Cours Réseaux Informatiques

Filière : Génie Informatique

Pr. Lamia ZIAD
École Supérieure de Technologie d'Essaouira

November 28, 2025

Contents

Structure des fichiers inclus

Les fichiers suivants sont inclus automatiquement dans ce document :

- Chapitre 1 : Architectures des Réseaux Informatiques
- Chapitre 2 : Modèle OSI et Architecture en Couches
- Chapitre 3 : Architecture TCP/IP et Protocoles
- Chapitre 4 : Adressage IP, Sous-réseaux et VLSM
- Chapitre 5 : Routage IP (Statique et Dynamique)
- Chapitre 6 : Configuration des Routeurs Cisco (IOS)

1. Architecture des Réseaux Informatiques

Objectifs du chapitre

À la fin de ce chapitre, l'étudiant sera capable de :

- comprendre la représentation de l'information dans les réseaux ;
- expliquer les circuits, liaisons et modes de transmission ;
- distinguer les supports (câbles, fibre, ondes) ;
- maîtriser la notion de réseau et les raisons de son existence ;
- décrire le modèle OSI et ses fonctions couche par couche ;
- analyser les topologies et technologies d'un réseau local ;
- étudier des cas réels d'implémentation LAN.

1.1 L'information et sa représentation

L'information transmise sur un réseau informatique peut prendre différentes formes : texte, audio, image, vidéo, signaux de capteurs, etc. Dans tous les cas, elle doit être représentée sous une **forme numérique**, c'est-à-dire une suite de bits (0 et 1).

1.1.1 Bit, Octet et Codage

- **Bit (Binary Digit)** : unité élémentaire d'information.
- **Octet (Byte)** : 8 bits.
- **Codage** : transformation d'une information réelle en une suite binaire.

Exemples de codage :

- **Texte** : ASCII, Unicode (UTF-8).
- **Images** : JPEG (compression), PNG (sans perte).
- **Audio** : MP3, WAV.

Remarque

Le choix du codage influence directement :

- le débit nécessaire ;
- la qualité finale ;
- la latence et le temps de traitement.

1.2 Circuits et liaisons de données

Un circuit désigne un chemin permettant la transmission des données entre deux équipements.

1.2.1 Types de liaisons

- **Simplex** : un seul sens (ex : télévision).
- **Half-duplex** : alternance des sens (ex : talkie-walkie).
- **Full-duplex** : les deux sens simultanément (ex : Internet).

1.2.2 Caractéristiques essentielles

- **Débit** (bps, kbps, Mbps, Gbps).
- **Bande passante**.
- **Latence**.
- **Gigue (jitter)**.
- **Taux d'erreur**.

1.3 Modes et techniques de transmission

1.3.1 Transmission numérique vs analogique

- Transmission analogique : signaux continus.
- Transmission numérique : signaux discrets.

1.3.2 Techniques

- **Bande de base** (Ethernet).
- **Bande passante** (modulation).

1.4 Supports de transmission

1.4.1 Câbles

- **Paires torsadées** : UTP, STP (Ethernet).
- **Câble coaxial**.

1.4.2 Fibre optique

- monomode : longues distances ;
- multimode : courtes distances.

1.4.3 Sans fil

- Wifi ;
- Bluetooth ;
- GSM/4G/5G.

1.5 Le concept de réseau

Un réseau interconnecte des équipements afin de :

- partager des ressources ;
- échanger des données ;
- permettre l'accès distant.

Catégories :

- **LAN** (Local Area Network) ;
- **MAN** ;
- **WAN**.

1.6 Le modèle OSI

Définition

Le modèle OSI (**Open Systems Interconnection**) est un modèle en 7 couches utilisé pour standardiser les communications.

1.6.1 Les 7 couches

1. Physique
2. Liaison de données
3. Réseau
4. Transport
5. Session
6. Présentation
7. Application

1.7 Architecture des réseaux locaux

1.7.1 Topologies

- bus ;
- étoile ;
- anneau ;
- maillée.

1.7.2 Technologies

- Ethernet ;
- Wifi ;
- VLANs.

1.8 Études de cas LAN

1.8.1 Cas 1 : Réseau d'entreprise

- segmentation VLAN ;
- serveurs internes ;
- DMZ.

1.8.2 Cas 2 : Réseau universitaire

- Wifi campus ;
- borne d'accès ;
- routage vers Internet.

Exercices du Chapitre 1

Exercice 1 : Analyse d'un signal

Expliquez la différence entre un signal analogique et un signal numérique. Donnez un exemple d'utilisation pour chaque type.

Exercice 2 : Débit

Calculer le temps nécessaire pour transmettre un fichier de 800 Mo sur un lien 100 Mbps.

Exercice 3 : Modèle OSI

Associez chaque protocole à la couche OSI correspondante : HTTP, IP, Ethernet, TCP, TLS.

Corrigés

- Ex1 : ...
- Ex2 : 800 Mo = 6400 Mb $\rightarrow$ 6400 / 100 = 64 s
- Ex3 : HTTP (7), IP (3), Ethernet (2), TCP (4), TLS (6)

2. Interconnexion des Réseaux Informatiques

Objectifs du chapitre

Ce chapitre explique les mécanismes fondamentaux qui permettent l'interconnexion des réseaux modernes :

- comprendre l'architecture TCP/IP ;
- maîtriser les protocoles IP, ARP, ICMP, UDP, TCP ;
- apprendre l'adressage IPv4, le sous-adressage et les masques ;
- comprendre le routage des datagrammes ;
- étudier les routeurs et leur configuration.

2.1 Concepts de l'interconnexion

L'interconnexion désigne la capacité de plusieurs réseaux de technologies différentes à communiquer entre eux. Elle repose sur :

- des équipements : **routeurs, commutateurs, passerelles** ;
- des protocoles : **IP, ARP, ICMP, TCP, UDP** ;
- des mécanismes : **routage, adressage, encapsulation**.

Principe d'encapsulation

Chaque protocole ajoute son propre en-tête avant transmission.

$$\text{Données} \rightarrow \text{Segment} \rightarrow \text{Paquet IP} \rightarrow \text{Trame Ethernet}$$

2.2 Architecture TCP/IP

Le modèle TCP/IP simplifie OSI en 4 couches :

TCP/IP	OSI
Application	Application / Présentation / Session
Transport	Transport
Internet	Réseau
Accès réseau	Liaison + Physique

2.2.1 Couche Accès Réseau

Responsable :

- adressage MAC,
- encapsulation en trame,
- détection d'erreurs locales.

2.2.2 Couche Internet

Elle transporte les paquets IP indépendamment du chemin emprunté.

2.2.3 Couche Transport

Fournit :

- TCP : fiable ;
- UDP : non fiable mais rapide.

2.2.4 Couche Application

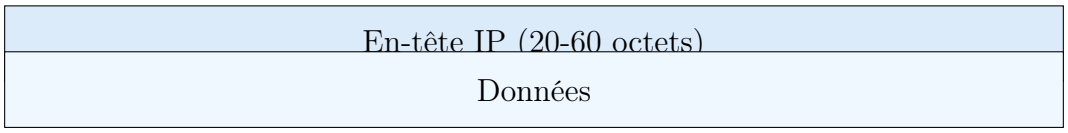
Protocoles : HTTP, DNS, SMTP, FTP, SSH...

2.3 Le protocole Internet (IP)

IP est un protocole :

- non fiable,
- non connecté,
- orienté datagramme.

2.3.1 Structure d'un datagramme IP



Champs importants :

- **TTL** : limite de sa durée de vie ;
- **Protocol** : indique si TCP, UDP, ICMP... ;
- **Source** / **Destination**.

2.4 Adressage Internet (IPv4)

Une adresse IPv4 est un nombre sur 32 bits.

2.4.1 Classes d'adresses

Classe A	0.0.0.0 – 127.255.255.255	/8
Classe B	128.0.0.0 – 191.255.255.255	/16
Classe C	192.0.0.0 – 223.255.255.255	/24

2.4.2 Adresses privées

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

2.4.3 Masque de sous-réseau

Permet de séparer :

- partie réseau ;
- partie hôte.

Exemple :

$$192.168.10.0/24 \Rightarrow 255.255.255.0$$

2.5 Sous-adressage (Subnetting)

Objectifs :

- diviser un réseau en plusieurs sous-réseaux ;
- optimiser les adresses ;
- réduire le broadcast.

Exemple : diviser 192.168.1.0/24 en 4 sous-réseaux

$$/24 \rightarrow /26$$

Résultat :

Sous-réseau	Adresse réseau	Broadcast
1	192.168.1.0	192.168.1.63
2	192.168.1.64	192.168.1.127
3	192.168.1.128	192.168.1.191
4	192.168.1.192	192.168.1.255

2.6 ARP : protocole de résolution d'adresse

ARP trouve l'adresse MAC correspondant à une adresse IP.

2.6.1 Fonctionnement

1. L'hôte envoie un ARP Request (broadcast).
2. Le destinataire répond par ARP Reply (unicast).

ARP Cache

Les résultats ARP sont enregistrés dans un cache pour accélérer les transmissions suivantes.

2.7 RARP : Résolution inverse

RARP fait l'opération inverse : obtenir une IP à partir d'une MAC. Aujourd'hui remplacé par DHCP.

2.8 Le protocole ICMP

Utilisé pour :

- signaler des erreurs,
- tester la connectivité (`ping`),
- tracer le chemin (`traceroute`).

Types courants :

- Echo Request / Echo Reply ;
- Destination Unreachable ;
- Time Exceeded.

2.9 Le protocole UDP

Caractéristiques :

- non fiable ;
- pas de connexion ;
- très rapide.

Utilisations :

- streaming,
- DNS,
- VoIP.

2.10 Le protocole TCP

TCP est fiable :

- accusés de réception (ACK) ;
- retransmissions ;
- contrôle de flux ;
- fenêtre glissante.

2.10.1 Établissement de connexion : 3-way handshake

$$\text{SYN} \rightarrow \text{SYN/ACK} \rightarrow \text{ACK}$$

2.11 Routage des datagrammes

Les routeurs :

- transmettent les paquets selon la table de routage ;
- choisissent le meilleur chemin ;
- utilisent les protocoles OSPF, RIP, BGP.

2.11.1 Table de routage

Chaque entrée contient :

- réseau de destination,
- masque,
- passerelle,
- interface.

2.12 Configuration des routeurs (exemples Cisco)

Configurer une interface

```
Router> enable
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Ajouter une route statique

```
Router(config)# ip route 10.0.0.0 255.255.255.0 192.168.1.254
```

Afficher la table de routage

```
Router# show ip route
```

Exercices du Chapitre 2

Exercice 1 : Subnetting

Diviser le réseau 172.16.0.0/16 en 8 sous-réseaux. Donnez les plages réseau + broadcast.

Exercice 2 : ARP

Décrire le fonctionnement complet d'une résolution ARP dans un LAN.

Exercice 3 : TCP vs UDP

Donner trois différences fondamentales entre TCP et UDP.

Corrigés

- Ex1 : /16 → /19. Sous-réseaux : 172.16.0.0, 172.16.32.0, 172.16.64.0, ...
- Ex2 : ARP Request → Broadcast → ARP Reply → Cache.
- Ex3 : Fiabilité, connexion, contrôle de flux.

3. Protocoles Réseau Avancés et Services d'Infrastructure

Objectifs du chapitre

À la fin de ce chapitre, l'étudiant sera capable de :

- comprendre les VLAN et leur utilité ;
- configurer un réseau segmenté avec VLAN et trunking ;
- expliquer et configurer DHCP ;
- comprendre la traduction d'adresses : NAT et PAT ;
- maîtriser DNS, VPN et les protocoles avancés ;
- analyser des architectures LAN/WAN complètes.

3.1 Introduction aux protocoles avancés

Les réseaux modernes nécessitent des services d'infrastructure essentiels pour fonctionner correctement et de manière sécurisée :

- **Segmentation logique (VLAN)** ;
- **Attribution automatique d'adresses (DHCP)** ;
- **Traduction d'adresses (NAT/PAT)** ;
- **Résolution de noms (DNS)** ;
- **Tunnels et VPN** ;
- **Sécurité de base (ACLs)**.

3.2 Les VLAN (Virtual Local Area Network)

Définition

Un VLAN est un réseau local logique indépendant, créé au sein d'une même infrastructure physique.

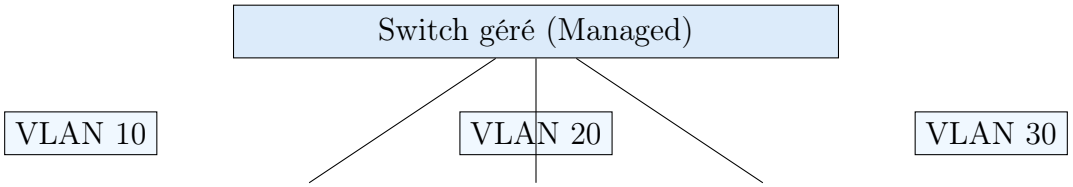
3.2.1 Objectifs des VLAN

- isoler les utilisateurs ;
- améliorer la sécurité ;
- réduire les domaines de broadcast ;
- optimiser la performance.

3.2.2 Principe général

Un VLAN regroupe des utilisateurs :

- par fonction (RH, Finance, IT...),
- par bâtiment,
- par niveau de sécurité.



3.2.3 Types de ports

- **Access port** : appartient à un seul VLAN.
- **Trunk port** : transporte plusieurs VLAN (802.1Q).

3.2.4 Encapsulation 802.1Q

Le tag VLAN inséré dans la trame Ethernet identifie le VLAN.

3.3 DHCP : Dynamic Host Configuration Protocol

Rôle

DHCP attribue automatiquement :

- adresse IP,
- masque,
- passerelle,
- DNS.

3.3.1 Le processus DORA

Discover → Offer → Request → Acknowledge

1. **Discover** : le client cherche un serveur DHCP.
2. **Offer** : le serveur propose une adresse.
3. **Request** : le client demande cette adresse.
4. **ACK** : le serveur valide.

3.4 NAT et PAT : Traduction d'adresses

3.4.1 Motivation

Les adresses IPv4 publiques sont limitées. NAT permet à plusieurs machines privées d'accéder à Internet.

3.4.2 Types de NAT

- **Static NAT** : 1 IP privée ↔ 1 IP publique.
- **Dynamic NAT** : pool d'adresses publiques.
- **PAT (Overload)** : plusieurs IP privées ↔ 1 IP publique (avec ports).

Exemple de PAT

192.168.1.10:1030 → 160.24.50.2:45000 192.168.1.11:1031 → 160.24.50.2:45001

3.5 DNS : Domain Name System

DNS traduit les noms en adresses IP.

3.5.1 Types d'enregistrements

- A : IPv4
- AAAA : IPv6
- CNAME : alias
- MX : serveur mail
- NS : serveur DNS

3.5.2 Processus

$$\text{Nom} \rightarrow \text{Résolveur} \rightarrow \text{Serveur DNS} \rightarrow \text{IP}$$

3.6 VPN : Virtual Private Network

Un VPN crée un tunnel crypté entre deux réseaux.

3.6.1 Types de VPN

- **VPN site à site** (entre agences) ;
- **VPN client-to-site** (télétravail).

3.6.2 Protocoles VPN

- IPsec ;
- SSL VPN ;
- L2TP.

3.7 Protocoles LAN et WAN avancés

3.7.1 Spanning Tree Protocol (STP)

Évite les boucles dans les réseaux commutés.

3.7.2 HSRP / VRRP

Permettent la redondance des routeurs.

3.7.3 MPLS

Technologie WAN à haute performance.

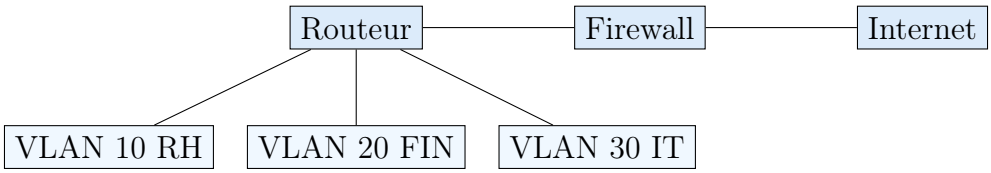
3.8 Étude de cas complète : Architecture d'entreprise

Scénario

Une entreprise possède trois départements : RH, Finance et IT. Objectifs :

- isoler les VLAN ;
- fournir Internet ;
- protéger les serveurs internes ;
- gérer le DHCP centralisé ;
- configurer le routage inter-VLAN.

Architecture simplifiée :



Exercices du Chapitre 3

Exercice 1 : VLAN

Créer un plan d'adressage pour 4 VLAN : VLAN 10 (30 hôtes), VLAN 20 (60 hôtes), VLAN 30 (100 hôtes), VLAN 40 (10 hôtes).

Exercice 2 : DHCP

Décrire en détail le processus DORA.

Exercice 3 : NAT vs PAT

Donner 3 différences entre NAT statique, dynamique et PAT.

Exercice 4 : DNS

Expliquer le fonctionnement d'une requête DNS récursive.

Corrigés

- Ex1 : utiliser subnetting — /27, /26, /25, /28.
- Ex2 : Discover → Offer → Request → ACK.
- Ex3 : statique (1:1), dynamique (pool), PAT (ports).
- Ex4 : résolveur → DNS root → TLD → serveur autoritaire.

4. Sécurité Réseau et Analyse de Paquets

Objectifs du chapitre

L'étudiant sera capable de :

- comprendre les menaces réseau et les vulnérabilités ;
- maîtriser le fonctionnement des pare-feux et ACL ;
- configurer des règles de filtrage ;
- analyser des paquets avec Wireshark ;
- comprendre la sécurité Wi-Fi et les mécanismes de chiffrement ;
- utiliser les outils de détection d'intrusion (IDS/IPS).

4.1 Principes de la sécurité réseau

La sécurité réseau vise à protéger :

- la confidentialité,
- l'intégrité,
- la disponibilité,
- l'authenticité,
- la traçabilité.

4.1.1 Le modèle CIA

- **Confidentialité** : empêcher l'accès non autorisé.

- **Intégrité** : empêcher la modification des données.
- **Disponibilité** : assurer la continuité de service.

4.2 Les menaces et attaques réseau

4.2.1 Attaques actives et passives

- passives : sniffing, écoute ;
- actives : modification, injection, détournement.

4.2.2 Attaques courantes

- **DoS / DDoS** : attaque par saturation ;
- **Spoofing** : usurpation d'identité IP/MAC ;
- **MITM (Man-In-The-Middle)** ;
- **ARP poisoning** ;
- **DNS poisoning** ;
- **Scanning / probing** ;
- **Password cracking**.

Exemple : ARP Poisoning

L'attaquant envoie de fausses réponses ARP pour rediriger le trafic vers sa machine.

4.3 Pare-feux (Firewalls)

Définition

Un pare-feu est un dispositif filtrant le trafic entre plusieurs zones réseau.

4.3.1 Types de pare-feux

- **Filtrage statique** : ACL simples ;
- **Stateful Firewall** : suit les connexions ;

- **Proxy Firewall** : intermédiaire applicatif ;
- **Next-Generation Firewall (NGFW)** : inspection approfondie, IDS/IPS intégré.

4.3.2 Règles classiques

- bloquer le trafic entrant par défaut ;
- autoriser les connexions internes sortantes ;
- permettre les protocoles essentiels : DNS, HTTP/HTTPS, DHCP.

4.4 ACL : Listes de Contrôle d'Accès

4.4.1 ACL standard

Filtre uniquement sur l'adresse source.

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

4.4.2 ACL étendue

Filtre selon :

- IP source,
- IP destination,
- protocole,
- port.

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
```

4.4.3 Application sur une interface

```
interface gig0/0
ip access-group 101 in
```

4.5 Sécurité Wi-Fi

4.5.1 Chiffrement

- WPA2 (AES) ;
- WPA3 (SAE) ;
- Éviter WEP (obsolète).

4.5.2 Menaces

- Evil Twin AP ;
- Déauth Attack ;
- Sniffing (Wireshark).

4.6 IDS / IPS

- **IDS** : détecte les attaques ;
- **IPS** : bloque les attaques en temps réel.

Sources :

- signatures ;
- analyse comportementale ;
- heuristique.

4.7 Analyse de paquets – Wireshark

Wireshark permet d'inspecter :

- les trames ;
- les paquets IP ;
- les segments TCP ;
- les messages ARP, DNS, HTTP...

4.7.1 Filtres utiles

```
ip.addr == 192.168.1.10
tcp.port == 80
arp
dns
http
```

4.7.2 Analyse d'une connexion TCP

$$\text{SYN} \rightarrow \text{SYN/ACK} \rightarrow \text{ACK}$$

Exemple Wireshark

Afficher uniquement les paquets DNS :

```
dns
```

4.8 Best Practices de sécurité réseau

- utiliser des VLAN et un firewall interne ;
- configurer des ACL restrictives ;
- mettre en place une authentification forte ;
- journaliser les événements (syslog, SIEM) ;
- surveiller le réseau via IDS/IPS ;
- segmenter les réseaux sensibles ;
- appliquer les mises à jour ;
- chiffrer les communications.

Exercices du Chapitre 4

Exercice 1 : Menaces

Classer les attaques suivantes en actives ou passives : sniffing, MITM, DoS, spoofing.

Exercice 2 : ACL

Écrire une ACL qui interdit le trafic HTTPS provenant du réseau 10.0.0.0/8.

Exercice 3 : Wireshark

Donner le filtre permettant de capturer uniquement les requêtes ARP.

Corrigés

- Ex1 : Sniffing (passive), MITM (active), DoS (active), spoofing (active).
- Ex2 :

```
access-list 110 deny tcp 10.0.0.0 0.255.255.255 any eq 443
```

- Ex3 :

```
arp
```

5. Routage IP : Statique et Dynamique

5.1 Introduction au routage IP

Le routage est le mécanisme permettant à des paquets IP d'être transmis d'un réseau à un autre jusqu'à atteindre leur destination. Dans un contexte de **Science des Données**, où l'accès aux ressources distribuées (clusters, datacenters, services cloud, API) est essentiel, comprendre le routage permet d'optimiser la connectivité, la performance et la sécurité.

Le routage assure principalement :

- la livraison de datagrammes entre des réseaux distincts ;
- la sélection du meilleur chemin disponible ;
- l'adaptation aux changements de topologie ;
- la résilience grâce aux routes alternatives.

Un **routeur** est l'équipement chargé de :

- inspecter les adresses IP source/destination ;
- choisir l'interface de sortie ;
- transférer les paquets vers l'étape suivante (next hop).

La base de décision d'un routeur est sa **table de routage**.

5.2 La table de routage

Une table de routage contient l'ensemble des réseaux connus par le routeur, ainsi que les informations suivantes :

- **préfixe réseau** (ex. 192.168.10.0/24) ;
- **masque de réseau** ;

- **next-hop** (routeur de prochaine étape) ;
- **interface de sortie** ;
- **métrique** (coût associé au chemin) ;
- **type de route** (statique, dynamique, directement connectée).

Exemple Cisco :

```
R1# show ip route
C   192.168.1.0/24 is directly connected, FastEthernet0/0
S   10.0.0.0/24 [1/0] via 192.168.1.2
R   172.16.0.0/16 [120/2] via 10.0.0.2
```

5.3 Les types de routage

Il existe deux catégories de routage :

5.3.1 Routage statique

Le routage statique consiste à configurer manuellement les routes.

Avantages :

- haute sécurité ;
- aucune consommation CPU/RAM ;
- prévisible et stable.

Inconvénients :

- non adapté aux grands réseaux ;
- aucune adaptation automatique ;
- configuration longue et sensible aux erreurs.

5.3.2 Routage dynamique

Dans le routage dynamique, les routeurs échangent automatiquement des informations sur la topologie du réseau.

Avantages :

- auto-adaptation aux pannes ;

- configuration plus simple ;
- optimisation du meilleur chemin.

Inconvénients :

- consommation de bande passante ;
- utilisation des ressources CPU ;
- risque de boucles si mal configuré.

5.4 Routage statique

5.4.1 Définition

Une route statique est créée manuellement par l'administrateur.

5.4.2 Syntaxe (Cisco)

```
R1(config)# ip route <réseau> <masque> <next-hop>
```

5.4.3 Exemple

```
R1(config)# ip route 10.0.0.0 255.255.255.0 192.168.1.2
```

5.4.4 Route par défaut

```
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Utilisée pour accéder à Internet ou à un réseau inconnu.

5.5 Routage dynamique — Principes généraux

Les protocoles de routage dynamique échangent automatiquement :

- les réseaux connus ;
- les métriques ;
- les adresses next-hop ;
- les changements de topologie.

Deux grandes familles :

5.5.1 Protocoles IGP versus EGP

- **IGP** (Interior Gateway Protocol) : au sein d'une organisation → RIP, OSPF, EIGRP, IS-IS
- **EGP** (Exterior Gateway Protocol) : entre opérateurs → BGP (utilisé dans Internet)

5.5.2 Protocoles à vecteur de distance

Les routeurs échangent l'information sous forme de "distance" vers une destination. Exemples : RIP, RIPv2.

Métrique typique : nombre de sauts (hop count)

5.5.3 Protocoles à état de liens

Les routeurs construisent une carte complète de la topologie. Exemples : OSPF, IS-IS.

Métrique typique : coût basé sur le débit.

5.6 RIPv2 : Routage dynamique simple

5.6.1 Introduction à RIP

- Protocole IGP basé sur le vecteur de distance.
- Métrique : nombre de sauts (max 15).
- Version utilisée : RIPv2 (support CIDR et VLSM).
- Mise à jour toutes les 30 secondes.

5.6.2 Activation

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# network 10.0.0.0
```

5.6.3 Affichage des routes RIP

```
R1# show ip protocols
R1# show ip route rip
```

5.7 OSPF : Routage avancé

5.7.1 Caractéristiques

- Protocole link-state (état de liens)
- Hiérarchie basée sur les zones
- Convergence rapide
- Métrique : le coût (basé sur la bande passante)

5.7.2 Activation

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.0.0.0 0.0.0.255 area 0
```

5.7.3 Affichage de la base LSDB

```
R1# show ip ospf database
```

5.8 Comparaison RIP vs OSPF

Caractéristique	**RIPv2**	**OSPF**
Type de protocole	Distance vector	Link-state
Métrique	Sauts	Coût (débit)
Taille réseau	Petite	Moyenne à grande
VLSM	Oui	Oui
Convergence	Lente	Rapide

5.9 Étude de cas — Routage dans un cluster de données

Dans un environnement **Science des Données**, un cluster nécessite :

- une haute disponibilité ;
- une latence minimale entre nœuds ;
- une tolérance aux pannes ;

- un routage optimal entre serveurs (ML, Spark, Hadoop...).

Exemples d'applications :

- routage OSPF dans les datacenters ;
- chemins redondants ;
- réseaux séparés pour stockage, calcul et management.

5.10 Conclusion

Le routage IP est un élément fondamental pour toute infrastructure moderne. Dans un contexte de **Data Science**, il conditionne la performance des clusters, la communication entre services distribués, et la disponibilité des ressources.

5.11 Routage Dynamique

Le routage dynamique repose sur des protocoles capables d'échanger des informations entre routeurs afin de construire automatiquement la table de routage. Il permet :

- d'adapter automatiquement les routes en cas de panne ;
- de détecter les changements topologiques ;
- de choisir les meilleurs chemins ;
- de réduire la configuration manuelle.

Les protocoles de routage sont classés en deux grandes familles :

1. **Protocoles à vecteur de distance (Distance Vector)** Exemples : RIP, IGRP.
2. **Protocoles à état de lien (Link-State)** Exemples : OSPF, IS-IS.

Chaque famille repose sur une philosophie différente pour construire la table de routage.

5.12 Protocoles à Vecteur de Distance (Distance Vector)

Les routeurs échangent périodiquement leur table de routage complète avec leurs voisins. Ils appliquent ensuite l'algorithme de **Bellman–Ford** pour calculer les distances.

5.12.1 Caractéristiques

- Faciles à configurer.
- Peu gourmands en ressources.
- Convergence lente.
- Vulnérables aux boucles de routage.

5.12.2 Exemples

- **RIP** (Routing Information Protocol)
- **IGRP** (propriétaire Cisco, ancien)

5.12.3 Méthodes de prévention des boucles

- Split Horizon
- Route Poisoning
- Hold-Down Timers

5.13 Protocoles à État de Lien (Link State)

Les routeurs échangent leur **carte complète du réseau** (topologie) et non des routes. Ils utilisent l'algorithme **Dijkstra (SPF – Shortest Path First)** pour calculer les chemins optimaux.

5.13.1 Caractéristiques

- Convergence rapide.
- Très adaptés aux grands réseaux.
- Plus stables et moins sensibles aux boucles.
- Requiert plus de ressources (mémoire et CPU).

5.13.2 Exemples

- **OSPF** (Open Shortest Path First)
- **IS-IS**

5.14 Protocole RIP

5.14.1 Principe

RIP utilise le nombre de sauts (*hop count*) comme métrique. Une route maximale est limitée à 15 sauts.

5.14.2 Caractéristiques

- Mise à jour toutes les 30 secondes.
- Métrique : nombre de routeurs traversés.
- Simple mais peu adapté aux grands réseaux.

Exemple de configuration RIP (Cisco)

```
router rip
version 2
network 192.168.0.0
network 10.0.0.0
```

5.15 Protocole OSPF

5.15.1 Introduction

OSPF appartient aux protocoles **Link-State** et offre :

- une convergence très rapide ;
- une gestion par zones ;
- une métrique basée sur le coût (bandwidth) ;
- un support natif des grands réseaux.

5.15.2 Métrique

$$\text{coût} = \frac{10^8}{\text{bande passante (bps)}}$$

Exemple : Une interface 100 Mbps a un coût de :

$$\frac{10^8}{10^8} = 1$$

Exemple OSPF (Cisco)

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.0.0.0     0.255.255.255 area 1
```

5.16 Tables de Routage : Détails

Chaque routeur maintient une **table de routage** listant le prochain saut vers chaque réseau.

5.16.1 Entrées typiques d'une table

- Réseau destination
- Masque de sous-réseau
- Passerelle (next hop)
- Interface de sortie
- Métrique ou coût
- Protocole d'origine (C, S, R, O, B...)

Exemple de table de routage (Cisco)

```
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R 10.0.0.0/8 [120/1] via 192.168.1.2, 00:00:12, FastEthernet0/1
O 172.16.0.0/16 [110/2] via 192.168.1.3, 00:00:30, FastEthernet0/1
```

L'origine du route apparaît :

- C = Connected
- S = Static
- R = RIP
- O = OSPF

5.17 Convergence des Protocoles de Routage

La convergence est le temps nécessaire pour que tous les routeurs du réseau :

- détectent un changement ;
- calculent de nouvelles routes ;
- mettent à jour leur table.

Comparaison :

- RIP : lente (30 à 180 secondes).
- OSPF : très rapide (quelques ms à secondes).

5.18 Résumé Global du Routage

Résumé Général

- Le routage dirige les paquets d'un réseau source à un réseau destination.
- Il existe deux types : **statique** et **dynamique**.
- Les protocoles dynamiques se répartissent en :
  - Vecteur de distance : RIP (simple, lent, limité).
  - État de lien : OSPF (puissant, rapide, évolutif).
- La table de routage contient le *next hop* et la métrique.

6. Configuration des Routeurs

Les routeurs sont des équipements essentiels dans toute architecture réseau. Ils assurent :

- l'orientation des paquets IP entre différents réseaux,
- la segmentation logique,
- la sécurisation et le filtrage réseau,
- la mise en œuvre du routage statique et dynamique,
- l'interconnexion via IPv4 et IPv6.

Ce chapitre présente les principes fondamentaux de la configuration d'un routeur, en particulier sous environnement Cisco IOS, largement utilisé dans l'enseignement et l'industrie.

6.1 Modes de configuration (Cisco IOS)

Les routeurs Cisco fonctionnent via une interface CLI (Command Line Interface). Il existe plusieurs modes :

1. **User EXEC mode** Mode limité : consultation, tests (ping, traceroute).

```
Router>
```

2. **Privileged EXEC mode** Accès aux commandes avancées.

```
Router> enable
Router#
```

3. **Configuration globale**

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

4. **Configuration d'interface**

```
Router(config)# interface FastEthernet0/0
Router(config-if)#
```

6.2 Configuration des Interfaces IP

Chaque interface nécessite :

- une adresse IP,
- un masque de sous-réseau,
- un état actif (no shutdown).

Configuration d'une interface IP

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Configuration d'une interface série

Les interfaces WAN série nécessitent l'horloge (clock rate) sur le DCE :

Configuration interface Serial

```
Router(config)# interface Serial0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# clock rate 64000
Router(config-if)# no shutdown
```

6.3 Routes Statiques

Une route statique permet de définir manuellement le chemin vers un réseau.

Syntaxe

```
ip route <réseau> <masque> <passerelle>
```

Exemple

Route statique

```
Router(config)# ip route 172.16.0.0 255.255.0.0 192.168.1.2
```

Route par défaut

Route par défaut

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

Visualisation des routes

```
Router# show ip route
```

6.4 Configuration du Routage Dynamique

Les protocoles vus au Chapitre 5 peuvent maintenant être configurés.

6.4.1 RIP Version 2

Configuration RIP v2

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
```

6.4.2 OSPF

Configuration OSPF

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0     0.255.255.255 area 1
```

6.5 Configuration des VLANs et du Routage Inter-VLAN

Les réseaux modernes utilisent le découpage en VLAN pour la segmentation logique.

6.5.1 Création d'un VLAN

Création VLAN

```
Switch(config)# vlan 10
Switch(config-vlan)# name Finance
```

6.5.2 Configuration d'un port

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

6.5.3 Routage Inter-VLAN (Router-on-a-Stick)

Routage Inter-VLAN

```
Router(config)# interface FastEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
```

6.6 NAT : Network Address Translation

Le NAT permet de traduire des adresses privées vers des adresses publiques.

6.6.1 Configuration du NAT dynamique

Configuration NAT

```
Router(config)# ip nat inside source list 1 interface Serial0/0 overload
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255

Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside

Router(config)# interface Serial0/0
Router(config-if)# ip nat outside
```

6.7 ACL : Listes de Contrôle d'Accès

Les ACL filtrent le trafic basé sur :

- l'adresse source ;
- l'adresse destination ;
- le protocole (TCP, UDP, ICMP) ;
- les ports.

6.7.1 ACL standard

ACL Standard

```
access-list 1 deny 192.168.1.5
access-list 1 permit any

interface FastEthernet0/0
 ip access-group 1 in
```

6.7.2 ACL étendue

ACL Étendue

```
access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 101 permit ip any any

interface FastEthernet0/1
 ip access-group 101 in
```

6.8 Sauvegarde et Restauration de la Configuration

6.8.1 Afficher la configuration courante

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

6.8.2 Sauvegarder en mémoire non volatile

```
Router# copy running-config startup-config
```

6.8.3 Effacer la configuration

```
Router# write erase
Router# reload
```

6.9 Résumé Général du Chapitre

Résumé du Chapitre 6

- Les routeurs disposent de plusieurs modes de configuration.
- Chaque interface doit être configurée (IP + masque + activation).
- Les routes peuvent être statiques ou dynamiques (RIP, OSPF).
- Les VLANs nécessitent un routage inter-VLAN.
- NAT permet la traduction d'adresses privées en publiques.
- ACL permet de sécuriser le trafic.
- La configuration doit être sauvegardée régulièrement.

Annexes – Exercices des Chapitres

Annexe 1 — Exercices Chapitre 1

Annexe — Exercices du Chapitre 1 : Architectures des réseaux informatiques

Partie 1 — Exercices fondamentaux

Exercice 1 : L'information

Donner trois exemples d'informations numériques et trois exemples d'informations analogiques.

Exercice 2 : Représentation de l'information

Expliquer la différence entre : bit, octet, mot, caractère.

Exercice 3 : Types de transmission

Classer les transmission suivantes : radio, fibre optique, paires torsadées, satellite en :

- support guidé,
- support non guidé.

Exercice 4 : Mode de transmission

Décrire les modes : simplex, half-duplex, full-duplex.

Exercice 5 : Débit et bande passante

Calculer le débit en bit/s : Un fichier de 80 Mo est transféré en 20 secondes.

Exercice 6 : Topologies

Illustrer et expliquer les topologies : bus, anneau, étoile.

Exercice 7 : Modèle OSI

Pour chaque couche OSI, donner :

- sa fonction principale,
- un protocole associé.

Exercice 8 : Encapsulation

Expliquer l'encapsulation dans le modèle OSI.

Exercice 9 : Différence LAN / WAN

Donner 3 différences entre un LAN et un WAN.

Exercice 10 : Types de câbles

Associer chaque situation au câble idéal :

- liaison très longue distance,
- liaison interne de quelques mètres,
- connexion backbone haut débit.

Partie 2 — Exercices avancés

Exercice 11 : Rôle des couches OSI

Analyser le trajet complet d'un paquet du PC1 au PC2 et indiquer pour chaque couche :

- l'unité de données (PDU),
- l'équipement intervenant,
- les informations ajoutées.

Exercice 12 : Signalisation

Comparer la codification NRZ, Manchester et 4B/5B.

Exercice 13 : Fibre optique

Lister 5 avantages et 3 inconvénients de la fibre optique.

Exercice 14 : Collision et accès au média

Expliquer le fonctionnement de CSMA/CD et CSMA/CA.

Exercice 15 : Architecture des réseaux locaux

Donner les caractéristiques techniques d'un LAN moderne :

- architecture,
- protocoles,
- performances.

Partie 3 — Mini-projet : Étude de cas réseau local

On souhaite concevoir un réseau local pour un bâtiment universitaire composé de :

- 3 étages,
- 120 postes,
- un serveur principal,
- un accès Internet centralisé.

Travail demandé

1. Proposer une architecture réseau complète (LAN).
2. Sélectionner les supports de transmission.
3. Décrire les topologies mises en œuvre.
4. Indiquer les équipements réseau nécessaires.
5. Expliquer comment assurer la redondance.

Partie 4 — Corrigés

Correction Exercice 5

Débit = taille / temps

$$80\ Mo = 80 \times 8 = 640\ Mbit$$

$$\text{Débit} = \frac{640}{20} = 32\ Mbit/s$$

Correction Exercice 7

Exemple (réponse courte) :

- Couche 1 : Transmission — Ethernet PHY
- Couche 2 : Liaison — Ethernet, PPP
- Couche 3 : Réseau — IP
- Couche 4 : Transport — TCP, UDP

Correction Mini-projet (extrait)

Une architecture valide doit inclure :

- topologie en étoile par étage,
- switch par étage, cœur de réseau central,
- fibre optique entre étages,
- redondance via un switch de backup ou double liaison.