cat5e;
- Gigabit Ethernet (1000BASE-T) : 1 Gbps, câbles UTP Cat5e ou Cat6;
- 10 Gigabit Ethernet (10GBASE-T) : 10 Gbps, câbles UTP Cat6a ou Cat7.

1.2. Évolution de la norme IEEE 802.3

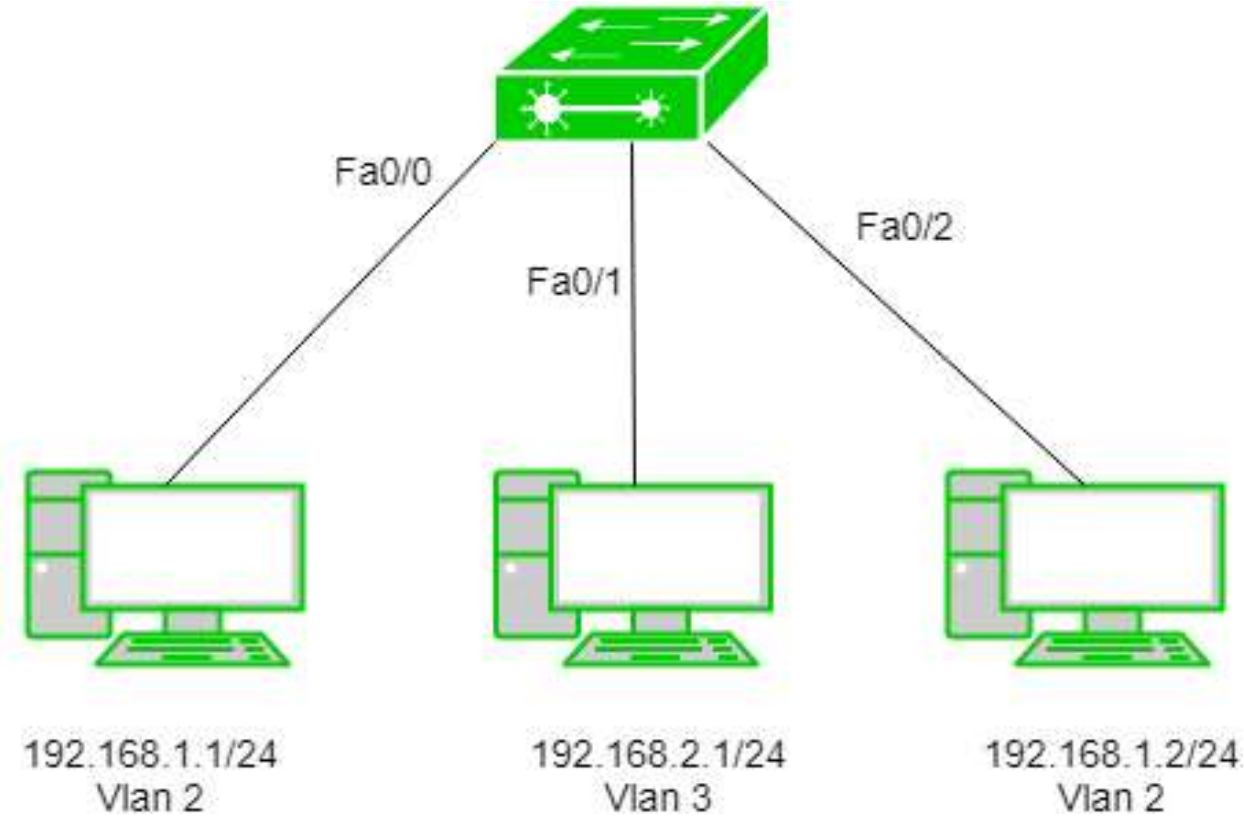
Progression des capacités de la norme pour s'adapter aux besoins croissants en bande passante.

- IEEE 802.3u : Fast Ethernet (100 Mbps).
- IEEE 802.3z : Gigabit Ethernet (1 Gbps sur fibre).
- IEEE 802.3ab : Gigabit Ethernet (1 Gbps sur cuivre).
- IEEE 802.3an : 10 Gigabit Ethernet.

1.3. Virtual Local Area Network (1/5)

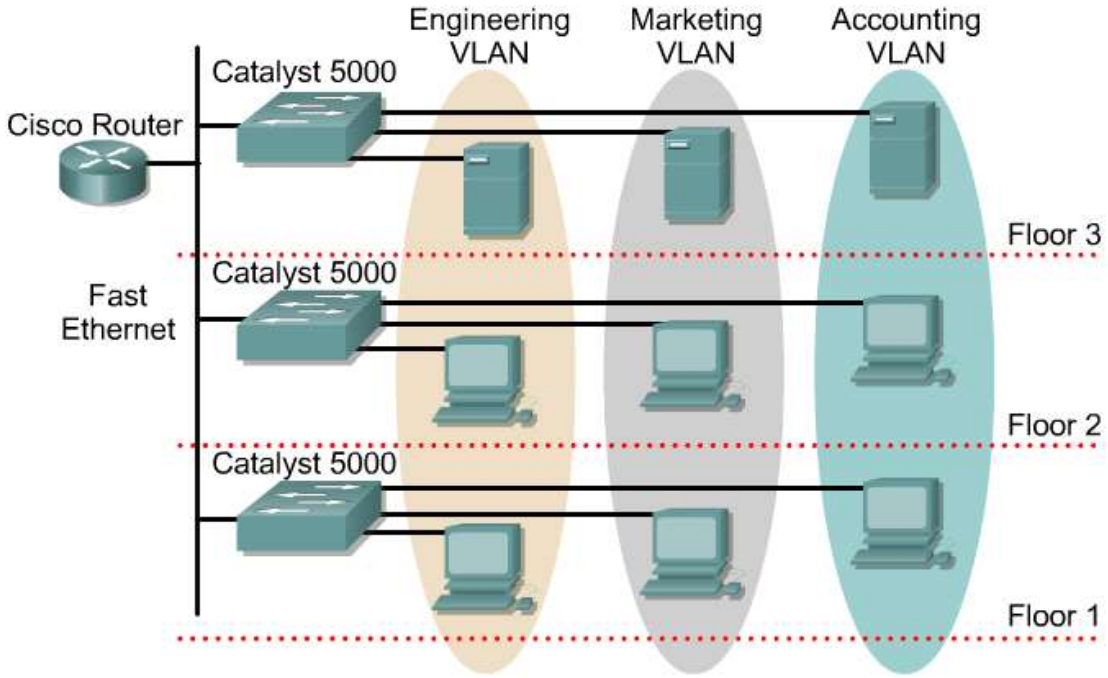
- Un Virtual Local Area Network (VLAN) permet de segmenter logiquement un réseau physique.
- Crée plusieurs réseaux virtuels à partir d'un seul switch physique.

1.3. Virtual Local Area Network (2/5)



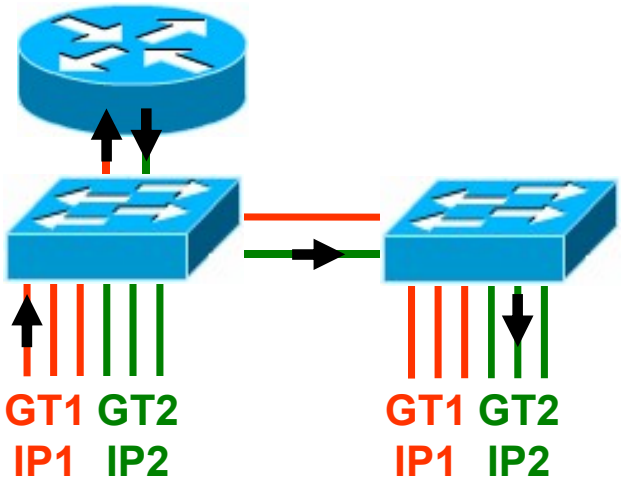
1.3. Virtual Local Area Network (3/5)

- Réseau logique, non tributaire de l'emplacement physique
- Les domaines de broadcast sont définis administrativement
- Les utilisateurs sont affectés par logiciel aux différents VLANs
- Un switch contient donc un IOS et une base de données montrant l'appartenance aux VLANs

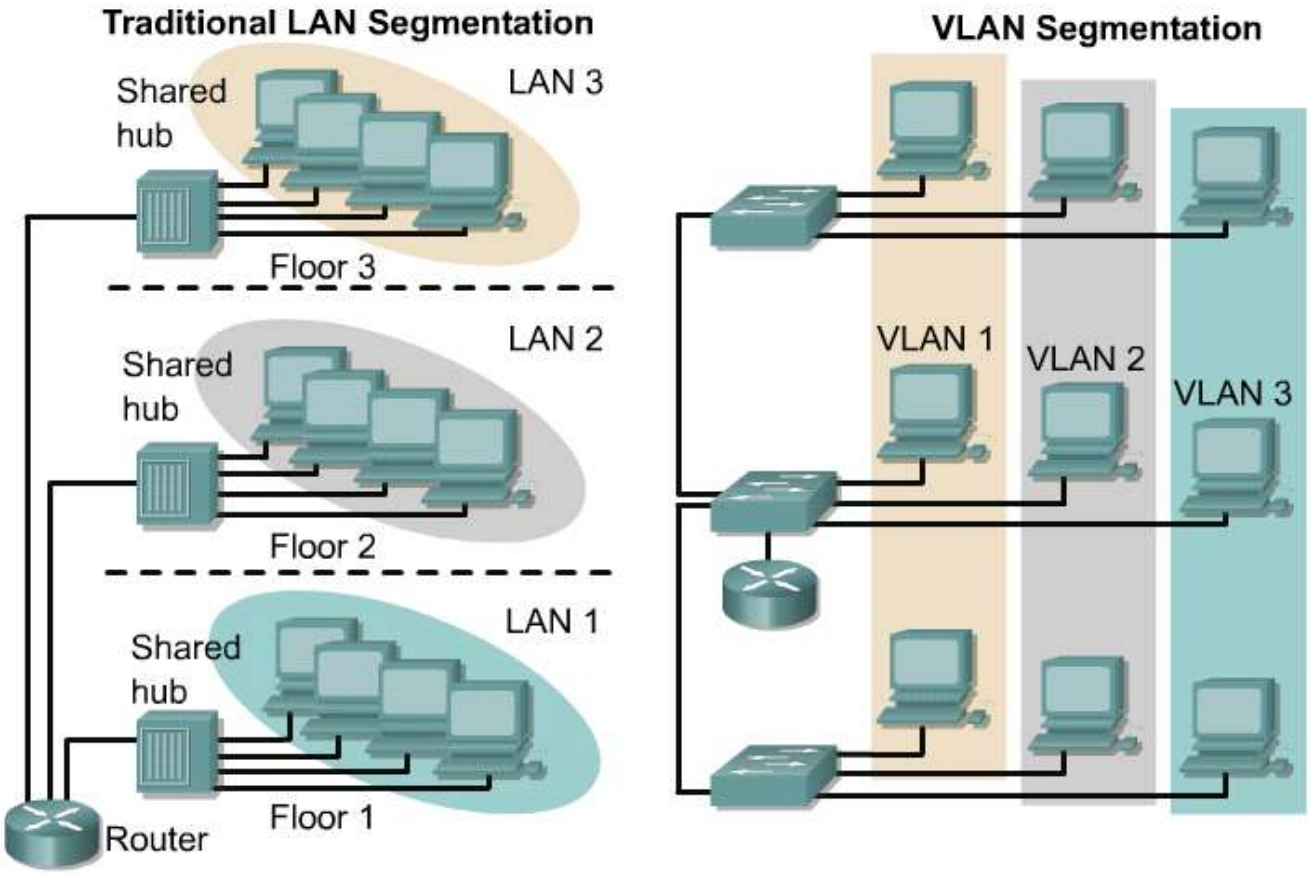


1.3. Virtual Local Area Network (4/5)

- La segmentation crée des groupes séparés strictement
- La séparation peut être rendue perméable par l'utilisation d'un routeur
- Ceci qui conduit alors à attribuer des réseaux IP différents pour chaque VLAN



1.3. Virtual Local Area Network (5/5)



1.4. Avantages des VLANs

- Sécurité : Les VLANs isolent le trafic entre différents groupes de travail.
- Performance : Réduction du domaine de diffusion, réduisant la congestion du réseau.
- Flexibilité : Les utilisateurs peuvent être regroupés logiquement sans être physiquement connectés à la même infrastructure.

1.5. Types de VLANs

- VLAN par port : Basé sur les ports du switch.
- VLAN par adresse MAC : Basé sur l'adresse MAC de l'appareil.
- VLAN par protocole : Basé sur le protocole réseau (par ex., IP, IPX).
- VLAN par sous-réseau : Basé sur la plage d'adresses IP.

1.6. IEEE 802.1Q

- IEEE 802.1Q est une norme qui définit le VLAN tagging (étiquetage de VLANs) dans les réseaux Ethernet.
- Elle permet d'identifier et de transporter des trames appartenant à différents VLANs sur le même lien physique, appelé trunk.

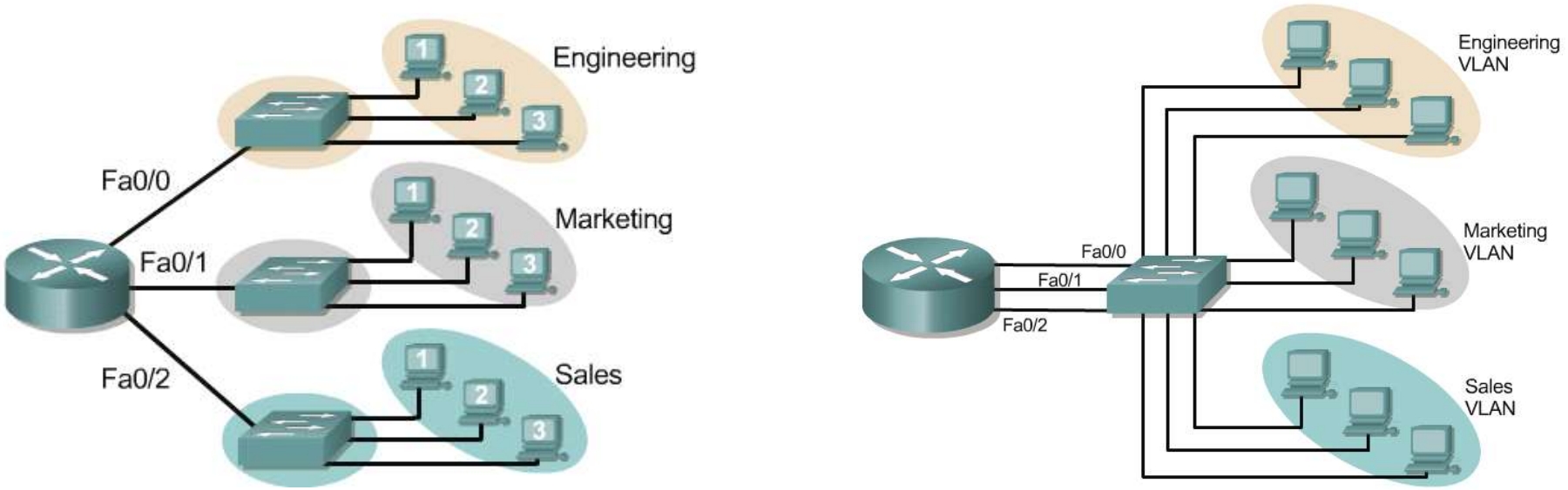
1.7. VLAN Tagging

- VLAN tagging ajoute une étiquette (tag) de 4 octets à une trame Ethernet pour identifier le VLAN auquel elle appartient.
- Ce tag contient l'ID VLAN (12 bits) et d'autres informations comme la priorité.

1.8. Trunking avec VLANs (1/3)

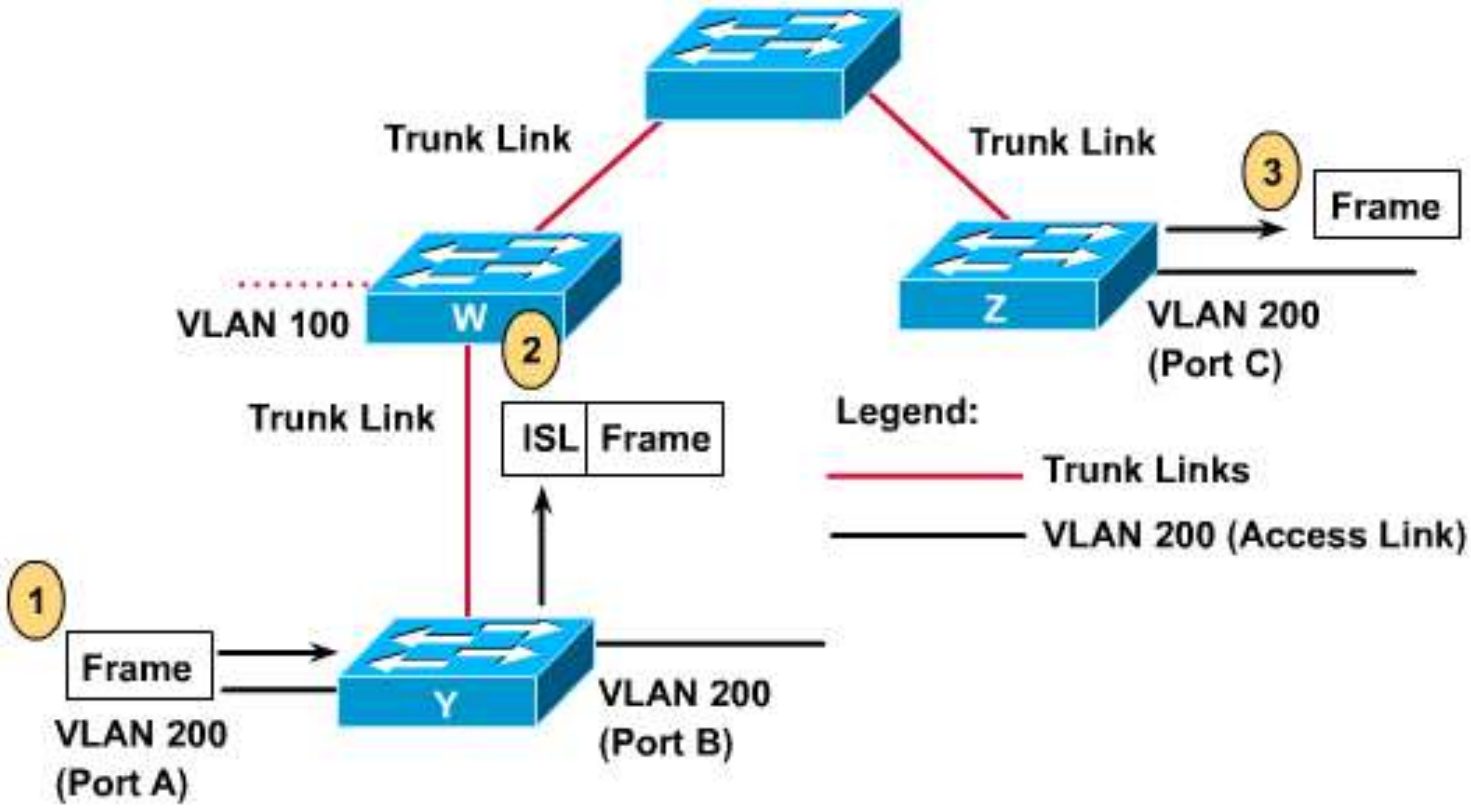
- Un trunk transporte plusieurs VLANs sur un seul lien entre des switches.
- Utilise les protocoles IEEE 802.1Q ou ISL pour identifier le VLAN de chaque trame.

1.8. Trunking avec VLANs (2/3)



- Trois domaines de broadcast dans les deux cas :
  - à gauche, sans VLAN : 1 routeur et 3 switch
  - à droite, avec VLAN : 1 routeur et 1 switch

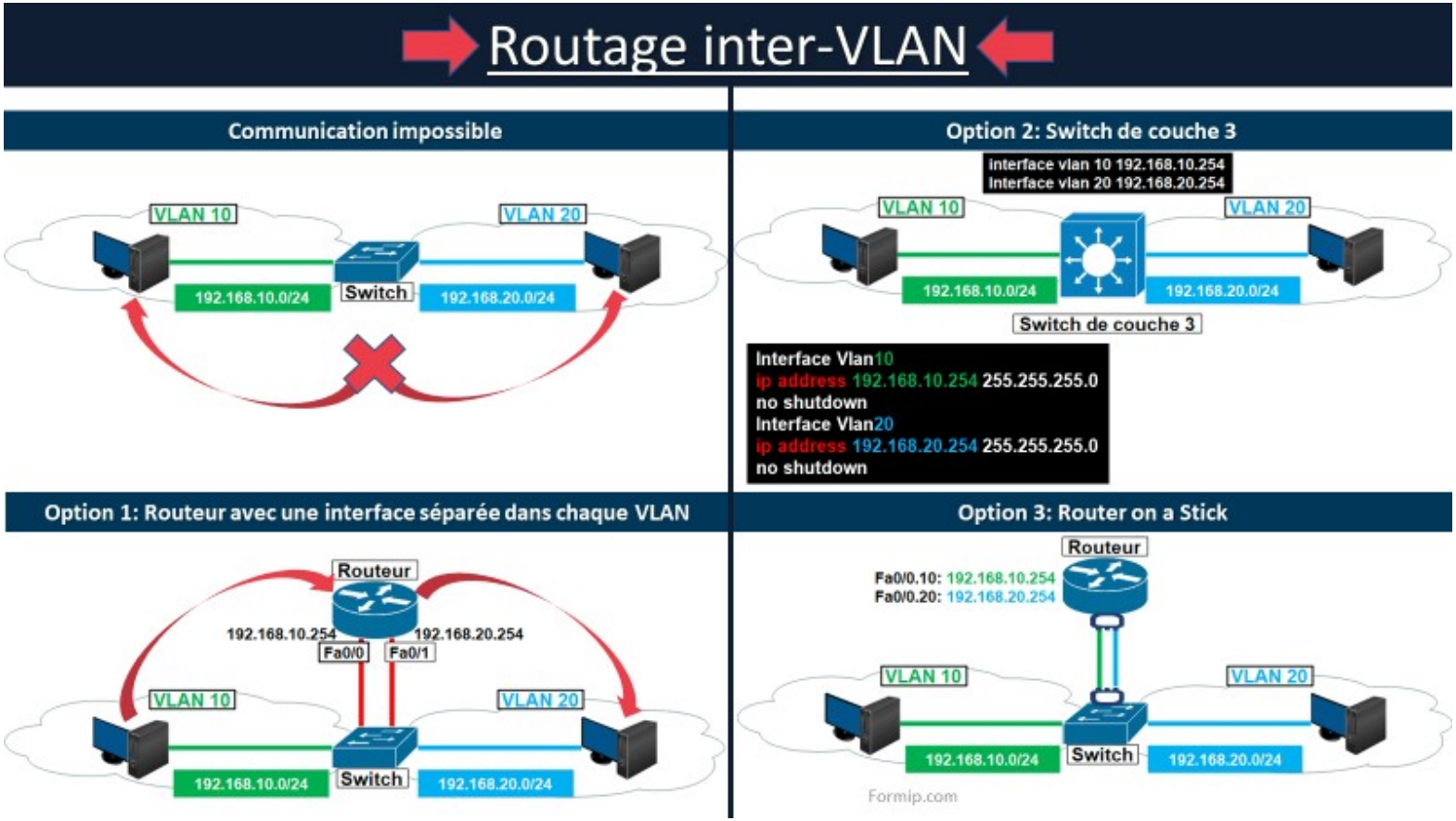
1.8. Trunking avec VLANs (3/3)



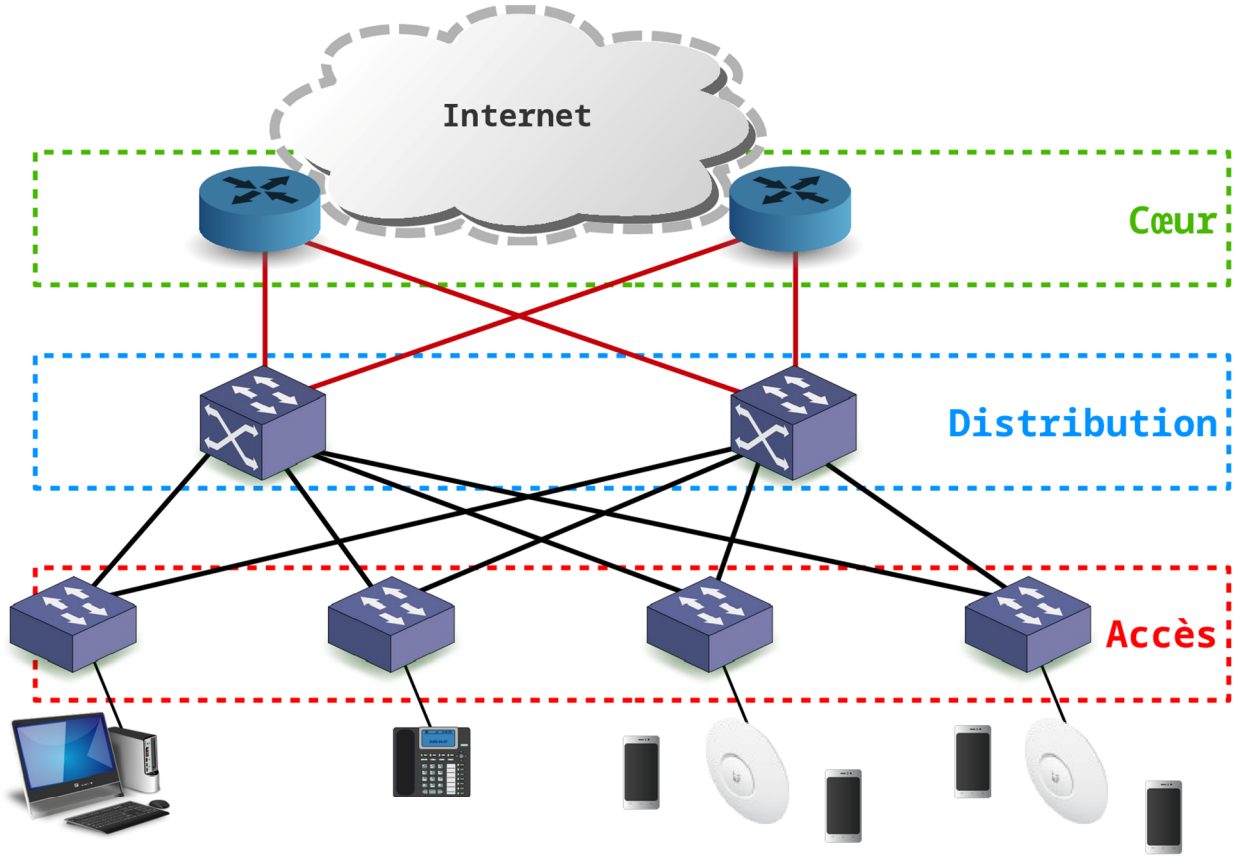
1.9. Routage Inter-VLAN

- Le routage inter-VLAN permet aux périphériques appartenant à différents VLANs de communiquer entre eux via un routeur ou un switch de niveau 3 (L3).
- Chaque VLAN correspond à un sous-réseau distinct.
- Sans routage inter-VLAN, les VLANs restent isolés.
- Nécessite un dispositif de niveau 3 (switch ou routeur) pour effectuer le routage.

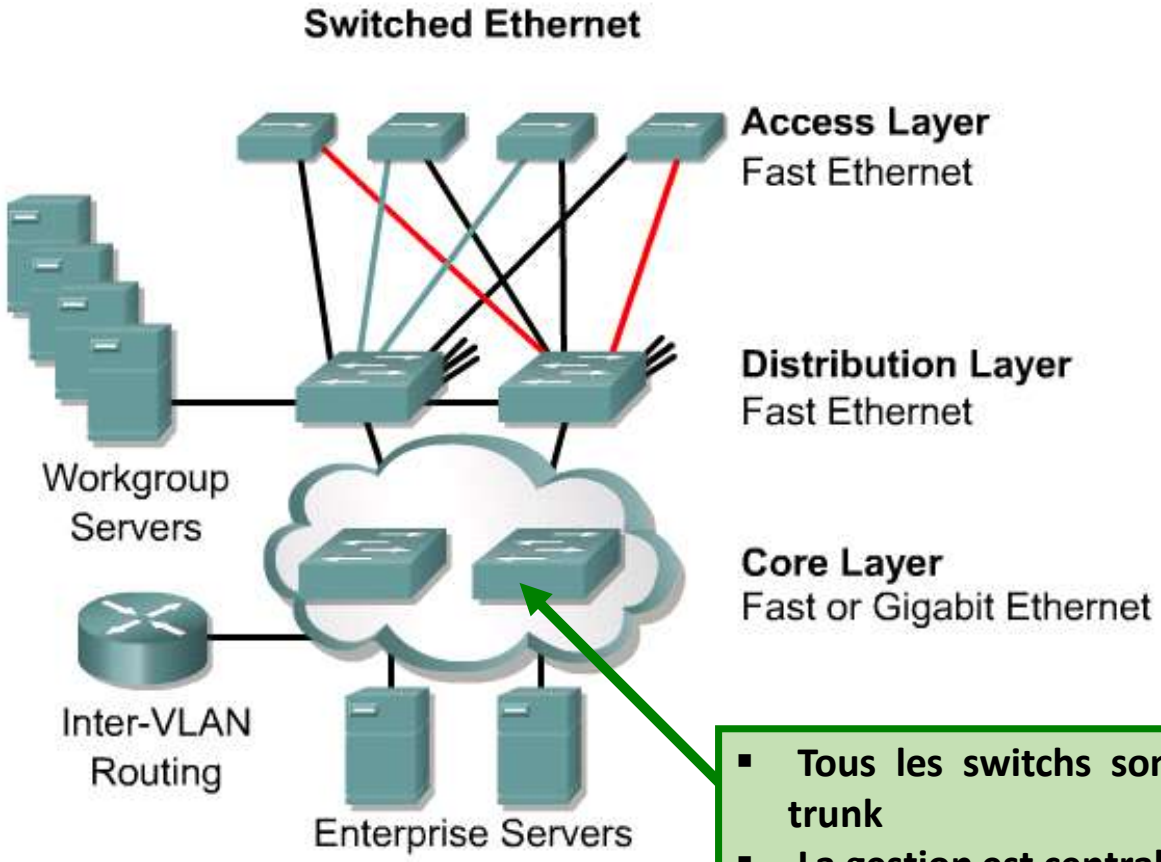
1.9. Routage Inter-VLAN



1.10. Architecture en couche (1/2)



1.10. Architecture en couche (2/2)



- **Tous les switchs sont reliés par des trunk**
- **La gestion est centralisée par VTP**
- **Un seul routeur pour tous les VLANs**

LAB 5: Configuration des VLANs

Configuration des VLANs sur un Switch

Switch# configure terminal

Switch(config)# vlan <VLAN-ID>

Switch(config-vlan)# name <VLAN-NAME>

Switch(config-vlan)# exit

Attribuer une Interface à un VLAN

Switch# configure terminal

Switch(config)# interface <INTERFACE-ID>

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan <VLAN-ID>

Switch(config-if)# exit

Configuration d’un Trunk (pour la communication entre plusieurs VLANs)

Switch# configure terminal

Switch(config)# interface <INTERFACE-ID>

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport trunk allowed vlan <VLAN-LIST>

Switch(config-if)# exit

Configuration du Routage Inter-VLAN avec un Routeur (Router-on-a-stick)

Switch# configure terminal

Switch(config)# interface <INTERFACE-ID>

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport trunk allowed vlan <VLAN-LIST>

Switch(config-if)# exit

Configurer le Routage Inter-VLAN sur le Routeur (Sous-interfaces)

Router# configure terminal

Router(config)# interface gig0/0

Router(config-if)# no shutdown

Router(config-if)# interface gig0/0.<SUBIF-ID>

Router(config-subif)# encapsulation dot1q <VLAN-ID>

Router(config-subif)# ip address <IP-ADDRESS> <SUBNET-MASK>

Router(config-subif)# exit

Configuration du Routage Inter-VLAN avec un Switch Layer 3

Switch# configure terminal

Switch(config)# interface vlan <VLAN-ID>

Switch(config-if)# ip address <IP-ADDRESS> <SUBNET-MASK>

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# ip routing

Vérification des configurations VLAN

Switch# show vlan brief

Switch# show interfaces trunk

Switch# show ip interface brief

Switch# show ip route

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 5: Commutation avancée

1.1. Qu'est-ce que le VTP ?

- Le VLAN Trunking Protocol (VTP) est un protocole Cisco propriétaire utilisé pour propager les informations de VLANs sur un réseau de switches.
- Facilite la gestion des VLANs en permettant la configuration centralisée sur un seul switch.

1.2. Modes de Fonctionnement du VTP

- VTP Server Mode : Le switch en mode serveur peut ajouter, supprimer et modifier des VLANs. Les modifications sont propagées aux autres switches.
- VTP Client Mode : Le switch en mode client reçoit les informations VLAN du serveur et ne peut pas effectuer de modifications.
- VTP Transparent Mode : Le switch en mode transparent ne participe pas à la gestion VTP mais transmet les messages VTP aux autres switches.

1.3. Avantages et Limitations du VTP

❑Avantages :

- Simplifie l'administration des VLANs.
- Réduit les erreurs manuelles lors de la configuration de plusieurs switches.

❑Limitations :

- Mauvaise configuration peut entraîner la propagation d'informations incorrectes dans tout le réseau.
- Fonctionne uniquement avec des switches Cisco.

1.4. Qu'est-ce que le Spanning Tree Protocol (STP) ?

- STP est un protocole réseau utilisé pour prévenir les boucles dans les réseaux Ethernet. Il garantit qu'il n'existe qu'un seul chemin actif entre deux switches dans un réseau local.
- STP crée une arborescence en désactivant les liaisons redondantes jusqu'à ce qu'elles soient nécessaires.
- Défini dans la norme IEEE 802.1D.

1.5. Comment Fonctionne STP ?

- STP élit un Root Bridge (switch racine) pour être le centre de l'arborescence.
- Tous les autres switches calculent le chemin le plus court vers le Root Bridge.
- Les liaisons redondantes sont mises en état bloqué pour prévenir les boucles.

1.6. États des Ports dans STP

❑Les ports dans STP passent par plusieurs états avant de devenir actifs :

- Blocking : Empêche les boucles en bloquant le trafic.
- Listening : Écoute les BPDU (Bridge Protocol Data Units) pour connaître la topologie.
- Learning : Apprend les adresses MAC, mais ne transmet pas de trafic.
- Forwarding : Transmet et reçoit le trafic.

❑La transition entre ces états prend un certain temps, environ 50 secondes.

1.7. Rapid Spanning Tree Protocol (RSTP)

- Rapid Spanning Tree Protocol (RSTP) est une version améliorée de STP qui permet une convergence plus rapide du réseau.
- Défini par la norme IEEE 802.1w, il réduit le temps de convergence à quelques secondes.

1.8. STP et RSTP

❑**STP** :

- **Avantages** : Prévention efficace des boucles, compatibilité universelle.
- **Limitations** : Temps de convergence lent.

❑**RSTP** :

- **Avantages** : Convergence rapide, meilleure gestion des liaisons redondantes.
- **Limitations** : Compatible avec des équipements modernes uniquement.

LAB 6: Configuration VTP et STP

Configuration du VTP (1/2)

Switch# configure terminal

Switch(config)# vtp mode <mode>

<mode> : Peut être server, client, ou transparent.

- server : Permet de créer, modifier, et supprimer des VLANs.
- client : Reçoit les informations VTP mais ne peut pas les modifier.
- transparent : Ne participe pas au VTP mais propage les messages VTP aux autres switches.

Configuration du VTP (2/2)

Switch(config)# vtp domain <domain-name>

Switch(config)# vtp password <password>

Switch(config)# vtp version <version-number>

Vérification de la Configuration VTP : Switch# show vtp status

Configuration du Spanning Tree Protocol (1/4)

Activer STP (par défaut sur les switches Cisco) :

Switch# configure terminal

Switch(config)# spanning-tree mode <mode>

<mode> : Peut être pvst, rapid-pvst, ou mst.

- pvst : Spanning Tree par VLAN (Per-VLAN Spanning Tree).
- rapid-pvst : Version plus rapide de PVST (utilise Rapid STP - RSTP).
- mst : Multiple Spanning Tree.

Configuration du Spanning Tree Protocol (2/4)

Définir une Priorité de Pont pour STP (Root Bridge) :

Switch(config)# spanning-tree vlan <vlan-id> priority <priority-value>

- <vlan-id> : Identifiant du VLAN auquel STP s'applique.
- <priority-value> : La priorité du switch pour devenir le Root Bridge (valeurs entre 0 et 61440, avec des pas de 4096). Plus la priorité est faible, plus le switch a de chances de devenir Root Bridge.

Configuration du Spanning Tree Protocol (3/4)

Faire du Switch le Root Bridge :

Switch(config)# spanning-tree vlan <vlan-id> root primary

- Cette commande force le switch à devenir le **Root Bridge** pour le VLAN spécifié.

Spécifier un Switch comme Secondaire (Backup Root Bridge) :

Switch(config)# spanning-tree vlan <vlan-id> root secondary

Configuration du Spanning Tree Protocol (4/4)

Activer PortFast (pour accélérer la transition des ports vers l'état actif) :

Switch(config)# interface <interface-id>

Switch(config-if)# spanning-tree portfast

- Cette commande est utilisée pour les ports connectés à des terminaux (PCs, serveurs), pas à d'autres switches.

Commandes Avancées pour STP (1/2)

Activer BPDU Guard (Protection contre les Boucles STP) :

Switch(config-if)# spanning-tree bpduguard enable

- BPDU Guard désactive un port dès qu'il reçoit un BPDU, utile pour les ports en PortFast pour éviter qu'ils deviennent des points de boucles.

Activer Root Guard (Protection contre Root Bridge non autorisé) :

Switch(config-if)# spanning-tree guard root

- Empêche les switches non autorisés de devenir Root Bridge.

Commandes Avancées pour STP (2/2)

Vérification de l'État de STP :

Switch# show spanning-tree

- Affiche l’état actuel du protocole STP sur le switch.

Vérifier les Ports avec PortFast activé :

Switch# show spanning-tree interface <interface-id> detail

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 6: Access Control List (ACL)

1.1. Qu'est-ce qu'une ACL ?

- ACL (Access Control List) : Un ensemble de règles permettant de filtrer et contrôler le trafic réseau. Les ACLs peuvent être appliquées aux interfaces pour filtrer le trafic entrant ou sortant.
- Objectif principal : Autoriser ou bloquer des paquets basés sur des critères tels que l'adresse IP, le protocole, ou le port.

1.2. Types d'ACLs

- ACLs Standard : Filtrent le trafic en se basant uniquement sur les adresses IP sources. Appliquées en général près de la destination.
- ACLs Étendues : Filtrent le trafic en se basant sur plusieurs critères, y compris l'adresse IP source, l'adresse IP de destination, le protocole, et les numéros de port. Appliquées près de la source.

1.3. Meilleures Pratiques pour l'Utilisation des ACLs

- Placer les ACLs Standards près de la destination.
- Placer les ACLs Étendues près de la source.
- Toujours tester les ACLs dans un environnement de test avant de les déployer en production.
- Documenter les ACLs pour une maintenance facile.

1.4. Implicit deny

- Tout le trafic qui ne correspond pas aux règles sera bloqué par défaut.
- Vérifiez l'impact avant d'appliquer les ACLs aux interfaces critiques.

1.5. Qu'est-ce que le NAT ?

- NAT (Network Address Translation) est une technologie permettant de modifier les adresses IP dans les paquets qui transitent par un routeur.
- Il est utilisé pour connecter plusieurs appareils privés à Internet via une seule adresse IP publique.

1.5. Pourquoi utiliser le NAT ?

- Conservation des adresses IPv4 : Il permet de réutiliser les adresses IP privées dans un réseau local, réduisant ainsi le besoin d'adresses IPv4 publiques.
- Sécurité : NAT masque les adresses IP internes, offrant une certaine forme de protection contre les attaques externes.
- Facilite la communication vers l'extérieur : Les appareils internes d'un réseau peuvent accéder à Internet via une adresse IP publique unique.

1.5. Types de NAT

Type de NAT	Description
NAT Dynamique	Associe dynamiquement une adresse IP publique à une adresse IP privée en fonction des besoins.
NAT Statique	Associe manuellement une adresse IP publique à une adresse IP privée spécifique.
PAT (Port Address Translation)	Plusieurs adresses privées partagent une seule adresse IP publique, chaque session étant identifiée par un port.

1.5. Avantages du NAT

- Économie d'adresses IPv4 : Réduction du nombre d’adresses publiques nécessaires.
- Sécurité : L'IP privée est cachée du réseau externe.
- Flexibilité : Permet l'utilisation d'IP privées en interne tout en facilitant l'accès à Internet.

1.5. Inconvénients du NAT

- Problèmes avec certaines applications : NAT peut poser des problèmes pour des applications comme les jeux en ligne ou la VoIP qui nécessitent des connexions directes.
- Ralentissement du réseau : L'association et la traduction des adresses peuvent ajouter une certaine latence.
- Sécurité limitée : Bien que NAT masque les IP privées, il ne remplace pas un pare-feu pour une véritable protection.

1.5. NAT Traversal

- Certains protocoles, comme STUN, TURN, et ICE, sont utilisés pour résoudre les problèmes de connectivité dans les environnements NAT, notamment pour la VoIP et les communications P2P.
- NAT Traversal aide à créer des connexions directes entre deux appareils situés derrière des routeurs NAT.

1.5. NAT et IPv6

- Avec l'arrivée d'IPv6, le besoin de NAT a diminué, car l'espace d'adressage IPv6 est suffisamment grand pour chaque appareil.
- IPv6 privilégie la communication de bout en bout, mais NAT64 peut être utilisé pour permettre la communication entre des hôtes IPv6 et IPv4.

LAB 7: Configuration des ACL

Configuration des ACLs Standards

Création d'une ACL Standard :

Router(config)# access-list <numéro> permit|deny <adresse-IP-source> <wildcard-mask>

Appliquer une ACL Standard à une Interface :

Router(config)# interface <interface-id>

Router(config-if)# ip access-group <numéro> in|out

- in : Applique l'ACL pour le trafic entrant.
- out : Applique l'ACL pour le trafic sortant.

Configuration des ACLs Étendues

Création d'une ACL Étendue :

Router(config)# access-list <numéro> permit|deny <protocole> <adresse-IP-source> <wildcard-mask-source> <adresse-IP-destination> <wildcard-mask-destination> [port]

- <numéro> : Un numéro compris entre 100 et 199 pour les ACLs étendues.
- protocole : Peut être tcp, udp, icmp, ou ip (pour tout type de protocole).
- adresse-IP-source : Adresse IP source à filtrer.
- wildcard-mask-source : Masque générique pour la source.
- adresse-IP-destination : Adresse IP destination à filtrer.
- wildcard-mask-destination : Masque générique pour la destination.
- port : Spécifie le numéro de port ou une plage de ports.

Configuration des ACLs Nommées (1/2)

Les ACLs nommées permettent une gestion plus facile car elles utilisent des noms au lieu de numéros.

Création d'une ACL Nommée Standard :

Router(config)# ip access-list standard <nom>

Router(config-std-nacl)# permit|deny <adresse-IP-source> <wildcard-mask>

Création d'une ACL Nommée Étendue :

Router(config)# ip access-list extended <nom>

Router(config-ext-nacl)# permit|deny <protocole> <adresse-IP-source> <wildcard-mask-source> <adresse-IP-destination> <wildcard-mask-destination> [port]

Configuration des ACLs Nommées (2/2)

Appliquer une ACL Nommée à une Interface :

Router(config)# interface <interface-id>

Router(config-if)# ip access-group <nom> in|out

Commandes de Vérification des ACLs

Router# show access-lists

Router# show access-lists <numéro|nom>

Router# show ip interface <interface-id>

Étapes pour configurer NAT dynamique (1/2)

Créer une liste d'accès pour spécifier le trafic IP interne :

Router(config)# access-list <numéro_liste> permit <réseau_interne> <wildcard_mask>

Créer un pool d'adresses IP publiques :

Router(config)# ip nat pool <nom_pool> <ip_debut_pool> <ip_fin_pool> netmask <masque_de_sous_reseau>

Associer la liste d'accès avec le pool d'adresses IP pour la traduction NAT :

Router(config)# ip nat inside source list <numéro_liste> pool <nom_pool>

Étapes pour configurer NAT dynamique (2/2)

Définir l'interface interne (LAN) et l'interface externe (WAN) :

Router(config)# interface <nom_interface_interne>

Router(config-if)# ip nat inside

Router(config)# interface <nom_interface_externe>

Router(config-if)# ip nat outside

Étapes pour configurer PAT (NAT Overloading)

Créer une liste d'accès pour spécifier les adresses internes :

Router(config)# access-list <numéro_liste> permit <réseau_interne> <wildcard_mask>

Associer la liste d'accès à l'adresse IP de l'interface externe avec surcharge (overload) :

Router(config)# ip nat inside source list <numéro_liste> interface <nom_interface_externe> overload

Configurer les interfaces internes et externes :

Router(config)# interface <nom_interface_interne>

Router(config-if)# ip nat inside

Router(config)# interface <nom_interface_externe>

Router(config-if)# ip nat outside

Étapes pour configurer PAT avec un pool d'adresses (1/2)

Créer une liste d'accès pour le trafic IP interne :

Router(config)# access-list <numéro_liste> permit <réseau_interne> <wildcard_mask>

Définir un pool d'adresses IP publiques :

Router(config)# ip nat pool <nom_pool> <ip_debut_pool> <ip_fin_pool> netmask <masque_de_sous_reseau>

Associer la liste d'accès avec le pool d'adresses IP et activer la surcharge :

Router(config)# ip nat inside source list <numéro_liste> pool <nom_pool> overload

Étapes pour configurer le port forwarding

Rediriger un port spécifique vers une machine interne :

Router(config)# ip nat inside source static tcp <ip_interne> <port_interne> <ip_externe> <port_externe>

Commandes de Vérification NAT

Router# show ip nat translations

Router# show ip nat statistics

Router# clear ip nat translations *

Master 1 Réseaux Informatiques

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

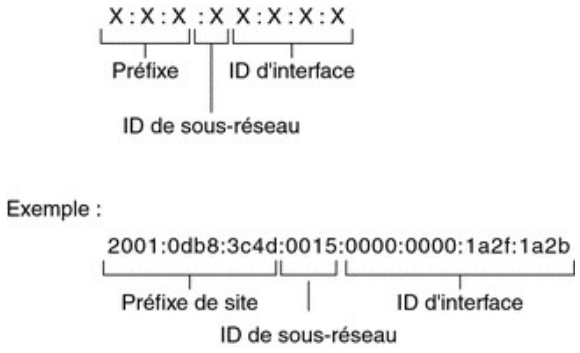
Partie 7: IPV6

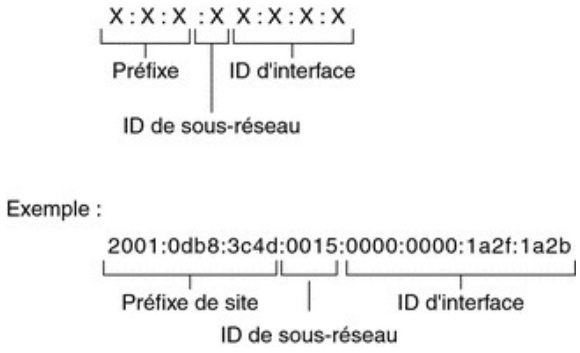
2.1. Pourquoi IPv6 ?

- Limites d'IPv4 : Pénurie d'adresses IP.
- IPv6 : Une solution durable avec un espace d'adressage beaucoup plus large.
- Avantages :
  - Plus grand espace d'adressage (128 bits contre 32 bits pour IPv4).
  - Simplification du routage et de la configuration.
  - Meilleure prise en charge de la sécurité native (IPsec).
  - Amélioration de la mobilité et de l'autoconfiguration.

2.2. Structure de l'Adresse IPv6 (1/2)

Une adresse IPv6 est longue de 128 bits et se compose de huit champs de 16 bits, chacun étant délimité par deux-points (:). Chaque champ doit contenir un nombre hexadécimal, à la différence de la notation en format décimal avec points des adresses IPv4. Dans l'illustration suivante, les x représentent des nombres hexadécimaux.





2.2. Structure de l'Adresse IPv6 (2/2)

- Les adresses peuvent être compressées (remplacement des zéros continus par "::").

Exemple d'adresse compressée
:2001:0db8:0000:0000:0000:ff00:0042:8329

Devient

2001:db8::ff00:42:8329

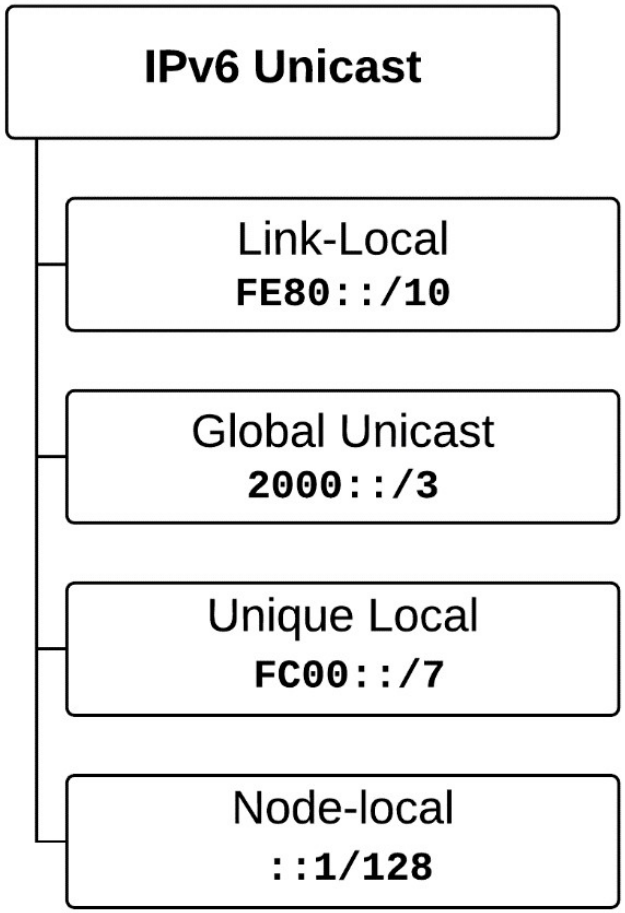
2.3. Comparaison IPv4 vs IPv6

Caractéristique	IPV4	IPV6
Longueur de l’adresse	32 bits	128 bits
Espaces d’adresses	4,3 milliards	340 sextillions
Configuration	Manuelle ou DHCP	Autoconfiguration (SLAAC)
Fragmentation	Routeur	Hôte d'origine
Support de la sécurité	Optionnel	Intégré (IPsec)

2.4. Types d'Adresses IPv6 (1/2)

- Unicast : Pour une communication point-à-point.
- Multicast : Pour envoyer un paquet à plusieurs destinations simultanément.
- Anycast : Adresse partagée par plusieurs dispositifs. Le paquet est envoyé au plus proche.

2.4. Types d'Adresses IPv6 (2/2)



2.5. Adressage IPv6 Link-Local Unicast(fe80::/10)

Une adresse Link-Local est une adresse qui ne porte que sur le lien et qui n'est jamais transféré par les routeurs. Elle sert à joindre les voisins sur un même lien. Toutes les interfaces IPv6 disposent d'une adresse Link-Local.

Ses 10 premiers bits sont codés en 1111111010 pour donner en hexadécimal un bloc fe80::/10.

1111111010 (10)	(54)	Interface ID (64)

2.6. Adressage IPv6 Global Unicast (2000::/3) (1/2)

On pourrait identifier plusieurs adresses Global Unicast sur les interfaces, soit l'équivalent de nos adresses IPv4 publiques. On les définira plus précisément comme des destinations publiées sur l'Internet. Les routeurs transfèrent le trafic vers ces destinations. Elles sont donc "globalement routables".

001 (3)	Global Routing Prefix (45)	Subnet ID (16)	Interface ID (64)

2.6. Adressage IPv6 Global Unicast (2000::/3) (2/2)

AFRINIC:

- 2001:4200::/23
- 2c00:0000::/12

2.7. Adressage IPv6 Unique Local (FC00::/7)

On identifiera un autre type d'adresses : Unique Local Address (ULA). Comparables aux adresses privées IPv4 RFC1918 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16 dans le sens où elles ne sont pas "globalement routables", elles ne connaissent pas de destination sur l'Internet. On les reconnaît par leur préfixe FD00::/8 dont les 40 bits suivants ont été générés aléatoirement pour compléter un préfixe /48.

1111110 (7)	1 (L)	Global ID (40)	Subnet ID (16)	Interface ID (64)

2.8. Autoconfiguration Stateless (SLAAC)

Permet à un appareil de générer automatiquement son adresse IPv6 sans besoin de serveur DHCP.

Utilise les messages ICMPv6 (Router Advertisement et Router Solicitation).

EUI-64 : Basé sur l'adresse MAC pour créer la partie hôte de l'adresse IPv6.

2.9. Processus d’autoconfiguration Stateless

- Le routeur envoie une annonce de routeur.
- Le dispositif configure automatiquement son adresse avec un préfixe réseau et un ID d'interface.

2.10. Transition d'IPv4 à IPv6

- Double Pile : Les dispositifs prennent en charge IPv4 et IPv6 simultanément.
- Tunneling : IPv6 encapsulé dans IPv4 (ex : 6to4, Teredo).
- Traduction d'adresses réseau (NAT64) : Convertit les adresses IPv6 en IPv4.

2.11. Routage IPv6

- Les protocoles de routage IPv6 sont similaires à ceux d'IPv4.
- Protocoles de routage pris en charge :
  - RIPng (RIP Next Generation)
  - OSPFv3 (Open Shortest Path First for IPv6)
  - EIGRP for IPv6
  - BGP-4+ (Border Gateway Protocol)

2.12. Sécurité et IPv6

- IPsec : Prise en charge obligatoire dans IPv6, contrairement à IPv4.
- Fonctionnalités supplémentaires :
  - Meilleure gestion du cryptage et de l'authentification.
  - Cryptage des communications entre les hôtes.
  - Protection contre le scan de réseau avec l'énorme espace d'adressage.

LAB 8: Configuration de IPV6

Configuration d'IPv6 sur une Interface

Activer IPv6 sur le Routeur:

Router(config)# ipv6 unicast-routing

Configurer une Adresse IPv6 Statique:

Router(config)# interface <interface-id>

Router(config-if)# ipv6 address <adresse-ipv6>/<prefixe>

Configurer l'Autoconfiguration avec SLAAC:

Router(config)# interface <interface-id>

Router(config-if)# ipv6 address autoconfig

Configuration d'IPv6 Link-Local (Obligatoire)

Chaque interface IPv6 a besoin d'une adresse link-local pour la communication sur le lien local. Si elle n'est pas configurée, le routeur génère automatiquement une adresse.

Configurer une Adresse Link-Local Manuellement:

Router(config)# interface <interface-id>

Router(config-if)# ipv6 address fe80::1 link-local

Activer ICMPv6 et SLAAC:

Pour que les clients IPv6 puissent s'autoconfigurer, les routeurs doivent envoyer des annonces de routeur (RA) via ICMPv6. Par défaut, cela est activé.

Router(config)# interface <interface-id>

Router(config-if)# ipv6 nd ra suppress

Routage IPv6 (1/2)

Le routage IPv6 peut être configuré en utilisant des protocoles de routage dynamiques comme RIPng, OSPFv3, ou EIGRP for IPv6.

Routage Statique IPv6:

Router(config)# ipv6 route <reseau-destination>/<prefixe> <adresse-next-hop>

Configuration de RIPng:

Router(config)# ipv6 router rip <nom>

Router(config-router)# interface <interface-id>

Router(config-if)# ipv6 rip <nom> enable

Routage IPv6 (2/2)

Configuration d'OSPFv3:

Router(config)# ipv6 router ospf <process-id>

Router(config-router)# router-id <router-id>

Router(config)# interface <interface-id>

Router(config-if)# ipv6 ospf <process-id> area <area-id>

Configuration de NAT64

NAT64 est utilisé pour permettre la communication entre des hôtes IPv6 et des hôtes IPv4.

Router(config)# interface <interface-id>

Router(config-if)# ipv6 nat64 enable

Router(config-if)# ipv6 nat64 prefix <prefixe>/96

Configuration de la Redirection de DNS pour IPv6

Si vous avez besoin d'une redirection de DNS pour IPv6, vous pouvez configurer le routeur pour fournir des adresses DNS IPv6.

Router(config)# ipv6 dhcp pool <nom-du-pool>

Router(config-dhcpv6)# dns-server <adresse-ipv6-dns>

Commandes de Vérification IPv6

Router# show ipv6 route

Router# show ipv6 interface

Router# show ipv6 dhcp pool

Router# show ipv6 nat64 translations