OFPPT
La voie de l'avenir

INFRASTRUCTURE DIGITALE

CONCEVOIR UN RÉSEAU INFORMATIQUE

OBJECTIF

A l’issue de ce module de compétence, vous serez capable d’identifier les éléments constitutifs d’un SI au sein des entreprises.

120 heures

SOMMAIRE

PARTIE 1

Expliquer les notions de base du réseau informatique

PARTIE 2

Notions de base sur la commutation

PARTIE 3

Routage d'un réseau d'entreprise

PARTIE 4

Sécuriser un réseau d'entreprise

PARTIE 1

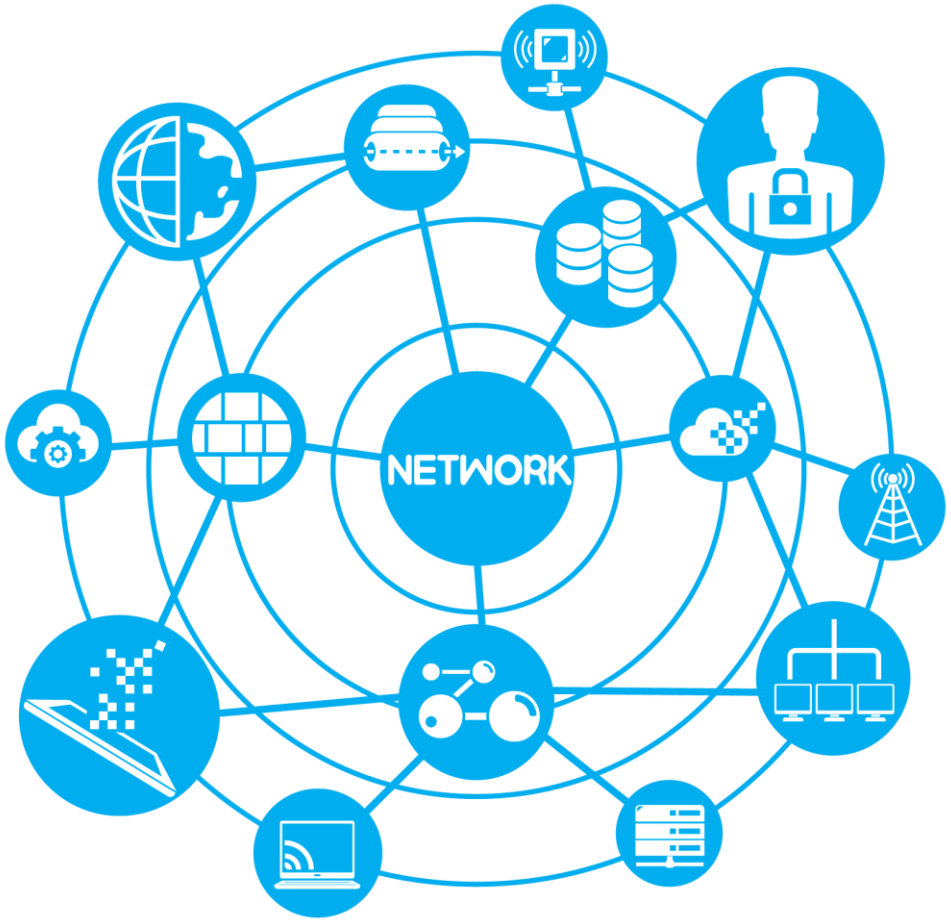
NOTIONS DE BASE DU RÉSEAU INFORMATIQUE

CHAPITRE 1

LES DIFFÉRENTS TYPES DE RÉSEAUX

Description d’un réseau

Un réseau informatique est l’ensemble d’équipements interconnectés entre eux dans une zone géographique.



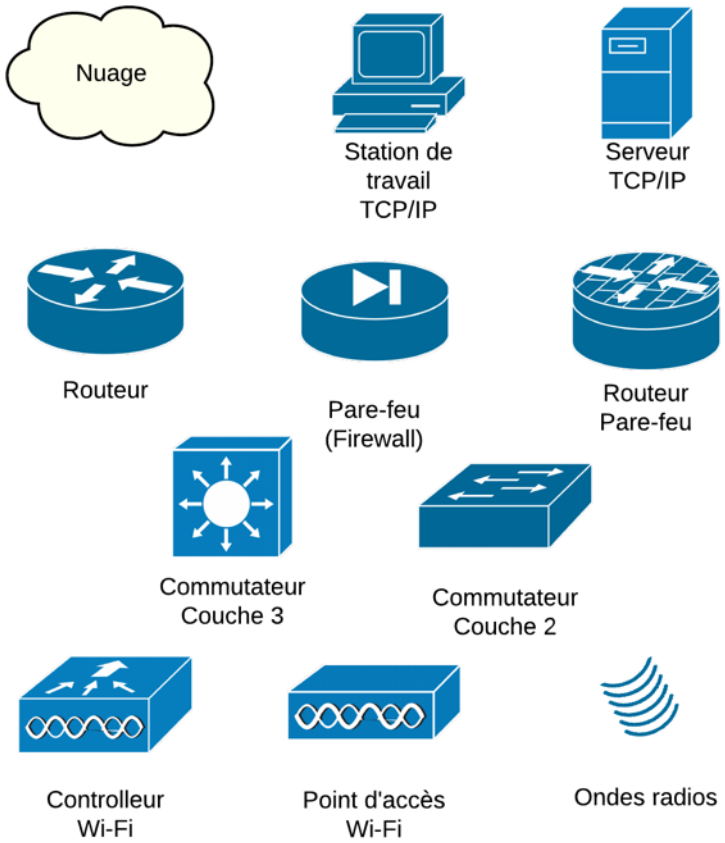
Description d’un réseau

- Les réseaux sont utilisés pour un certain nombre de raisons, il s’agit généralement de partager:
  - **Informations**: pour des applications telles que le courrier électronique ou pour accéder à certains sites Web.
  - **Partage de fichiers**: les utilisateurs puissent accéder à un lecteur réseau partagé avec des documents, des images et / ou d’autres fichiers.
  - **Partage des ressources** : pour connecter une imprimante au réseau utilisé par plusieurs utilisateurs. Pas besoin de connecter une imprimante directement à chaque ordinateur.
  - **Partage d’application** : avoir des utilisateurs qui ont besoin d’accéder à la même application. Par exemple, un service financier avec cinq utilisateurs qui ont besoin d’accéder au même logiciel de comptabilité.

CHAPITRE 1

LES DIFFÉRENTS TYPES DE RÉSEAUX

Composants d’un réseau



- Les équipements de réseau sont utilisés pour étendre les connexions de câble, concentrer les connexions, convertir les formats de données et gérer les transferts de données.
- Chacun de ces périphériques est associé à une couche du modèle OSI et qui offre un ensemble de fonctionnalités.

Composants d’un réseau

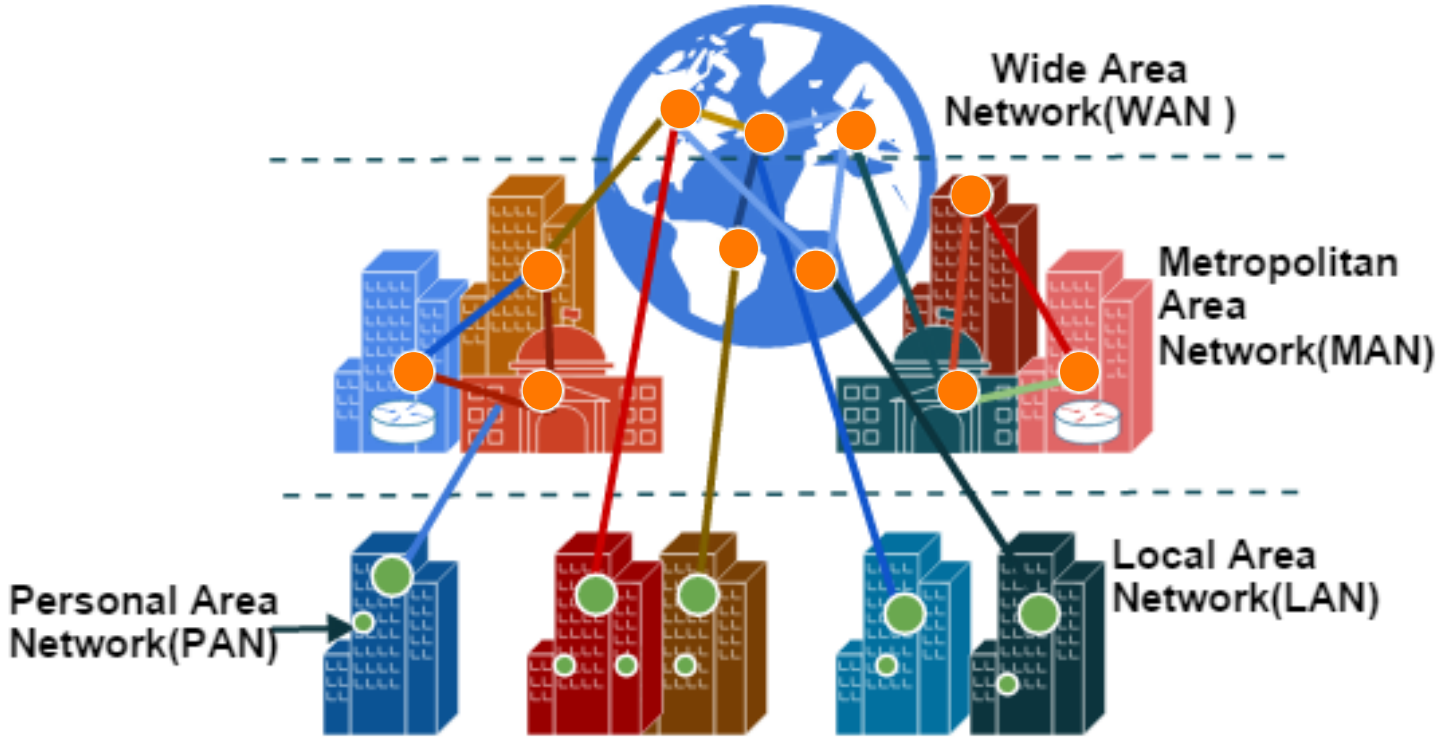
- On peut les positionner dans un niveau (couche: Layer)

Périphérique	Couche
Routeur (Router)	L3
Commutateur (Switch) L3	L2/L3
Commutateur (Switch) L2	L2
Pont (Bridge)	L2
Concentrateur (Hub)	L1
Répéteur (Repeater)	L1
Contrôlleur WLAN	L2/L3/L7
Point d'accès sans-fil (AP) Wi-Fi	L1/L2
Carte réseau (NIC)	L2
Hôte terminal	L3/L4/L7

CHAPITRE 1

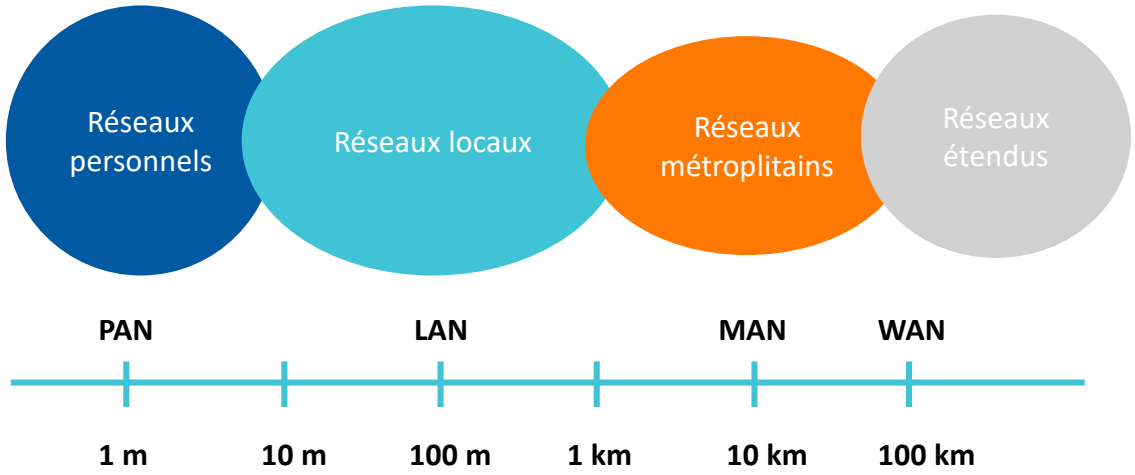
LES DIFFÉRENTS TYPES DE RÉSEAUX

Différents types de réseaux



Critère de classification

Le critère de classification est la distance qui sépare les équipements informatique.



CHAPITRE 1

LES DIFFÉRENTS TYPES DE RÉSEAUX

1 – Description d’un réseau

2 – Composants d’un réseau

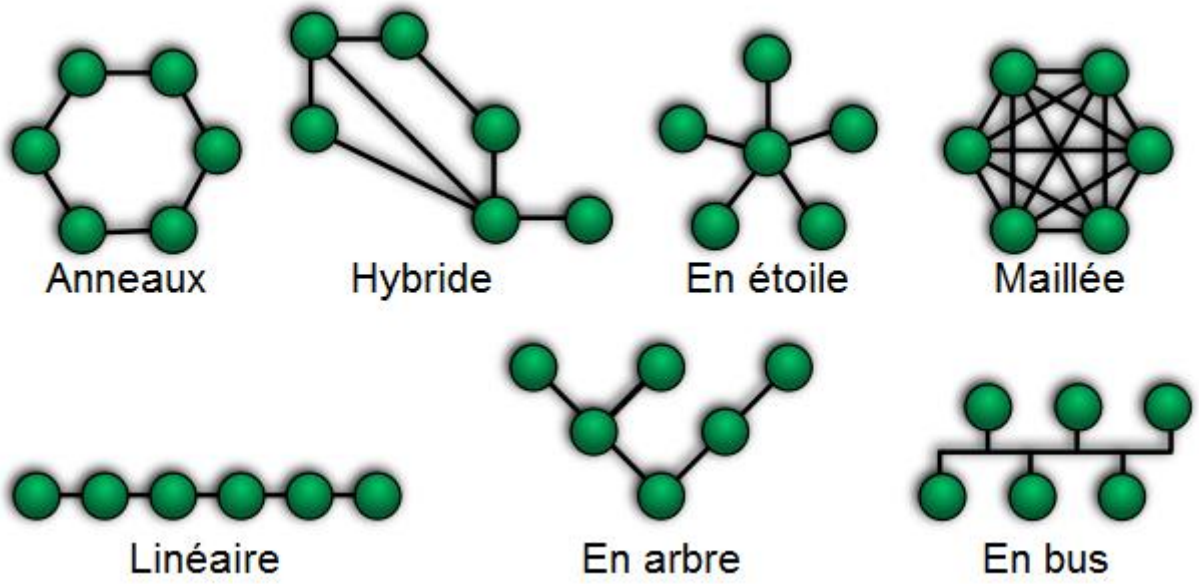
3 - Différents types de réseaux

4 - Avantages et inconvénients des différentes topologies

5- Tendances des réseaux

Topologie

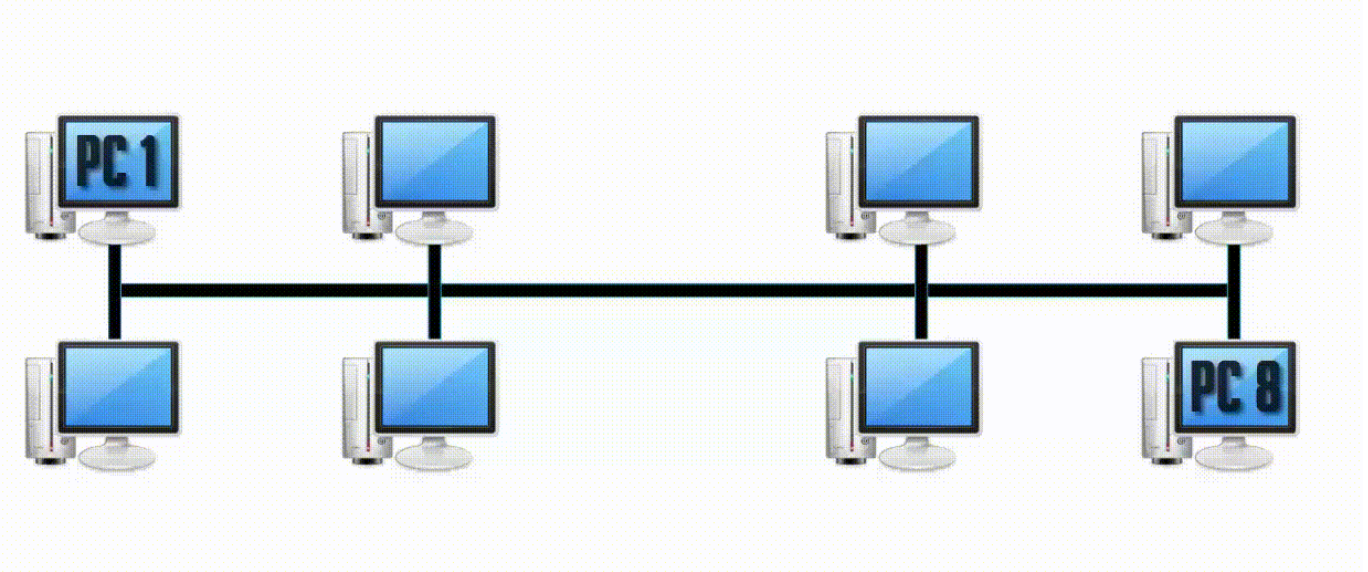
C’est la **façon** d’interconnecter les équipements dans une zone géographique.



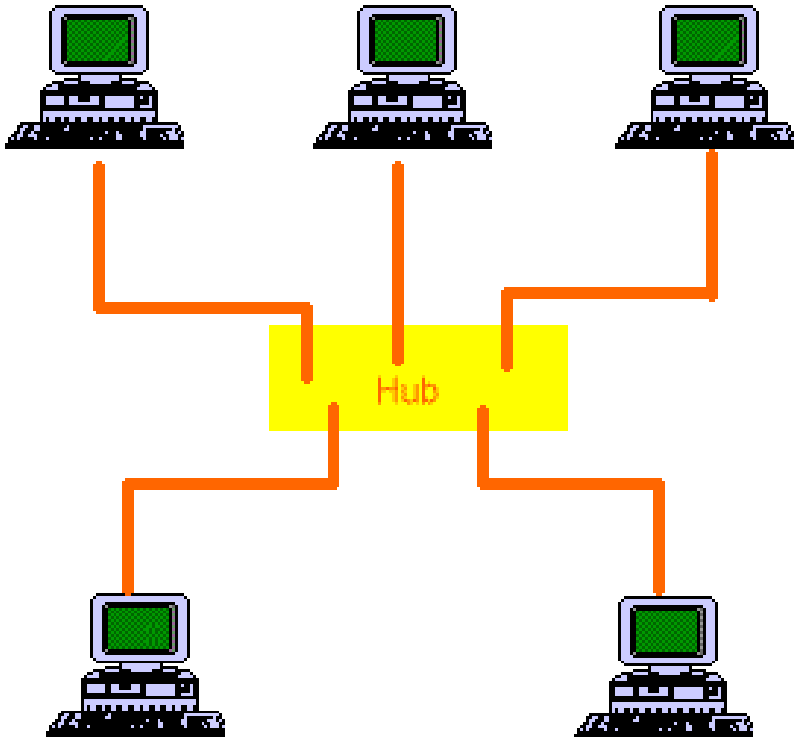
Topologie Physique et logique en BUS

Les inconvénients les plus fréquents:

- Diffusion
- Collision
- Qualité et débit faible



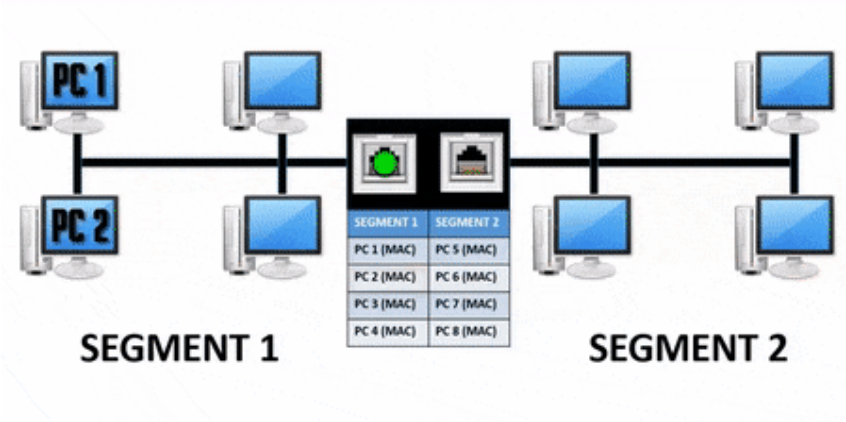
Topologie Physique Etoile avec HUB

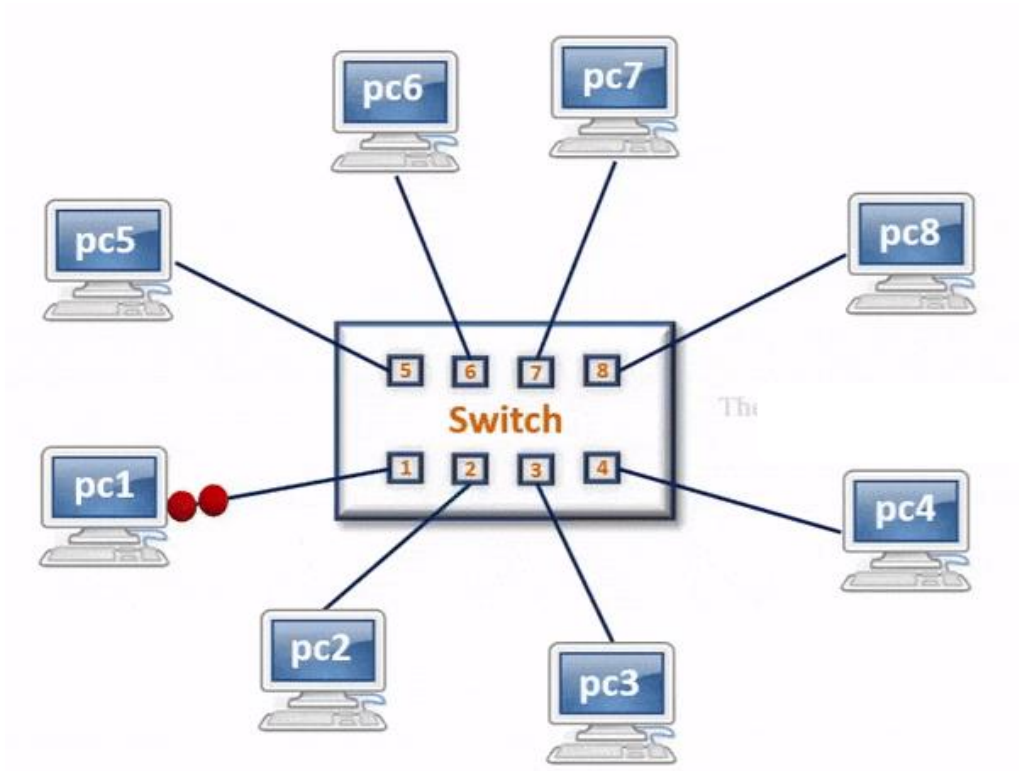


Topologie Physique Etoile avec SWITCH

Les avantages:

- Pas de collision
- Qualité et débit améliorés





CHAPITRE 1

LES DIFFÉRENTS TYPES DE RÉSEAUX

1 – Description d’un réseau

2 – Composants d’un réseau

3 - Différents types de réseaux

4 - Avantages et inconvénients des différentes topologies

5- Tendances des réseaux

Tendances des réseaux

- À mesure que de nouvelles technologies et de nouveaux appareils d'utilisateurs finaux arrivent sur le marché, les entreprises et les consommateurs doivent continuer à s'adapter à cet environnement en constante évolution.

- Il existe plusieurs tendances en matière de réseautage qui affectent les organisations et les consommateurs :
  - Bring Your Own Device (BYOD)
  - Collaboration en ligne
  - Communications vidéo
  - Cloud Computing

Tendances des réseaux

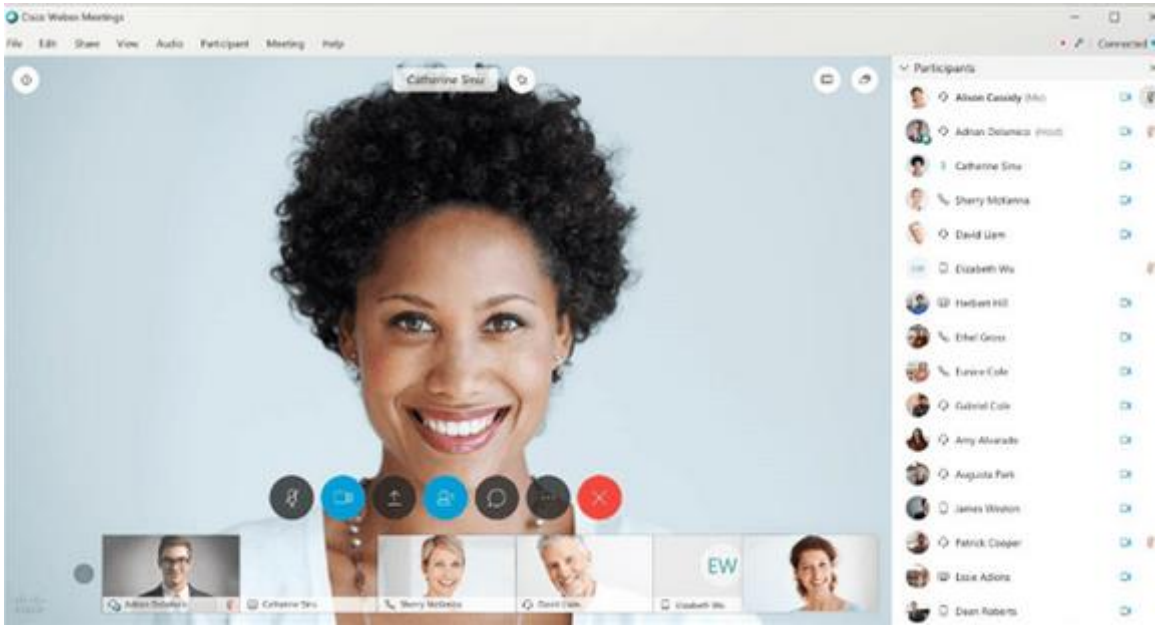
- Le **BYOD** donne aux utilisateurs finaux la liberté d'utiliser des outils personnels pour accéder aux informations et communiquer sur un réseau d'entreprise ou de campus.

- Il s'agit notamment des ordinateurs portables, des ordinateurs portables, des tablettes, des téléphones intelligents et des lecteurs électroniques.

Tendances des réseaux

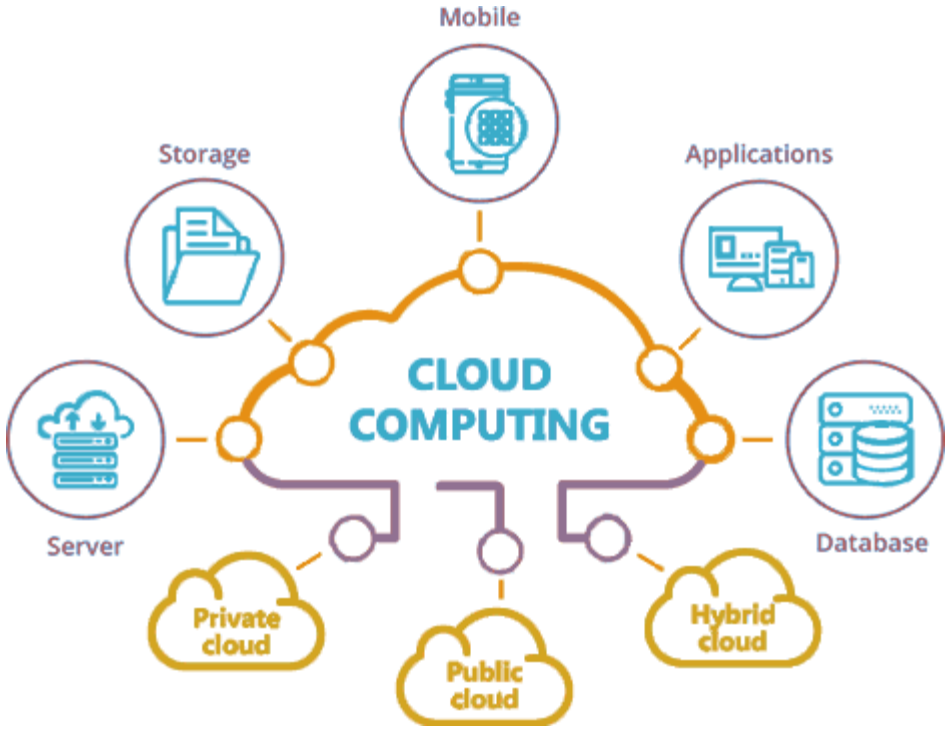
- La **collaboration** est définie comme « l'acte de travailler avec un autre ou d'autres sur un projet commun ».

- Les outils de collaboration, tels que Cisco WebEx, offrent aux employés, aux étudiants, aux enseignants, aux clients et aux partenaires un moyen de se connecter instantanément, d'interagir et d'atteindre leurs objectifs.



Tendances des réseaux

- Le **cloud computing** est l'un des moyens par lequel nous accédons aux données et les stockons.
- Le cloud computing nous permet de stocker des fichiers personnels, voire de sauvegarder un disque entier sur des serveurs sur Internet.
- Des applications telles que le traitement de texte et la retouche photo sont accessibles à l'aide du cloud.

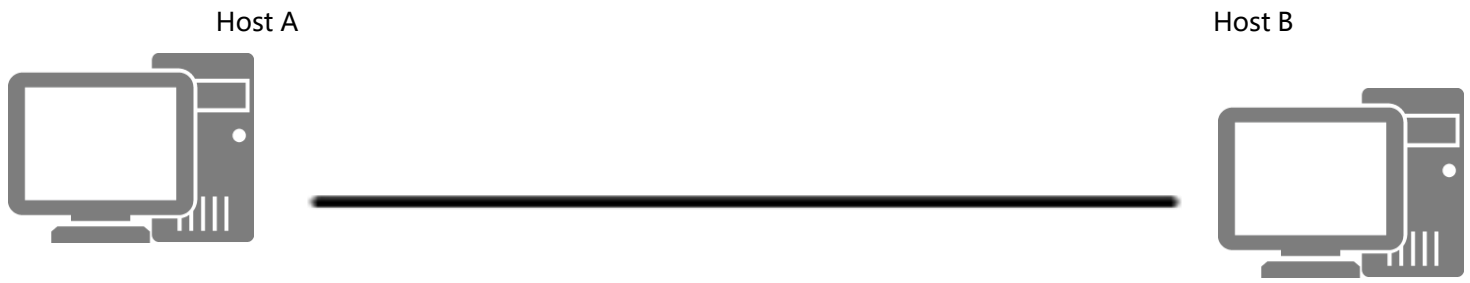


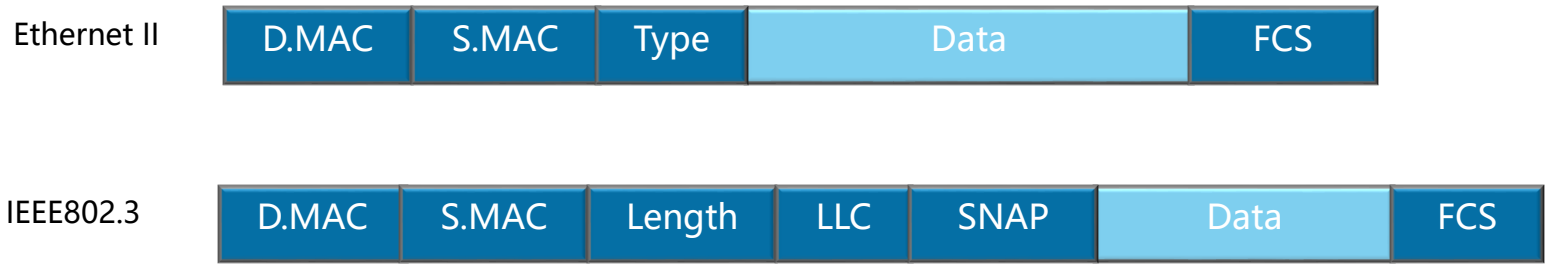
CHAPITRE 2

LES RESEAUX LOCAUX

Les trames de la couche liaison

Les trames de la couche liaison de données sont utilisés pour la transmission sur le support de communication

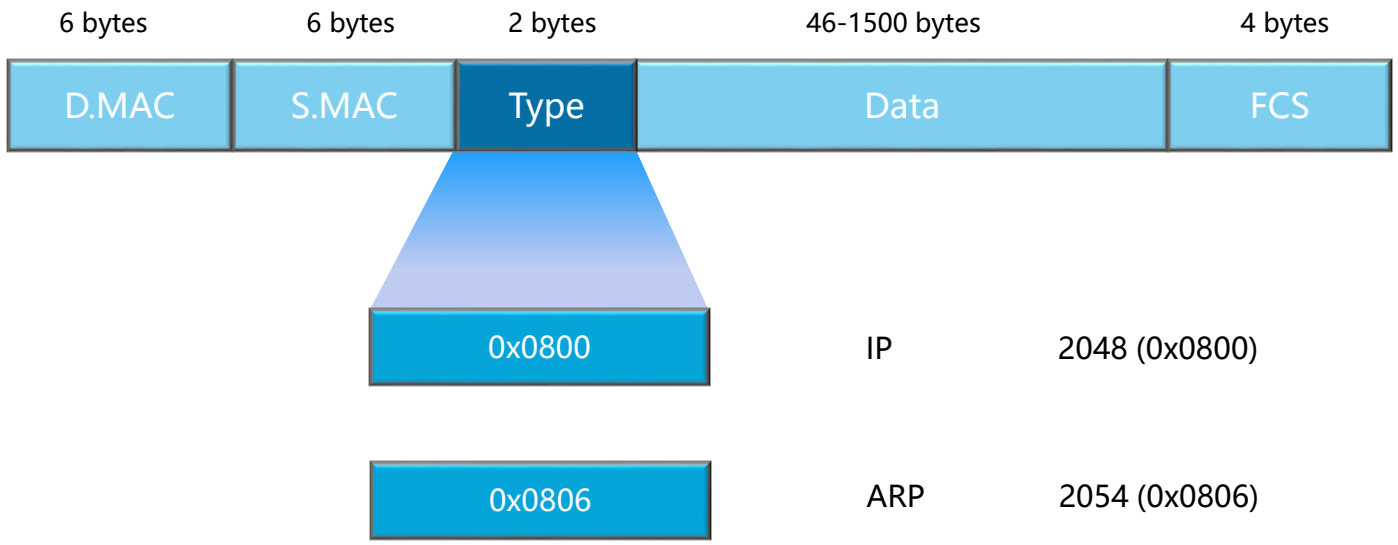




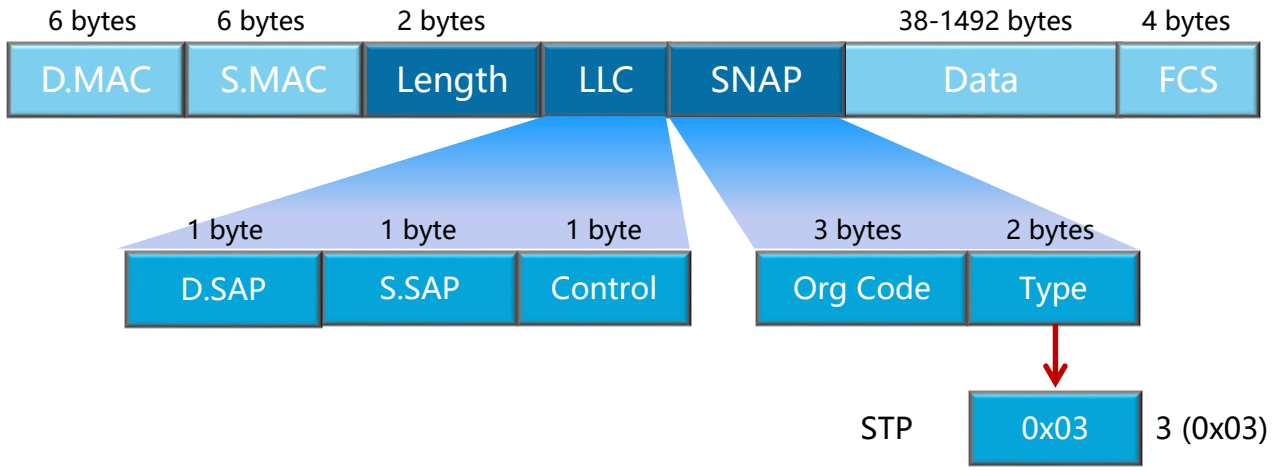
Field Value >= 1536 (0x0600) Ethernet II

Field Value <= 1500 (0x05DC) IEEE802.3

Le type de trame Ethernet II est associé à des protocoles d'une valeur de type supérieure à 1536 (0x600)



Le type de trame IEEE 802.3 est associé à des protocoles d'une valeur de type inférieure à 1500 (0x05DC)



CHAPITRE 2

LES RESEAUX LOCAUX

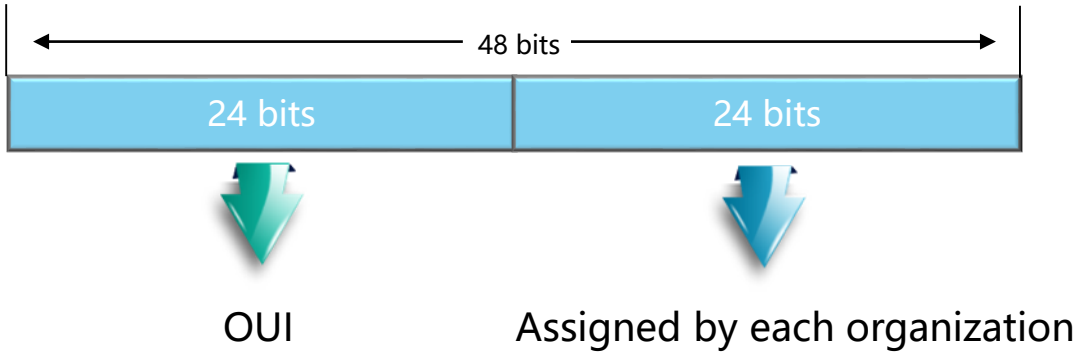
1 - Différentes versions d'Ethernet

2 - Adresse MAC Ethernet

3 - Méthodes de transmission et vitesse de commutation

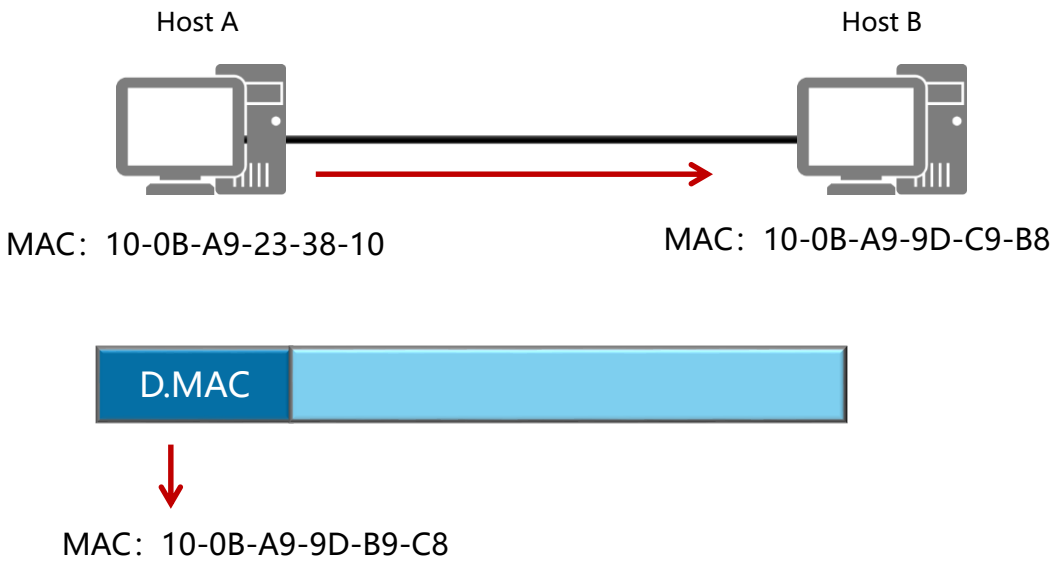
4 - Introduction aux réseaux sans fil (802.11x)

Adresse MAC Ethernet



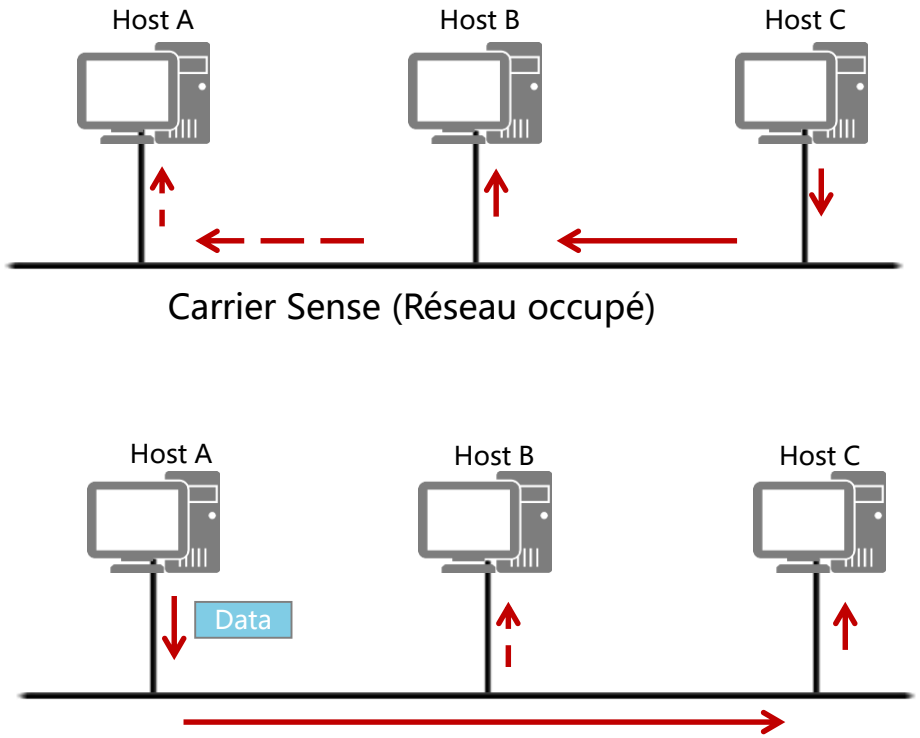
Les adresses MAC sont composées d'un identificateur unique sur le plan organisationur et d'une valeur d'adresse attribuée par le fournisseur

Adresse MAC Ethernet

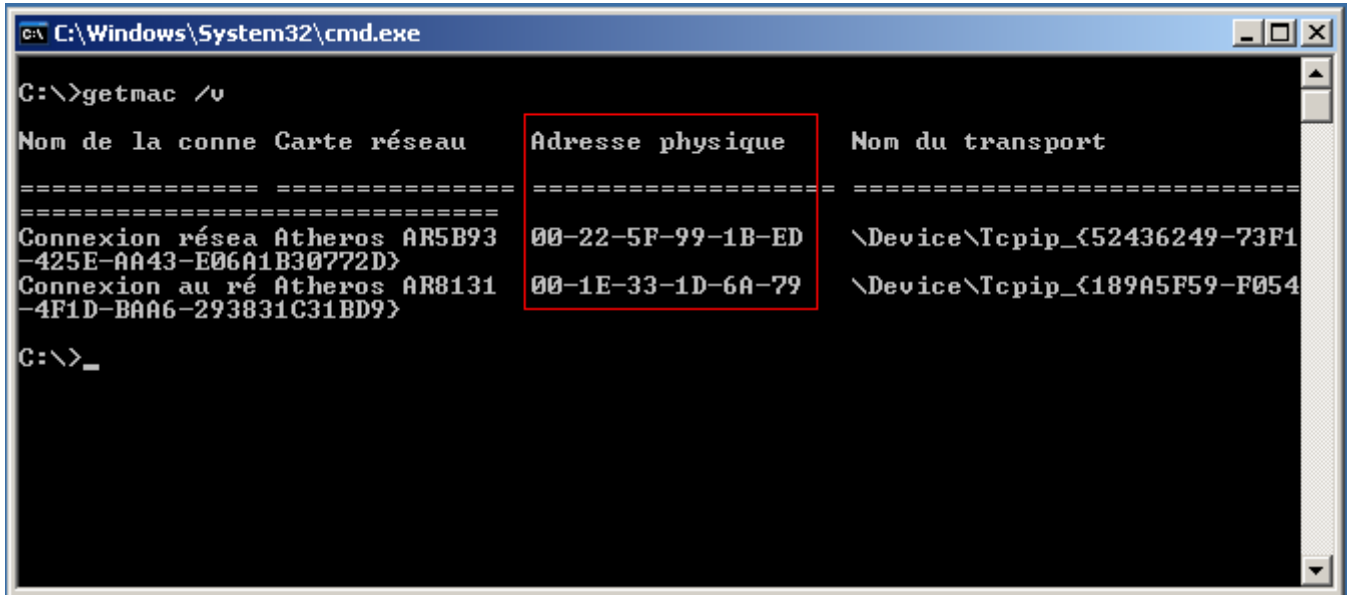


Le contrôle de l'accès aux médias (MAC) facilite la communication de la couche de liaison de données.

Adresse MAC Ethernet

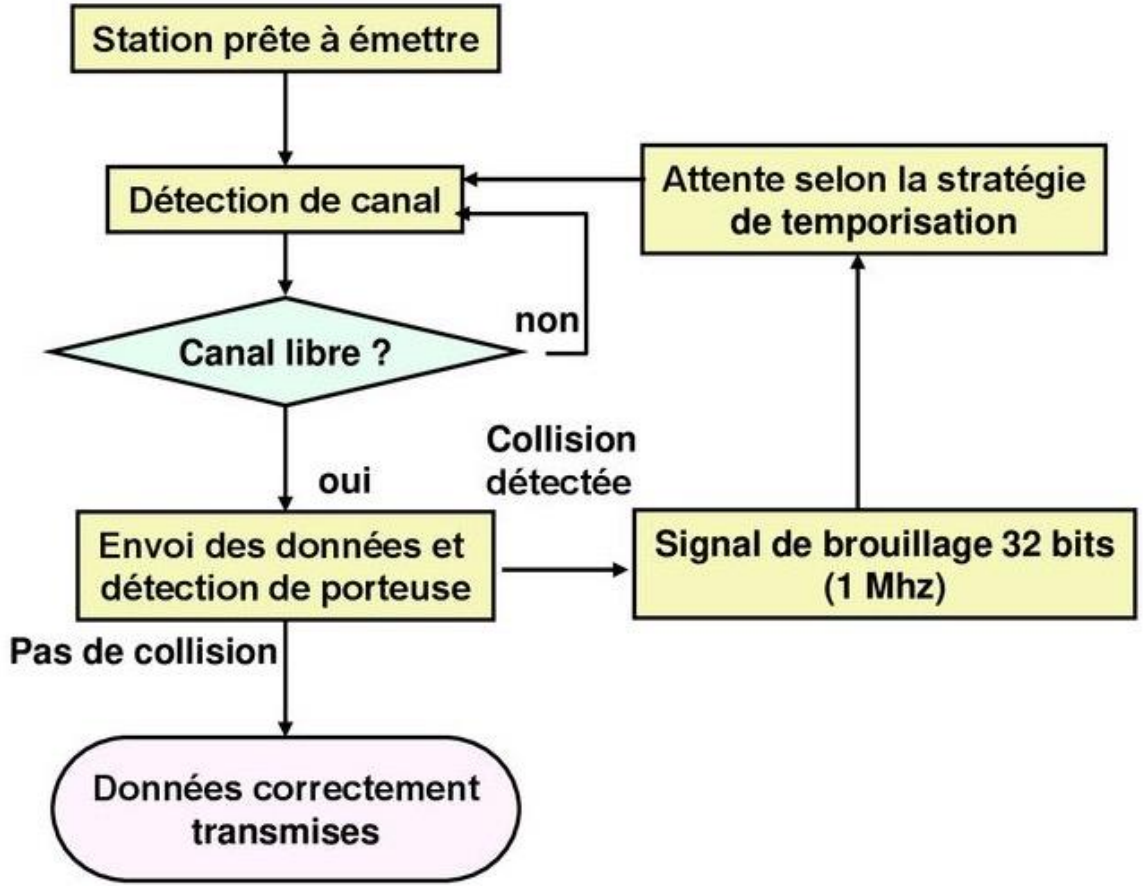


Adresse MAC Ethernet



On peut retrouver l'adresse MAC sous Windows grâce à la commande « **ipconfig /all** » ou bien « **getmac** »

Adresse MAC Ethernet



CHAPITRE 2

LES RESEAUX LOCAUX

1 - Différentes versions d'Ethernet

2 - Adresse MAC Ethernet

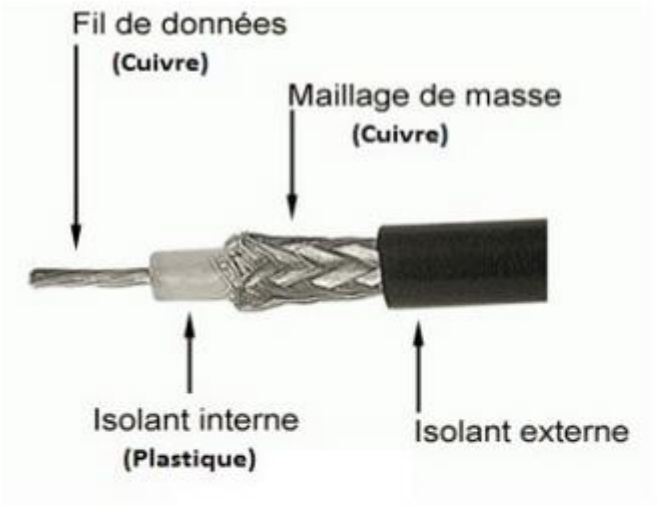
3 - Méthodes de transmission et vitesse de commutation

4 - Introduction aux réseaux sans fil (802.11x)

Méthodes de transmission et vitesse de commutation

Le câble coaxial

- Capable à s'étendre sur une plus grande distance.



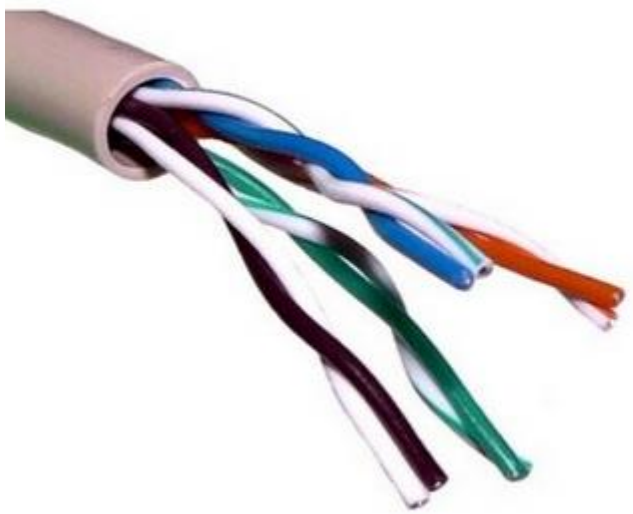
Connecteur BNC

Fiche technique	
Désignation	Coaxial
Vitesse	10-100 Mbits/s
Longueur max.	500m
Raccordement	Connecteur BNC (British Naval Connector)
Impédance	150 Ω
Coût	Peu cher

Méthodes de transmission et vitesse de commutation

Le câble à paires torsadées non blindées (UTP)

- Un câble UTP est composé de 4 paires de fils torsadées 2 à 2



Fiche technique	
Désignation	UTP (Unshielded Twisted Pair)
Vitesse	10-100 Mbits/s
Longueur max.	100m
Raccordement	Connecteur RJ45
Impédance	100 Ω
Coût	Faible

Méthodes de transmission et vitesse de commutation

Le câble à paires torsadées blindées (STP)

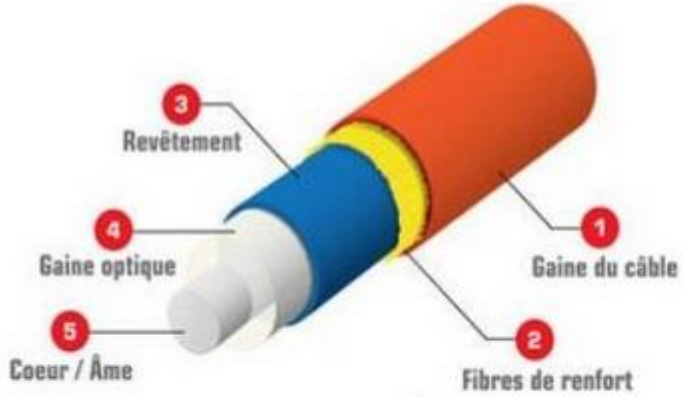
- Ajoute aux spécifications de l'UTP une méthode de blindage

Fiche technique	
Désignation	UTP (Shielded Twisted Pair)
Vitesse	10-100 Mbits/s
Longueur max.	100m
Raccordement	Connecteur RJ45
Impédance	100 Ω
Coût	Moyennement cher

Méthodes de transmission et vitesse de commutation

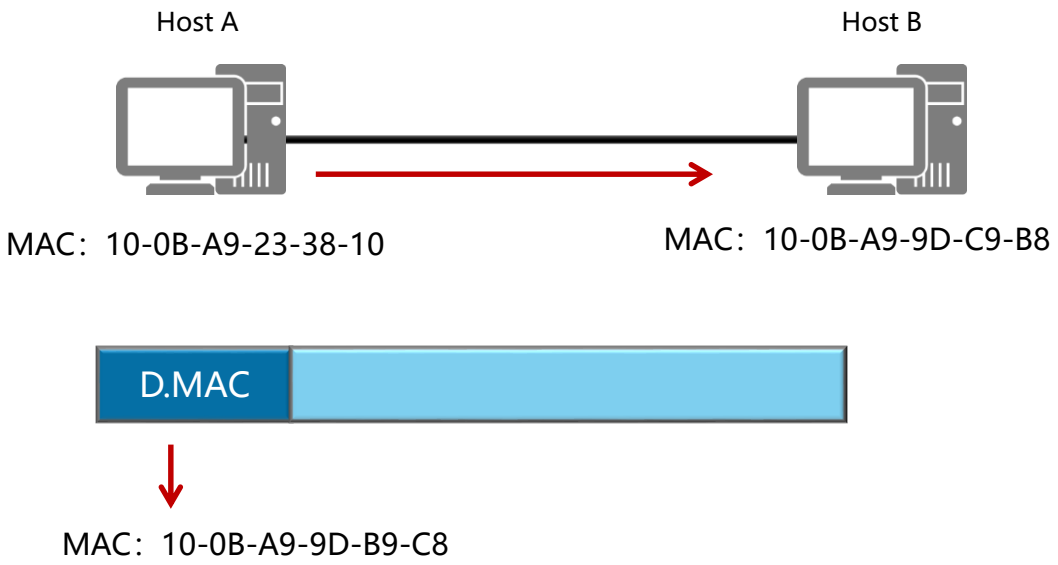
La fibre optique

- Transmission des données à un haut débit (Plus de 100Mbits/s).



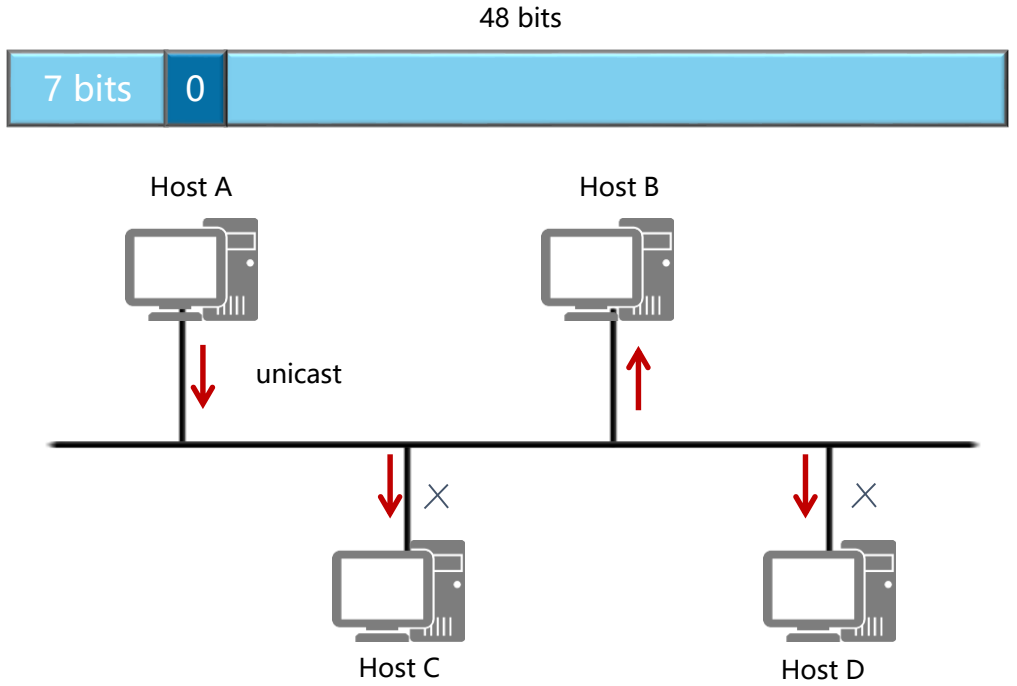
Fiche technique	
Désignation	Fibre Optique
Vitesse	100+ Mbits/s
Longueur max.	2 km en multimode 3 km en monomode
Raccordement	Connecteur multimode ou monomode
Coût	Cher

Méthodes de transmission et vitesse de commutation



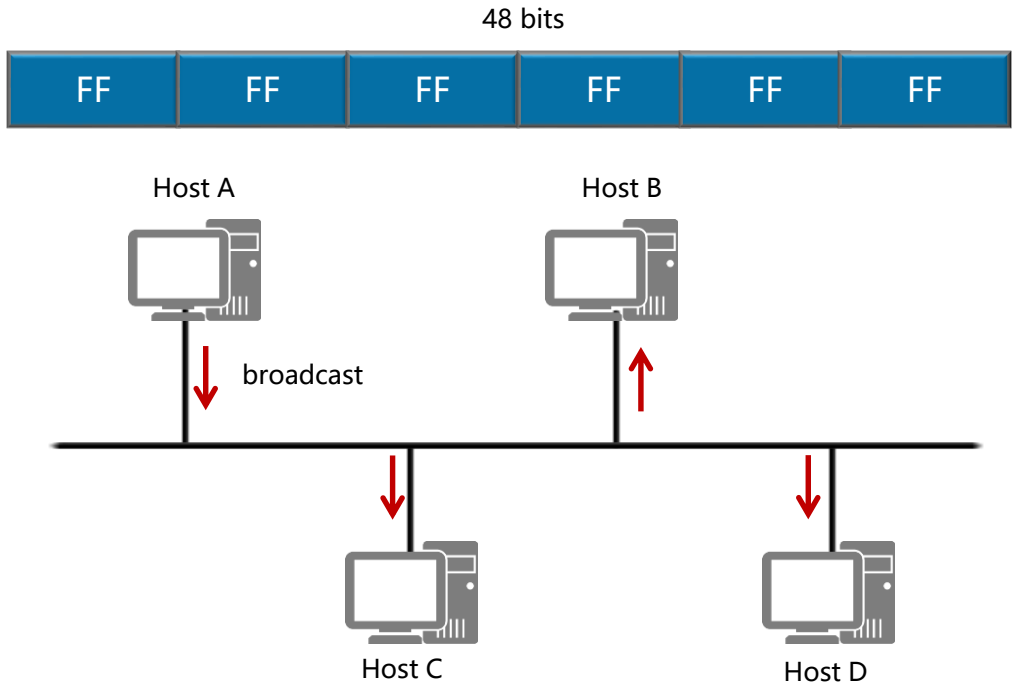
Le contrôle de l'accès aux médias (MAC) facilite la communication de la couche de liaison de données.

Méthodes de transmission et vitesse de commutation



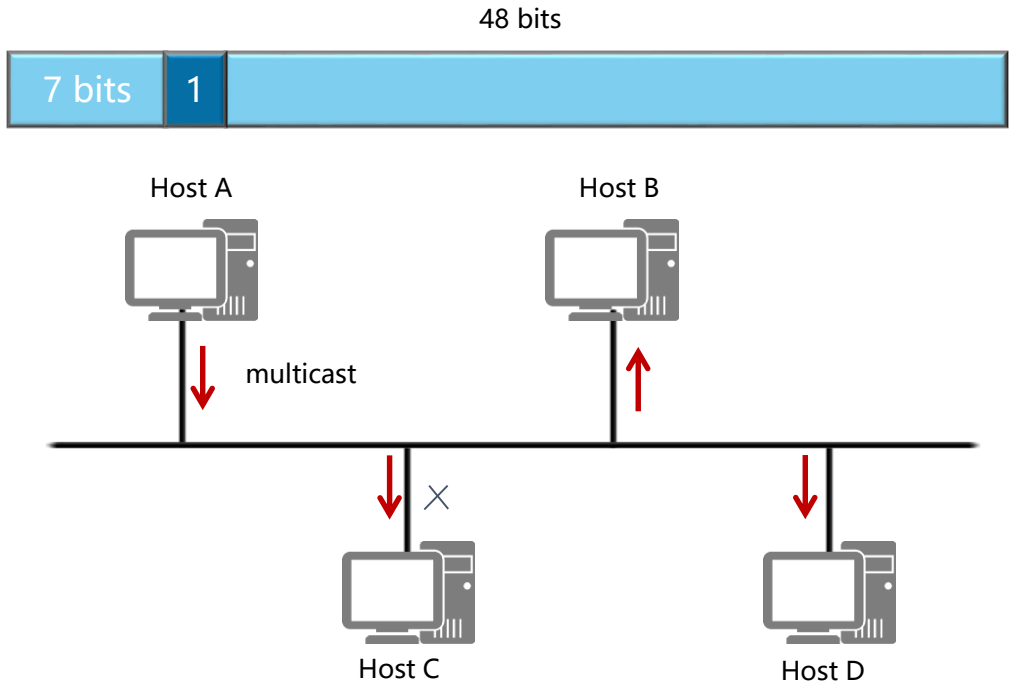
Trame « **unicast** » ou « mono diffusion » elle a une seule destination.

Méthodes de transmission et vitesse de commutation



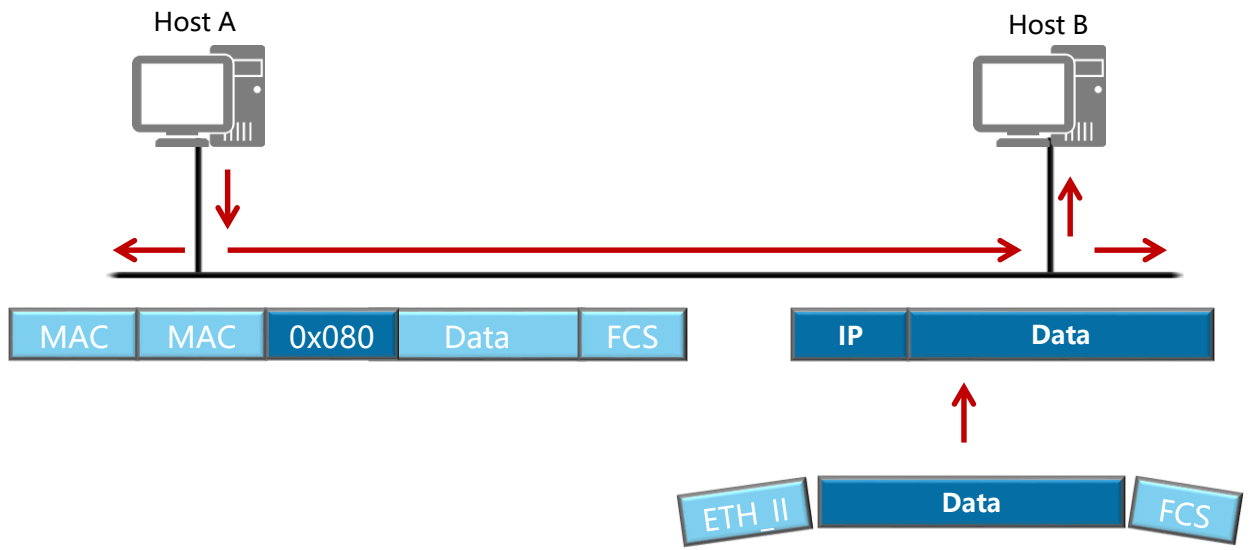
Trame « **broadcast** » ou « diffusion » elle est destinée à toutes les machines en réseau local.

Méthodes de transmission et vitesse de commutation



Trame « **multicast** » ou « multi-diffusion » elle est destinée à un group de machines en réseau local.

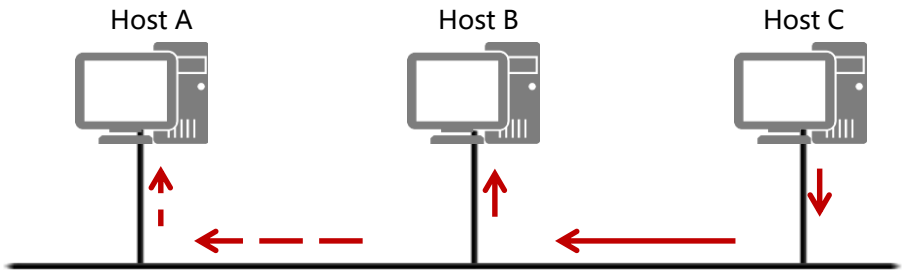
Méthodes de transmission et vitesse de commutation



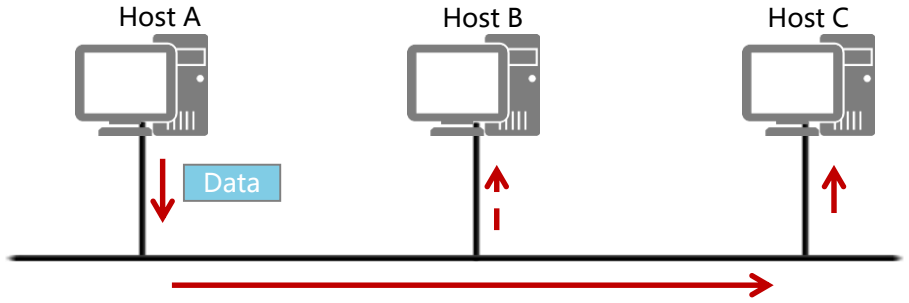
Les instructions de liaison de données (trames) sont reçues, traitées et rejetées

Carrier-sense multiple access (CSMA)

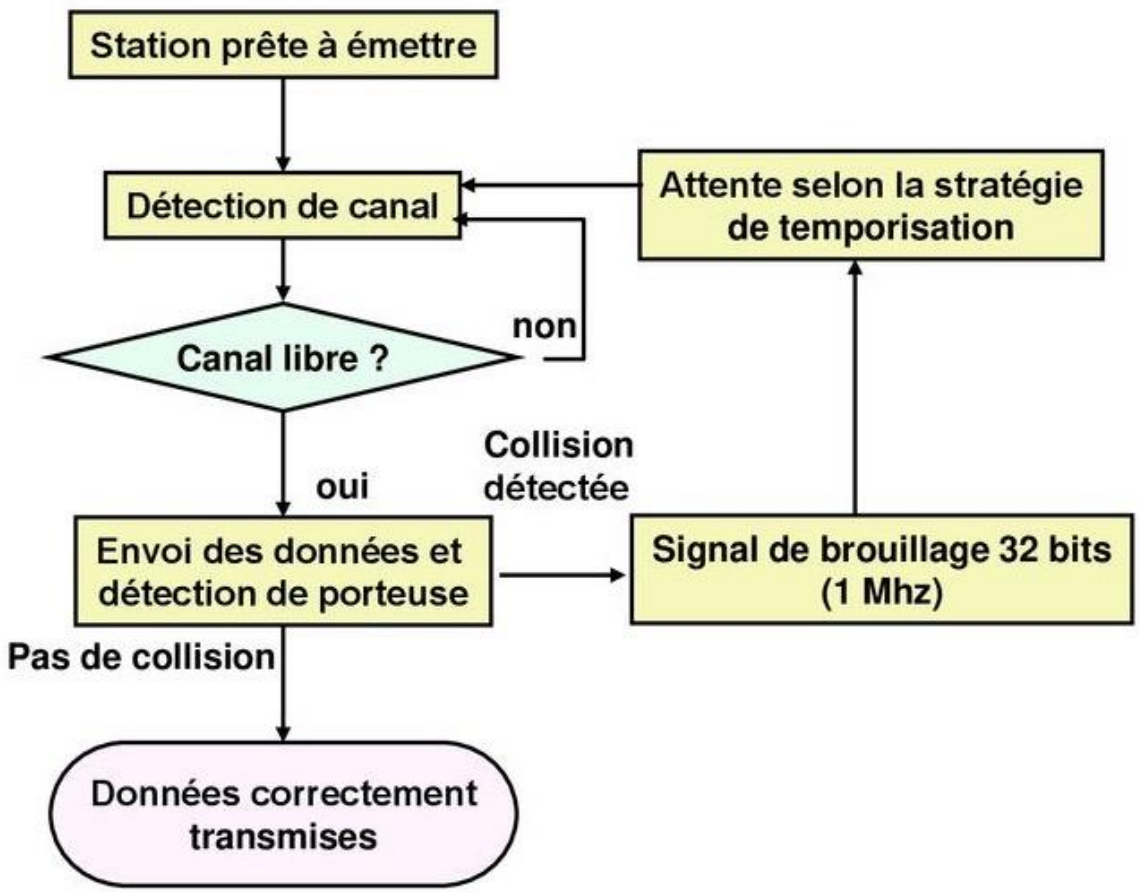
Carrier-sense multiple access (CSMA) est un protocole mac (Media Access Control) dans lequel un nœud vérifie l'absence d'autre trafic avant de transmettre sur un support de transmission partagé.



Carrier Sense (Réseau occupé)



CSMA/CD


Station prête à émettre
Détection de canal
Attente selon la stratégie de temporisation
Canal libre ?
non
oui
Collision détectée
Envoi des données et détection de porteuse
Signal de brouillage 32 bits (1 Mhz)
Pas de collision
Données correctement transmises

CHAPITRE 2

LES RESEAUX LOCAUX

1 - Différentes versions d'Ethernet

2 - Adresse MAC Ethernet

3 - Méthodes de transmission et vitesse de commutation

4 - Introduction aux réseaux sans fil (802.11x)

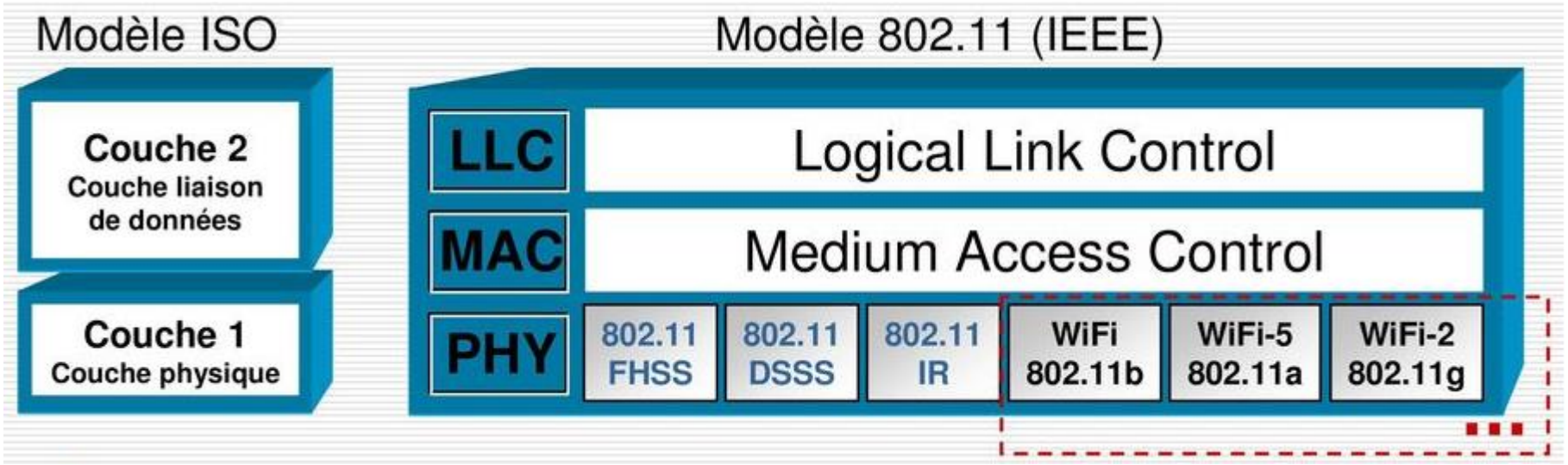
Introduction aux réseaux sans fil (802.11x)

- Il existe différentes technologies et normes sans fil dans lesquelles les communications couvrent des zones de couverture plus petites ou plus grandes.
- Les technologies sans fil incluent le cellulaire, Bluetooth et Zigbee.
- Toutes ces différentes technologies sans fil peuvent être organisées dans les quatre principales topologies sans fil :
  1. Réseau étendu sans fil (WWAN)
  2. Réseau métropolitain sans fil (WMAN)
  3. Réseau personnel sans fil (WPAN)
  4. Réseau local sans fil (WLAN)

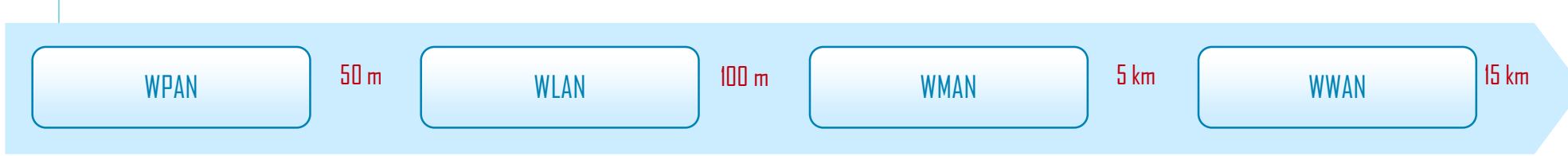
Introduction aux réseaux sans fil (802.11x)

- La norme 802.11 d'originale a été publiée en juin 1997, et elle est souvent appelée 802.11 Prime car c'était la première norme WLAN.

- L'IEEE définit spécifiquement les technologies 802.11 au niveau de la couche physique et la sous-couche MAC de la couche liaison de données.



Transmission distance (Radius)

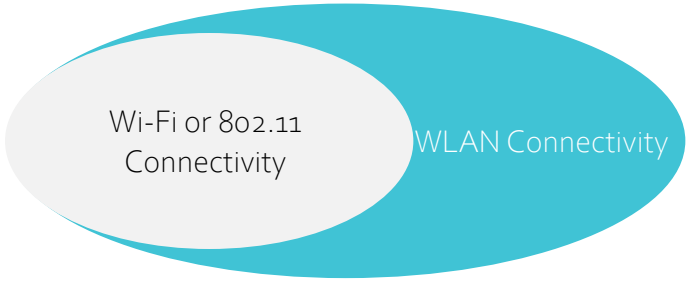


- Bluetooth
- ZigBee
- NFC

- Wi-Fi
- WPAN-related technologies are often used on WLANs.

- WiMax

- GSM
- CDMA
- WCDMA
- TD-SCDMA
- LTE
- 5G

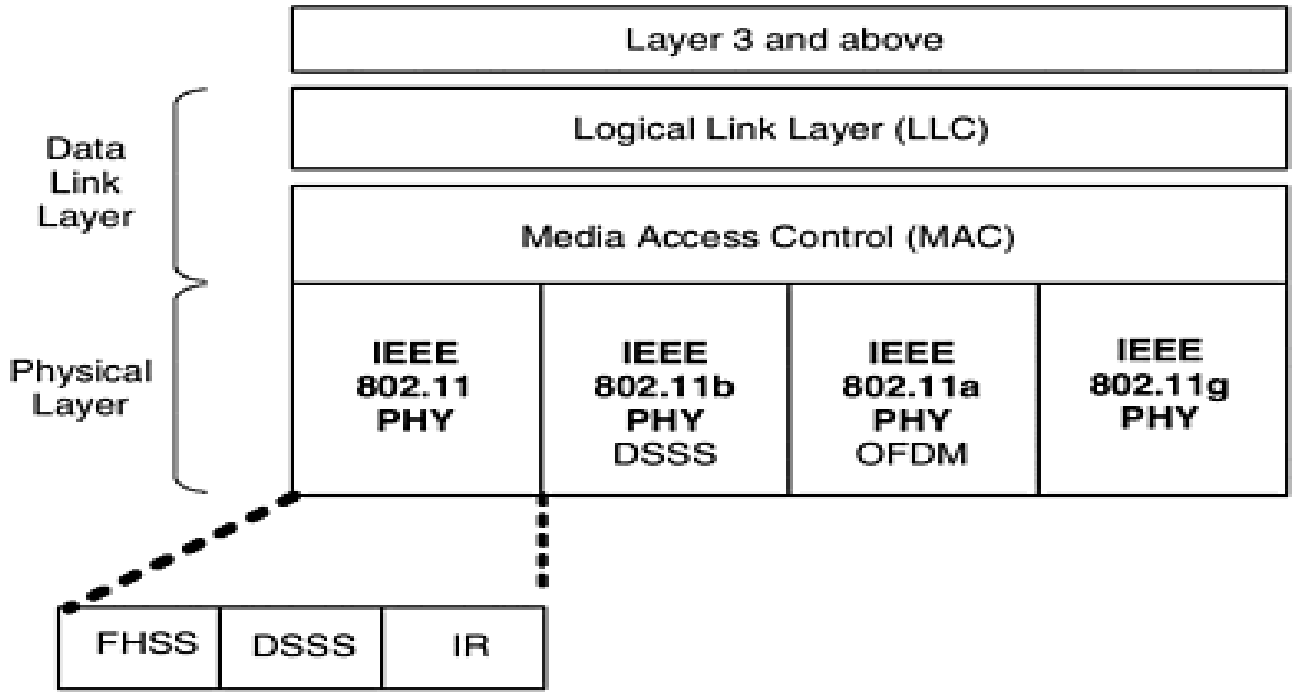
WLAN	Wi-Fi
 Le WLAN est une combinaison de réseaux informatiques et de technologies de communication sans fil. C'est une extension des réseaux filaires. Les connexions sans fil facilitent la construction du réseau et permettent aux utilisateurs de se déplacer sans interrompre la communication.	Wi-Fi est une marque commerciale de Wi-Fi Alliance. Il s'agit d'une technologie WLAN basée sur la norme IEEE 802.11.

La différence entre le Wi-Fi et le WLAN est que IEEE 802.11 est une norme WLAN tandis que le Wi-Fi est une implémentation de la norme IEEE 802.11.

Introduction aux réseaux sans fil (802.11x)

- La couche PHY a défini trois spécifications originales :

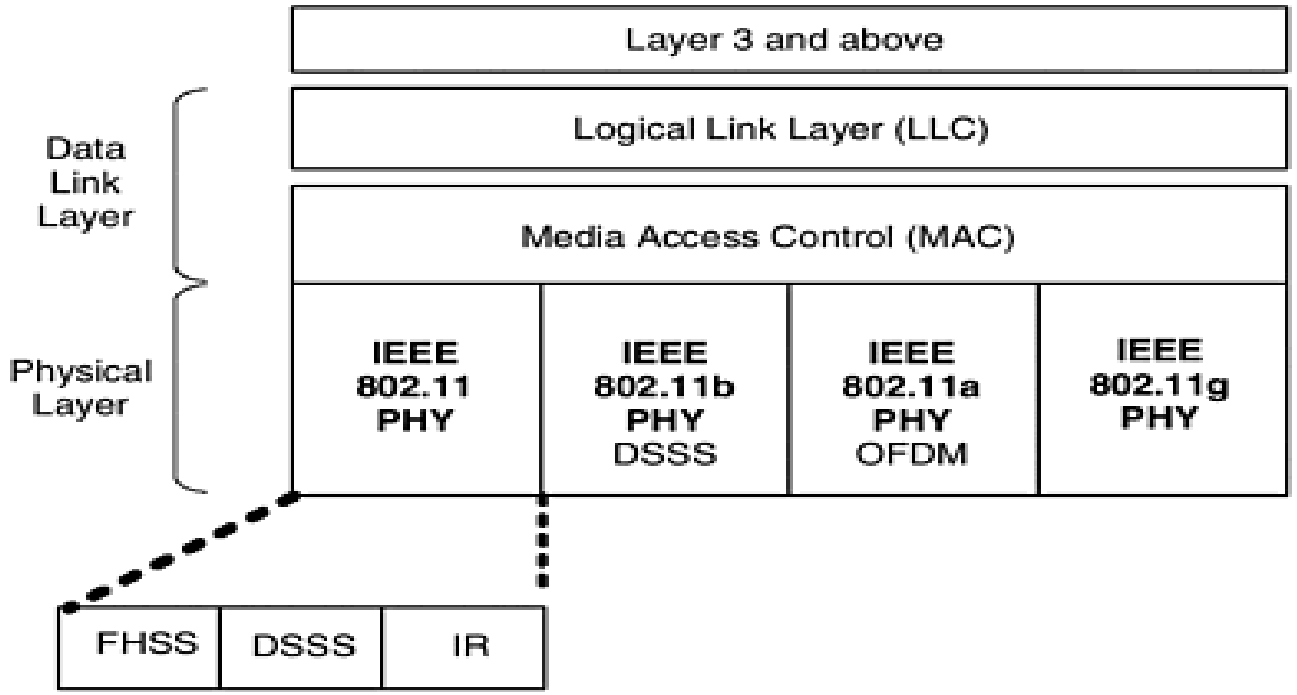
1. **La technologie infrarouge infrarouge (IR**) utilise un milieu à base de lumière. Elle a été désapprouvé et retiré de la norme 802.11-2016.



Introduction aux réseaux sans fil (802.11x)

- La couche PHY a défini trois spécifications originales :

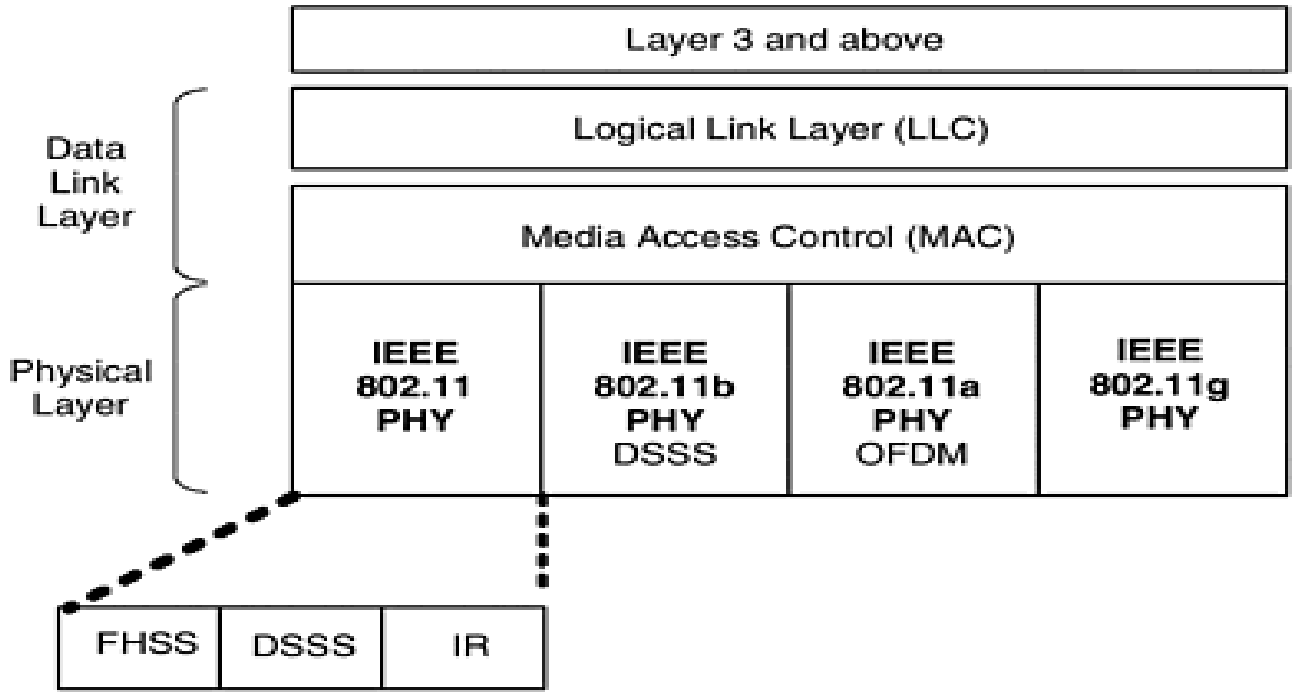
2. **Frequency-Hopping Spread-Spectrum** : (FHSS) est une technologie à spectre étalé qui a été brevetée pour la première fois pendant la Seconde Guerre mondiale. Elle a été abandonné et supprimé de la norme 802.11-2016.



Introduction aux réseaux sans fil (802.11x)

- La couche PHY a défini trois spécifications originales :

3. **Direct-Sequence Spread-Spectrum** : (DSSS) est une autre technologie à spectre étalé qui utilise des canaux fixes. Les radios DSSS 802.11 sont appelées « Clause 15 devices ».



CHAPITRE 3

ADRESSAGE IP

Systèmes numériques

Bit Order	1	1	1	1	1	1	1	1
Binary Power	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary	128	64	32	16	8	4	2	1

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08

Decimal	Binary	Hexadecimal
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
...	...	...
255	11111111	FF

Systèmes numériques

Format	Value Range	Base Value
Binary	0 — 1	2
Decimal	0 — 9	10
Hexadecimal	0 — F	16

Binaires et hexadecimal sont des systèmes de numérotation communs utilisés dans les réseaux IP.

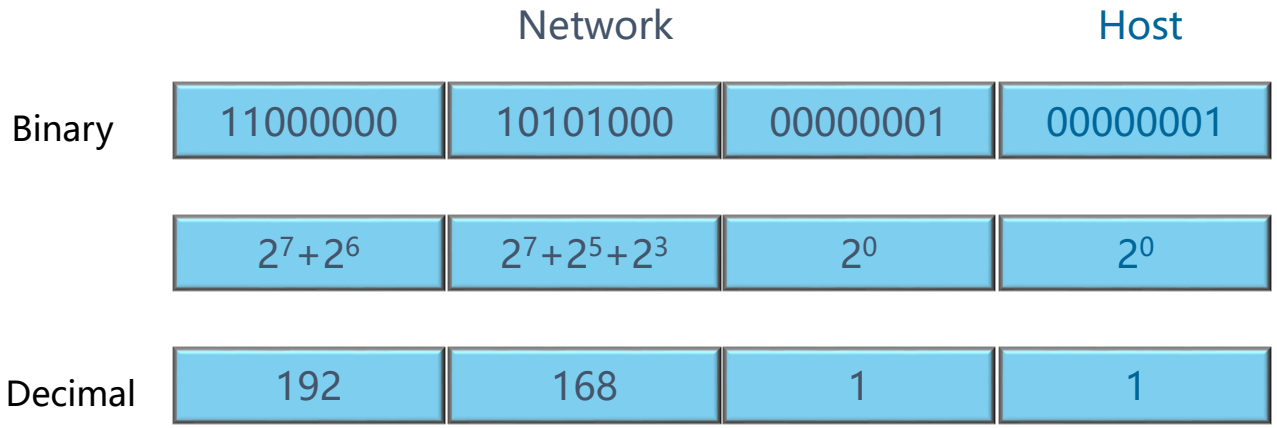
Systèmes numériques

Bit Order	1	1	1	1	1	1	1	1
Binary Power	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary	128	64	32	16	8	4	2	1

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08

Decimal	Binary	Hexadecimal
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
...	...	...
255	11111111	FF

Systèmes numériques



CHAPITRE 3

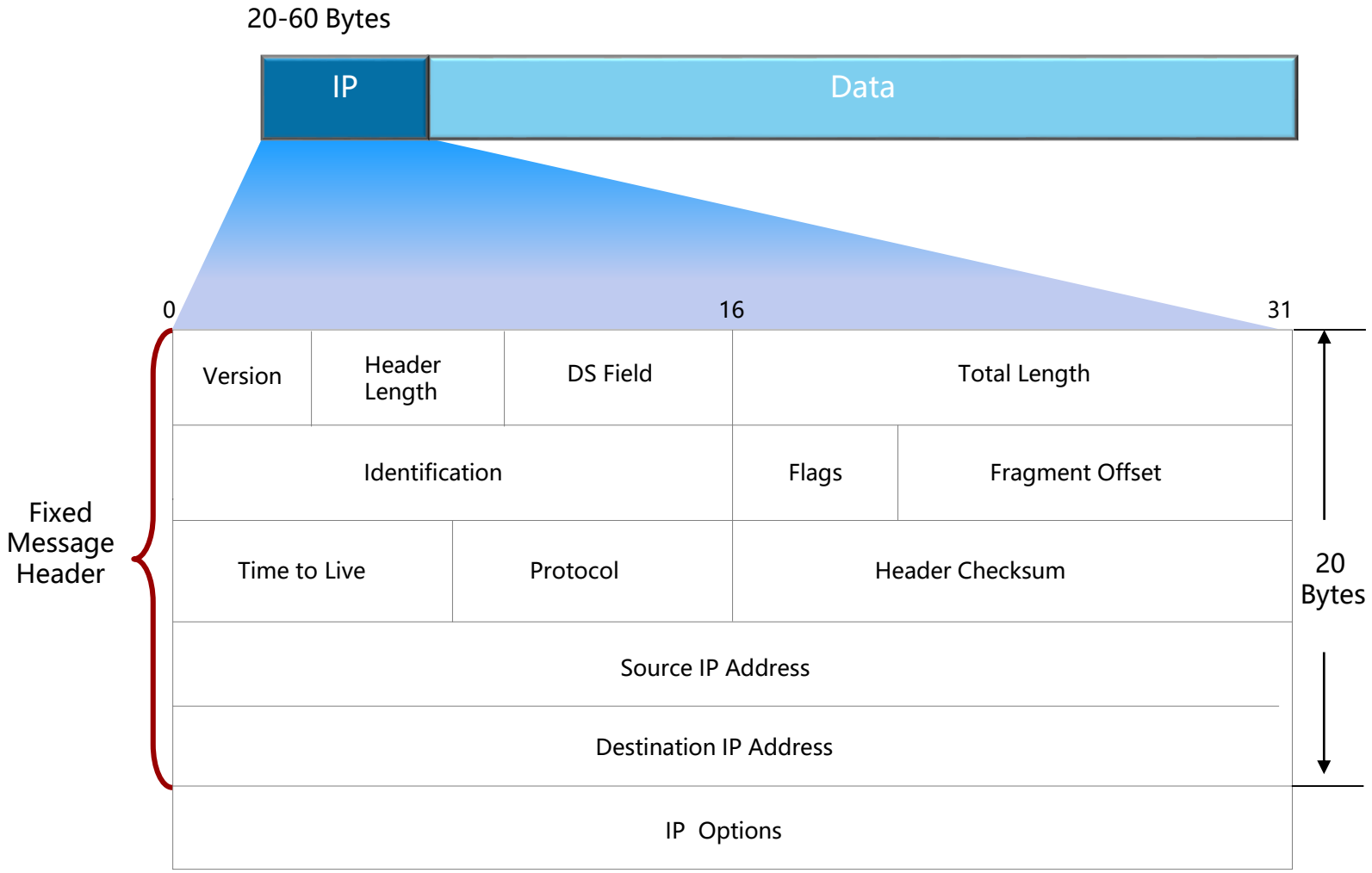
ADRESSAGE IP

1 - Systèmes numériques

2 - Adressage IPv6/IPV6

3 - Segmentation d’un réseau IPv4 /IPv6 en sous-réseau

4 - VLSM


20-60 Bytes
IP
Data
0
16
31
Version
Header Length
DS Field
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP Options
Fixed Message Header
20 Bytes

Adressage

L’adresse IP identifie les réseaux et les hôtes réseau.

Binaire est le système de numérotation de base utilisé pour l’adressage IP.

Network	Host
192.168.1	.1
11000000.10101000.00000001	.00000001

Adresses hôtes réservées

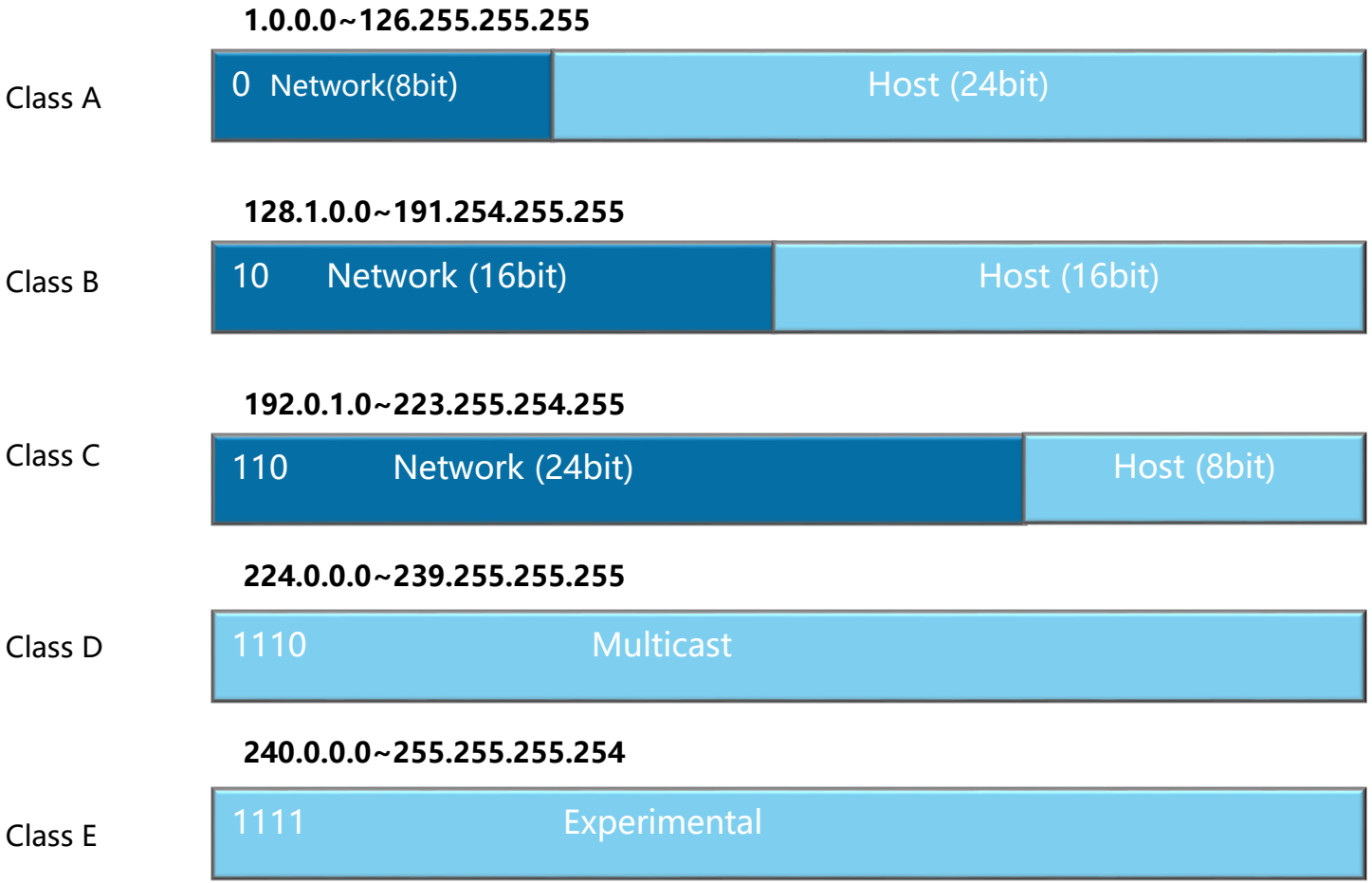
Les valeurs d’adresse supérieure et inférieure de la plupart des adresses hôtes sont réservées

Network Address

192.168.1	.0
11000000.10101000.00000001	.00000000

Broadcast Address

192.168.1	.255
11000000.10101000.00000001	11111111


1.0.0.0~126.255.255.255
Class A
0 Network(8bit)
Host (24bit)
128.1.0.0~191.254.255.255
Class B
10 Network (16bit)
Host (16bit)
192.0.1.0~223.255.254.255
Class C
110 Network (24bit)
Host (8bit)
224.0.0.0~239.255.255.255
Class D
1110 Multicast
240.0.0.0~255.255.255.254
Class E
1111 Experimental

Plage d’adresse IP

La plage d’adresses réseau IP a été divisée, et certaines adresses et plages affectées à des fonctions spéciales dans le réseau.

Private Address Ranges	
Class A	10.0.0.0~10.255.255.255
Class B	172.16.0.0~172.31.255.255
Class C	192.168.0.0~192.168.255.255

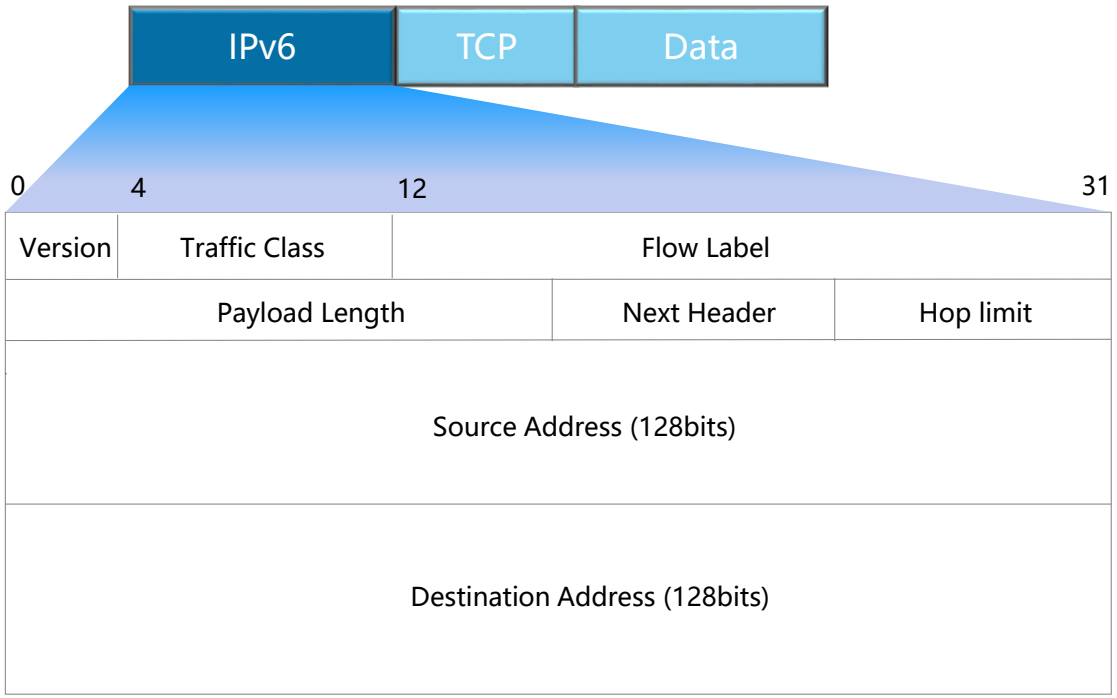
Special Addresses	
Diagnostic	127.0.0.0 ~ 127.255.255.255
Any Network	0.0.0.0
Network Broadcast	255.255.255.255

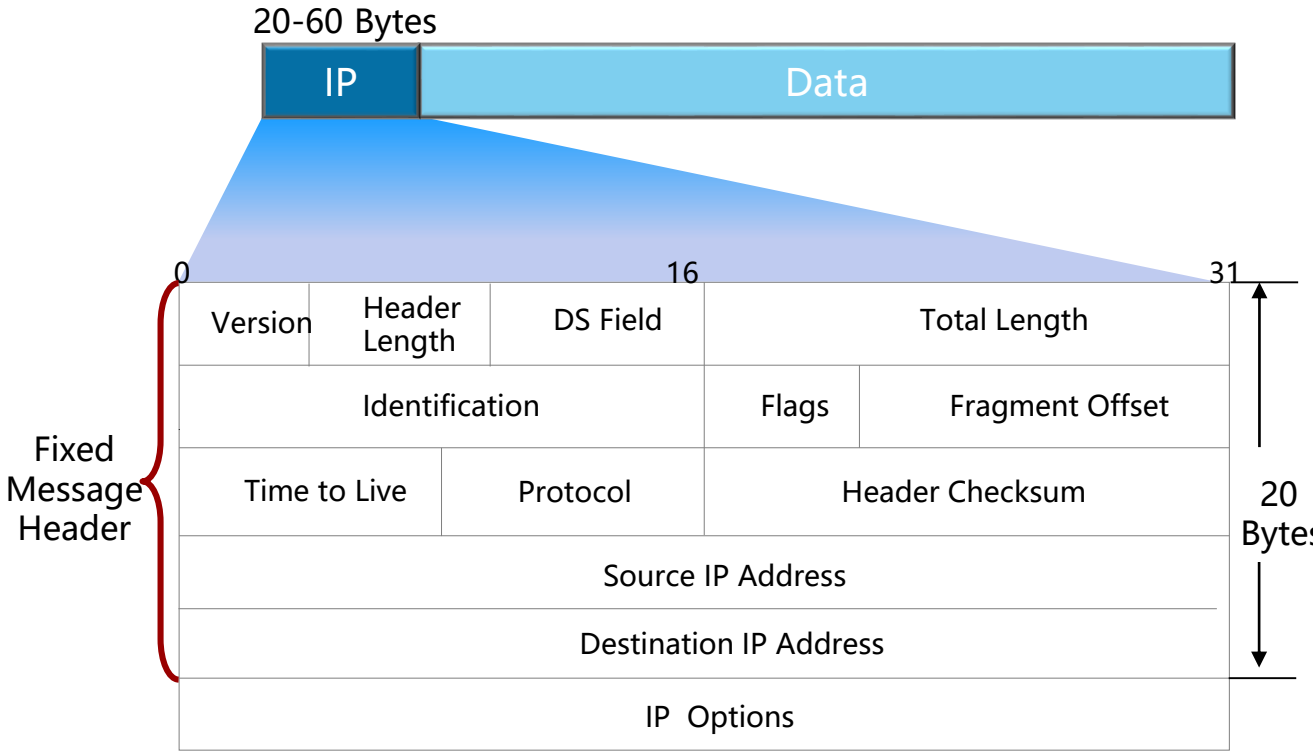
Adressage IPv6

Épuisement de l'espace d'adresse IPv4 limité.

IPv6 s'adressant mis en œuvre pour résoudre les problèmes de IPv4.

Version	Address size	Total Number of Addresses
IPv4	32 bit	4,294,967,296
IPv6	128 bit	340,282,366,920,938,463,463,374,607,431,768,211,456

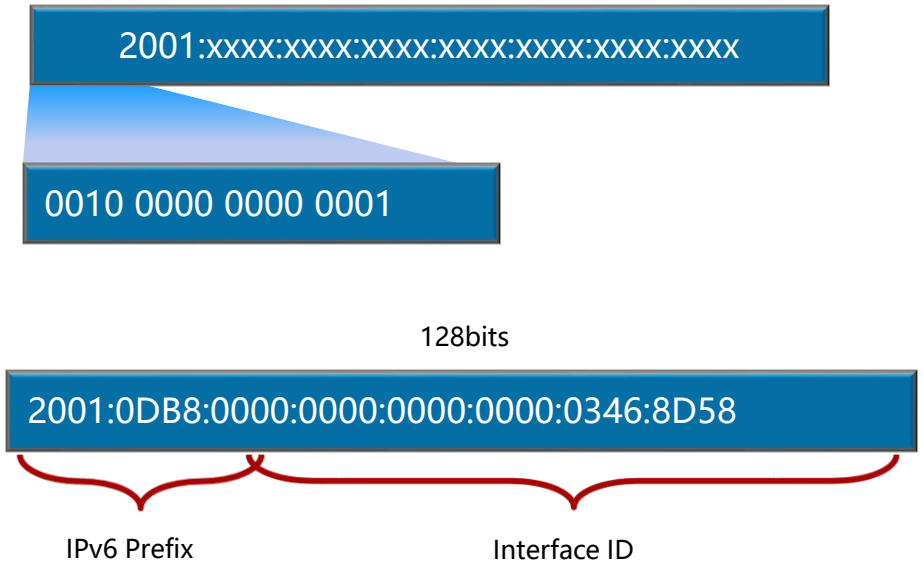

IPv6
TCP
Data
0
4
12
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop limit
Source Address (128bits)
Destination Address (128bits)


20-60 Bytes
IP
Data
0
16
31
Version
Header Length
DS Field
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP Options
Fixed Message Header
20 Bytes

Syntaxe adresse IPV6

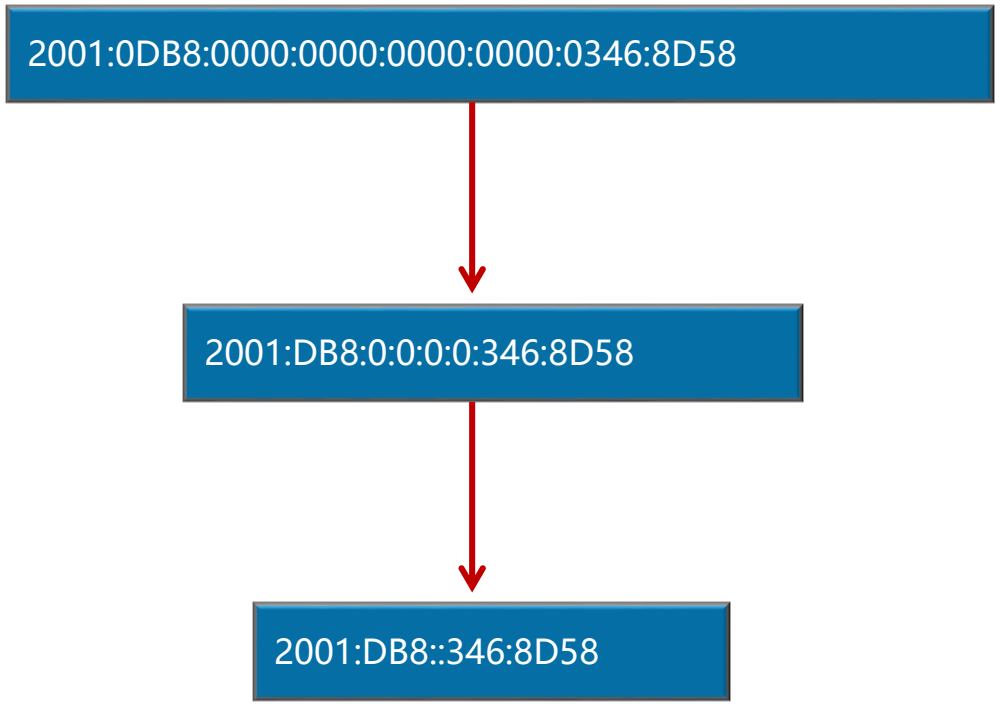
L’adresse IPv6 se compose d’un préfixe et d’un identificateur d’interface.

Les adresses sont généralement affichées en format hexadecimal.



IPV6

Les adresses peuvent être condensées en supprimant les zéros à gauche.
Le :: l'opérateur condensera encore des chaînes de valeurs nulles



Attribution des plages

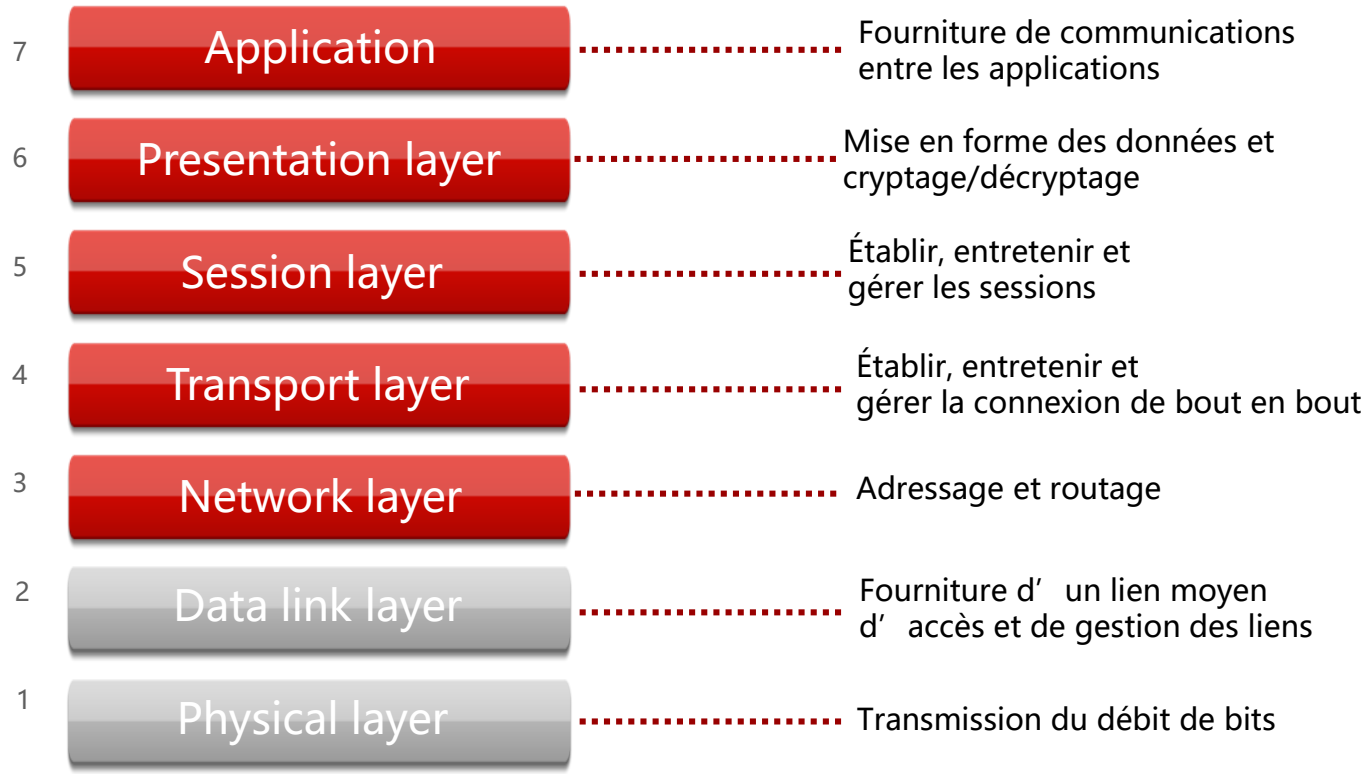
Des plages d'adresses ont été attribuées en IPv6 pour unicast et multicast, ainsi que des adresses spéciales pour le support opérationnel.

Plage d' adresses	Description
2000::/3	Current Global Unicast Range
2001:0DB8::/32	Reserved for Documentation
FE80::/10	Link Local Unicast Address Range
FF00::/8	Multicast Address Range
::/128	Unspecified Address
::1/128	Loopback Address

CHAPITRE 4

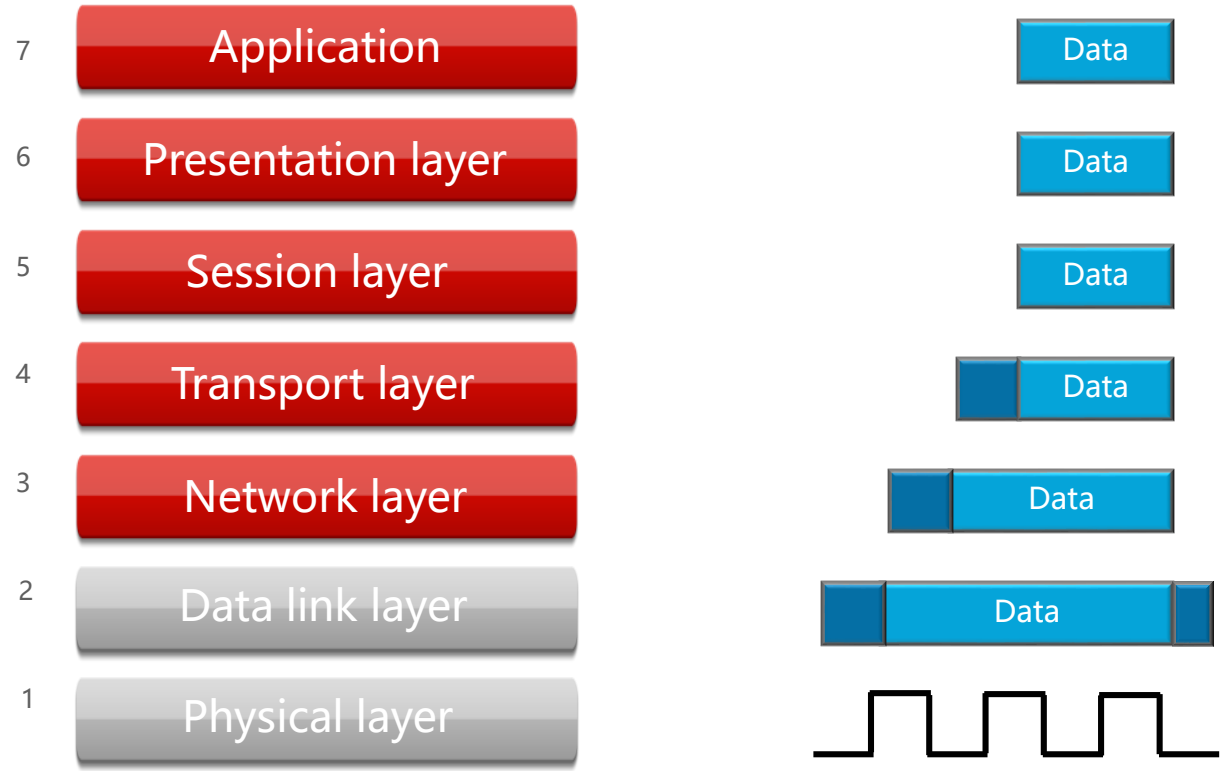
LES MODÈLES ET LES PROTOCOLES

Modèle OSI

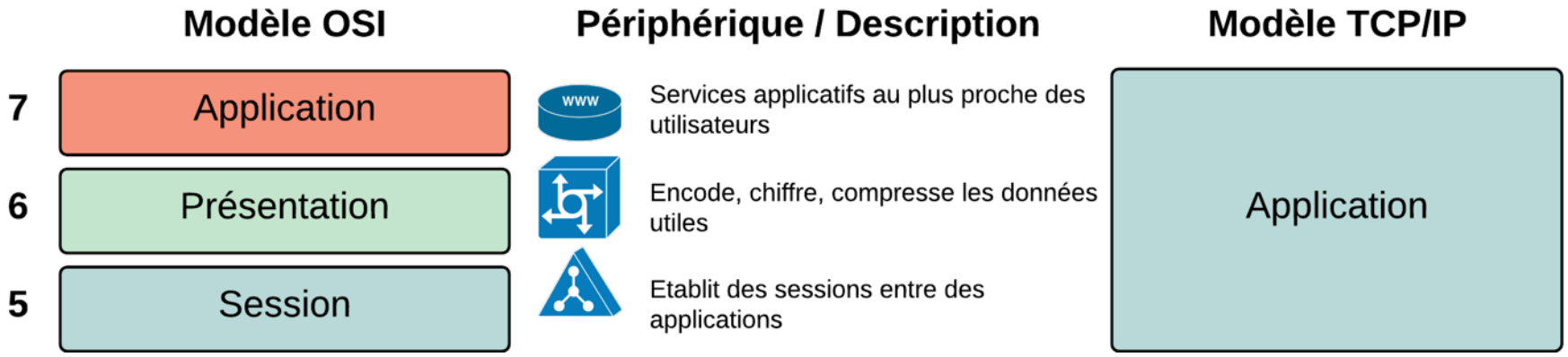

7
Application
Fourniture de communications entre les applications
6
Presentation layer
Mise en forme des données et cryptage/décryptage
5
Session layer
Établir, entretenir et gérer les sessions
4
Transport layer
Établir, entretenir et gérer la connexion de bout en bout
3
Network layer
Adressage et routage
2
Data link layer
Fourniture d' un lien moyen d' accès et de gestion des liens
1
Physical layer
Transmission du débit de bits

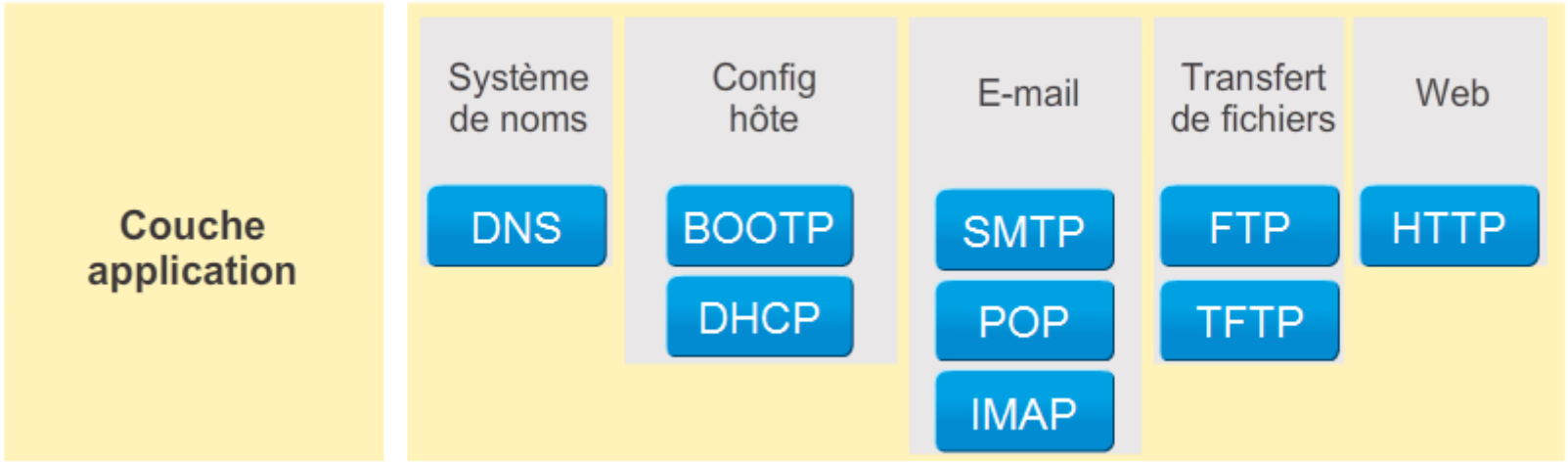
Modèle OSI

Encapsulation



Couche application





CHAPITRE 4

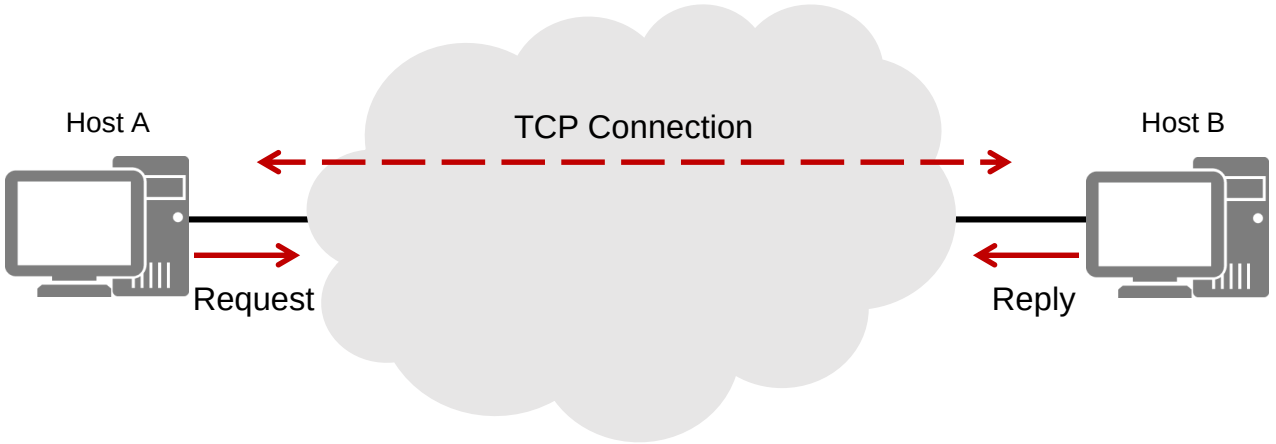
LES MODÈLES ET LES PROTOCOLES

1 - Modèles OSI et ses couches

2 – Modèles TCP/IP et ses couches

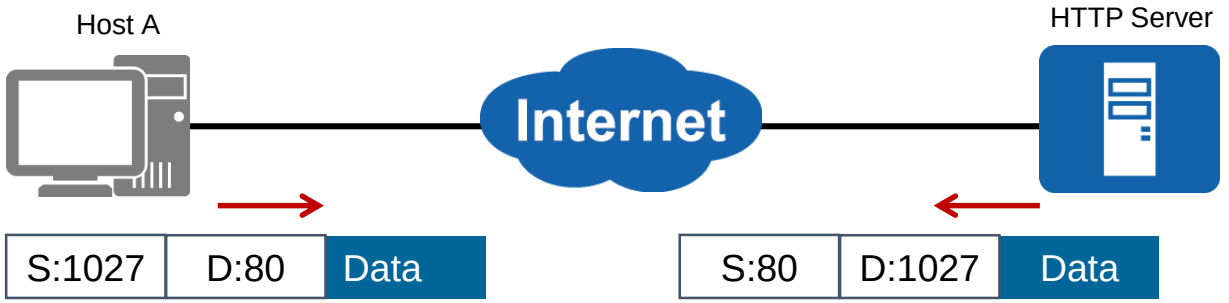
3 – Comparaison entre OSI et TCP/IP

Transmission Control Protocol



Une connexion est établie avant l'envoi des données

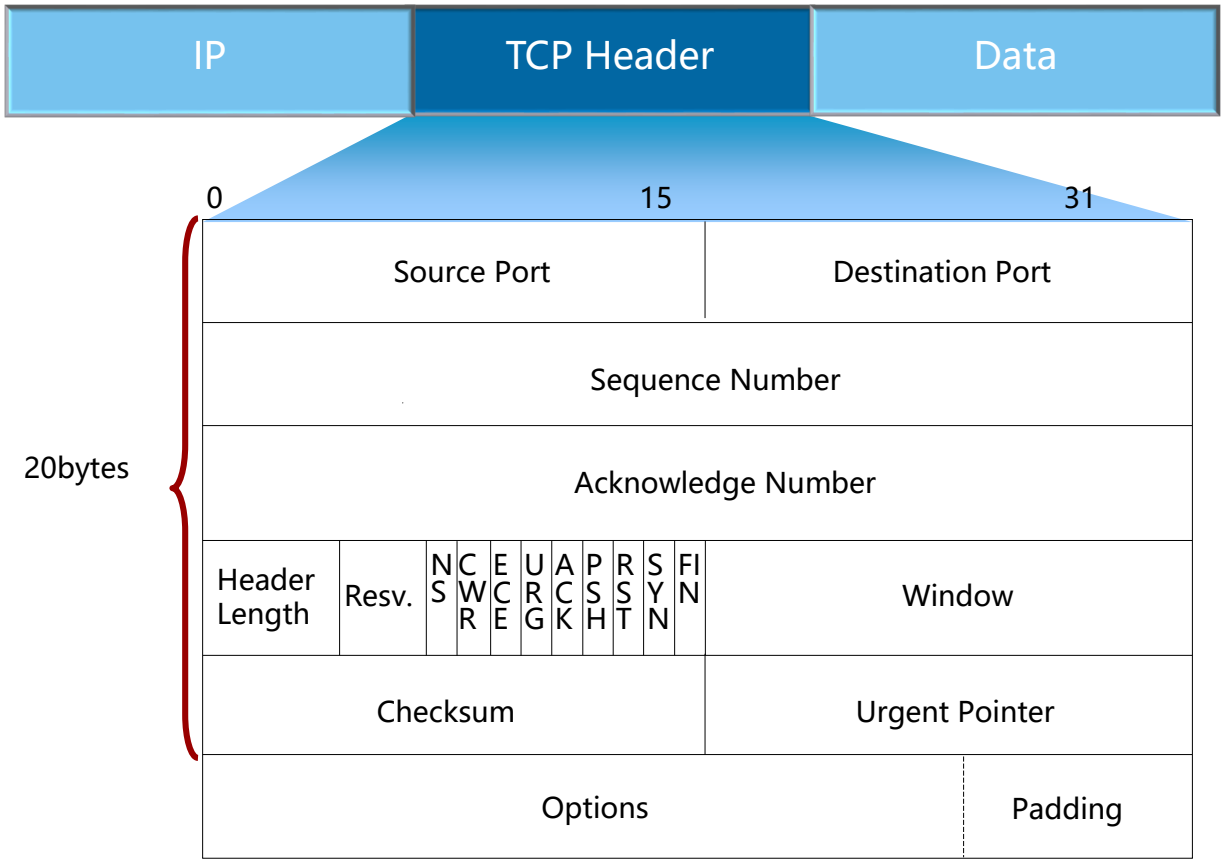
Transmission Control Protocol



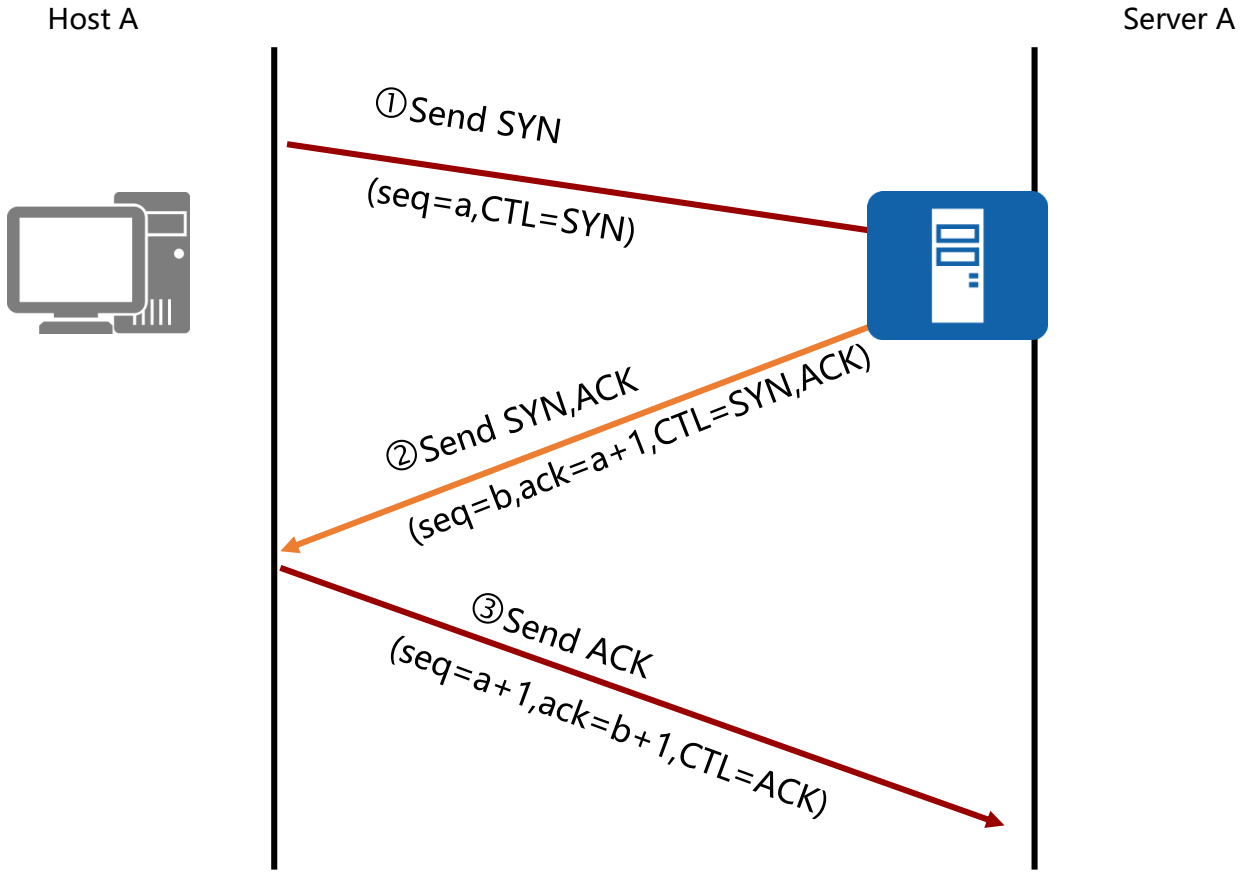
Protocol	Port
FTP	20 - 21
HTTP	80
TELNET	23
SMTP	25

Les ports représentent des services individuels.

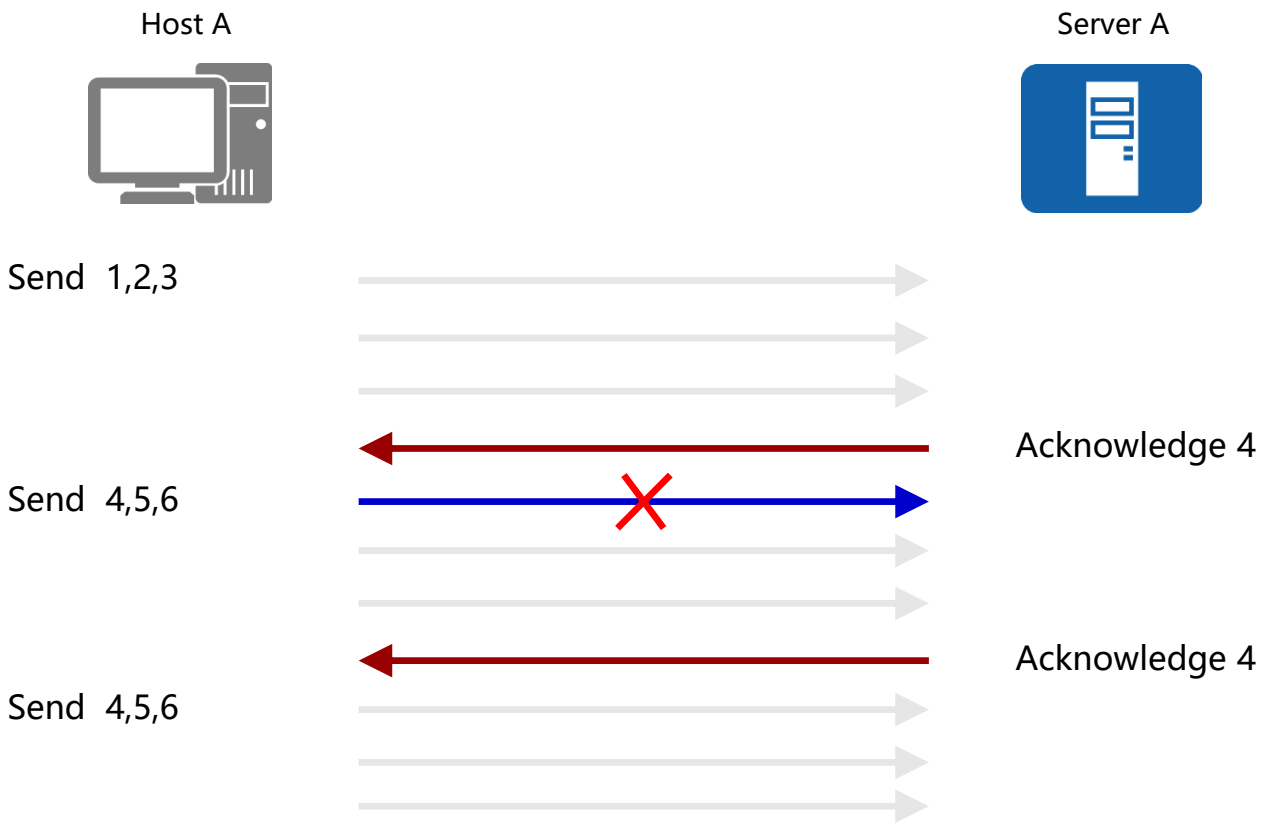
Transmission Control Protocol



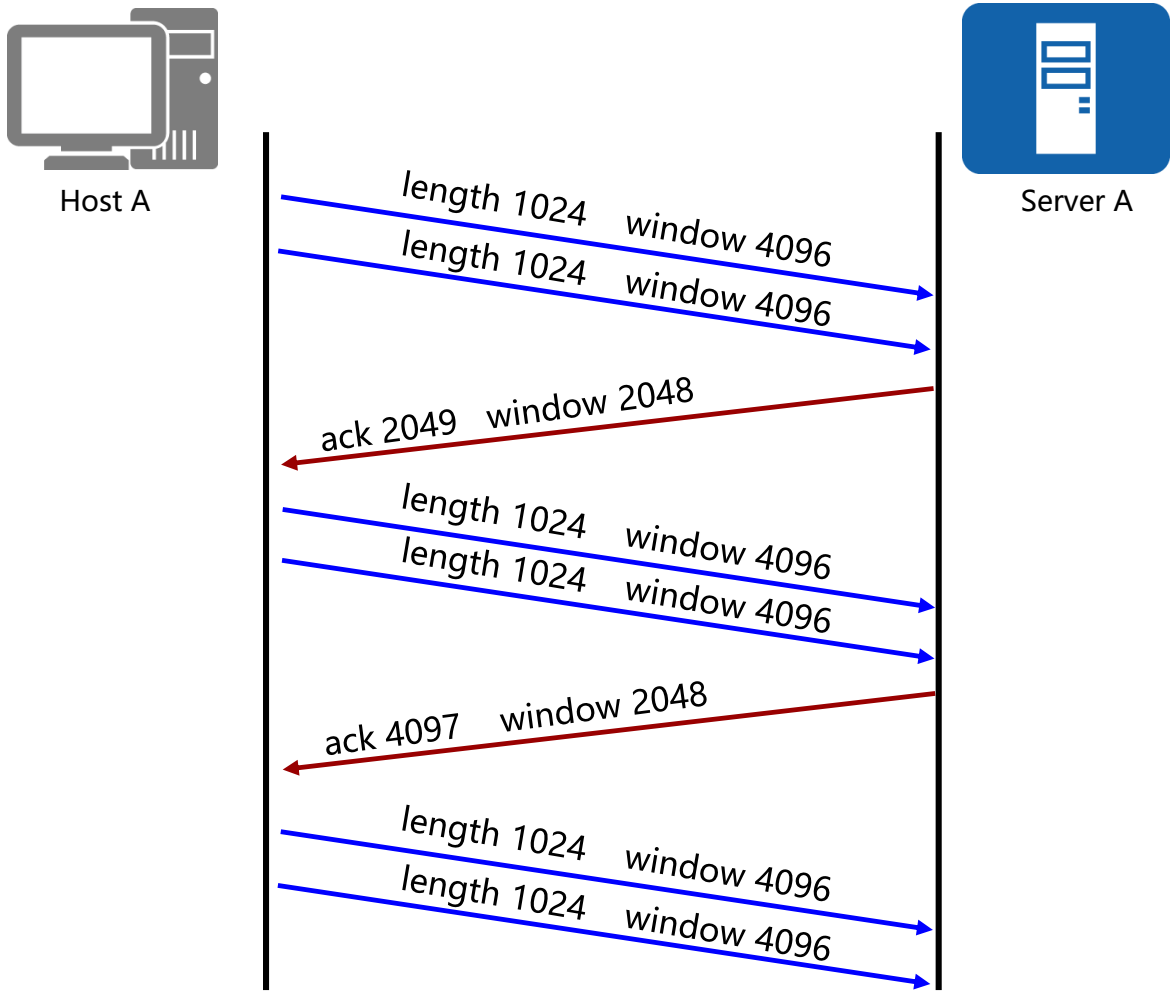
Transmission Control Protocol : établissement de session



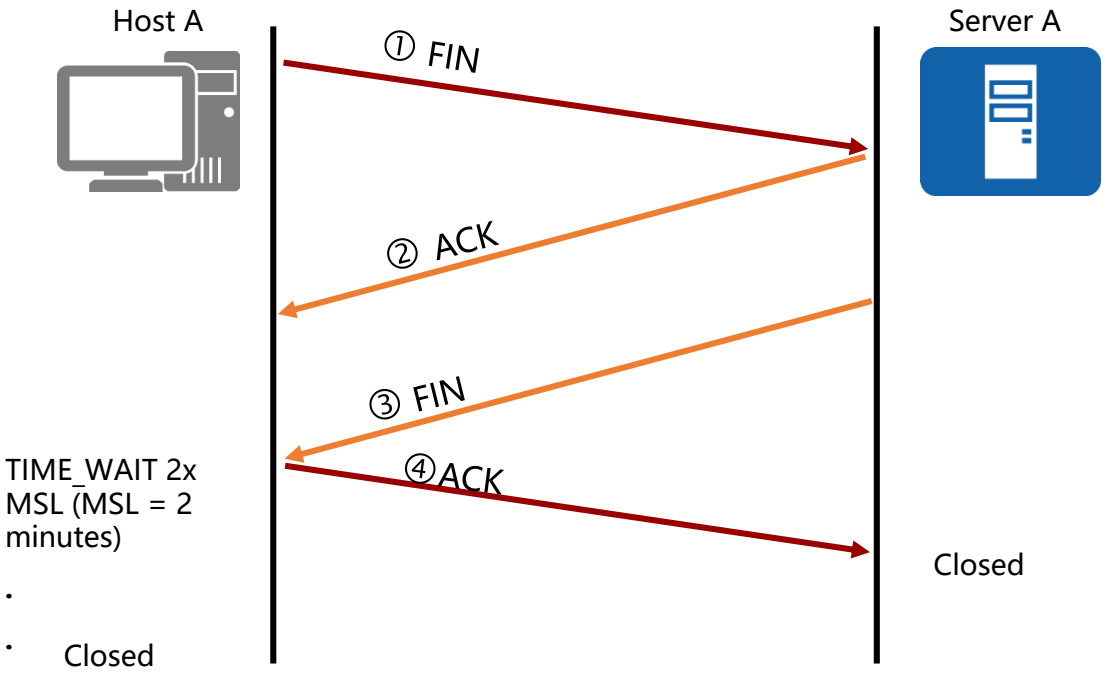
Transmission Control Protocol: processus de transmission



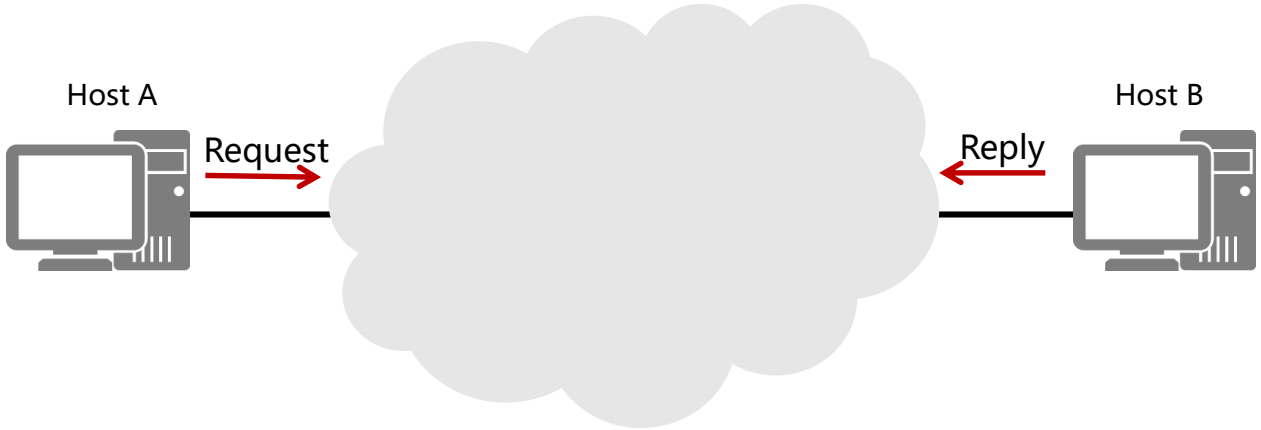
Transmission Control Protocol: Control de flux



Transmission Control Protocol: fin de session



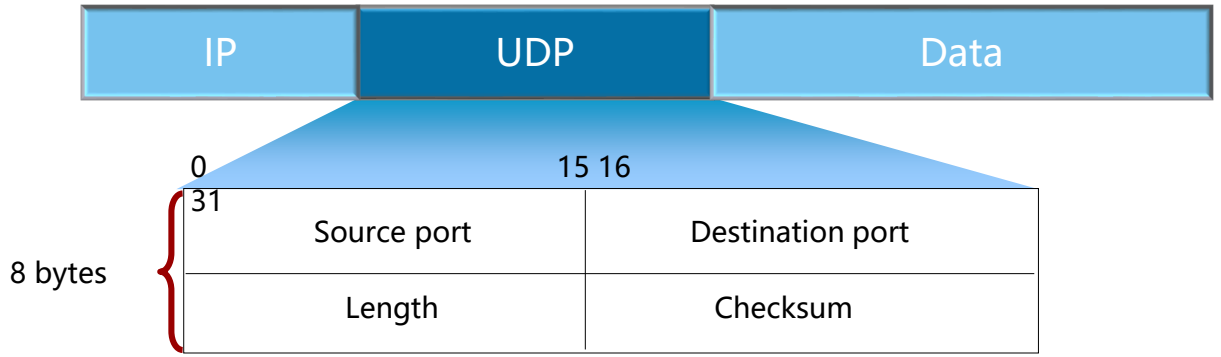
User Datagram Protocol



Les données basées sur UDP sont envoyées sans établir de connexion

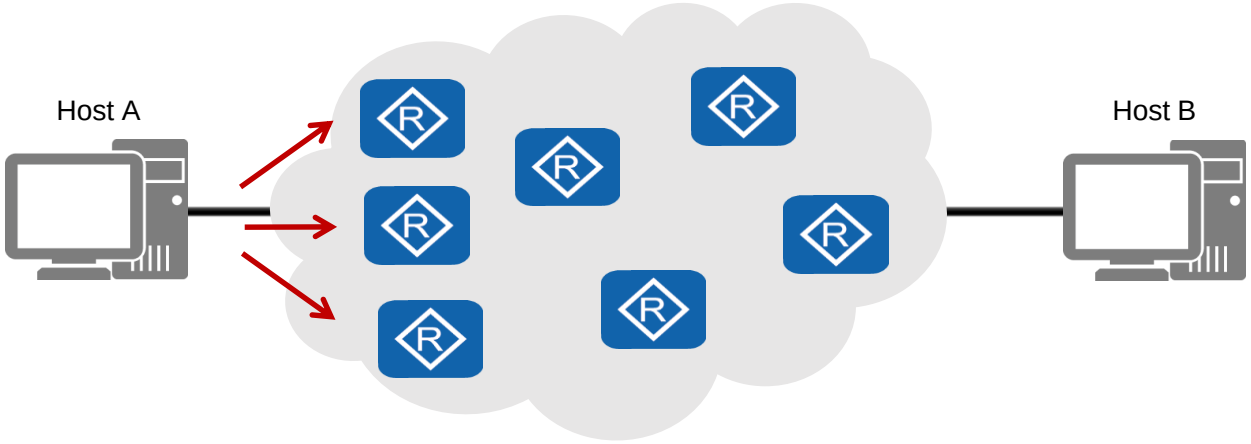
User Datagram Protocol

- UDP réalise un minimum de frais généraux pour chaque datagram.
- La livraison de Datagram n'est pas garantie avec UDP



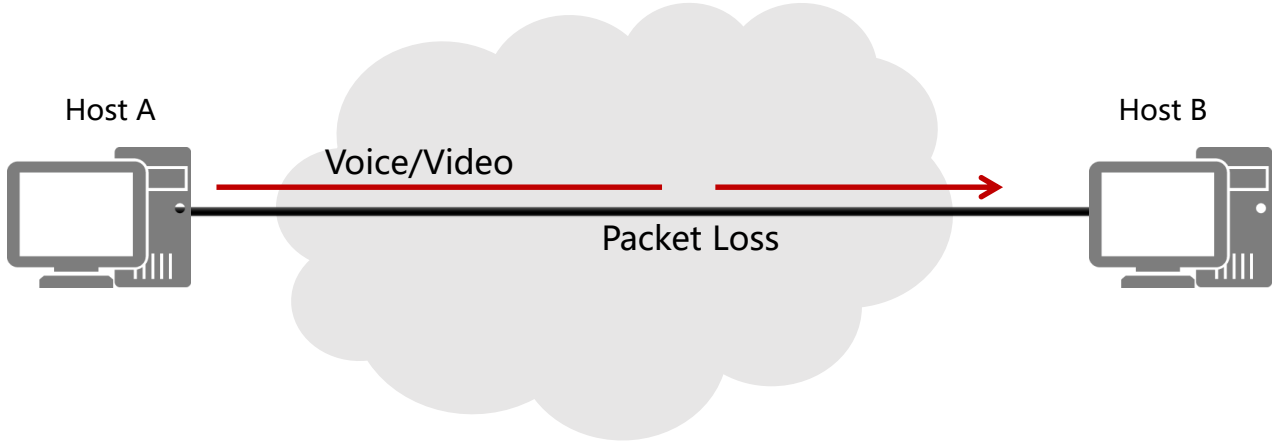
User Datagram Protocol

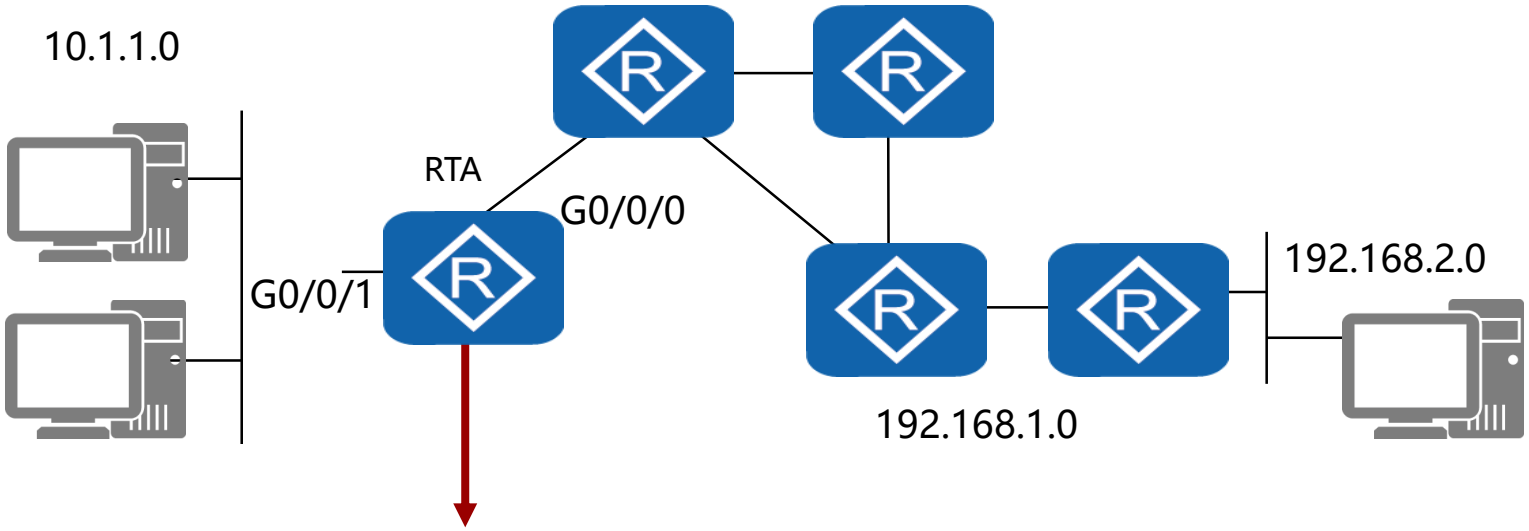
UDP sensible à la possibilité d'une duplication de datagram ou d'une livraison non ordonnée de datagrams



User Datagram Protocol

- Il n’y a pas de ACKs, donc les paquets perdus ne sont pas retransmis, ce qui est toutefois bénéfique pour retarder les données sensibles





Source de la route	Le réseau cible	Interface
Direct	10.1.1.0	G0/0/1
Static	192.168.1.0	G0/0/0
OSPF	192.168.2.0	G0/0/0

CHAPITRE 4

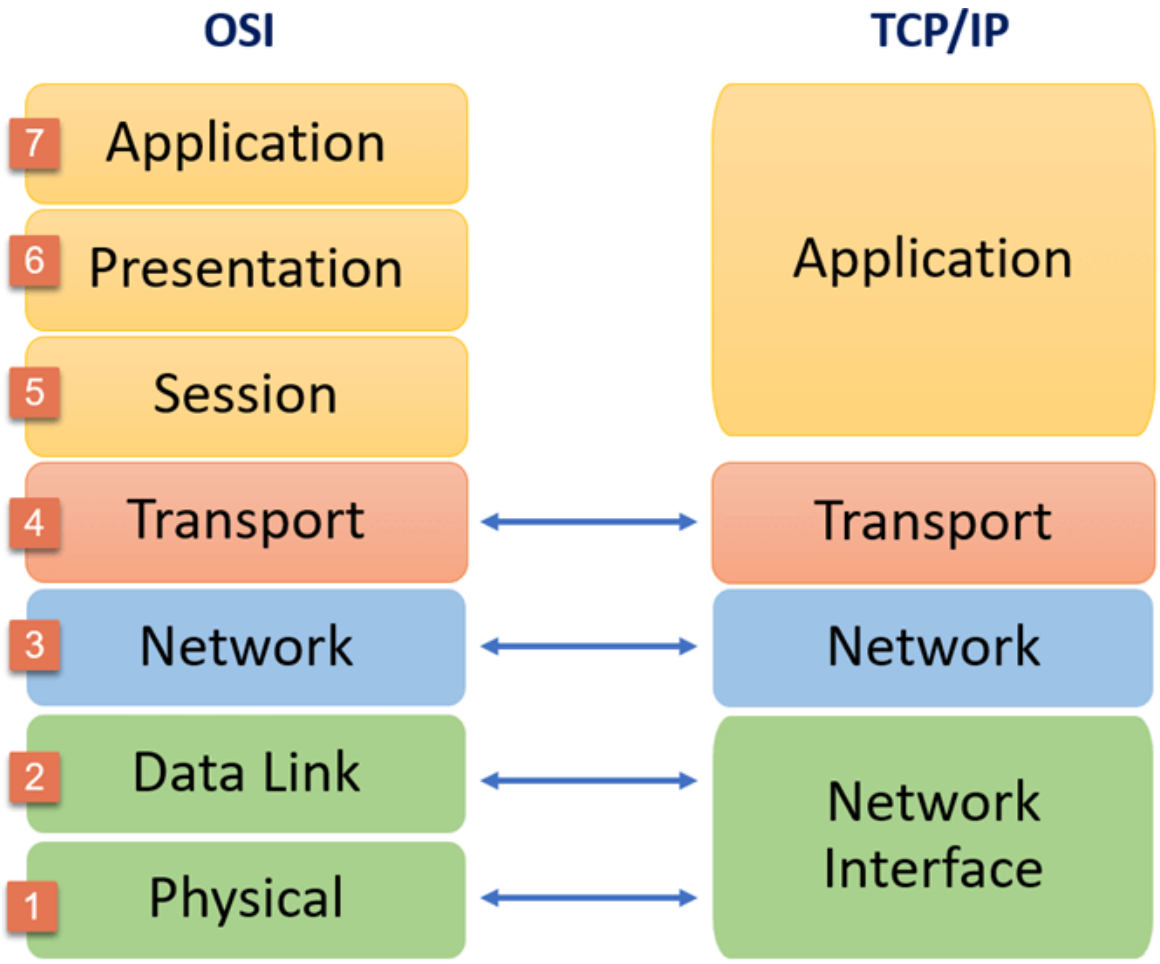
LES MODÈLES ET LES PROTOCOLES

1 - Modèles OSI et ses couches

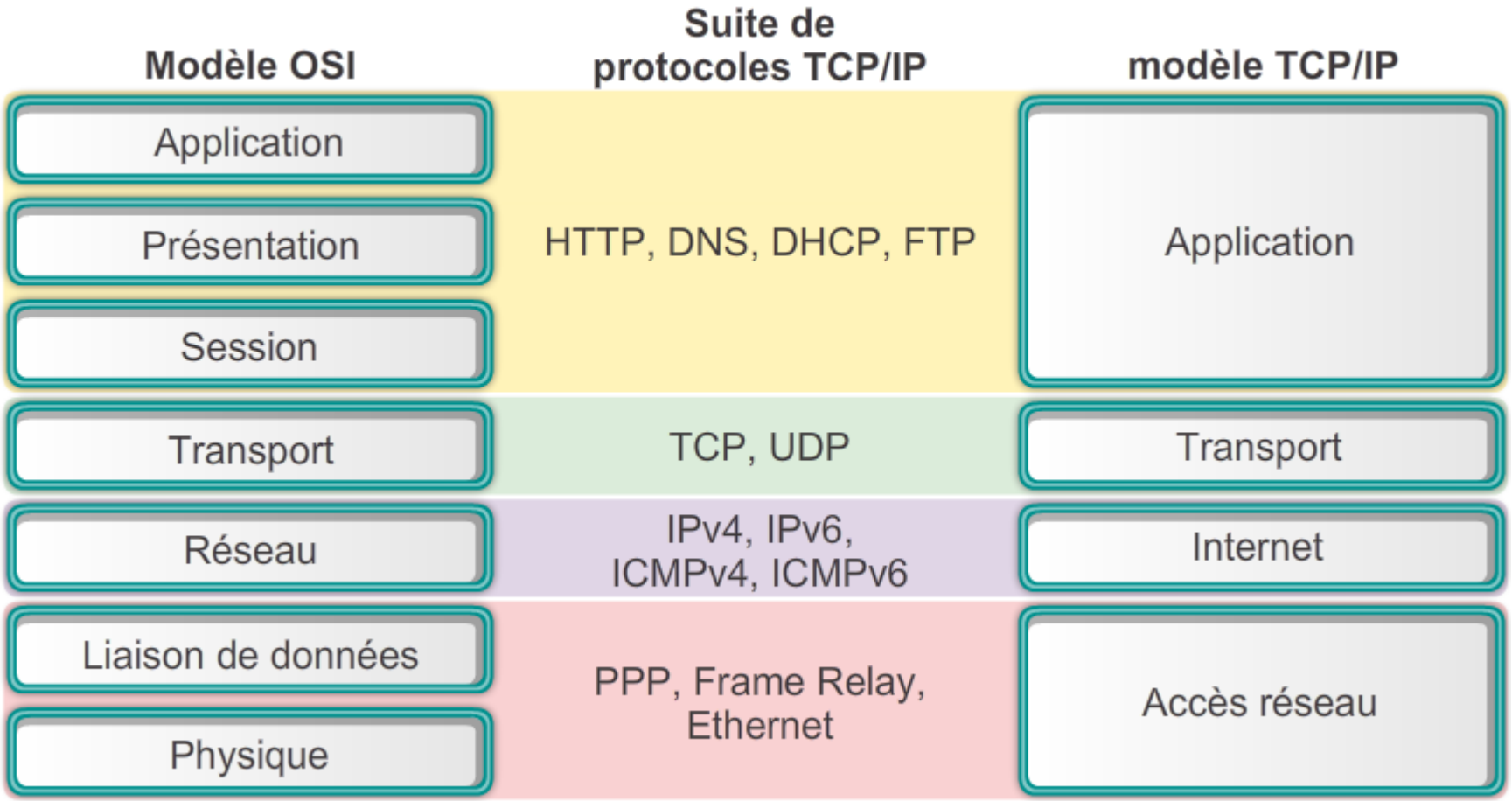
2 – Modèles TCP/IP et ses couches

3 – Comparaison entre OSI et TCP/IP

Modèle OSI vs modèle TCP/IP



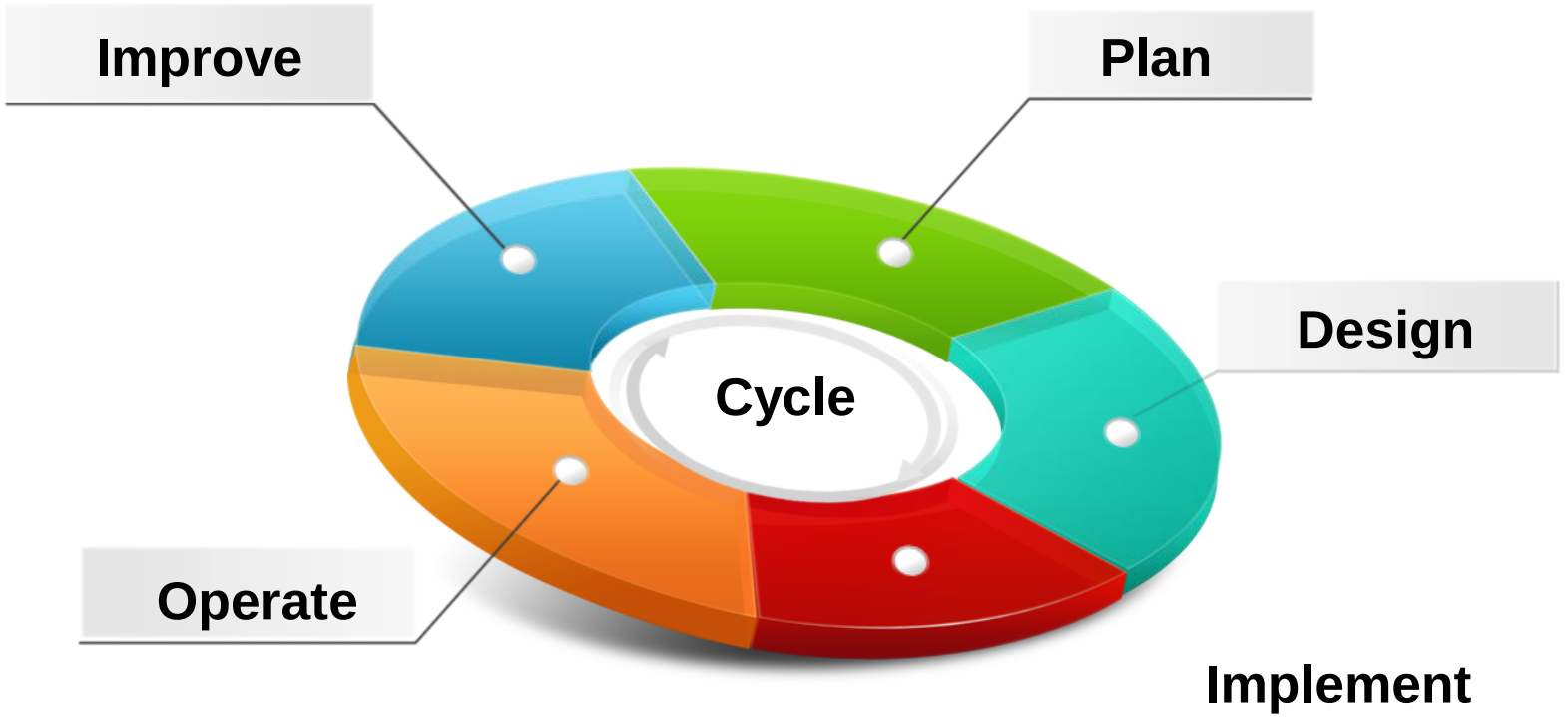
Comparaison entre OSI et TCP/IP



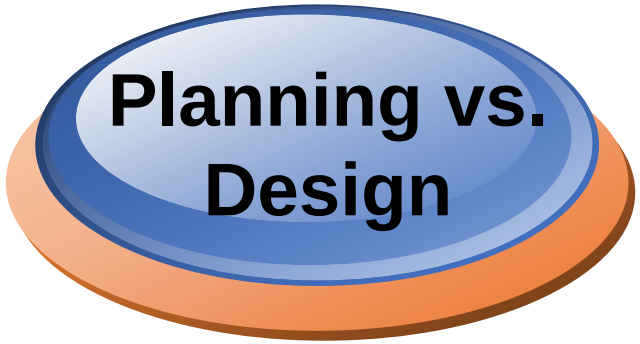
CHAPITRE 5

METTRE EN PLACE UN RÉSEAU LAN

Conception d’un réseau



Conception d’un réseau

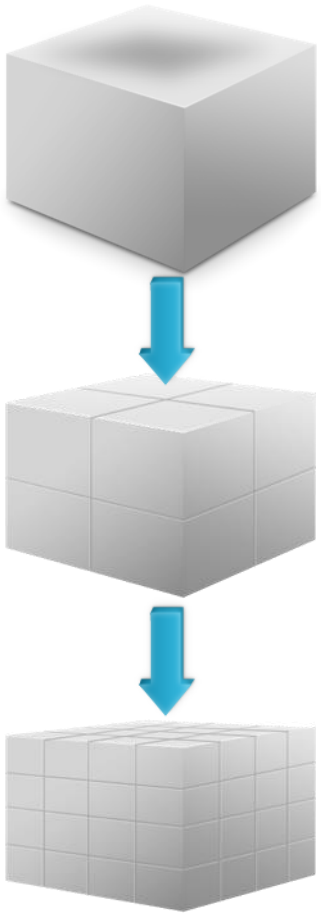


Planning:

Se concentre sur la recherche des exigences et les conditions extérieures de mise en œuvre.

Design:

Se concentre sur la mise en œuvre technologique. Répond aux exigences du réseau confirmées lors de la planification à l’aide de diverses méthodes techniques.



Conception de réseau physique:

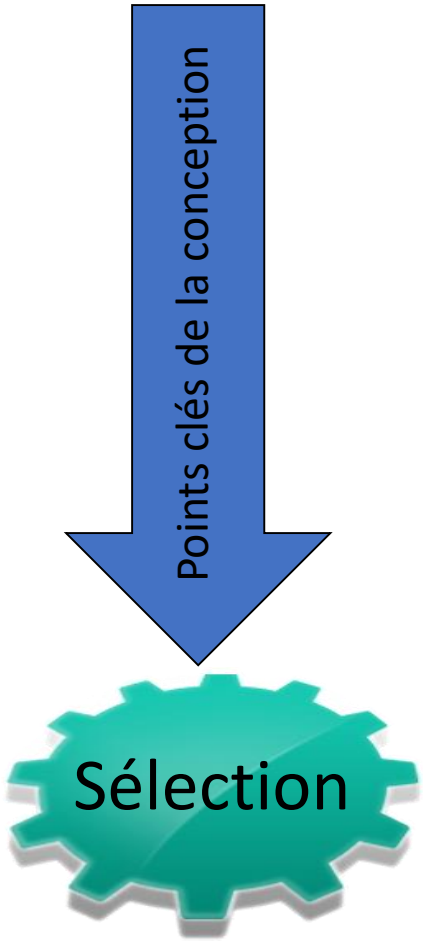
- Conception de la topologie physique
- Sélection du périphérique matériel
- Sélection de la liaison d'interconnexion
- Configurations de base des appareils

Conception logique du réseau:

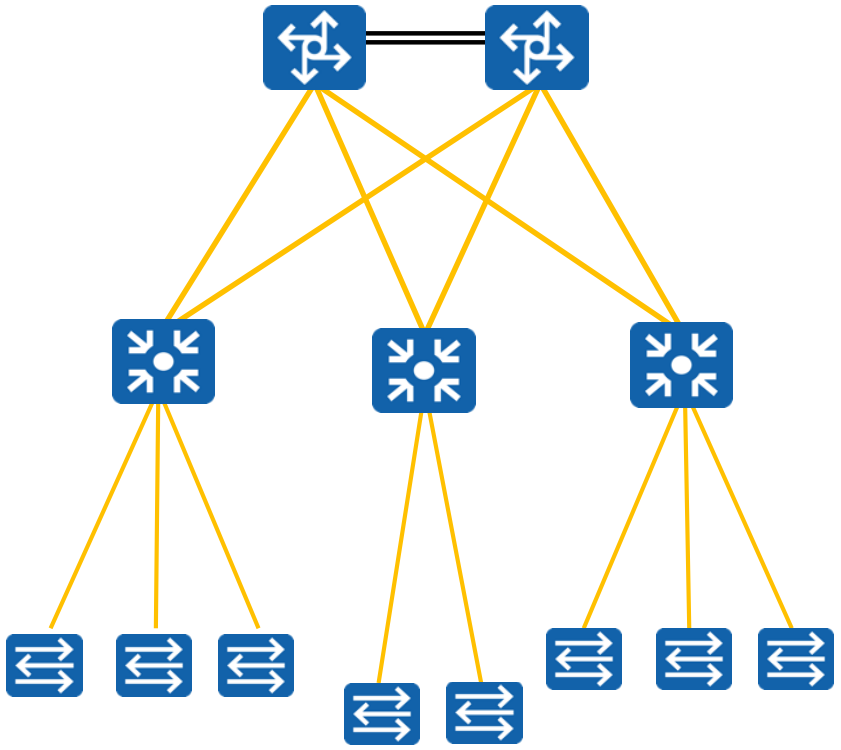
- Conception LAN
- Conception WAN
- Conception de la structure de routage
- Conception de sortie de réseau
- Conception haute disponibilité

Conception du sous-système reseau:

- Conception VPN
- Conception WLAN
- Conception de centres de données
- Conception de la gestion de réseau



Réseau hiérarchique



Core layer

Aggregation layer

Access layer

CHAPITRE 5

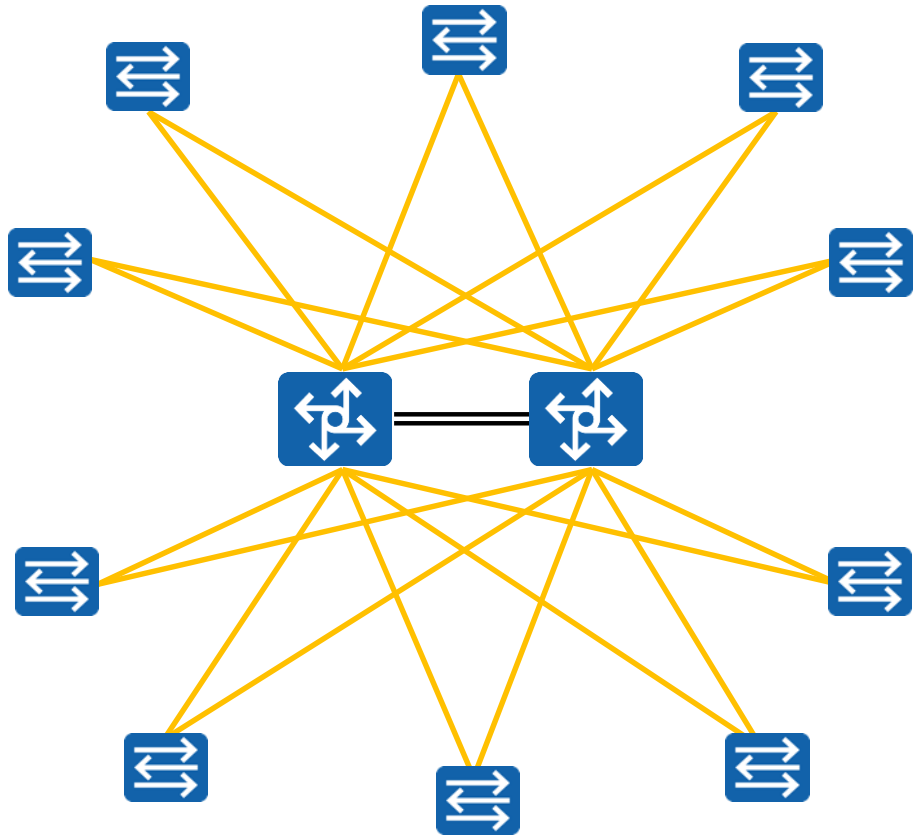
METTRE EN PLACE UN RÉSEAU LAN

1 - Conception d’un réseau LAN

2 - Optimisation d’un réseau LAN

3 - Dépannage d’un réseau LAN

Architecture à deux couches



Access layer

Core layer

Access layer

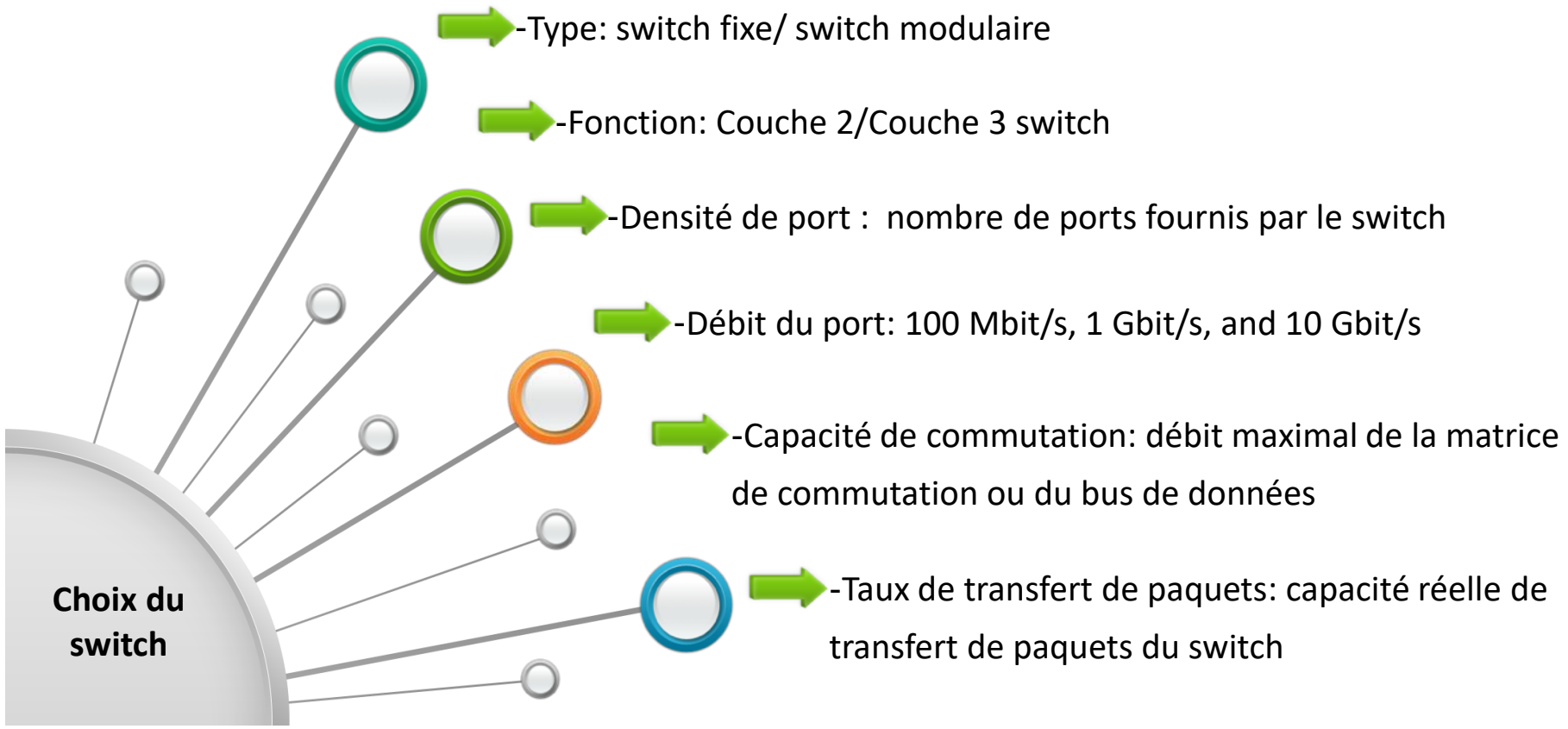
Classification des équipements réseaux

Layer 2 switch

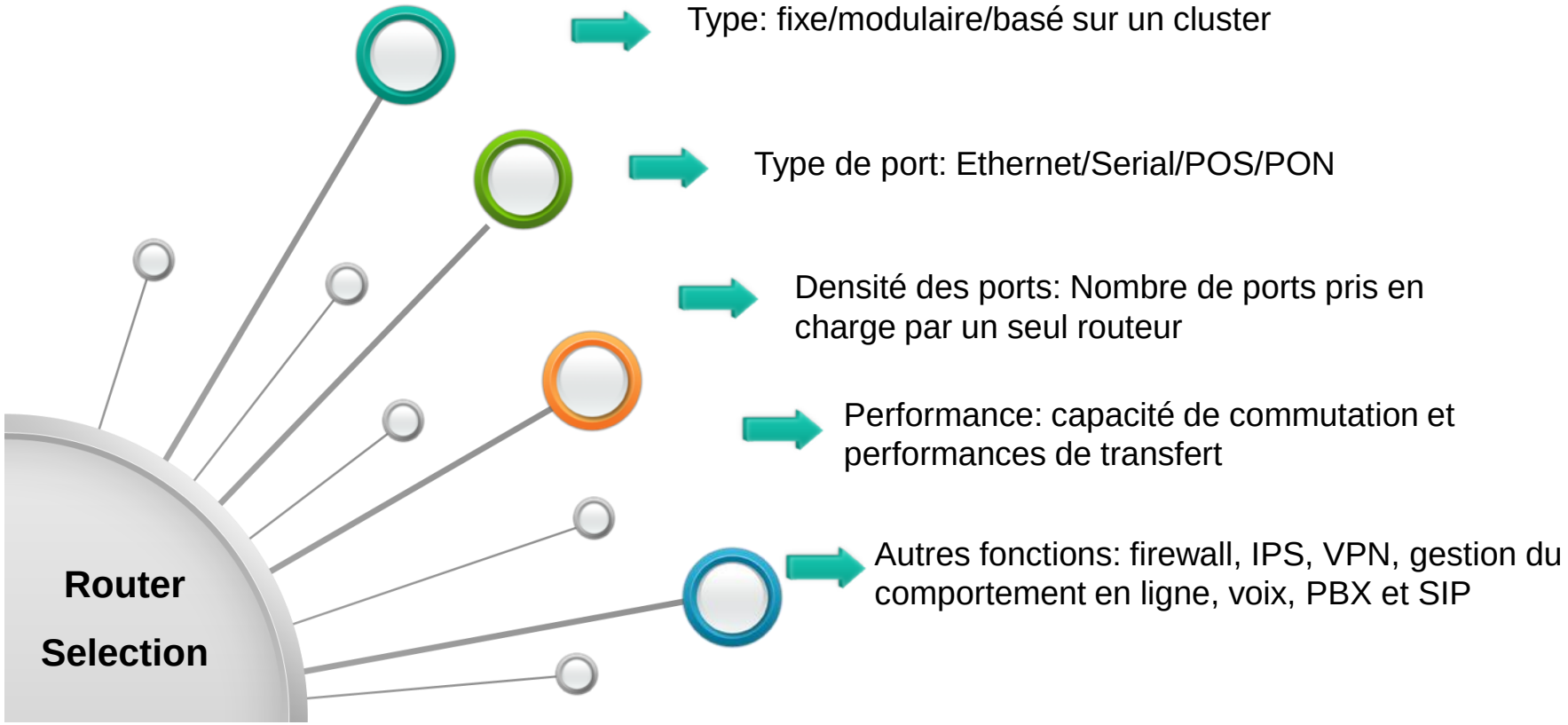
Layer 3 switch

Router

Classification des équipements réseaux



Classification des équipements réseaux



Conception de la sécurité réseau de couche 2

Type d'attaque de couche 2	Mécanisme deprotection de couche 2
Attaques DoS sur les appareils	Défense du processeur de commutation
Surcharge de trafic	Suppression du trafic et contrôle des tempêtes
Usurpation d'adresse MAC	Sécurité de port
Attaque DHCP	DHCP snooping
Attaque ARP	Limite de débit, solidification, isolation et DAI
Usurpation d'adresse IP	IPSG

CHAPITRE 5

METTRE EN PLACE UN RÉSEAU LAN

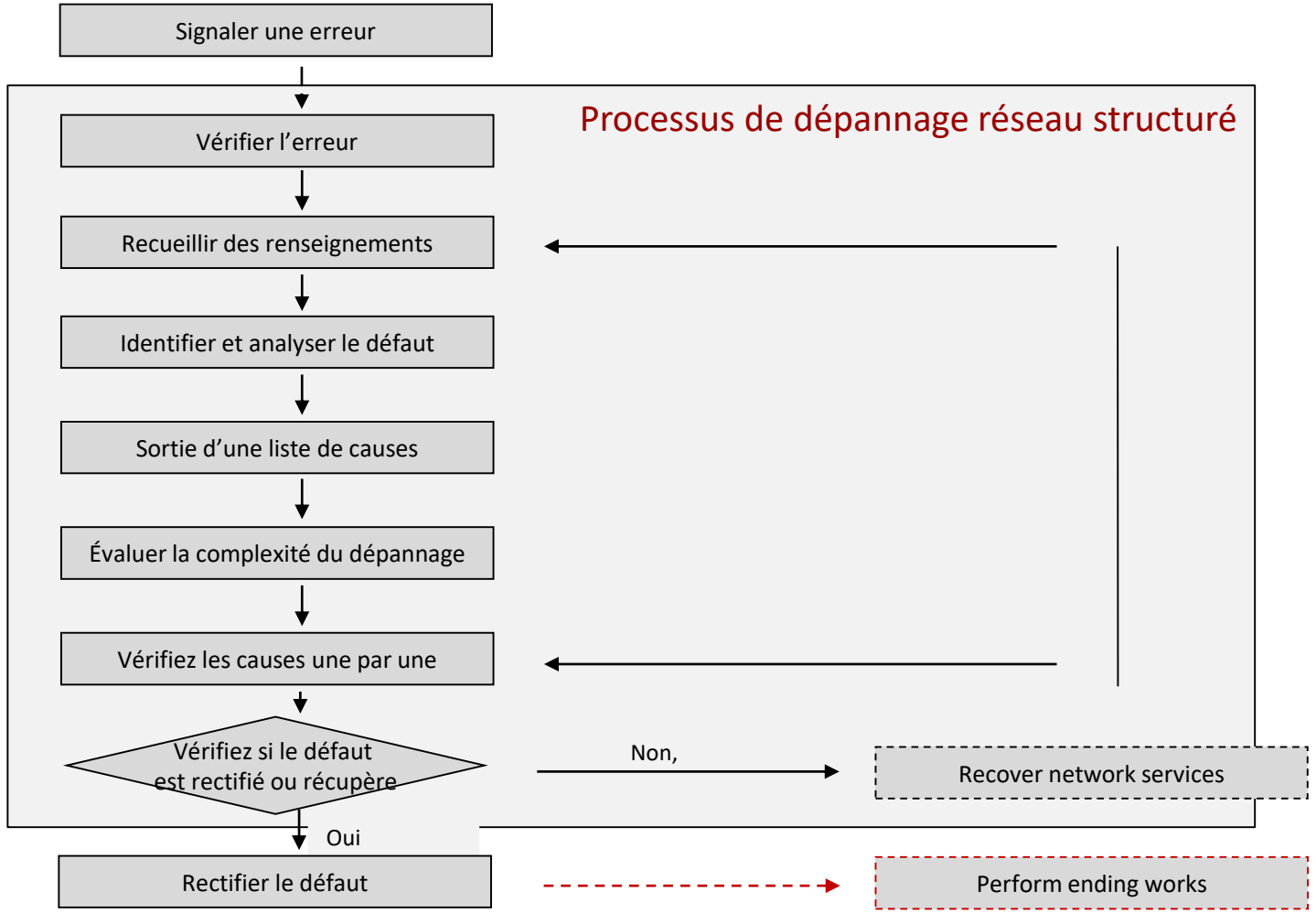
1 - Conception d’un réseau LAN

2 - Optimisation d’un réseau LAN

3 - Dépannage d’un réseau LAN

Dépannage d'un réseau LAN

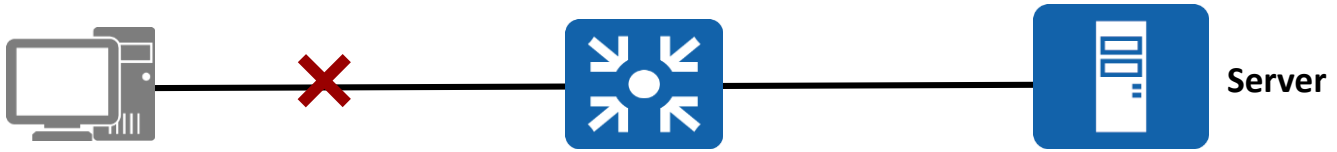
Processus de dépannage réseau structuré



Dépannage d’un réseau LAN

Raison de la vérification de l’erreur

- La description de l’erreur d’un utilisateur peut ne pas être claire et le point de défaillance signalé par un utilisateur peut être erroné.
- Par conséquent, un ingénieur expérimenté est nécessaire pour vérifier le défaut.



Dépannage d’un réseau LAN

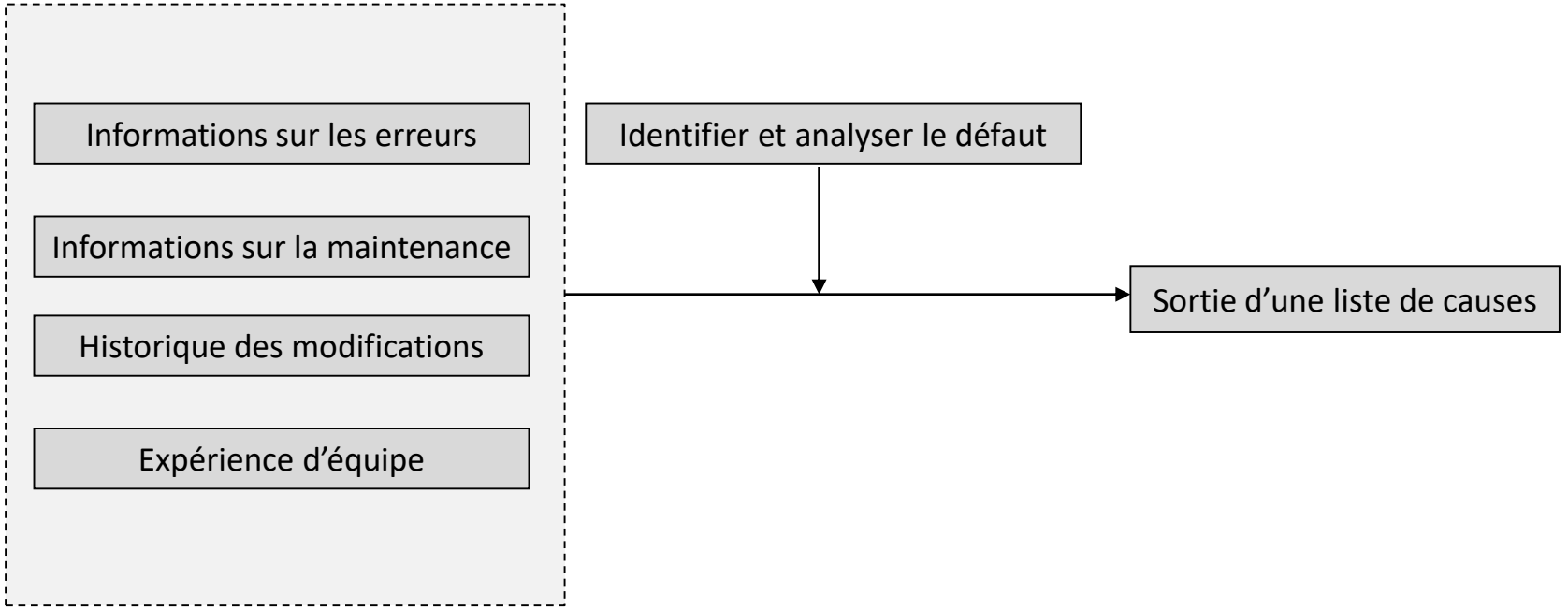
Vérification de l’erreur

- Quatre éléments clés dans la vérification des défauts :
  1. Entité
  2. Symptôme
  3. Heure
  4. Emplacement

- Fournissez une description précise du symptôme.
- Déterminez si la faute relève de votre responsabilité.

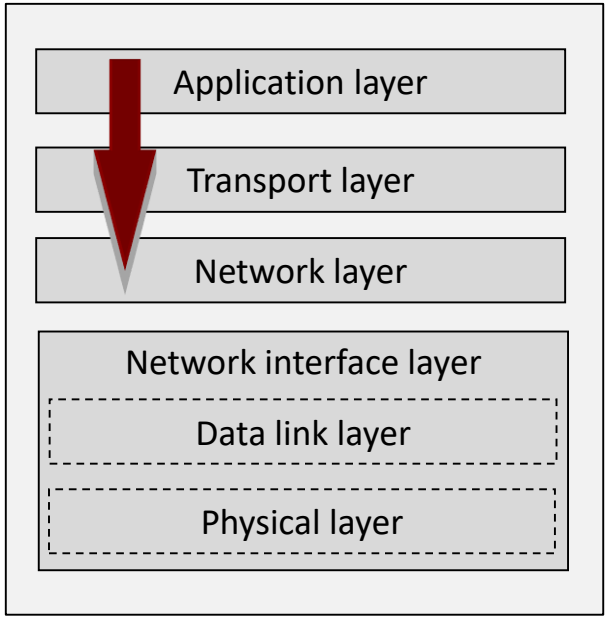
Dépannage d’un réseau LAN

Identification et analyse de la panne



Dépannage d'un réseau LAN

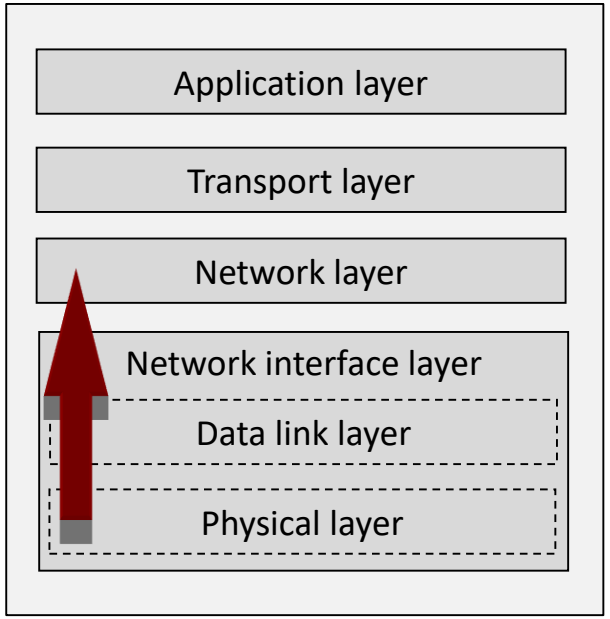
La méthode Top/Down



Si aucune erreur n'est détectée dans la connectivité de la couche réseau, utilisez cette méthode pour localiser la panne.

Dépannage d'un réseau LAN

La méthode Bottom/up



Si une erreur est détectée dans la connectivité de la couche réseau, utilisez cette méthode pour localiser la panne.

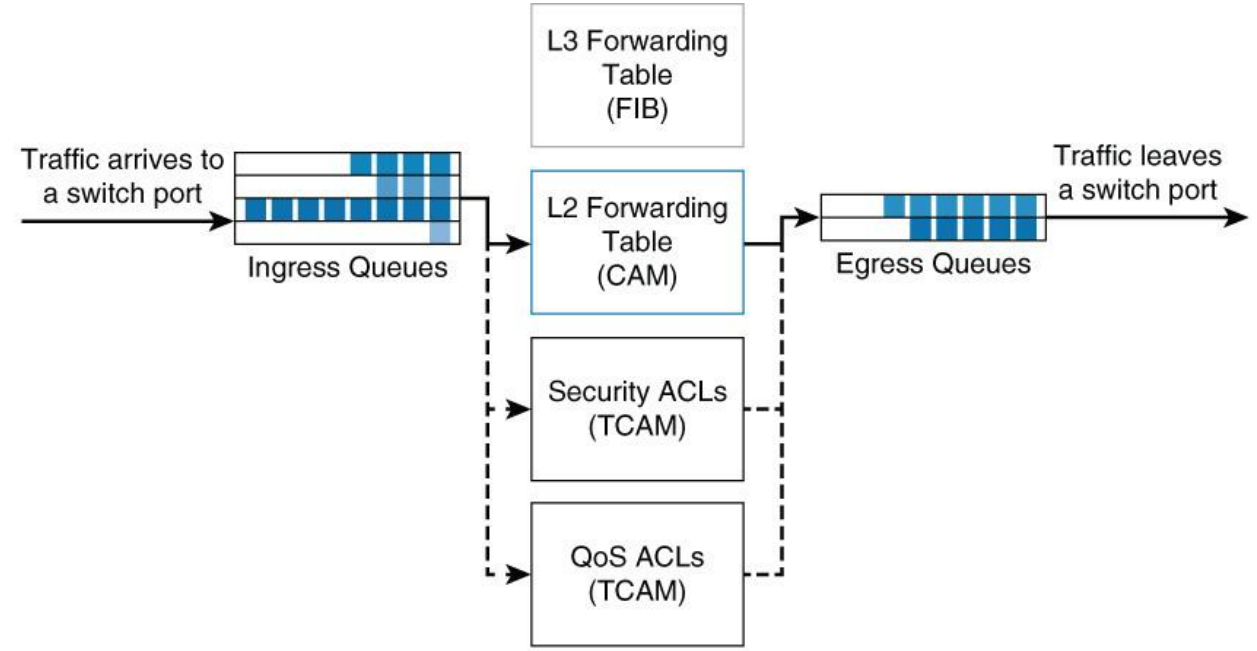
PARTIE 2

NOTIONS DE BASE SUR LA COMMUTATION

CHAPITRE 1

VLANs

Différents types de switch



FIB Table

IP Address	Next-Hop IP Address	Next-Hop MAC Address	Egress Port

CAM Table

MAC Address	Egress Port	VLAN

Différents types de switch

Switches à configuration fixe

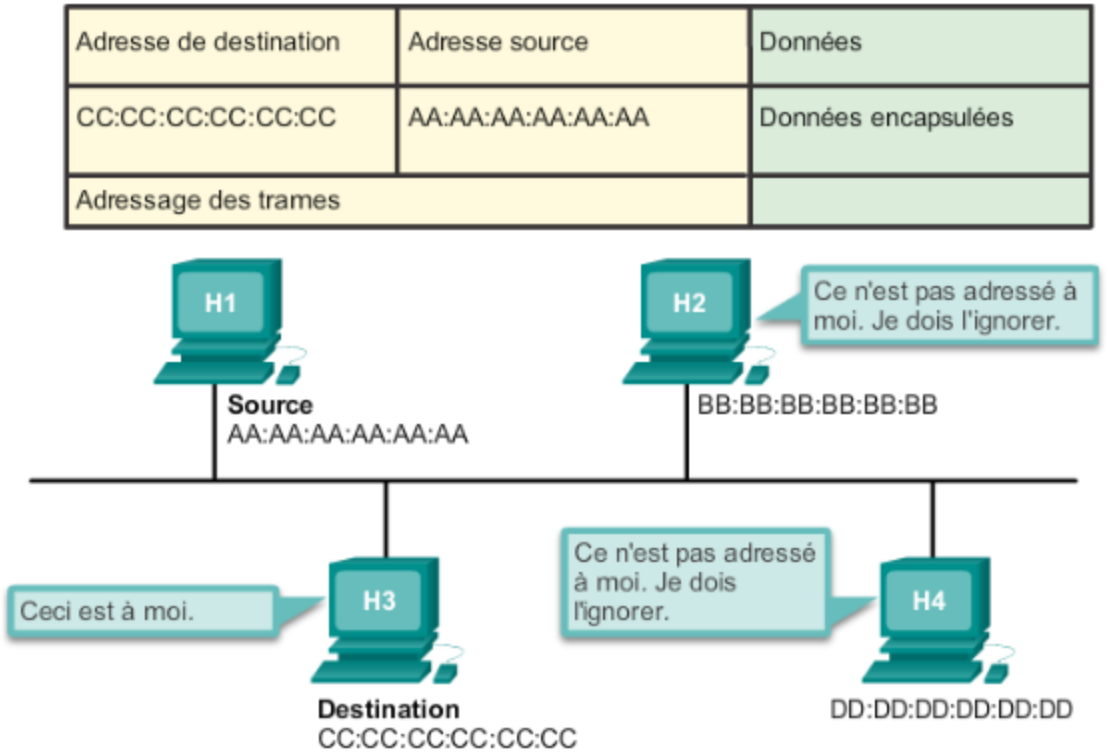
Switches à configuration modulaire

Switches à configuration empilable

CHAPITRE 1

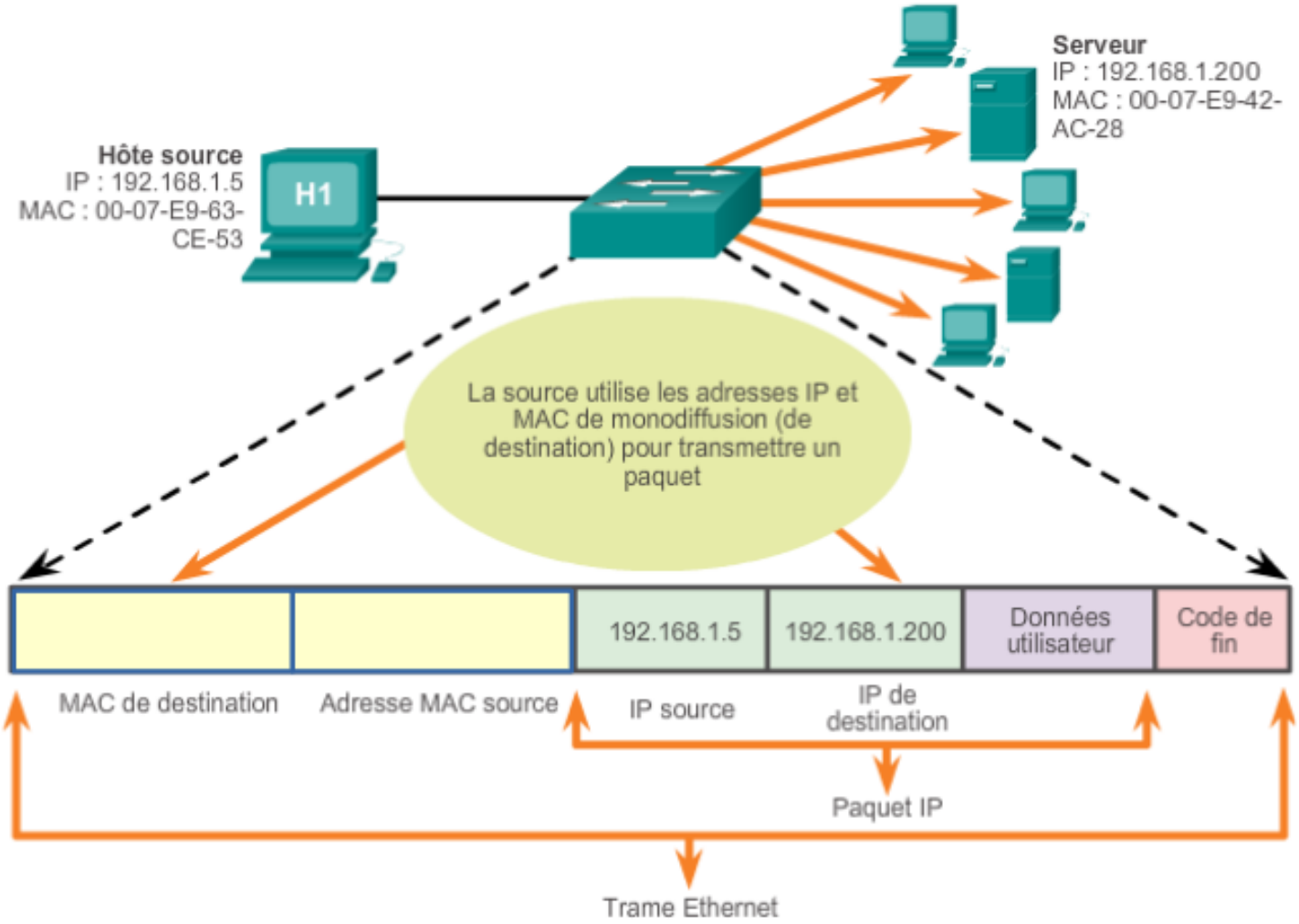
VLANs

Transfert de trame

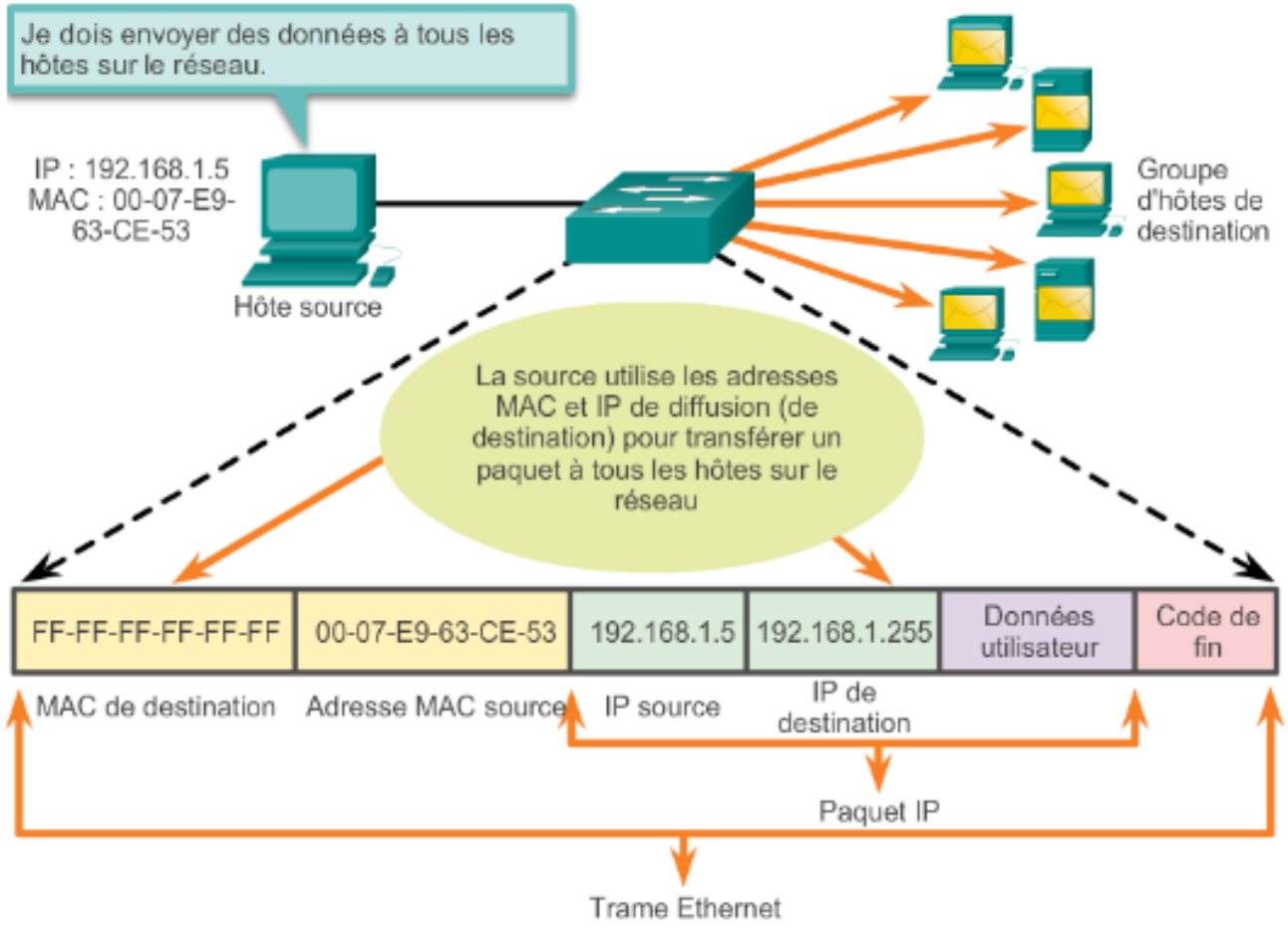


Les éléments de la trame Ethernet qui permettent d'identifier les nœuds participant à l'échange sont les adresses MAC (Media Acces Control) de destination et source

Transfert de trame



Transfert de trame



CHAPITRE 1

VLANs

1 - Différents types de switch

2 - Transfert de trame

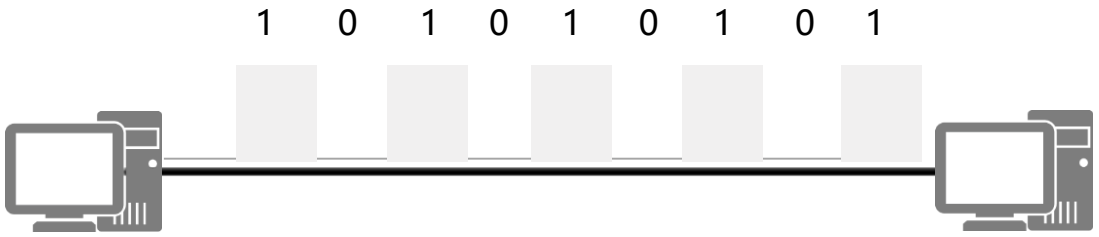
2 - Domaines de commutation

3 - Protocole ARP

4 - Principe de fonctionnement des VLANs

Domaines de commutation

Codage des données de signal

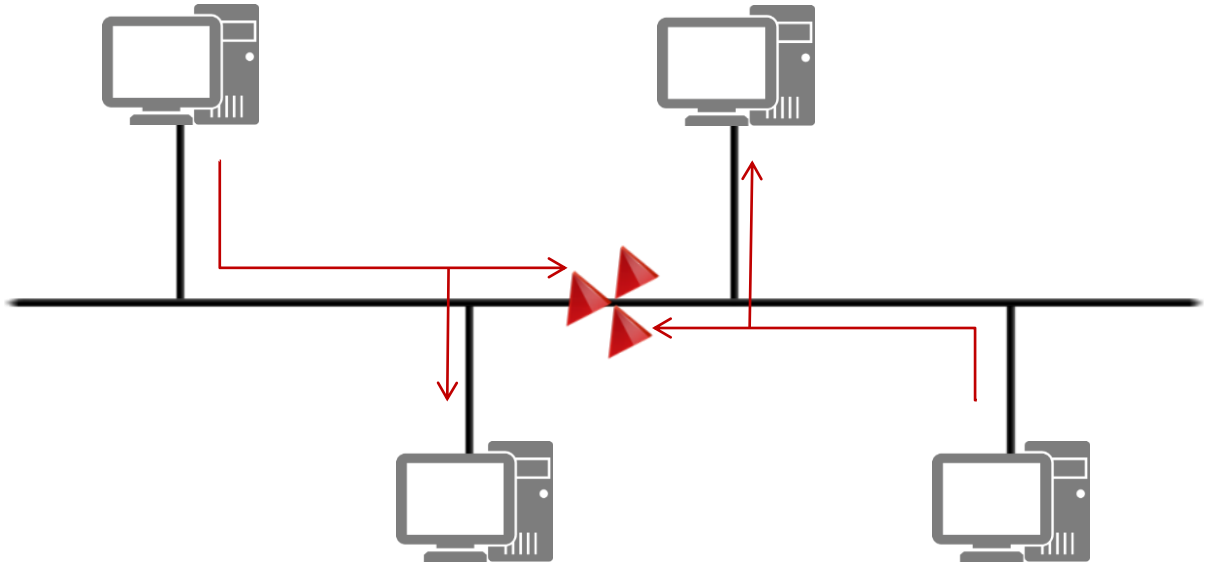


0000	0001	0010	0011	0100
0	1	2	3	4

- Modèles de signaux utilisés pour l'interprétation de la communication.
- L'encodage est utilisé pour synchroniser la transmission.

Domaines de commutation

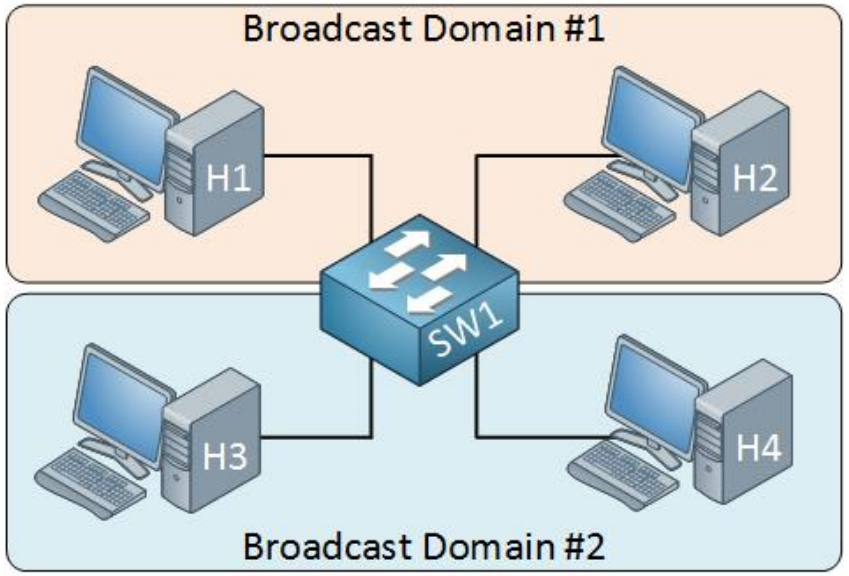
Domaines de collision

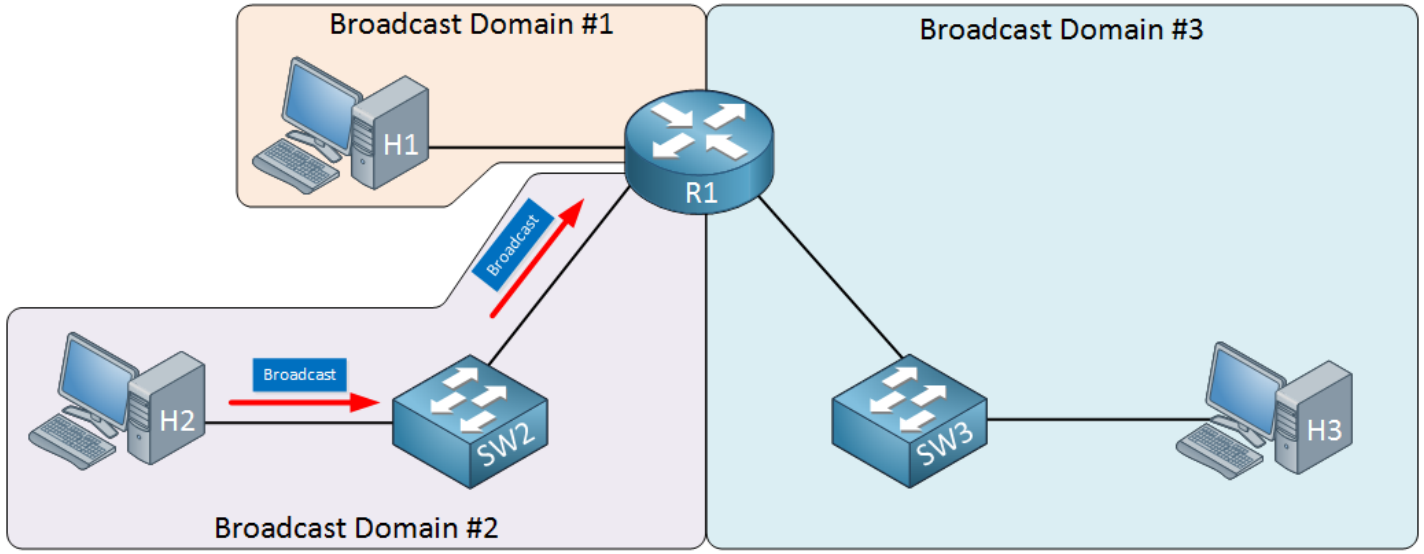


- Les signaux d'un réseau partagé sont sensibles aux collisions.
- Un mécanisme de détection des collisions est utilisé pour identifier les collisions.

Domaines de commutation

Domaines de diffusion





CHAPITRE 1

VLANs

1 - Différents types de switch

2 - Transfert de trame

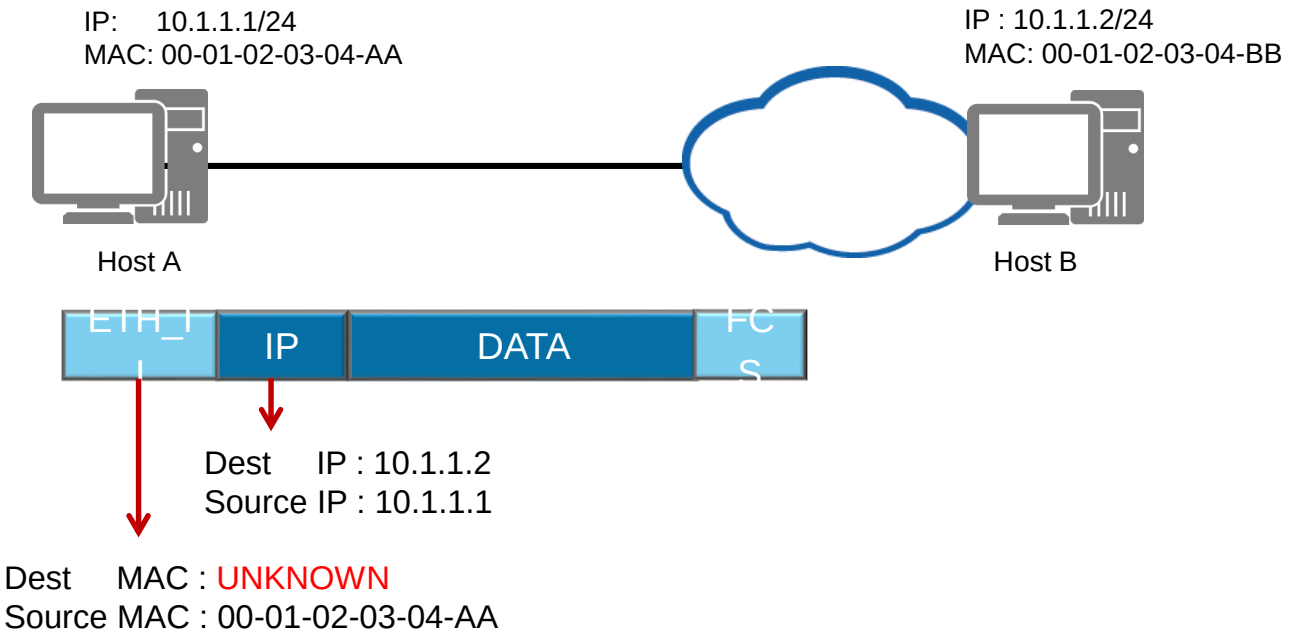
2 - Domaines de commutation

3 - Protocole ARP

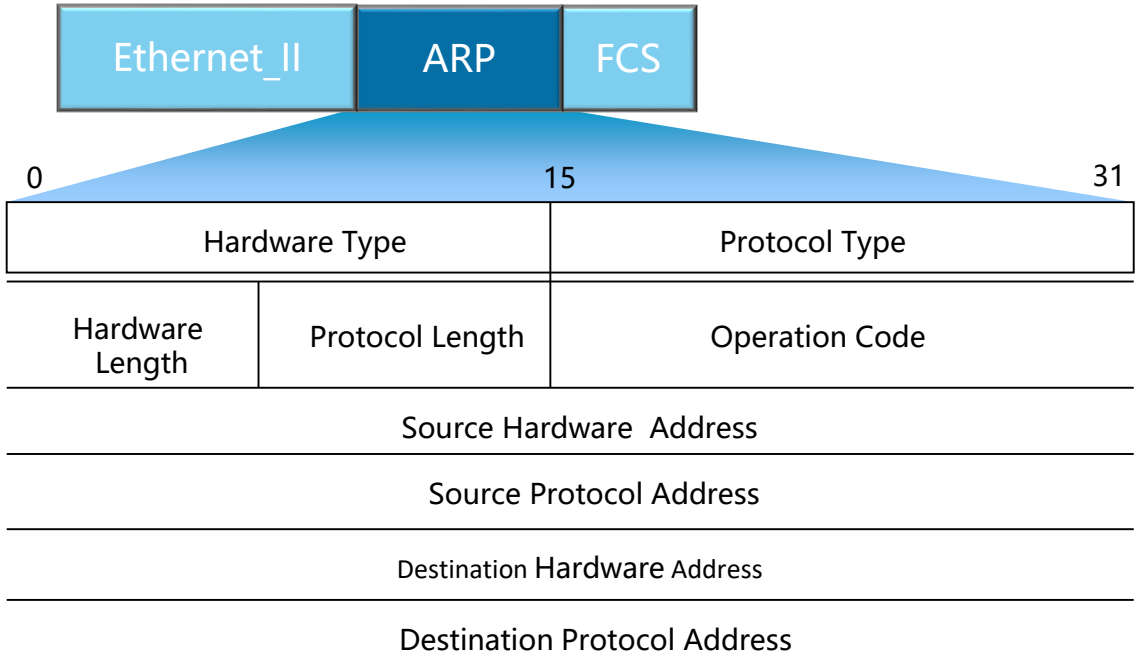
4 - Principe de fonctionnement des VLANs

Protocole ARP

La transmission des données repose sur la connaissance de l'adresse MAC de la destination de la couche de liaison de données.

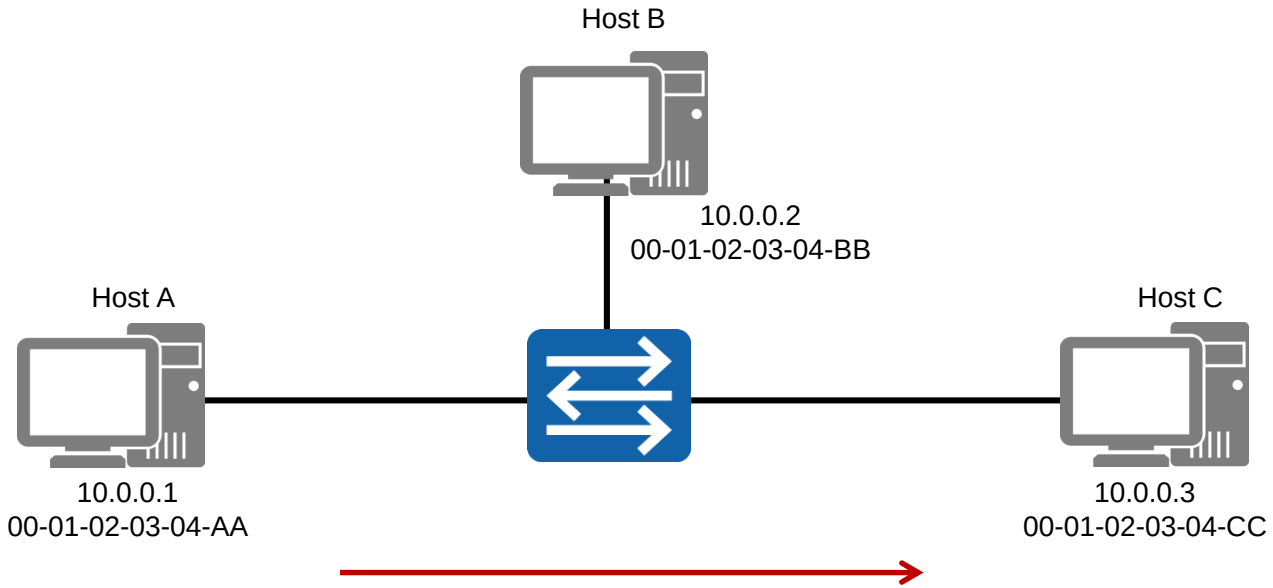


Le paquet ARP

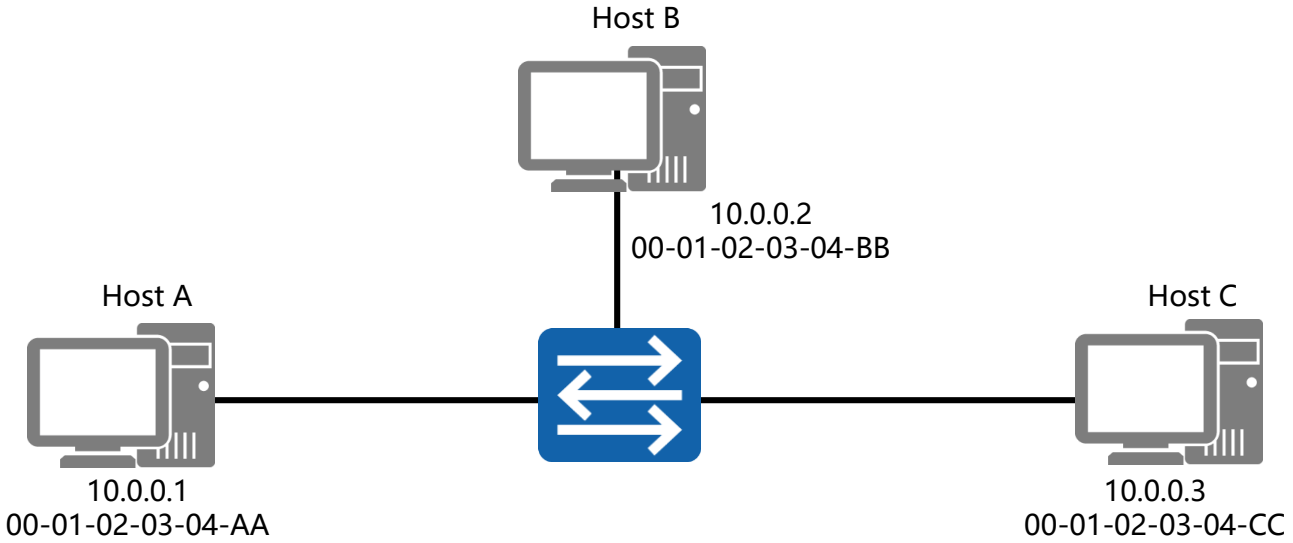


Le paquet ARP fonctionne dans les limites de la couche de liaison de données, comme on peut le comprendre par l'absence d'en-tête IP

Protocole ARP



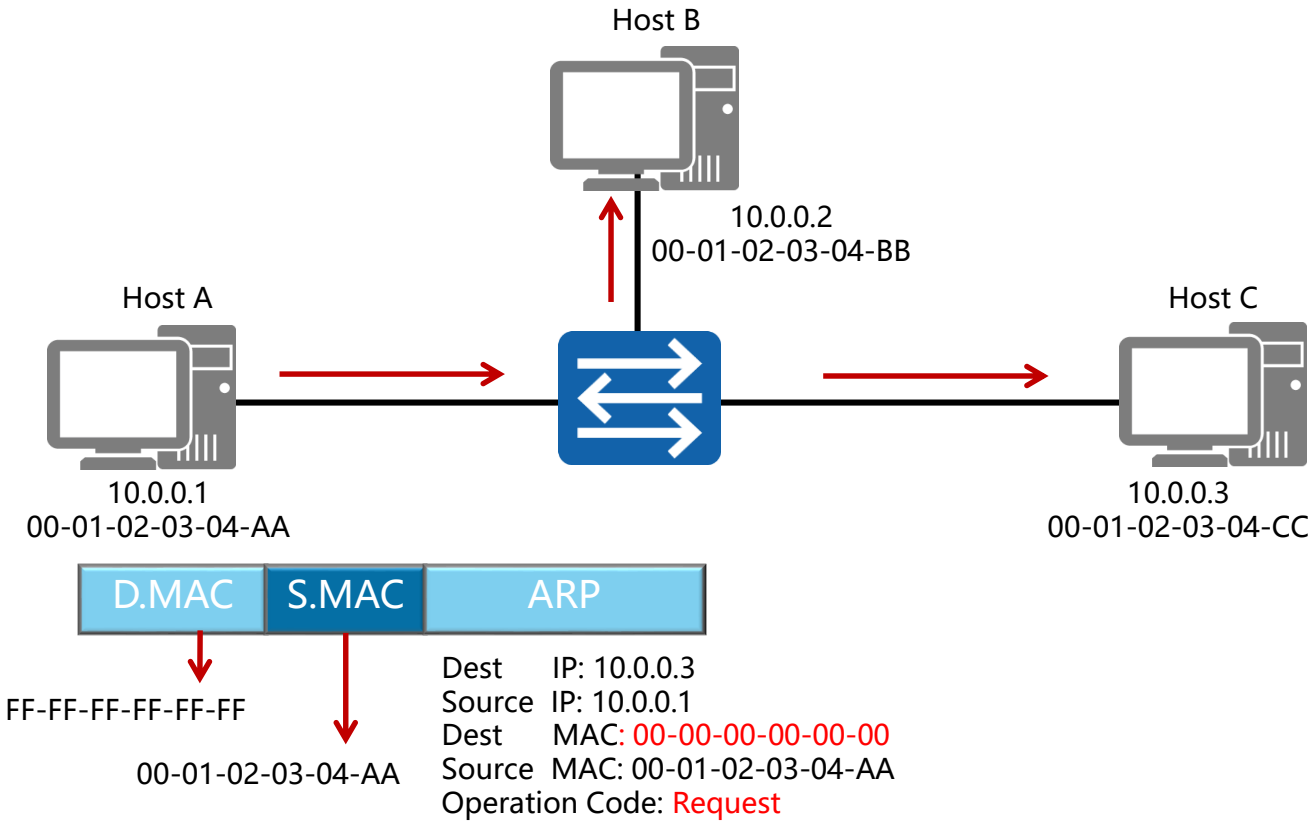
Protocole ARP



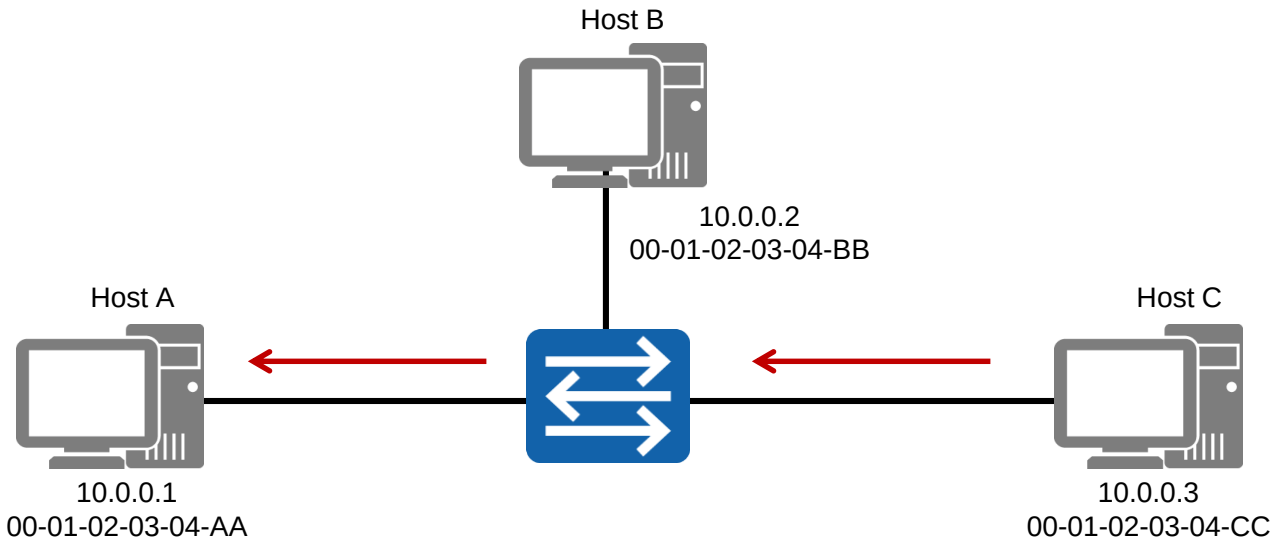

```
Host A>arp -a

Internet Address    Physical Address    Type
```

Protocole ARP

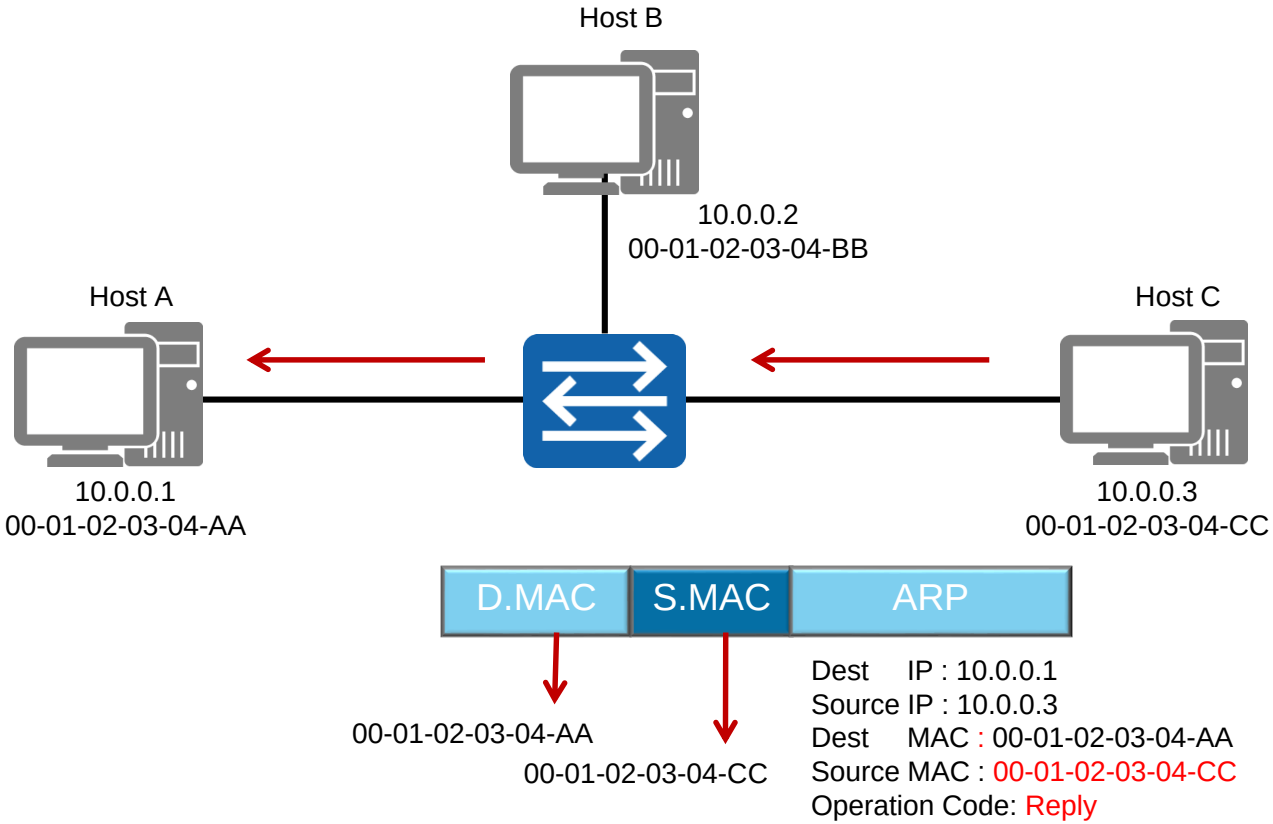


Protocole ARP



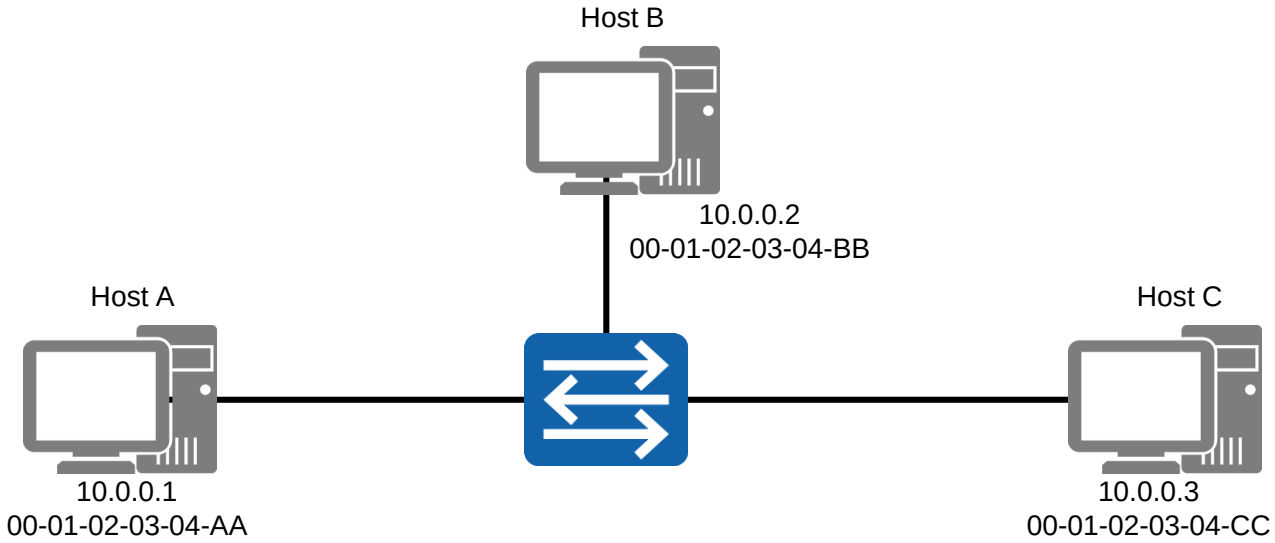

```
Host C>arp -a
Internet address  Physical address      Type
 10.0.0.1         00-01-02-03-04-AA     Dynamic
```

Protocole ARP



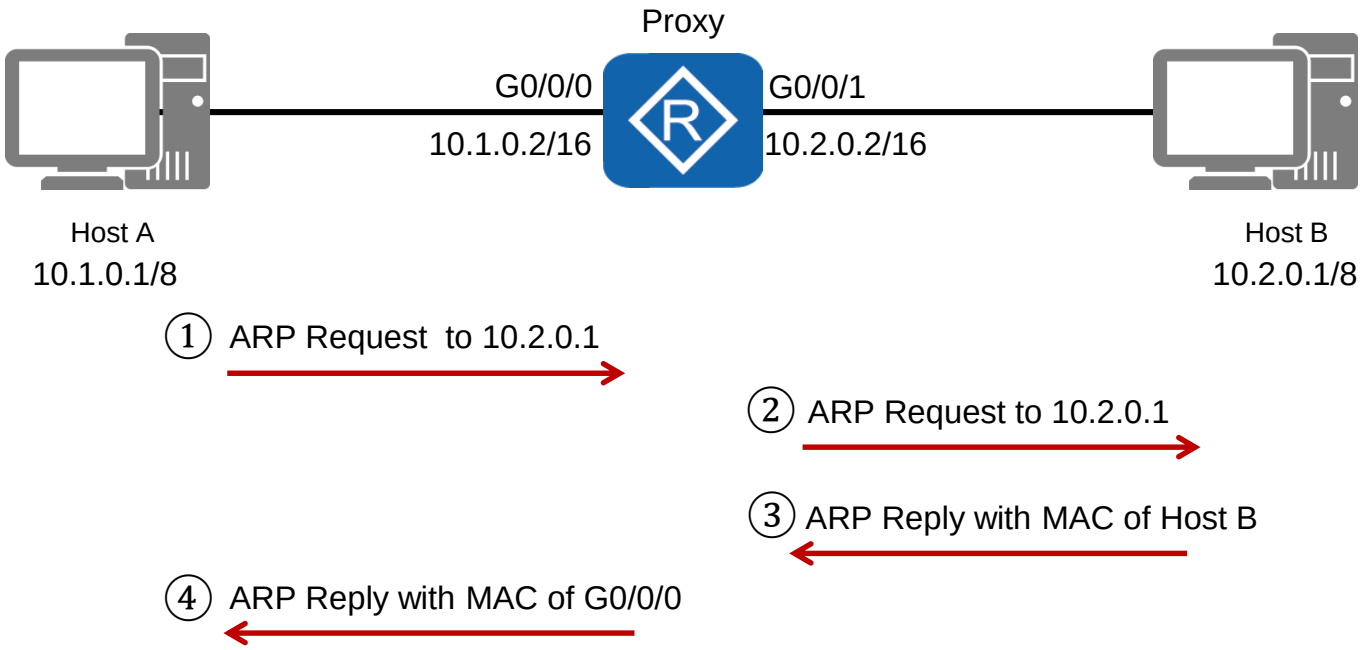
2-Protocole ARP

Cache ARP

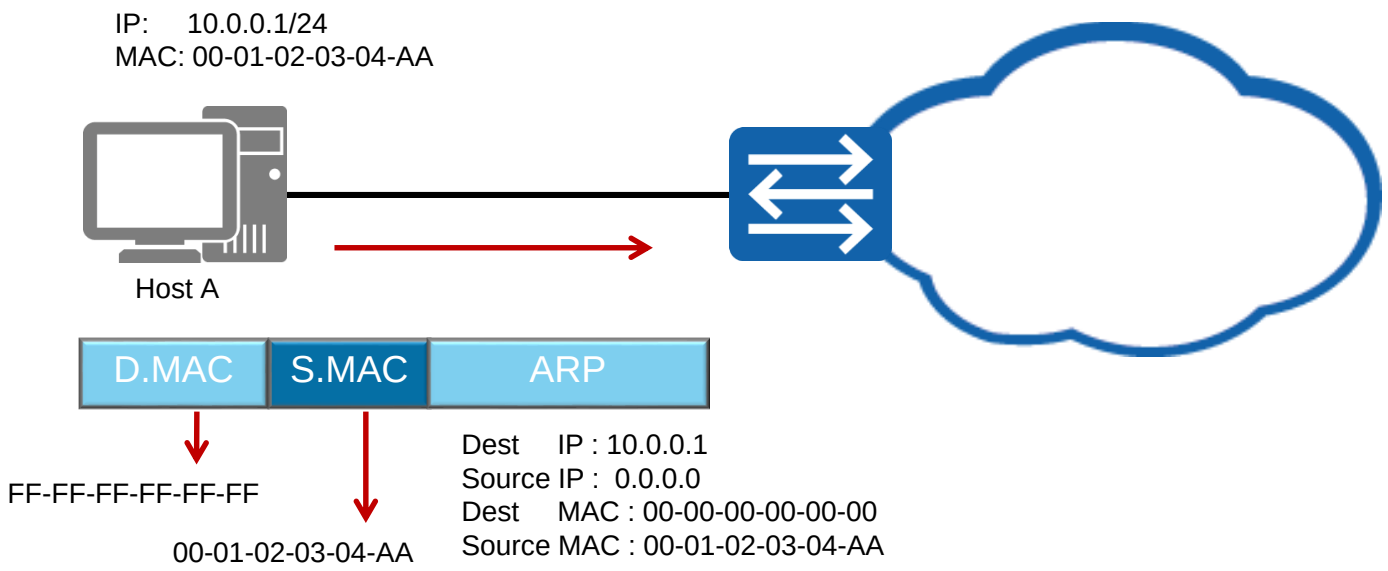



```
Host A>arp -a
Internet address  Physical address      Type
 10.0.0.3         00-01-02-03-04-CC     Dynamic
```

Proxy ARP


Proxy
G0/0/0
10.1.0.2/16
G0/0/1
10.2.0.2/16
Host A
10.1.0.1/8
Host B
10.2.0.1/8
① ARP Request to 10.2.0.1
② ARP Request to 10.2.0.1
③ ARP Reply with MAC of Host B
④ ARP Reply with MAC of G0/0/0

ARP gratuit


IP: 10.0.0.1/24
MAC: 00-01-02-03-04-AA
Host A
D.MAC
S.MAC
ARP
FF-FF-FF-FF-FF-FF
00-01-02-03-04-AA
Dest IP : 10.0.0.1
Source IP : 0.0.0.0
Dest MAC : 00-00-00-00-00-00
Source MAC : 00-01-02-03-04-AA

CHAPITRE 1

VLANs

1 - Différents types de switch

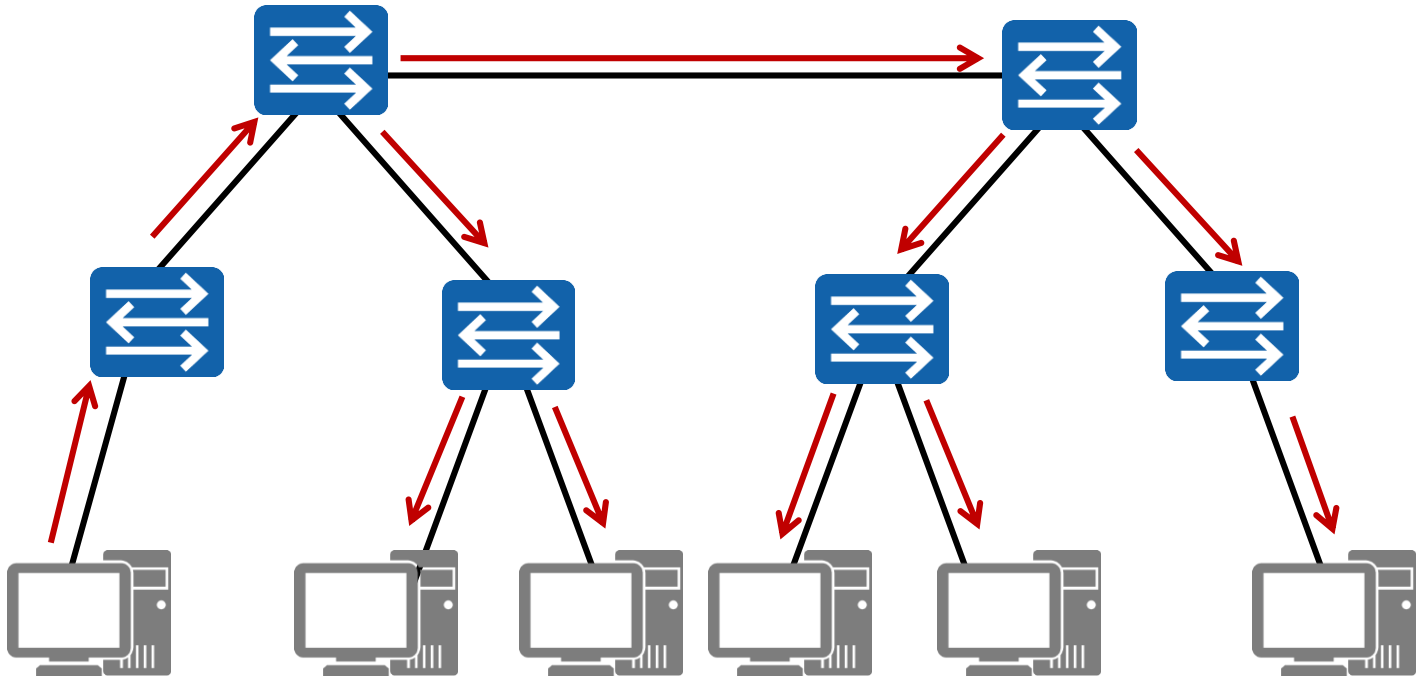
2 - Transfert de trame

2 - Domaines de commutation

3 - Protocole ARP

4 - Principe de fonctionnement des VLANs

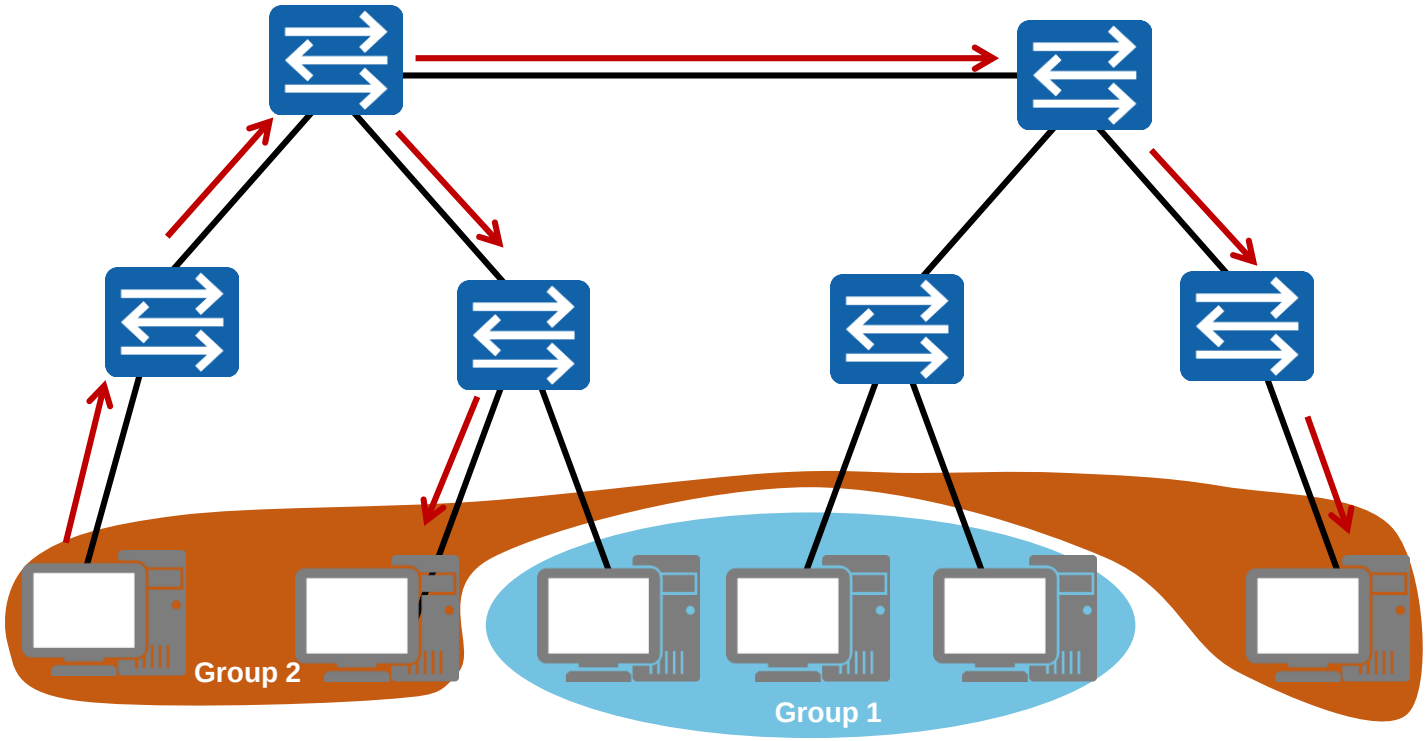
Les limites des LAN



Pas de domaine de diffusion pour gérer l'expansion des réseaux locaux

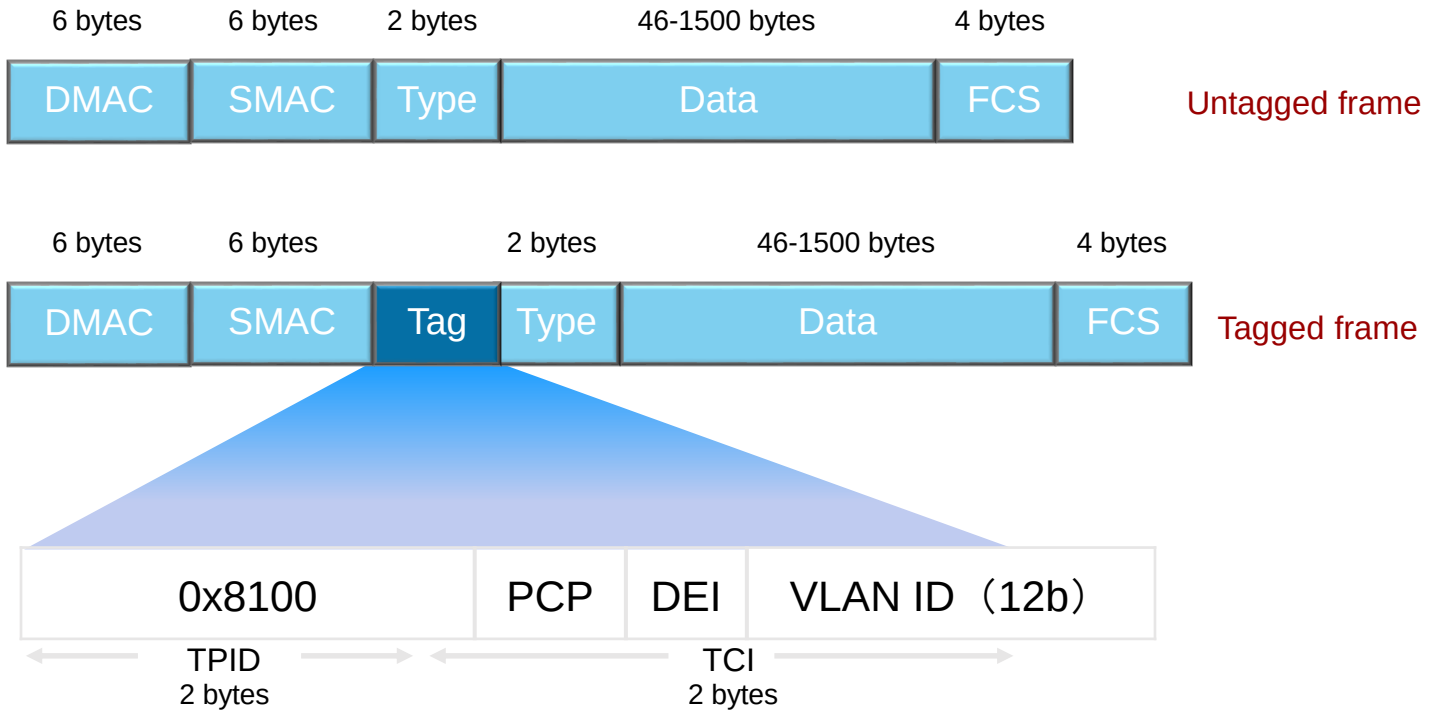
Les limites des LAN

Un VLAN permet un isolement logique du trafic à la couche de liaison de données.



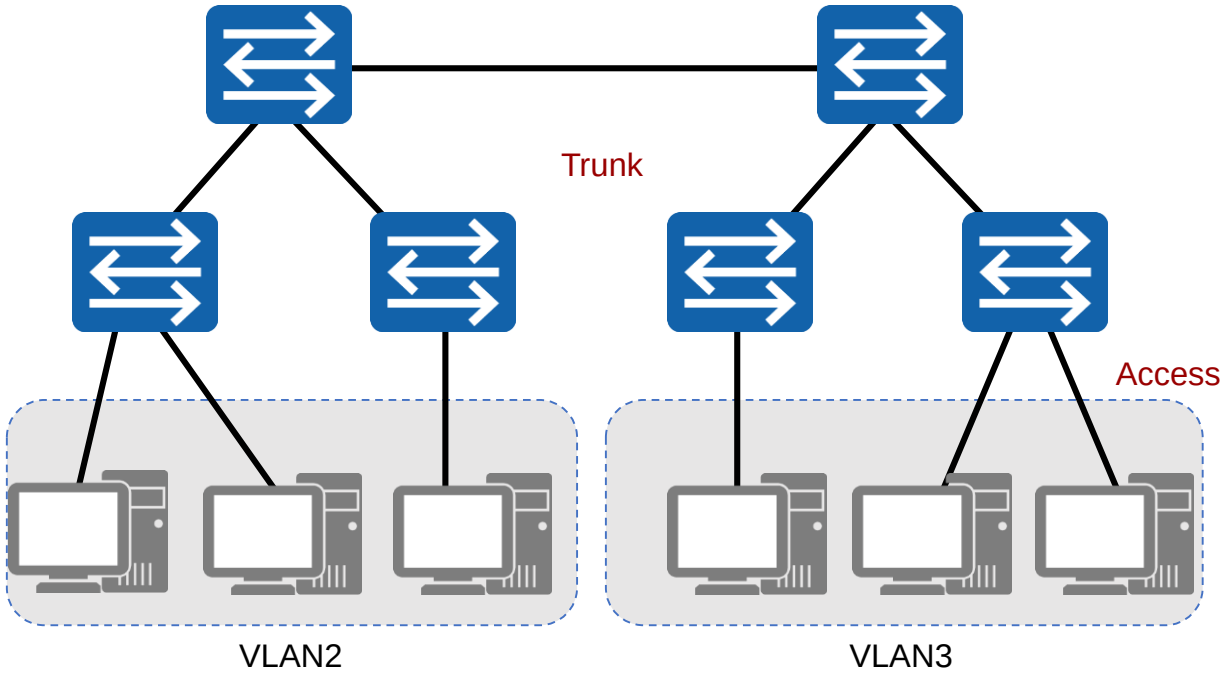
Structure de trame

Un tag VLAN est insérée pour distinguer les trames pour chaque VLAN.



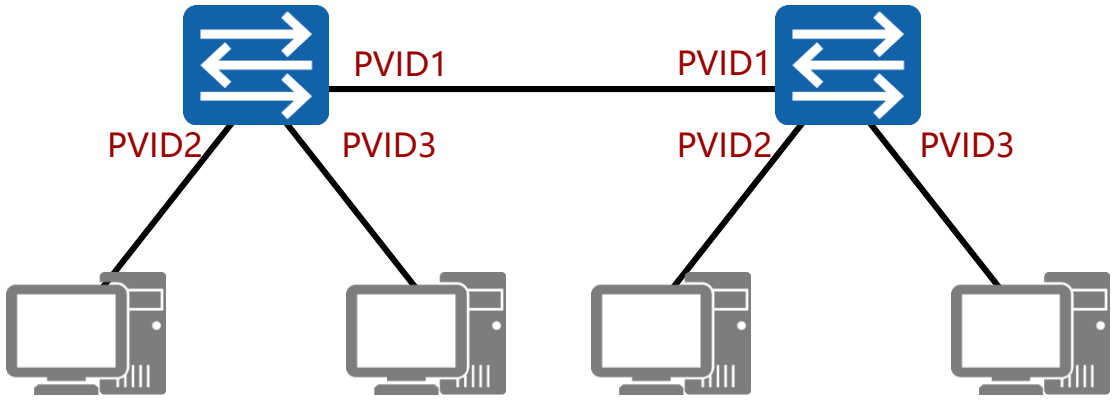
Type des liens

Le trunk représente le backbone pour la transmission du trafic VLAN entre les commutateurs.

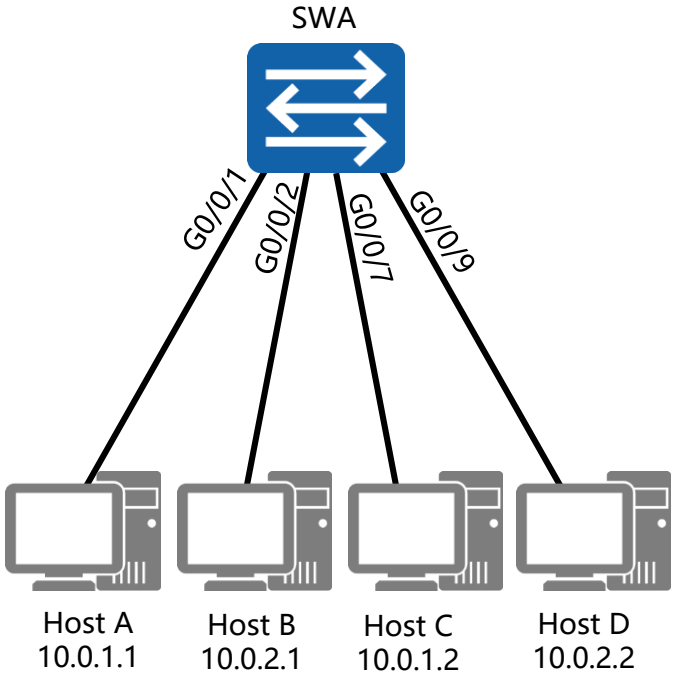


ID VLAN

- PVID représente le VLAN par défaut pour chaque interface.
- Le PVID est défini sur VLAN 1 pour tous les ports par défaut.



Affectation des VLANs

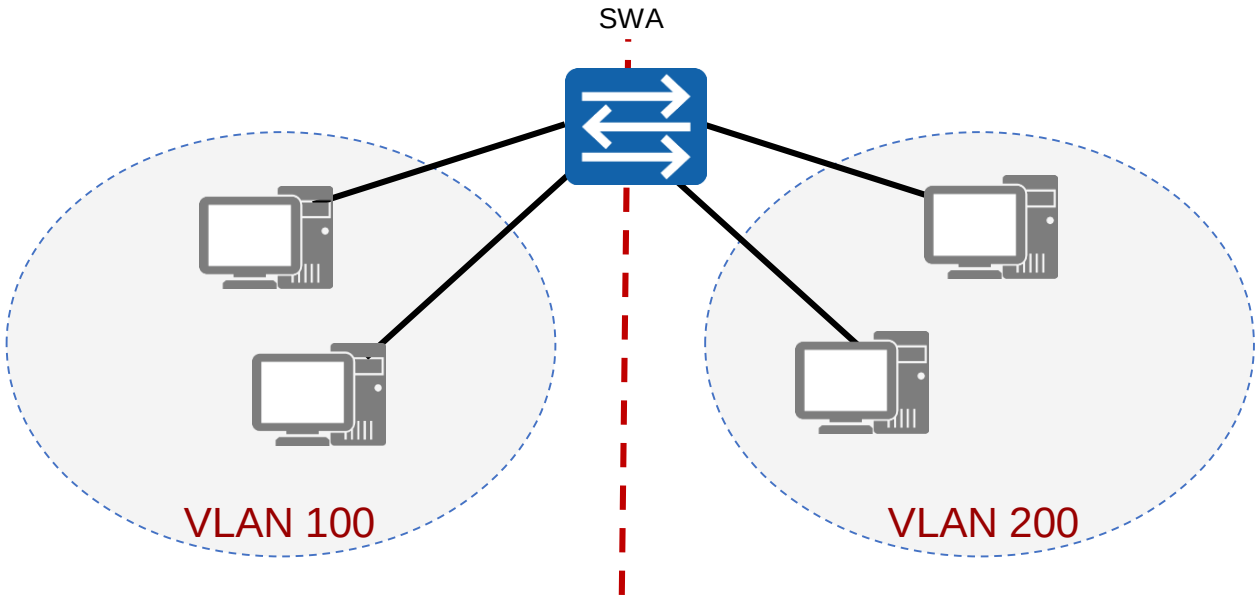


Assignment Method	VLAN 5	VLAN 10
Port based	G0/0/1, G0/0/7	G0/0/2 G0/0/9
MAC based	00-01-02-03-04-AA 00-01-02-03-04-CC	00-01-02-03-04-BB 00-01-02-03-04-DD
IP Subnet based	10.0.1.*	10.0.2.*
Protocol based	IP	IPX
Policy based	10.0.1.* + G0/0/1+ 00-01-02-03-04-AA	10.0.2.* + G0/0/2 + 00-01-02-03-04-BB

- Cinq méthodes d'affectation VLAN sont possibles.
- L'affectation VLAN basée sur le port est la méthode d'affectation par défaut.

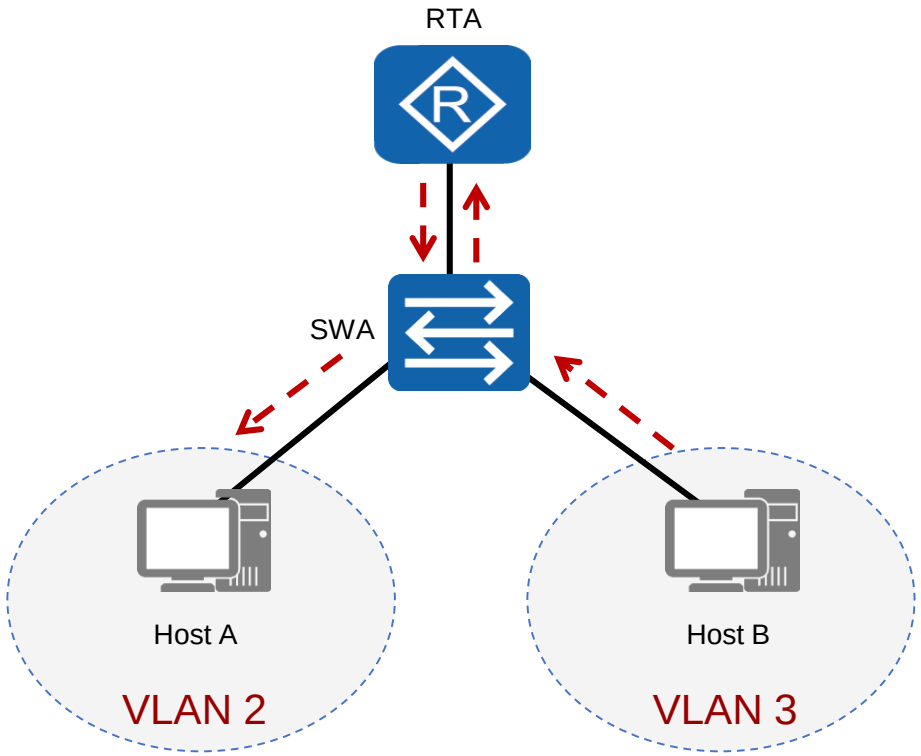
Les limites des VLANs

Visent à limiter la taille du domaine de diffusion grâce à l'implémentation VLAN isolent les utilisateurs.



Routage entre les VLANs

Les trames VLANs sont acheminés au-dessus d'un lien de tronc pour la conservation de port.



CHAPITRE 2

REDONDANCE

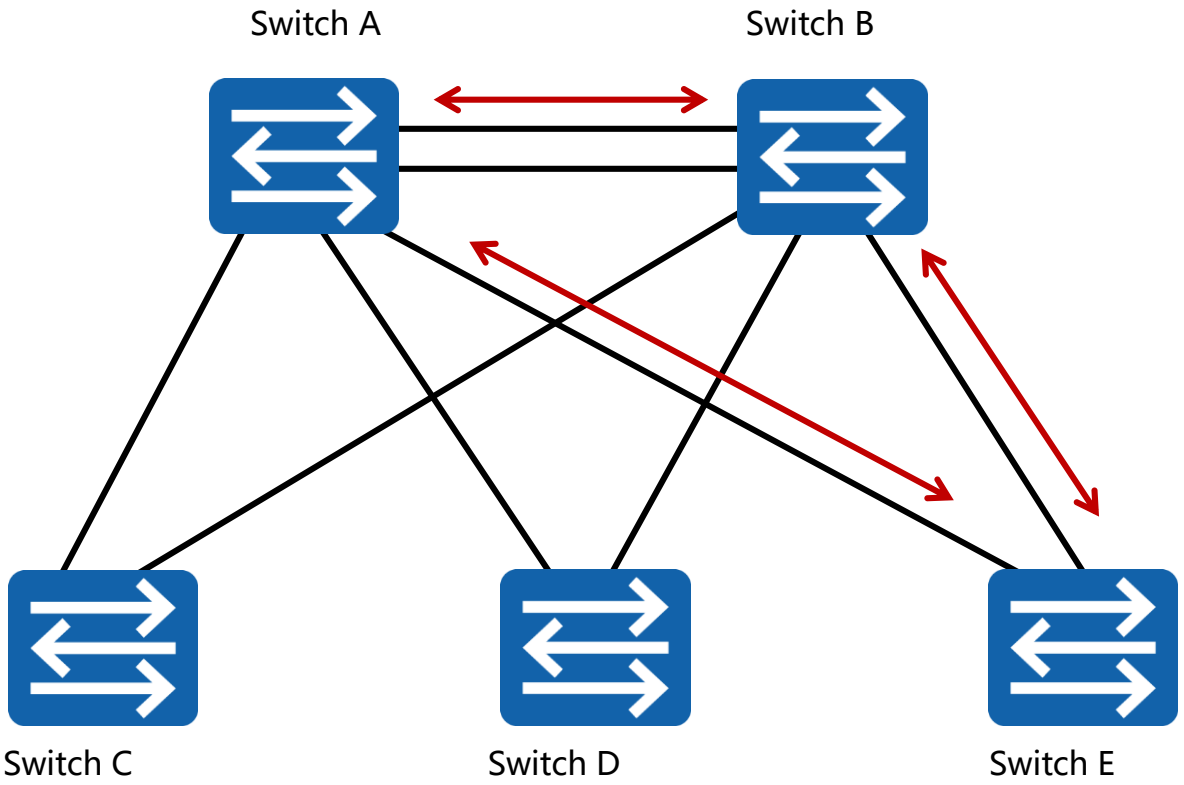
1 - Avantages et inconvénients de la redondance en réseau

2 - Protocole STP

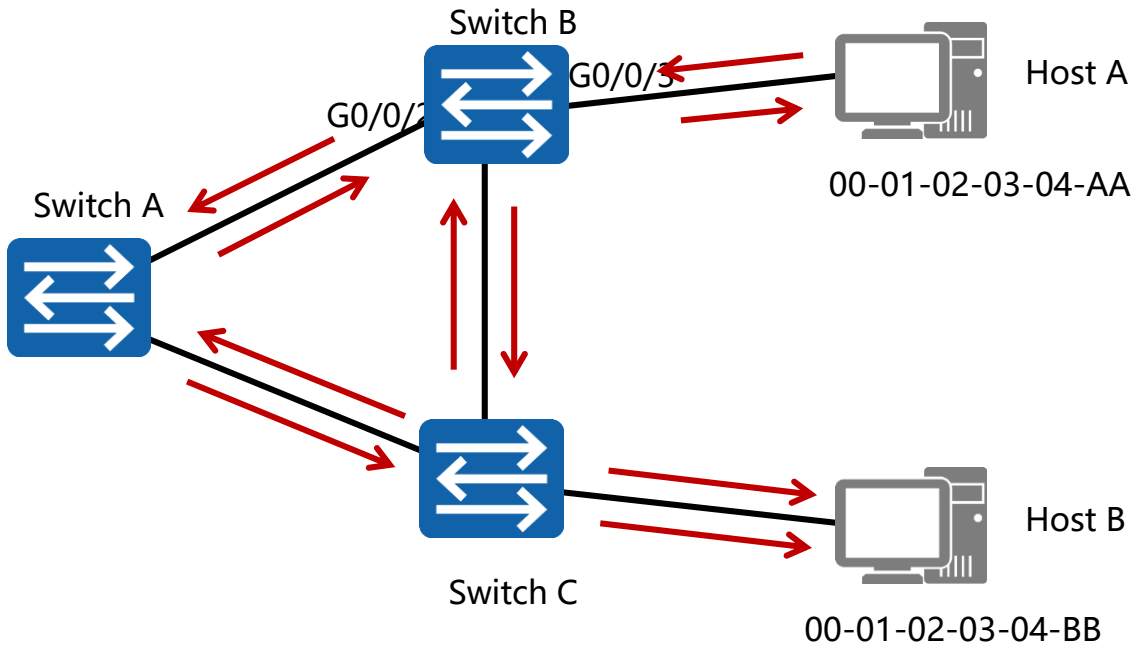
3 – Protocole VRRP

Avantage de la redondance

La redondance dans un réseau de commutation minimise les échecs de connexion, mais génère des boucles de commutation potentielle.

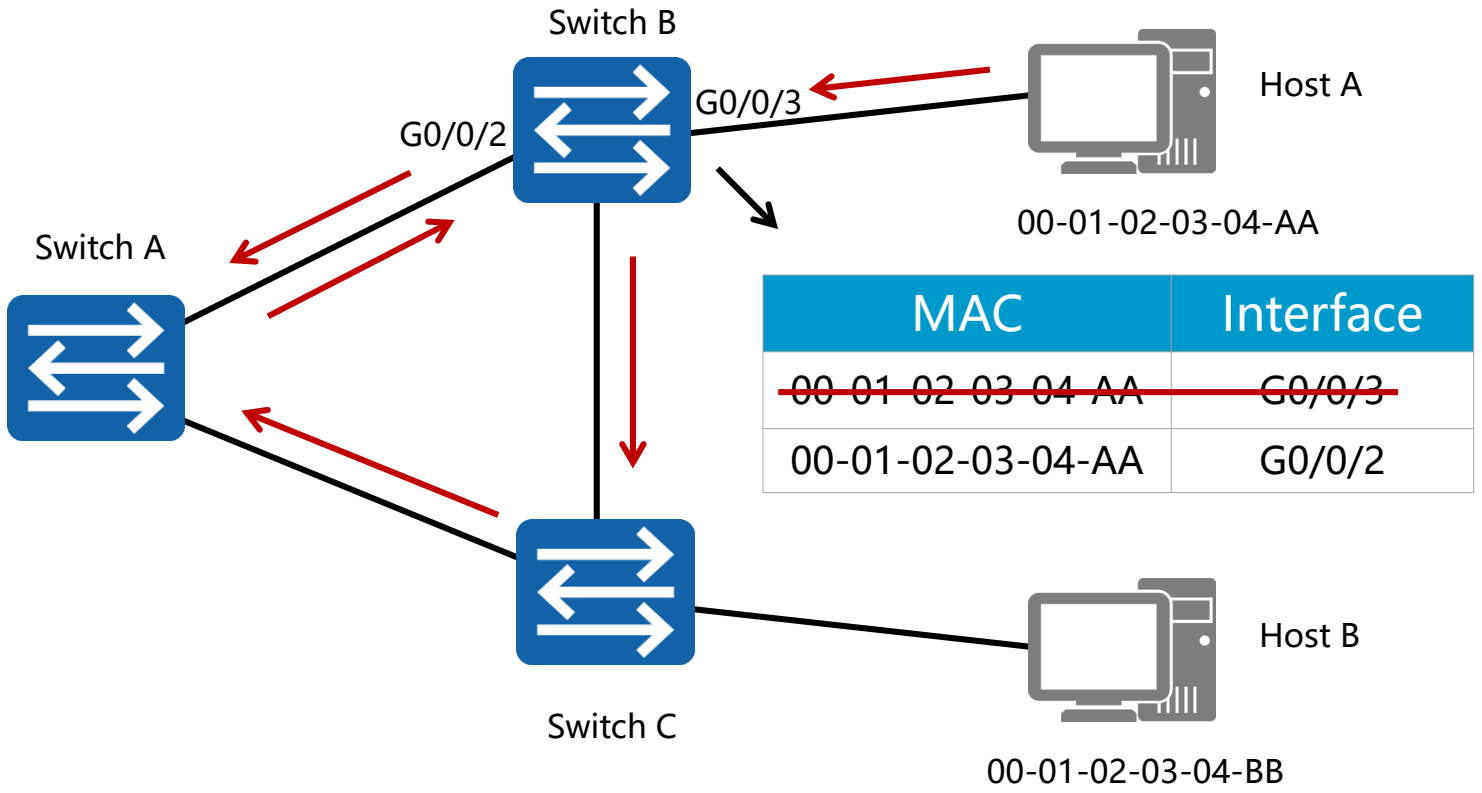


Tempêtes de diffusion



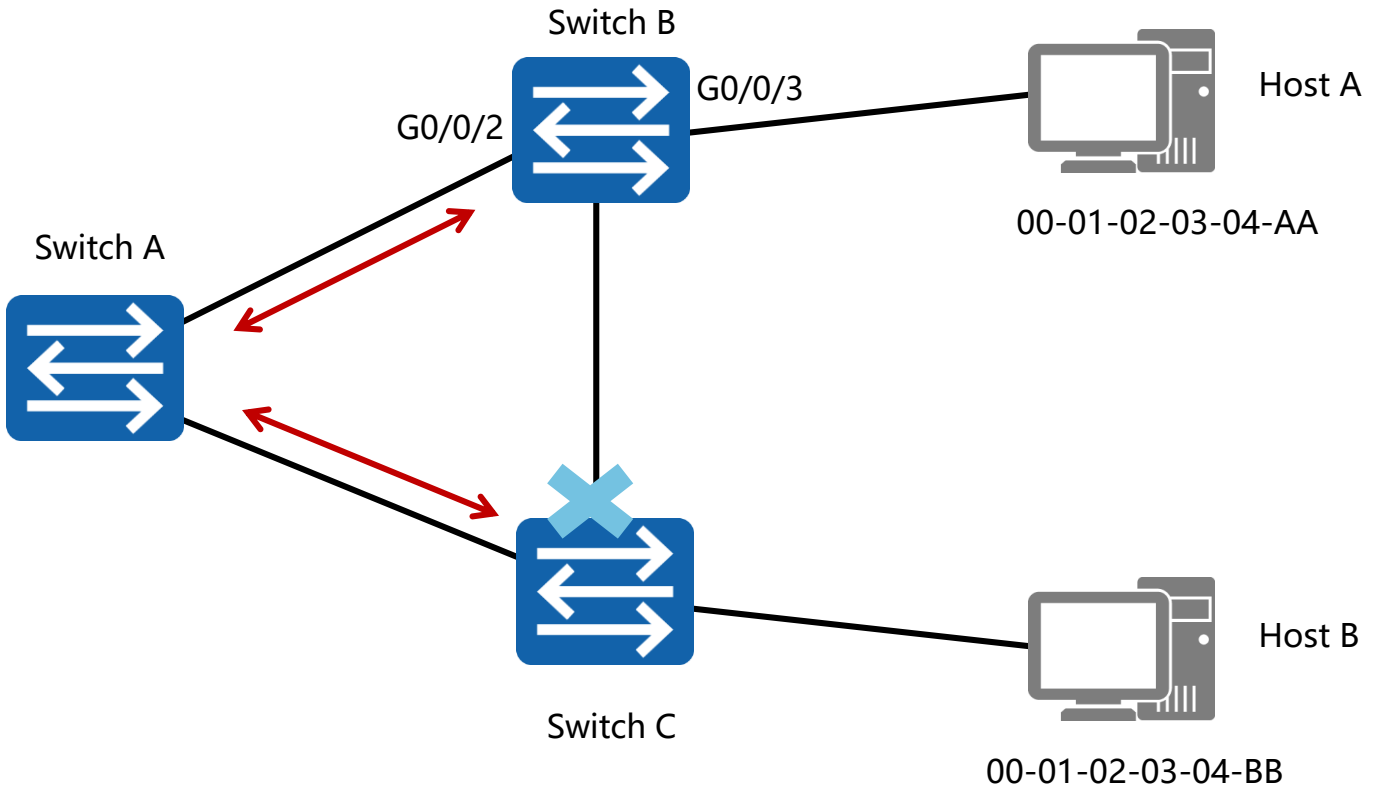
Les boucles de commutation permettent aux tempêtes de diffusion de se produire et à la duplication des trames d'être reçues par les stations d'extrémité.

Instabilité du MAC



La réception de trames précédemment transmises génère de fausses entrées MAC et une instabilité dans la table d'adresses MAC.

Les boucles sont éliminées en limitant le flux de trafic sur les chemins redondants.



CHAPITRE 2

REDONDANCE

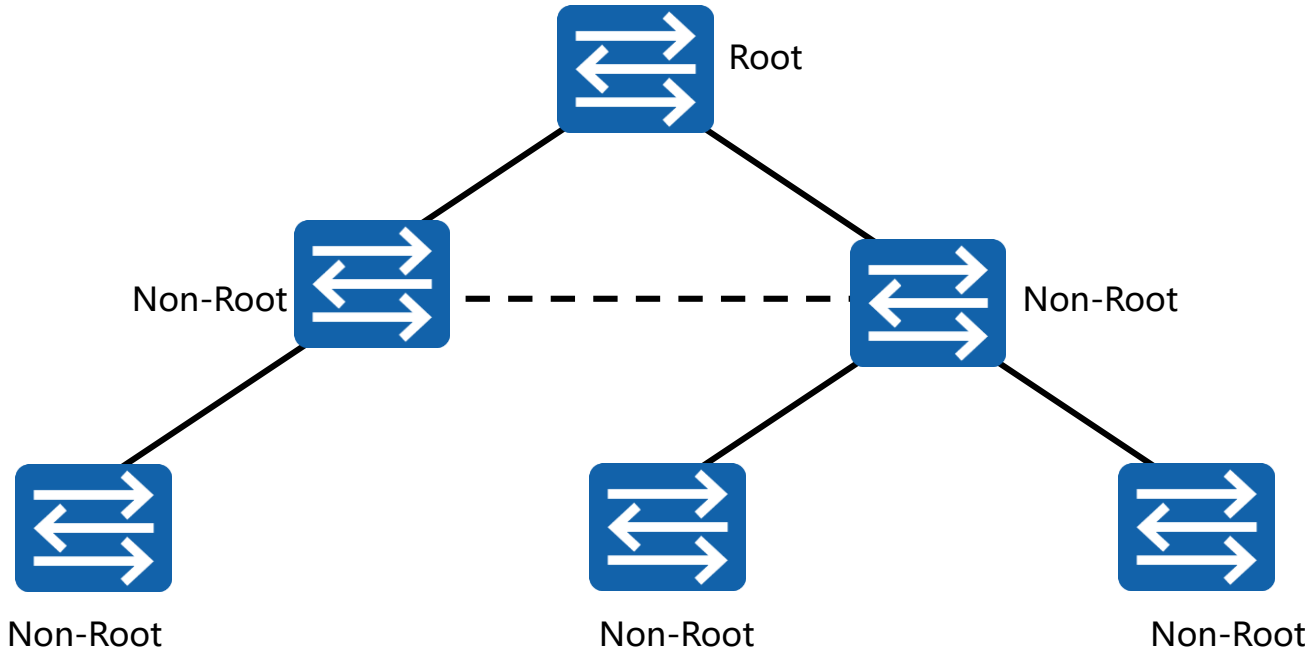
1 - Avantages et inconvénients de la redondance en réseau

2 - Protocole STP

3 – Protocole VRRP

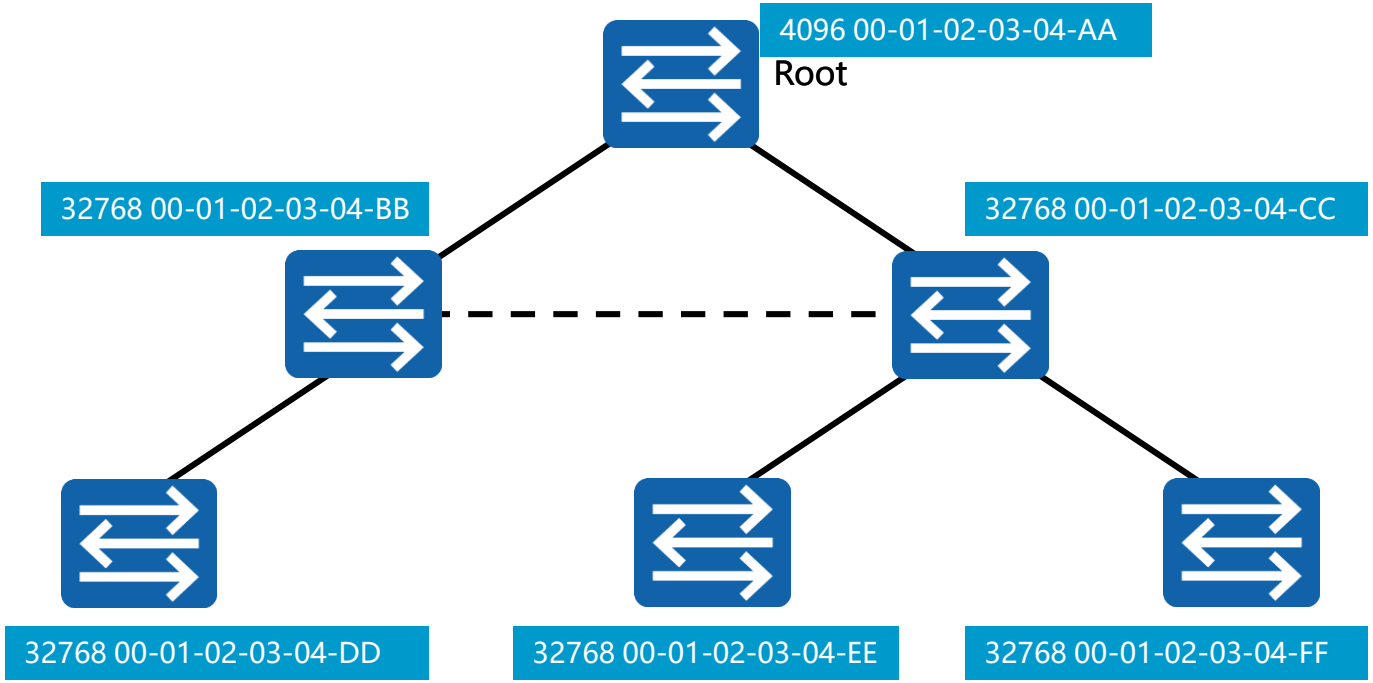
Protocole STP

- Une architecture d'arbre inversée est créée de STP.
- Le pont racine représente la base de la spanning tree

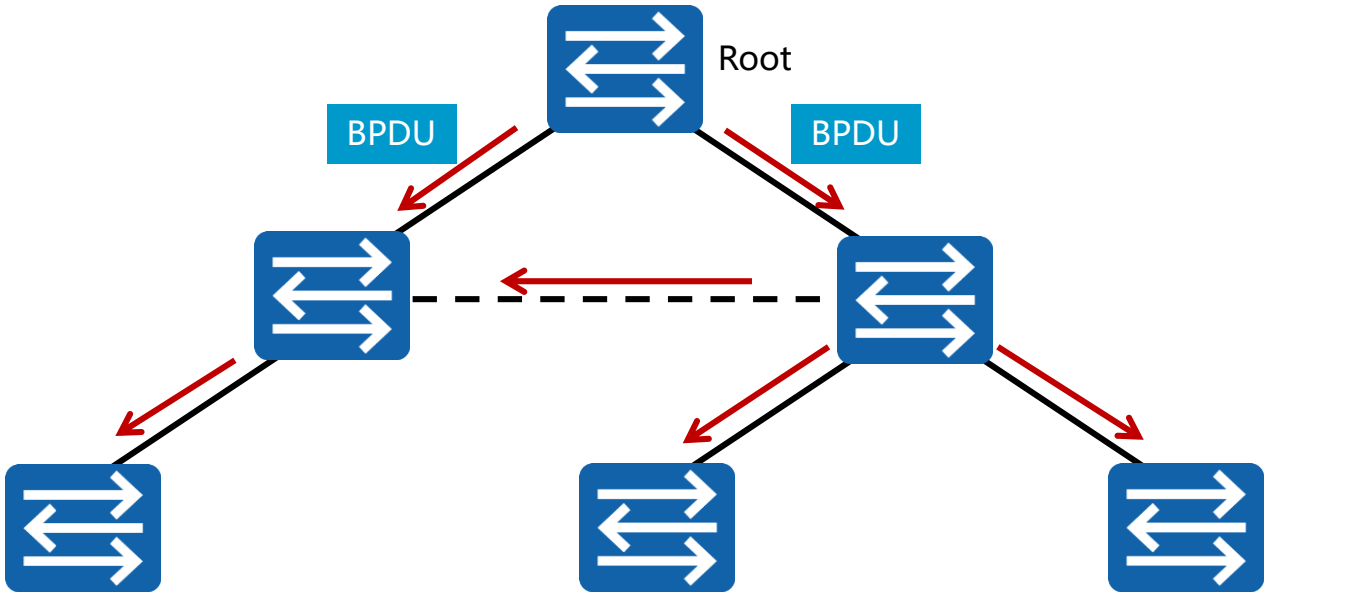


Bridge ID

- Les identificateurs de pont sont utilisés pour élire le pont-racine.
- La priorité du pont peut être manipulée pour forcer la sélection des racines



Protocole STP



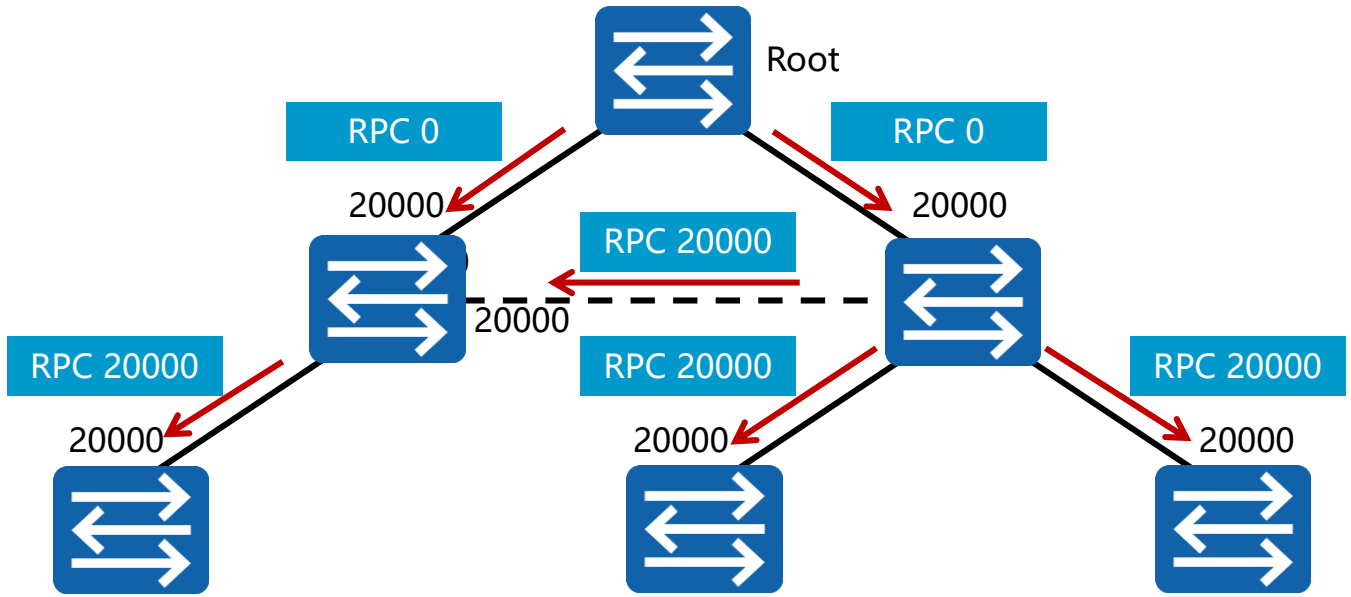
PID	PVI	BPDU Type	Flags	Root ID	RPC	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Fwd Delay

Configuration

TCN

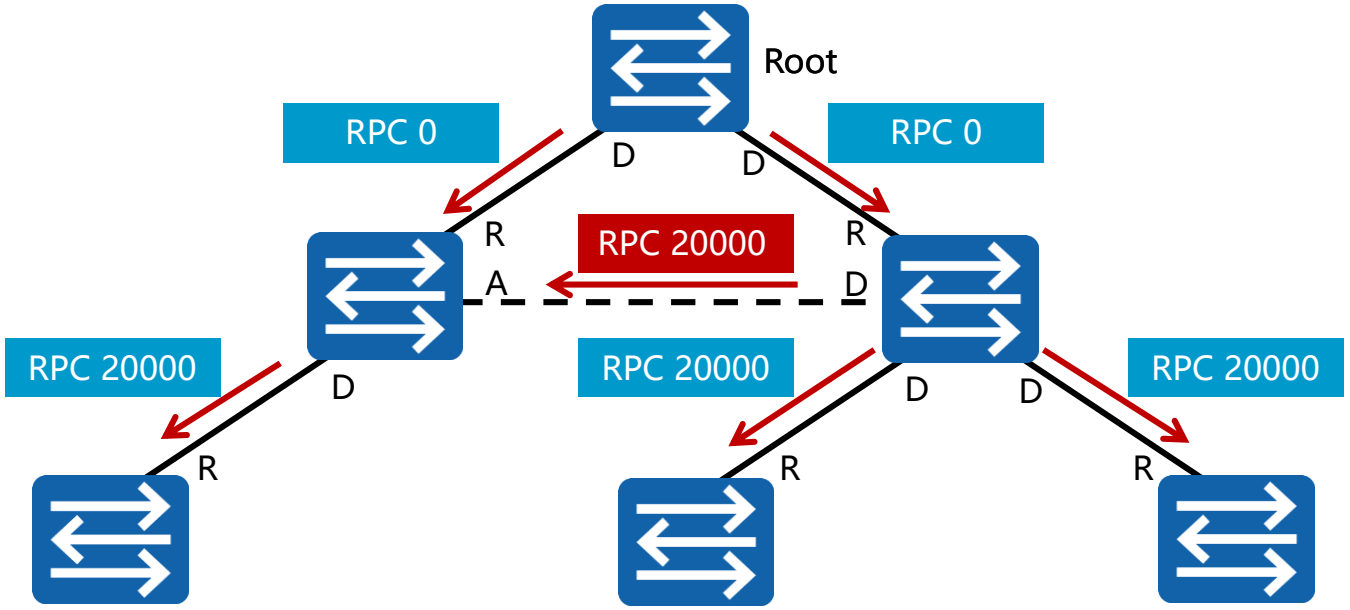
Cout des liens

Le coût du lien des switches est porté dans le BPDU et utilisé pour déterminer le chemin le plus court vers la racine.



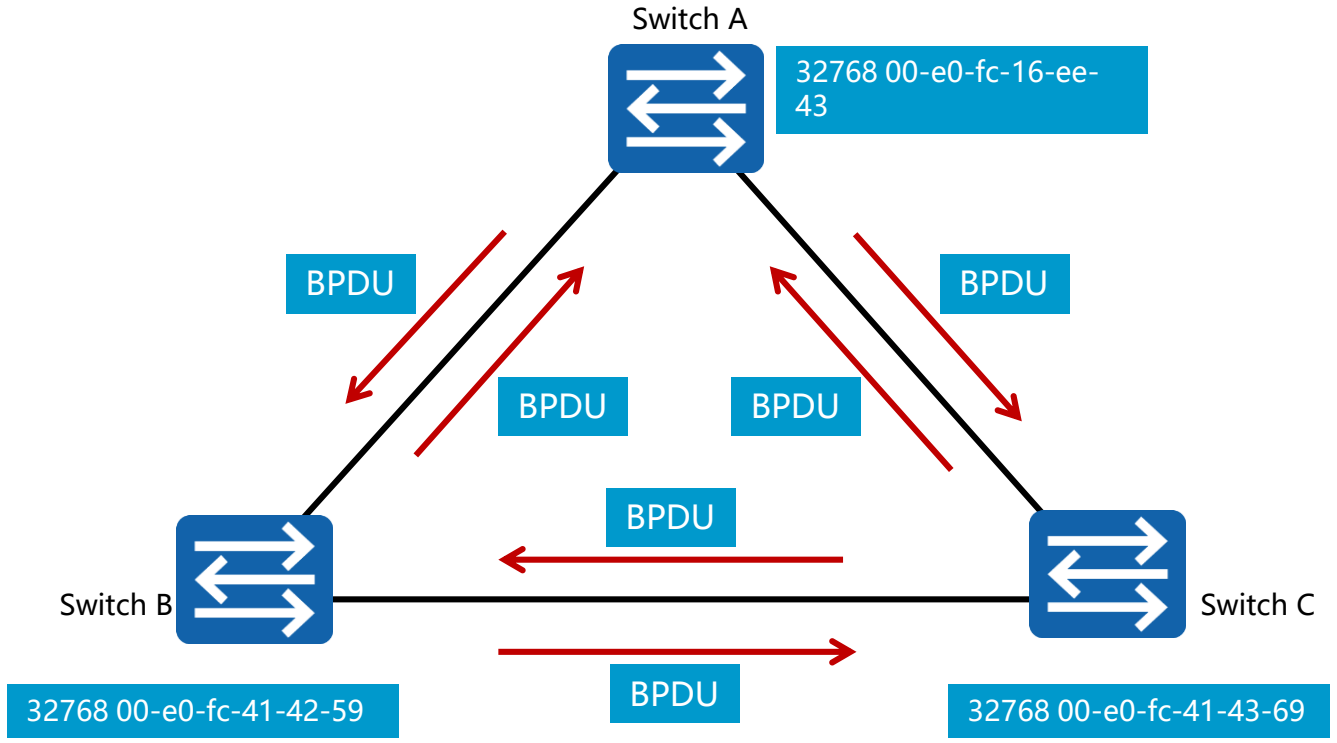
Rôle des ports

- Spanning tree soutient les rôles désignés, root et autres ports.
- Le coût de la trajectoire des racines permet de déterminer les rôles portuaires



Processus d’élection du root

- Tous les commutateurs STP annoncent BDPU à leurs pairs avec soi-même comme racine.



CHAPITRE 2

REDONDANCE

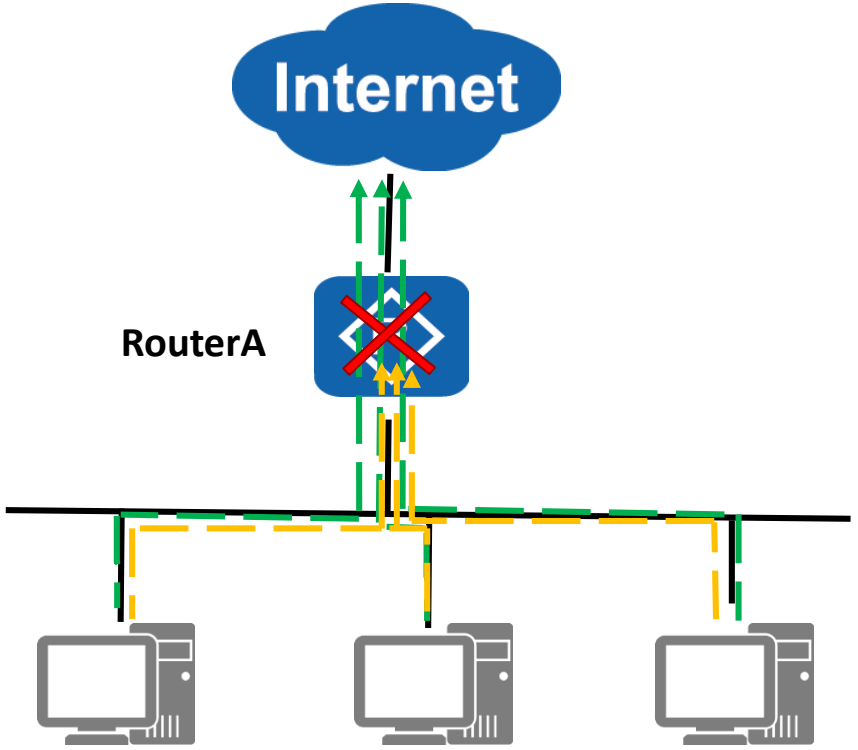
1 - Avantages et inconvénients de la redondance en réseau

2 - Protocole STP

3 – Protocole VRRP

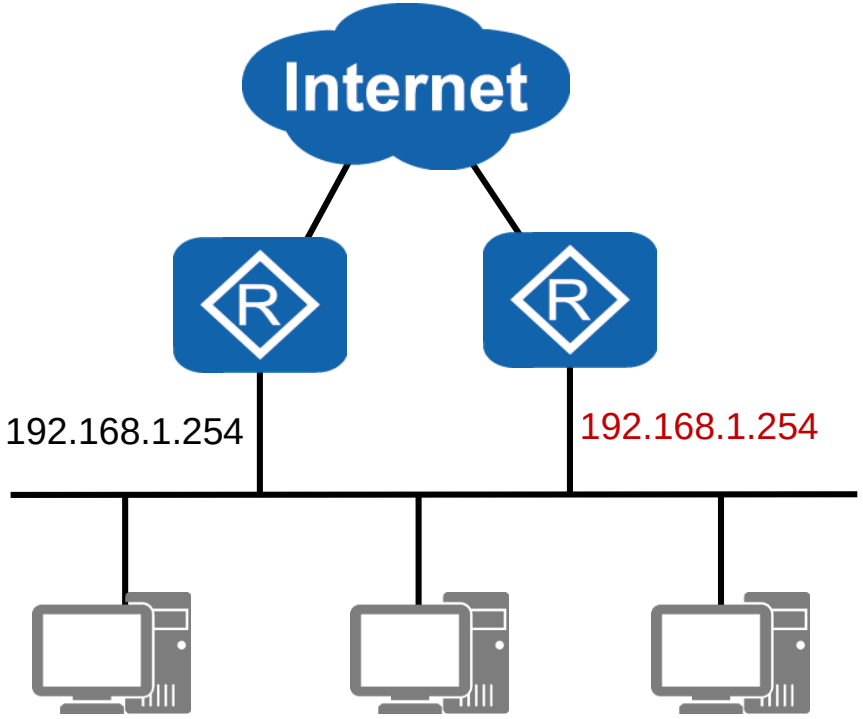
Limites d’une seule passerelle

Lorsque RouterA échoue, les périphériques qui utilisent RouterA comme passerelle ne peuvent pas se connecter à l’Internet.

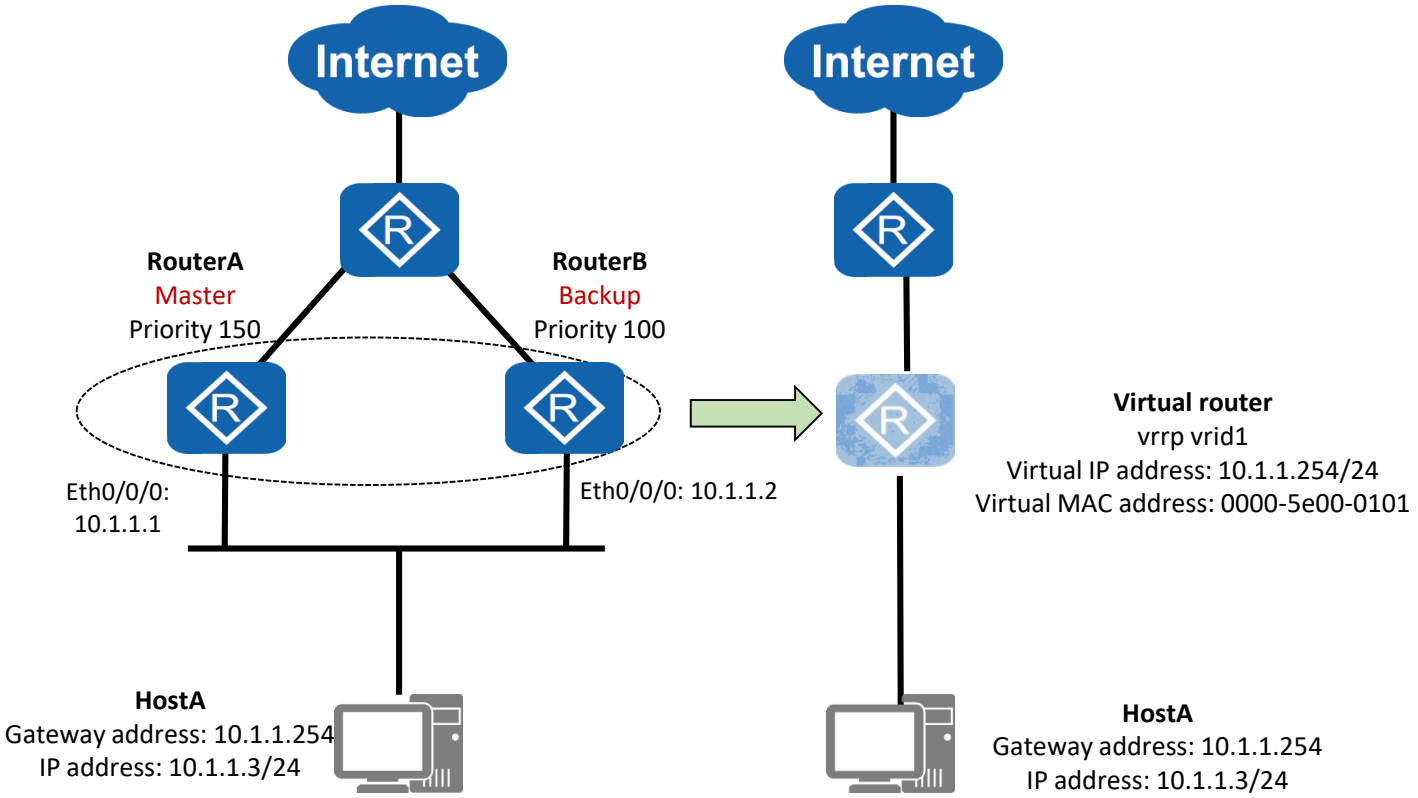


Problèmes de multiple passerelles

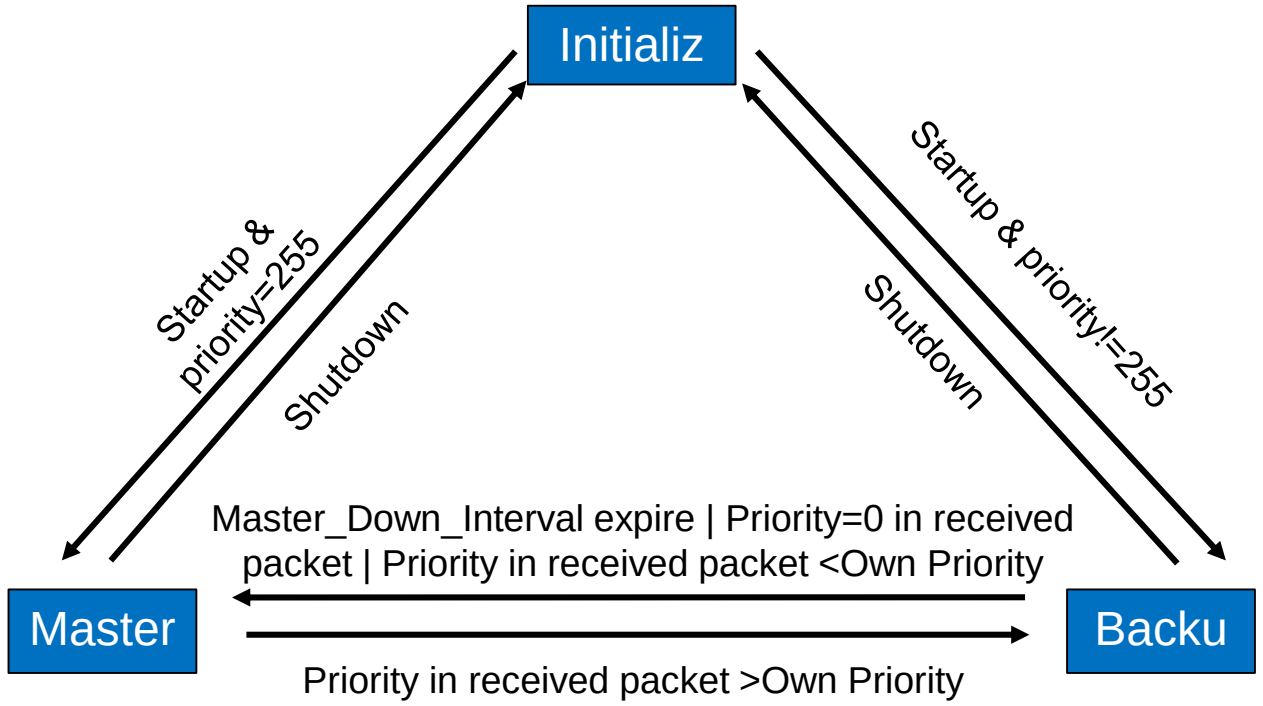
- Plusieurs passerelles peuvent être déployées pour implémenter la sauvegarde de passerelle.
- Cependant, de nombreux problèmes peuvent survenir. Les adresses IP des passerelles entrent en conflit et les hôtes utilisent fréquemment des sorties différentes.



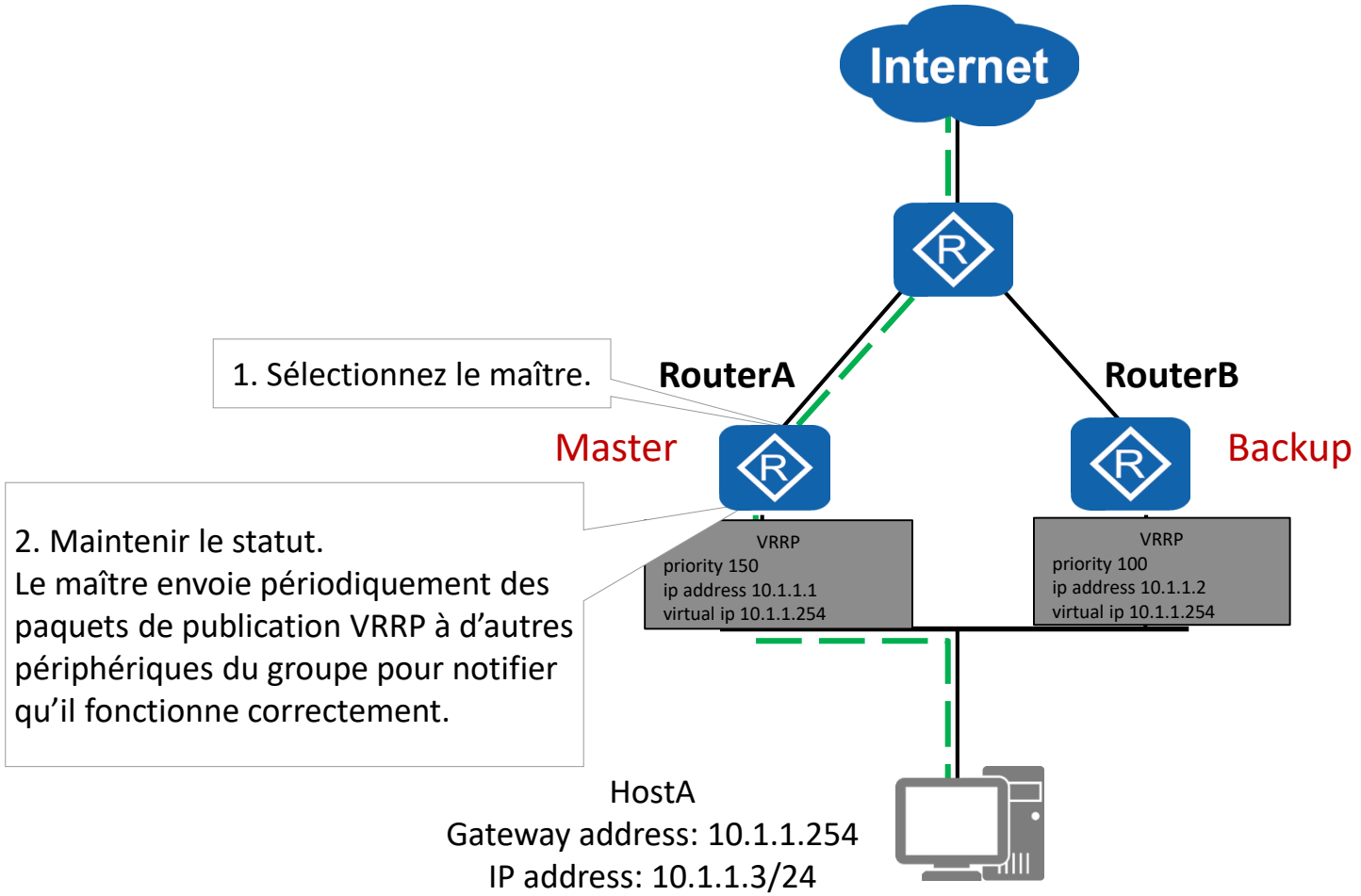
Protocole VRRP



Etat de machine



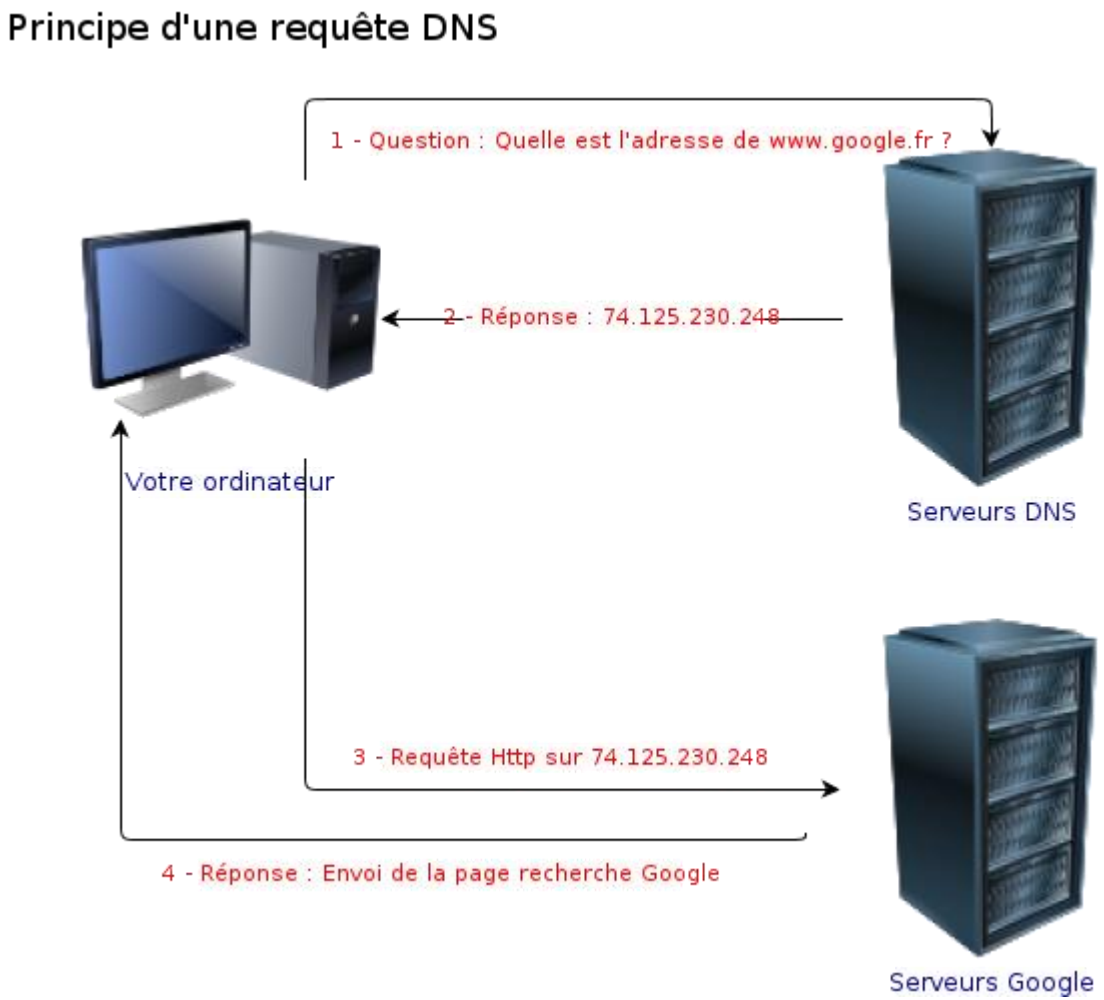
Etat de machine



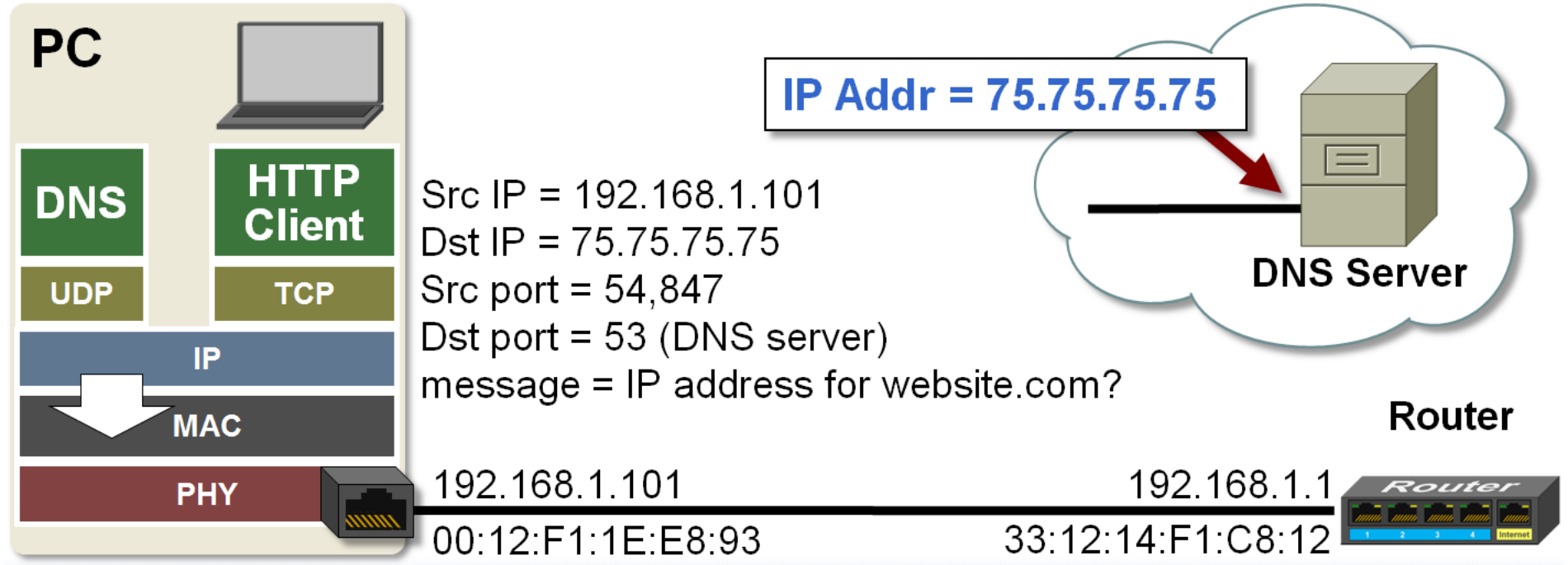
CHAPITRE 3

LES APPLICATIONS TCP-IP

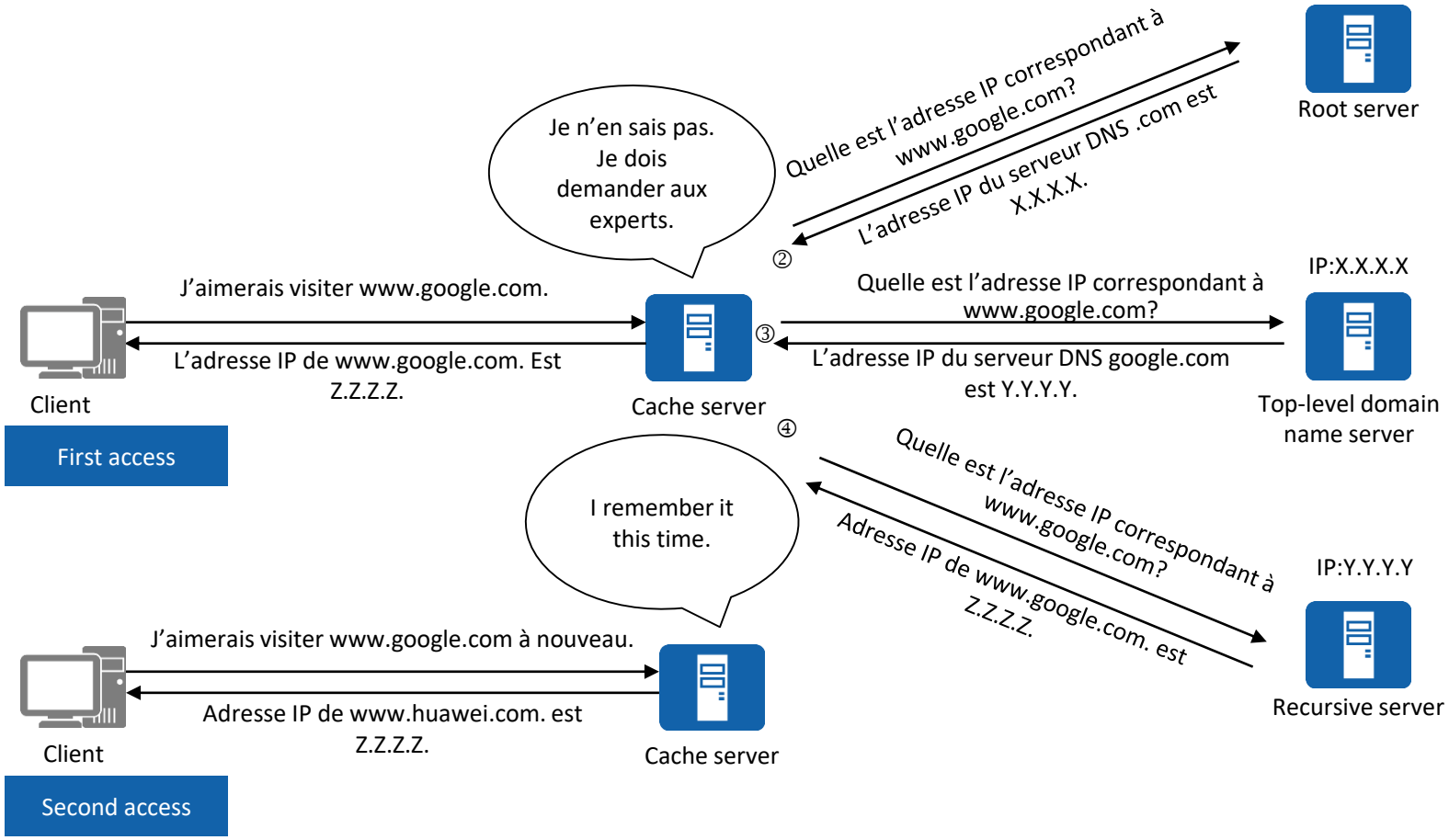
Service de nom : DNS



Service de nom : DNS



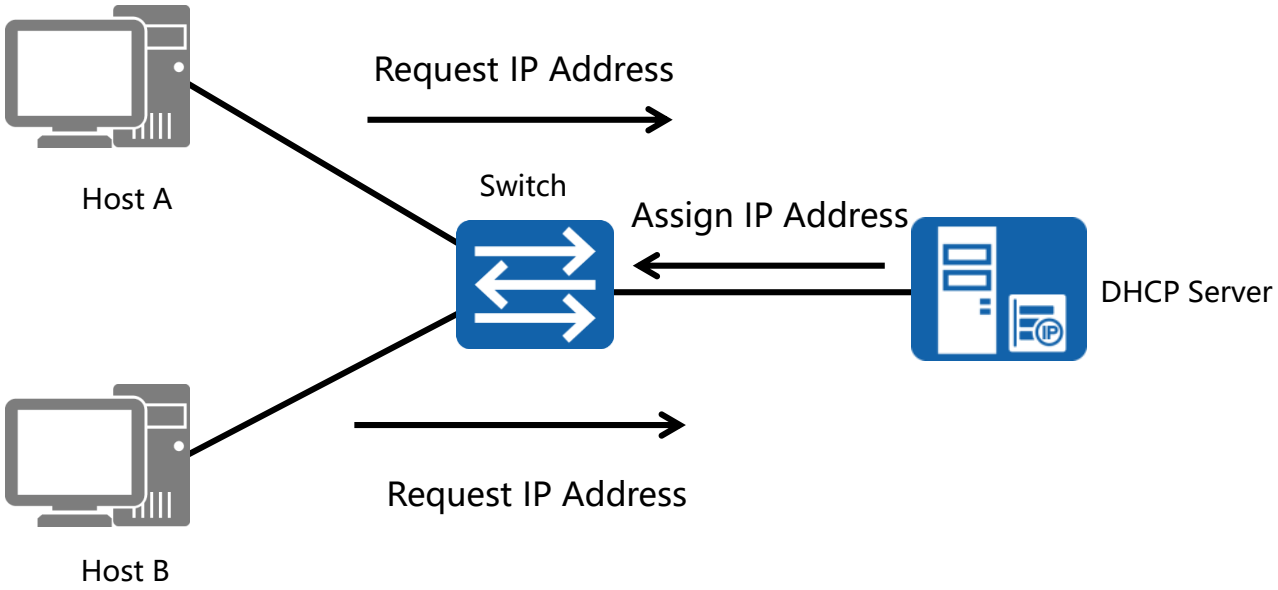
Service de nom : DNS



CHAPITRE 3

LES APPLICATIONS TCP-IP

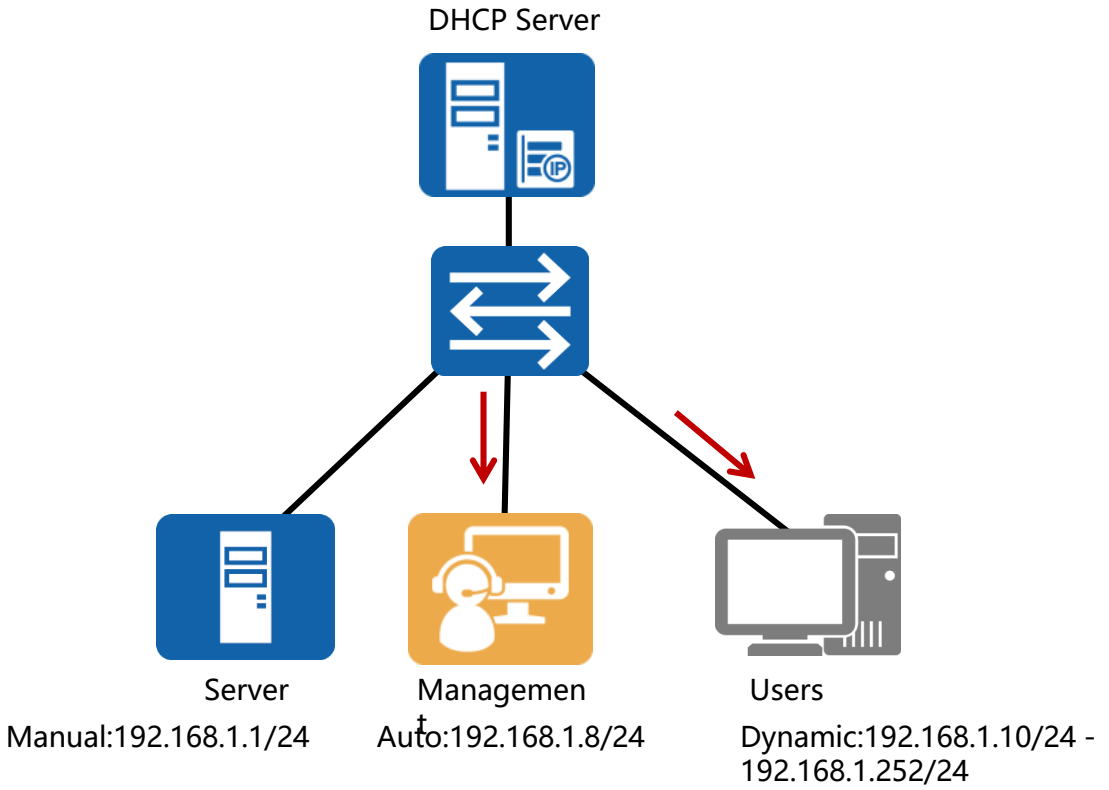
Protocole DHCP



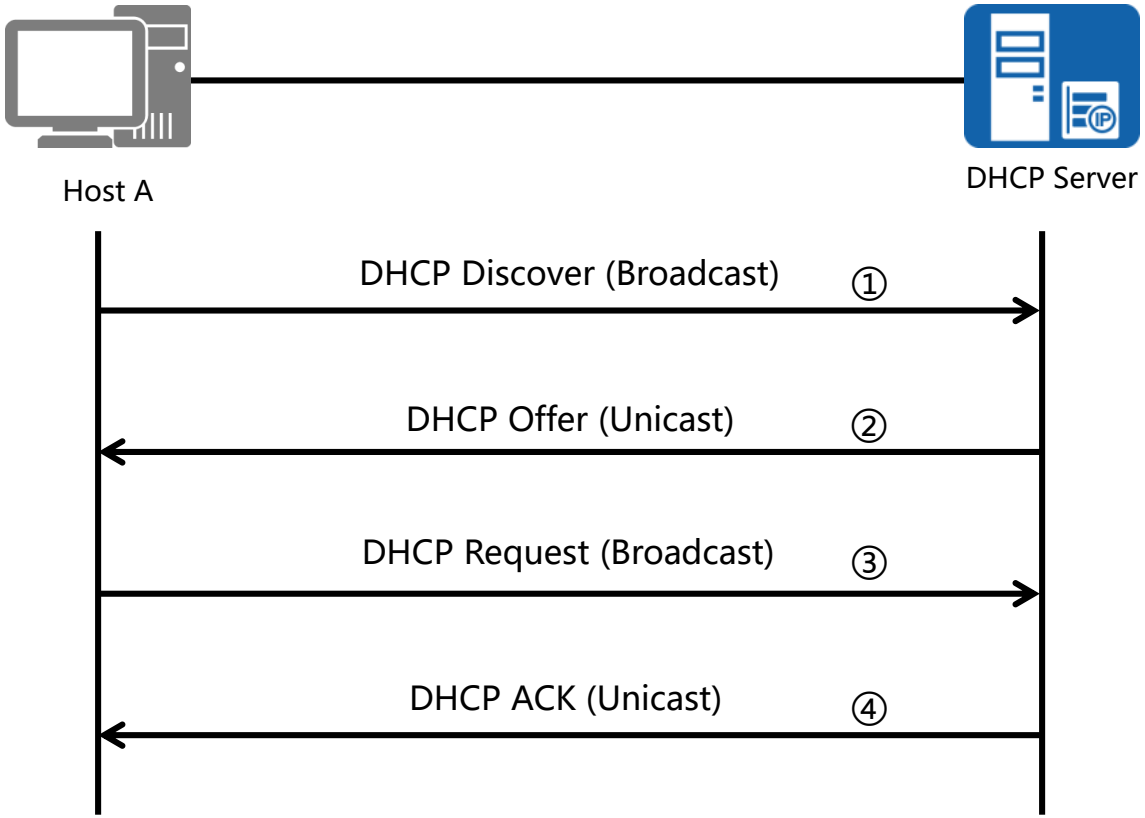
Les réseaux composés d'un grand nombre d'utilisateurs nécessitent un système central de gestion de l'attribution des adresses IP.

Protocole DHCP

Le DHCP soutient trois mécanismes d'attribution des adresses IP

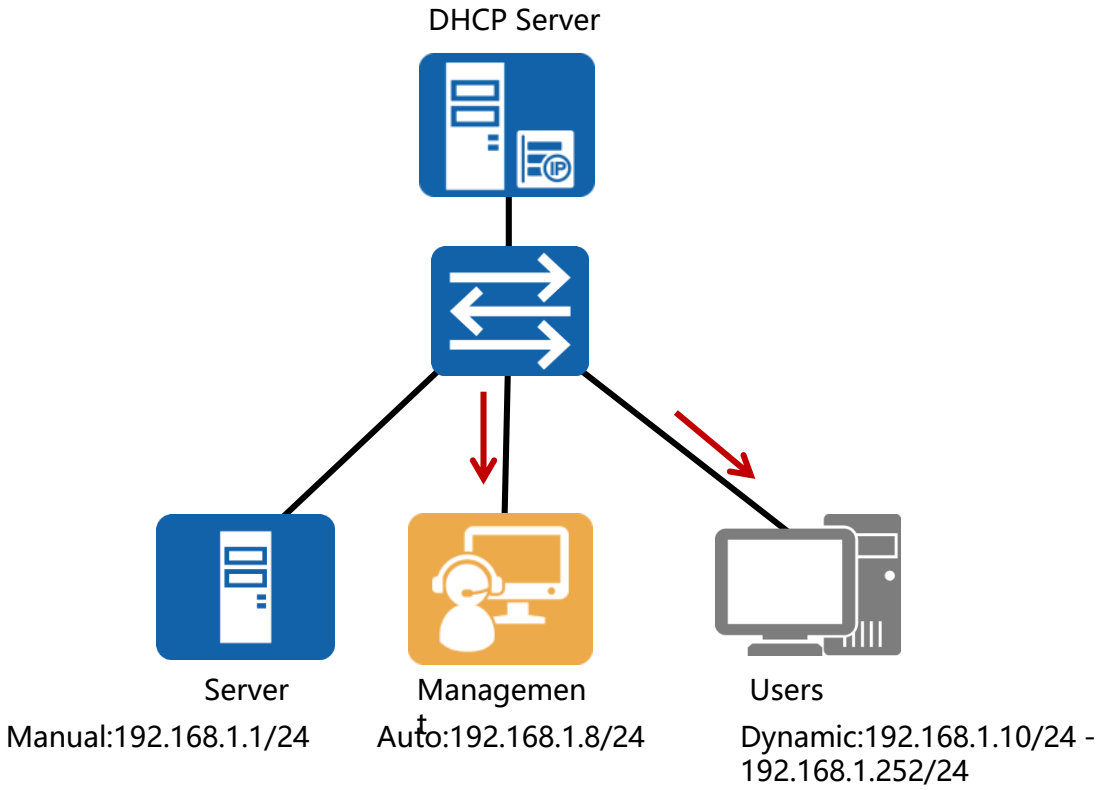


Protocole DHCP



Le DHCP soutient trois mécanismes d’attribution des adresses IP

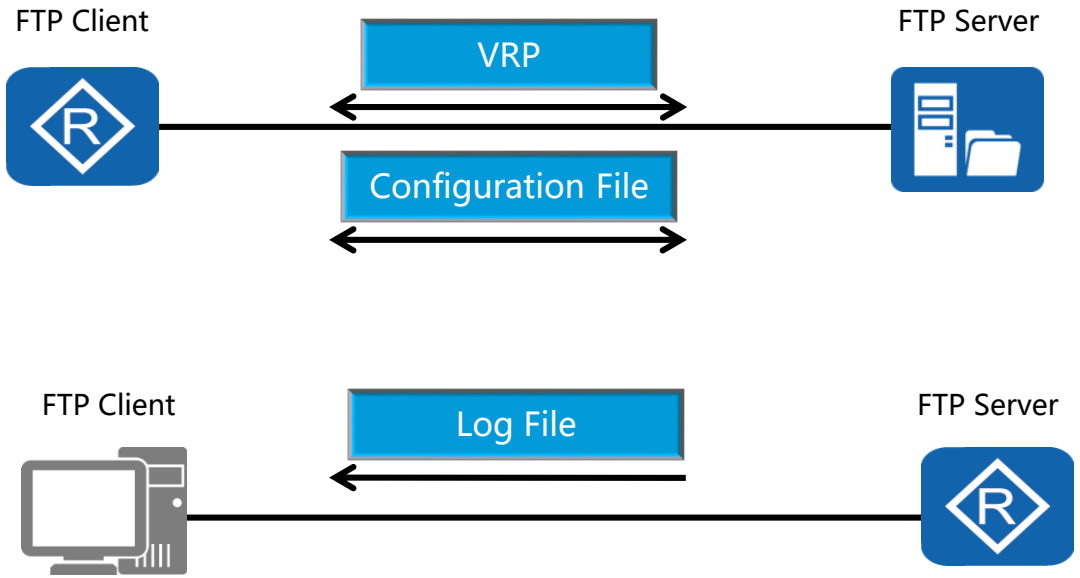
Le DHCP soutient trois mécanismes d’attribution des adresses IP



CHAPITRE 3

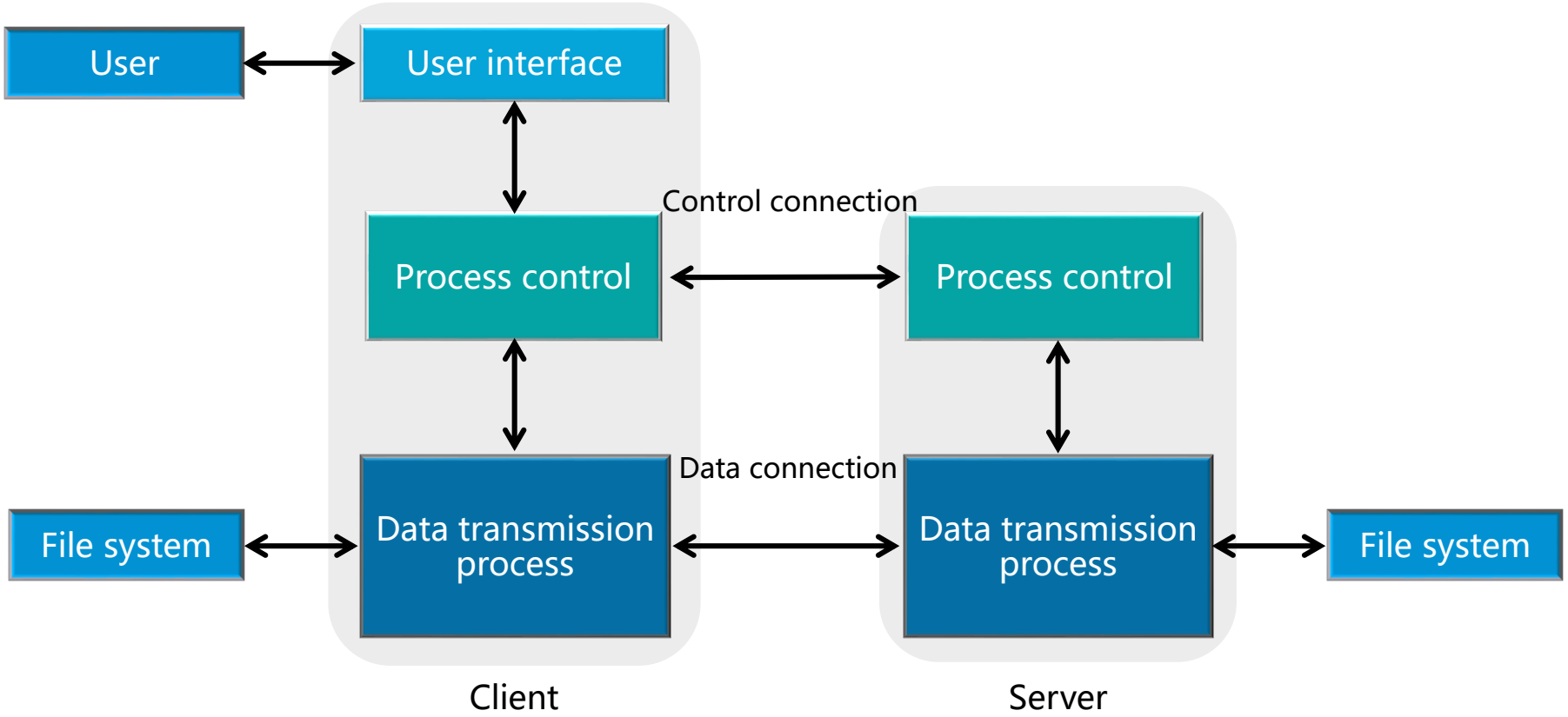
LES APPLICATIONS TCP-IP

Protocole de transfert FTP



FTP fournit un moyen efficace pour la sauvegarde et la récupération de fichiers importants.

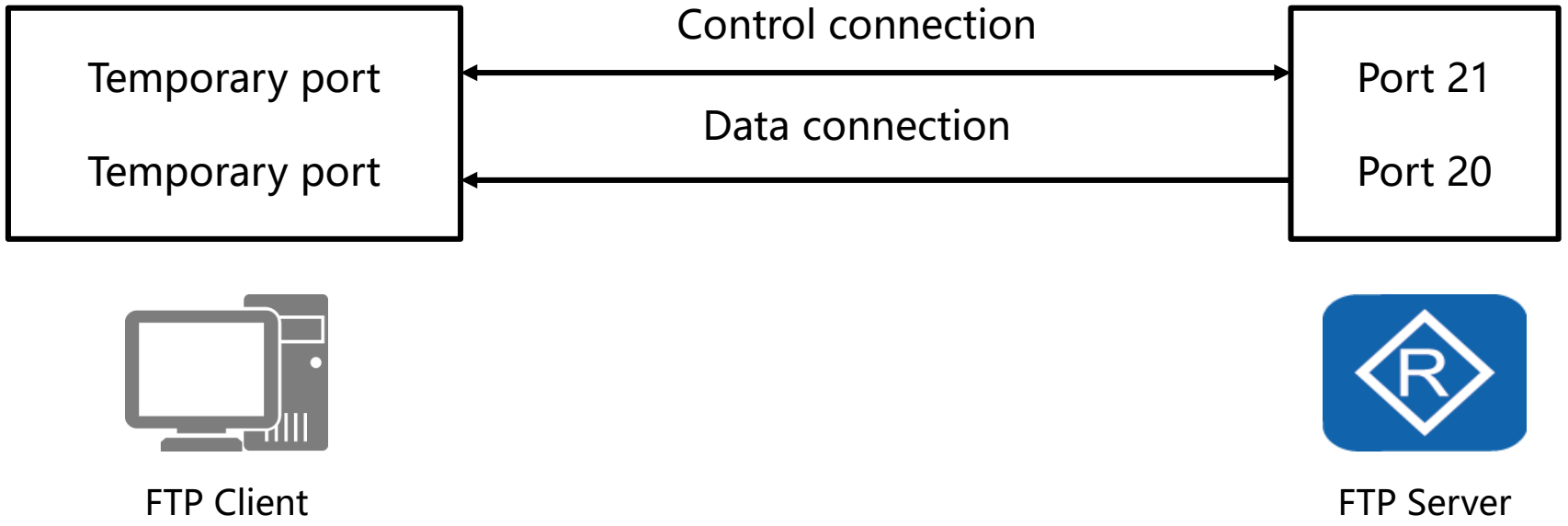
Protocole de transfert FTP



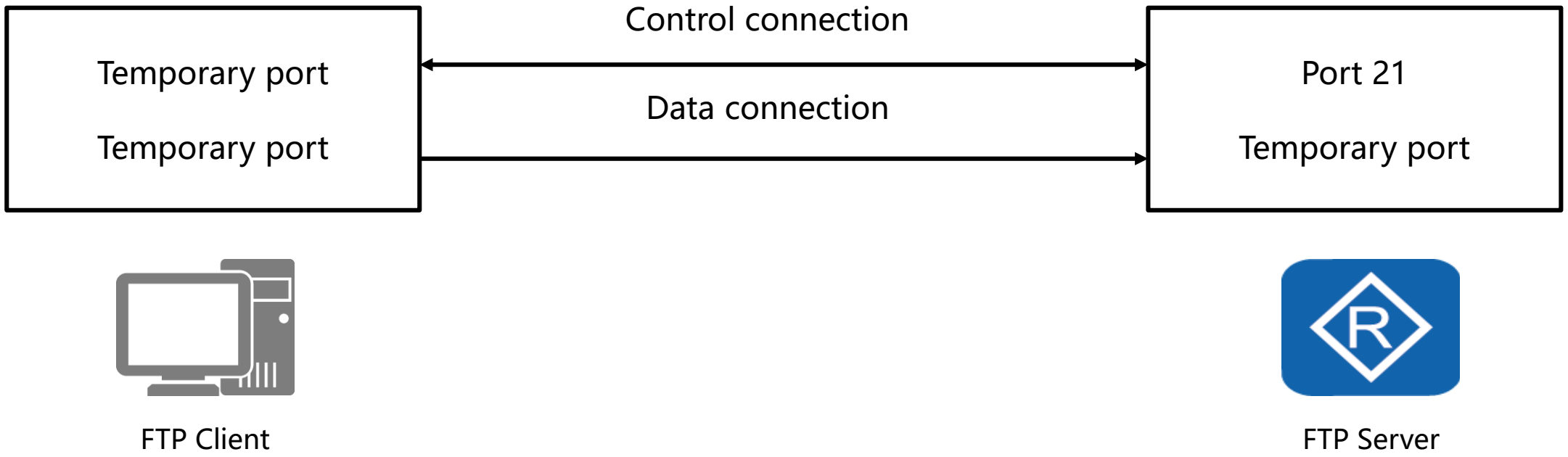
Protocole de transfert FTP

- FTP prend en charge deux modes: le mode actif et le mode passif. En mode actif, qui est utilisé par défaut, le client configure la connexion de contrôle et le serveur configure la connexion de données. En mode passif, le client configure les deux connexions. Les utilisateurs peuvent changer de mode via des commandes.

- Configuration de la connexion FTP en mode actif:



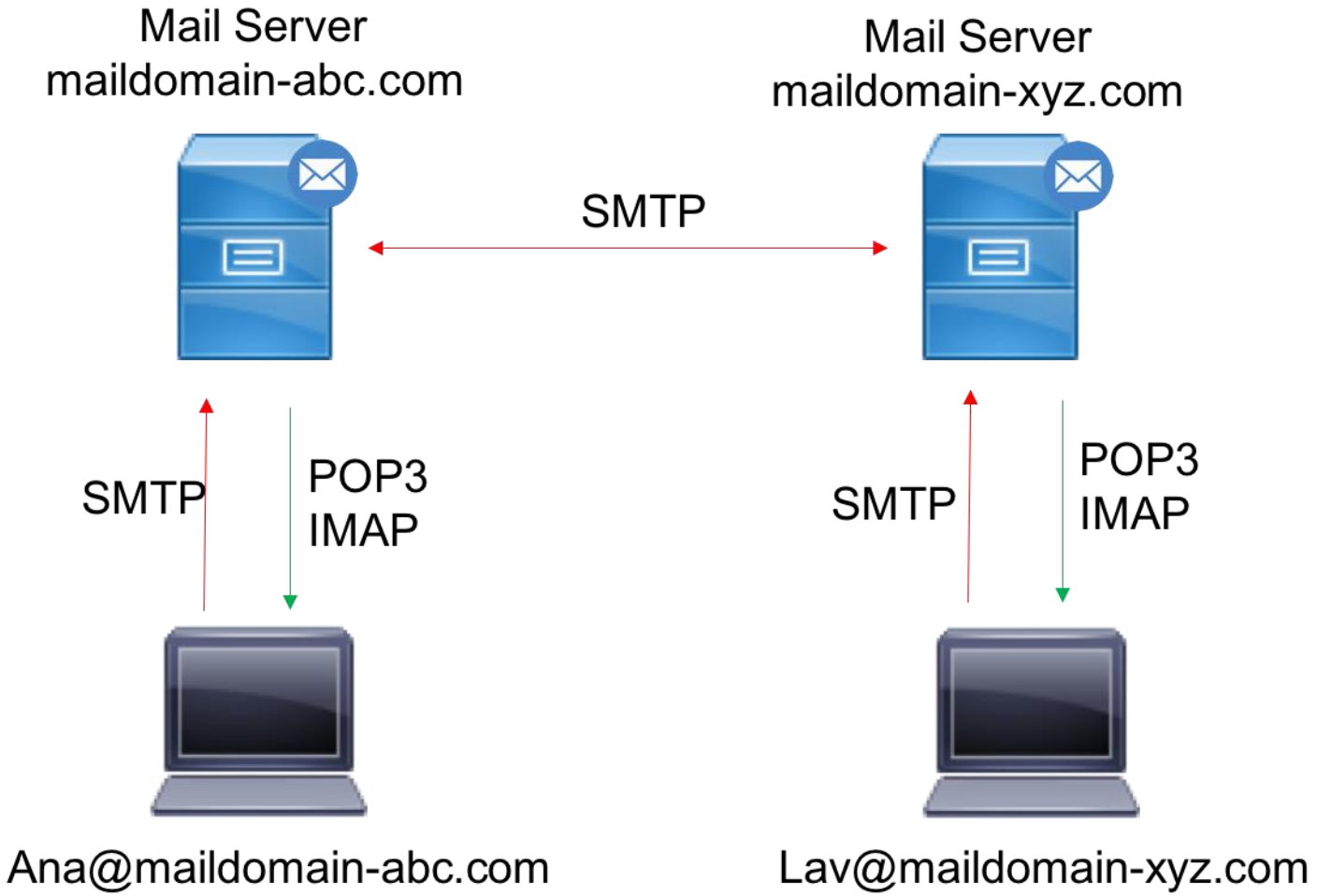
Configuration de la connexion FTP en mode passif



CHAPITRE 3

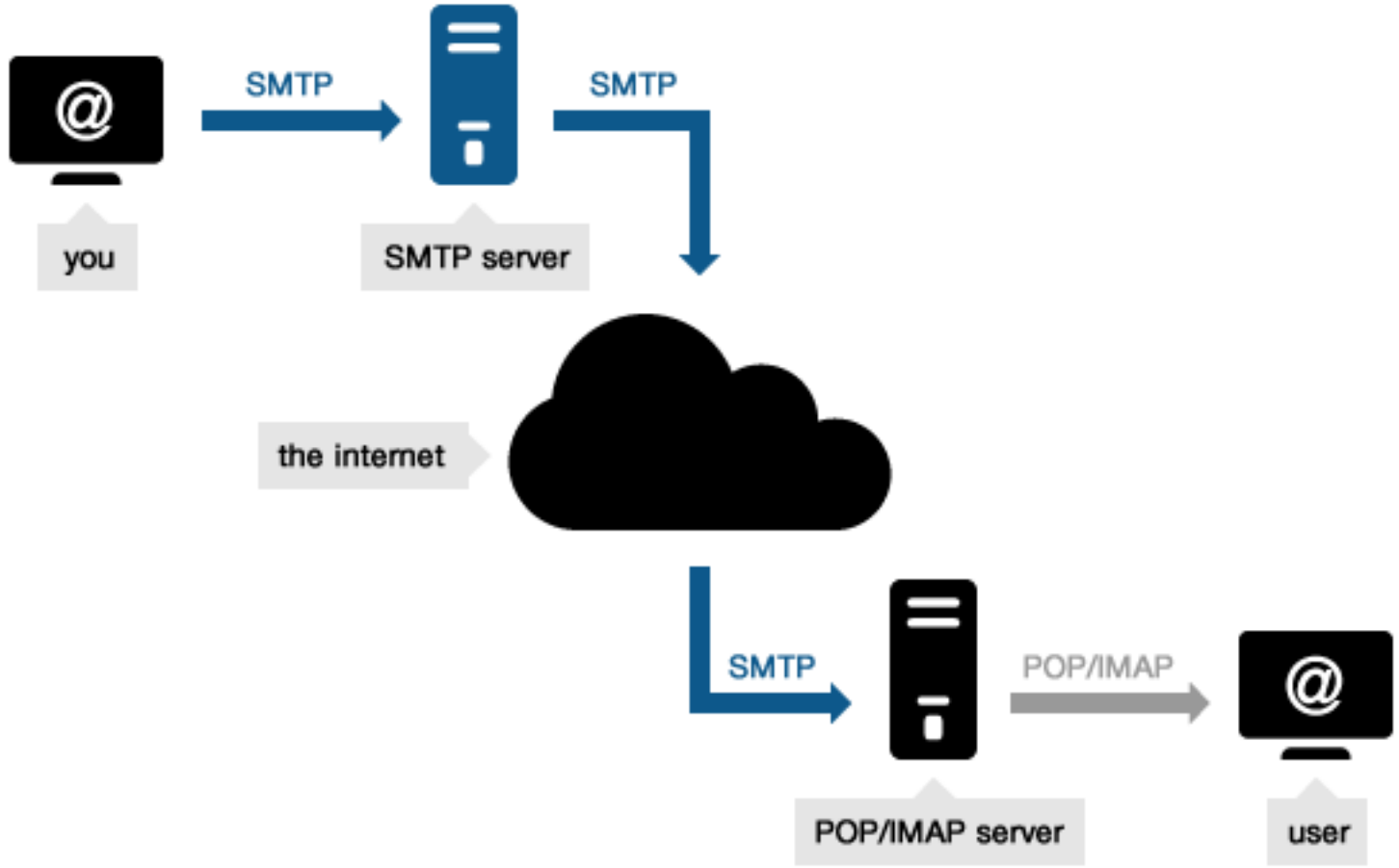
LES APPLICATIONS TCP-IP

Messagerie et les protocoles SMTP, POP et IMAP



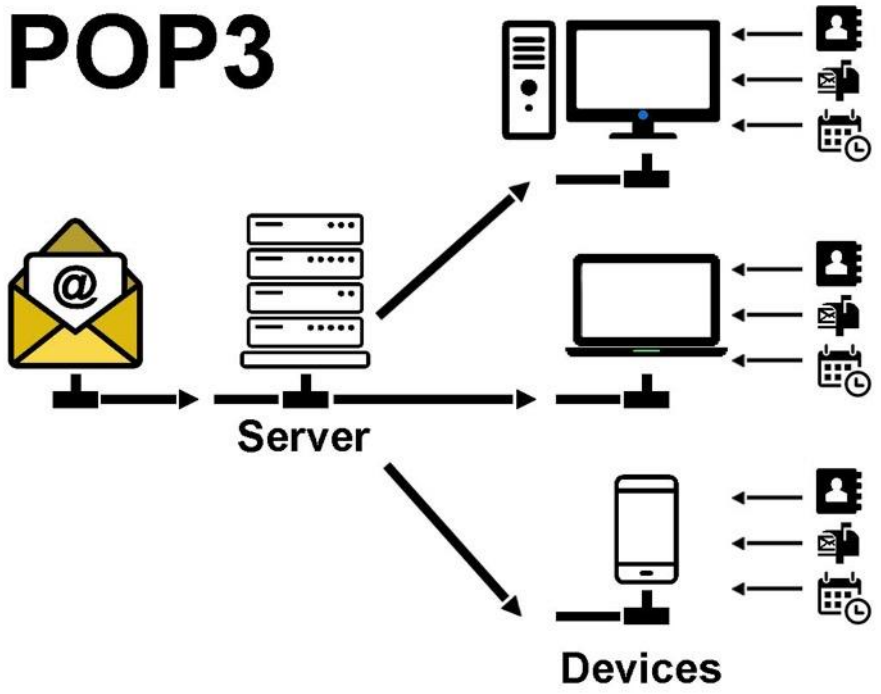
Messagerie et les protocoles SMTP, POP et IMAP

SMTP (Simple Mail Transfer Protocol) est une technologie qui facilite l'envoi d'e-mails d'un serveur à un autre jusqu'à ce qu'ils arrivent à la destination finale qui est la boîte de réception du destinataire.



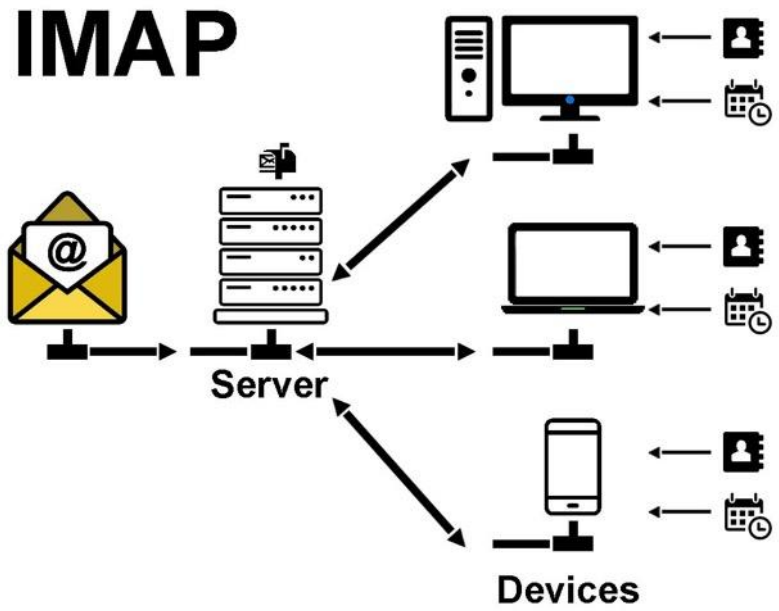
Messagerie et les protocoles SMTP, POP et IMAP

- POP3 est la méthode la plus ancienne et donc la plus connue pour recevoir des e-mails.
- Du fait de leur ancienneté, l'éventail des fonctionnalités est bien entendu quelque peu limité et limité à l'essentiel, à savoir la gestion des e-mails sur le serveur lui-même.

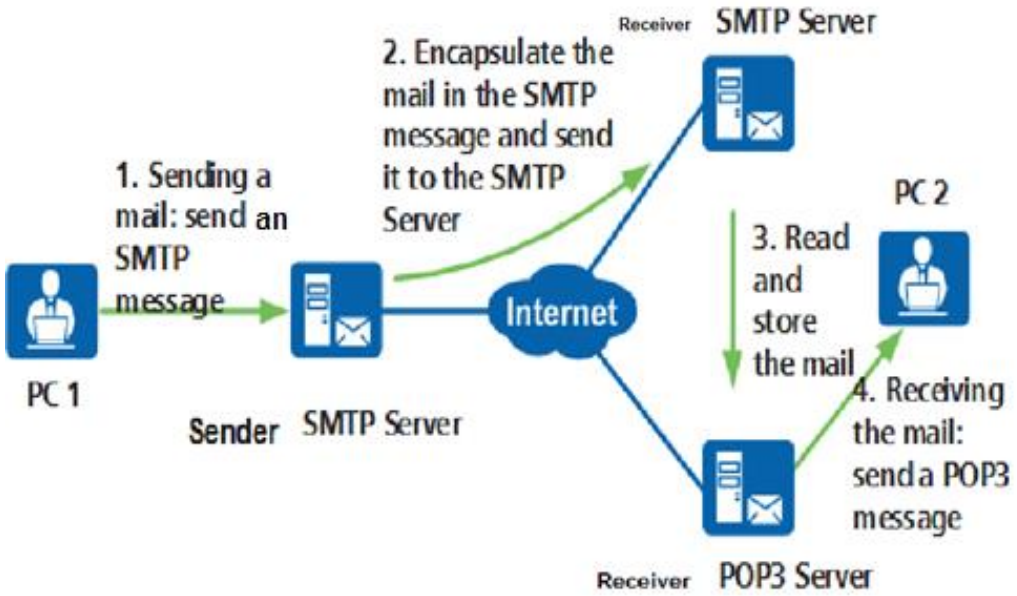


Messagerie et les protocoles SMTP, POP et IMAP

- IMAP peut être compris comme un développement ultérieur de POP3.
- Cette méthode est également en grande partie responsable de la réception des e-mails.
- Vous disposez d'un fournisseur de messagerie qui peut vous fournir un espace de stockage sur un serveur de messagerie.
- Pourtant, IMAP fonctionne un peu différemment de POP3.



Messagerie et les protocoles SMTP, POP et IMAP

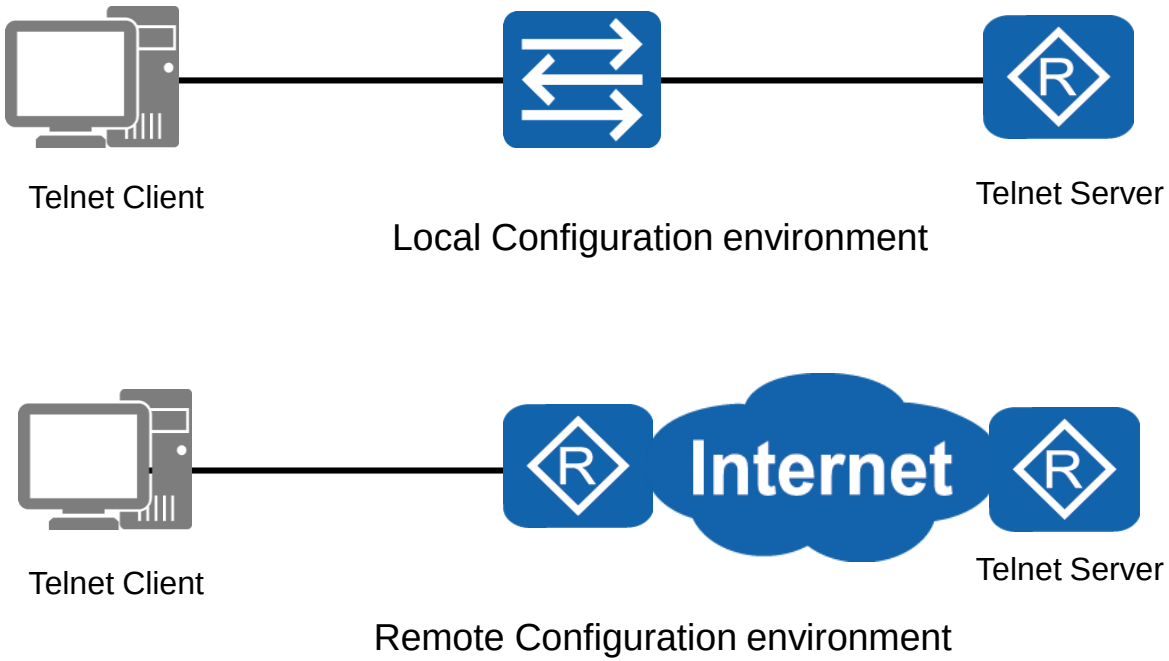


- SMTP définit la façon dont les PC envoient le courrier à un serveur SMTP et le transfert du courrier entre les serveurs SMTP.
- Post Office Protocol 3 (POP3) et IMAP (Internet Mail Access Protocol) spécifient comment les PC gèrent et téléchargent le courrier sur le serveur de messagerie via un logiciel client.
- SMTP et POP3 (ou IMAP) sont déployés sur le serveur de messagerie par un administrateur et un logiciel client de messagerie (tel que Microsoft Outlook ou Foxmail) est installé sur le PC d'un utilisateur.

CHAPITRE 4

SÉCURISER LES COMMUTATEURS

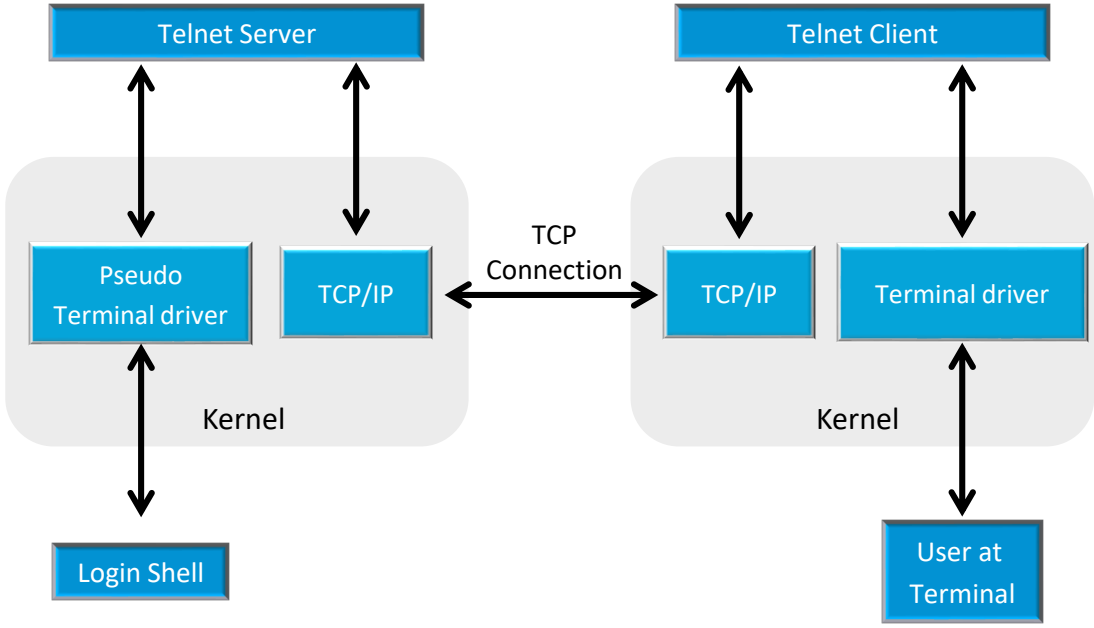
Protocoles Telnet et SSH



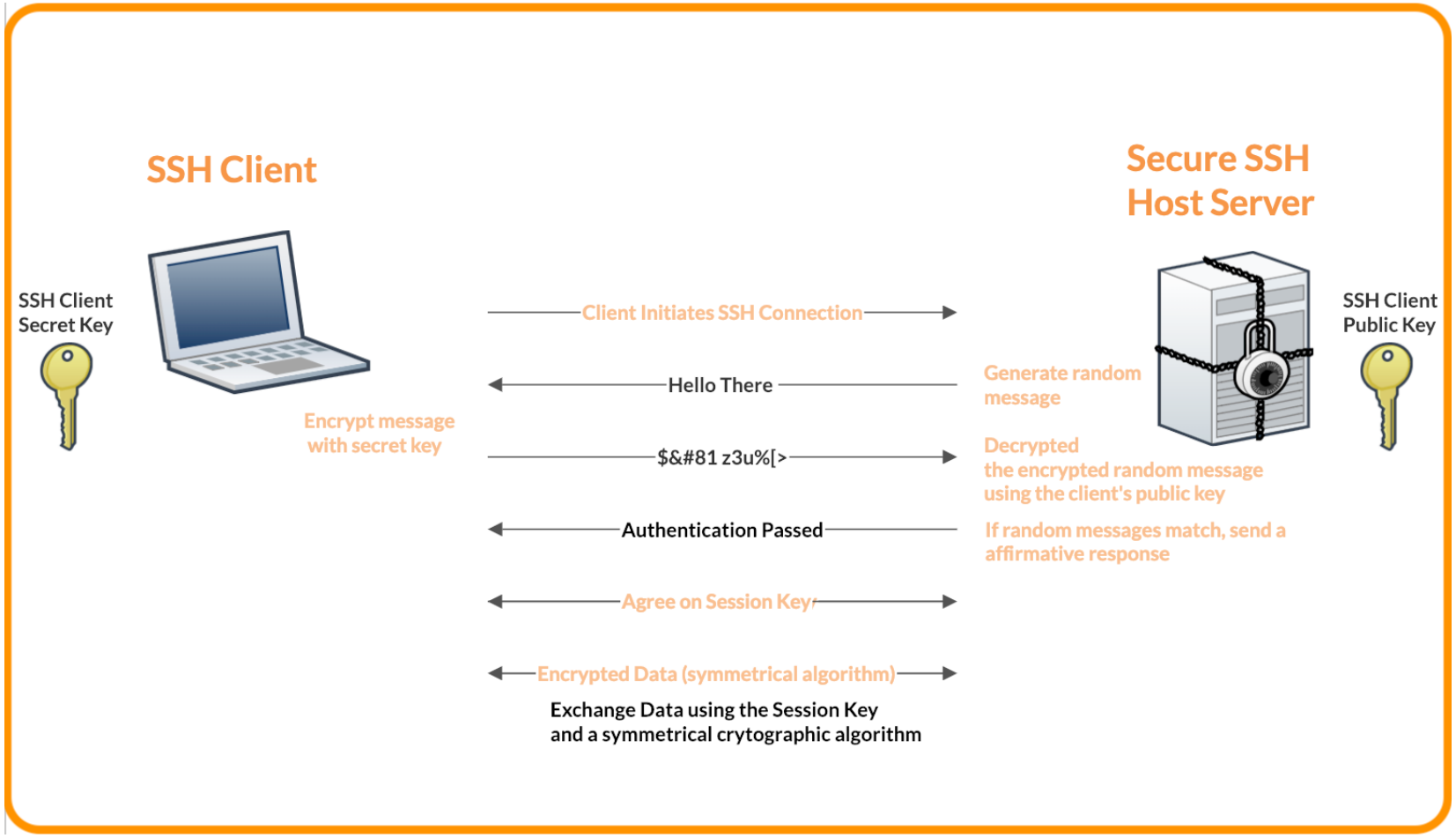
Telnet représente un programme d'émulation de terminal bidirectionnel basé sur du texte pour une utilisation sur des réseaux locaux et distants.

L’architecture Telnet

L’architecture Telnet montre comment les utilisateurs sont interprétées par les pilotes de terminal avant la livraison via TCP qui s’ensuit.



Protocoles Telnet et SSH



CHAPITRE 4

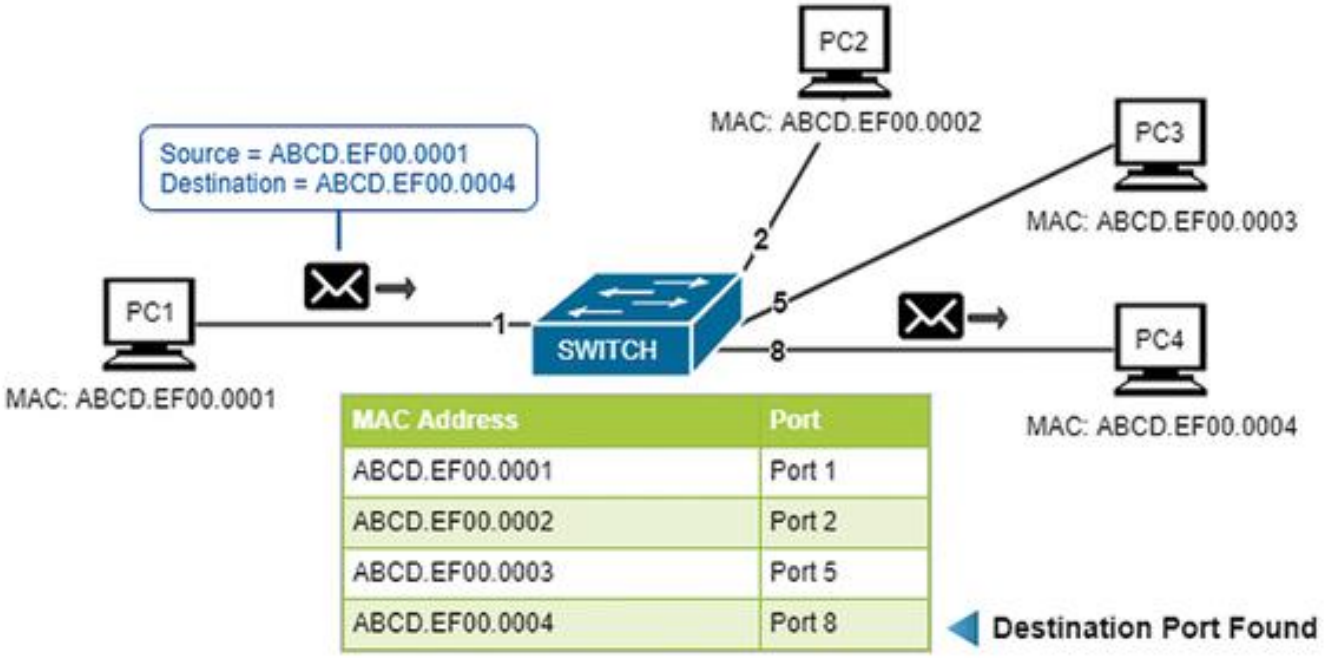
SÉCURISER LES COMMUTATAEURS

1 - Protocoles Telnet et SSH

2 - Sécurisation des ports d'un commutateur

3 – Protocoles de sécurité sans fil

Sécurisation des ports d'un commutateur



MAC Address	Port
ABCD.EF00.0001	Port 1
ABCD.EF00.0002	Port 2
ABCD.EF00.0003	Port 5
ABCD.EF00.0004	Port 8

A quoi sert la sécurité de port ?

A limiter le nombre d'adresse MAC dernière un port
A se protéger du MAC Address Flooding
A restreindre l'accès à certaines adresses MAC
A désactiver le port / envoyer des logs en cas de violation

CHAPITRE 4

SÉCURISER LES COMMUTATAEURS

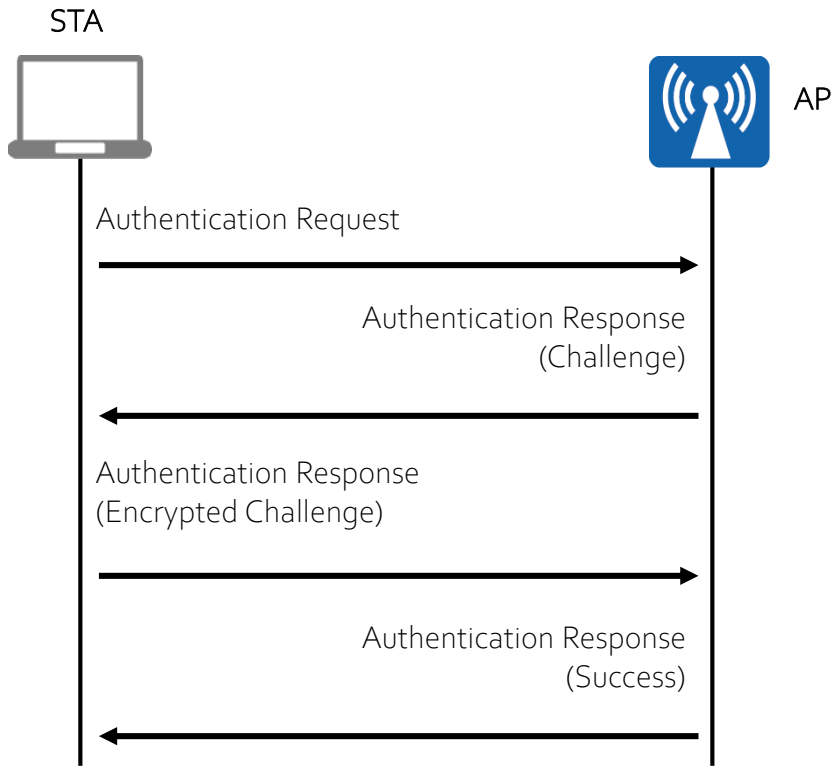
1 - Protocoles Telnet et SSH

2 - Sécurisation des ports d’un commutateur

3 – Protocoles de sécurité sans fil

Authentification clé partagée

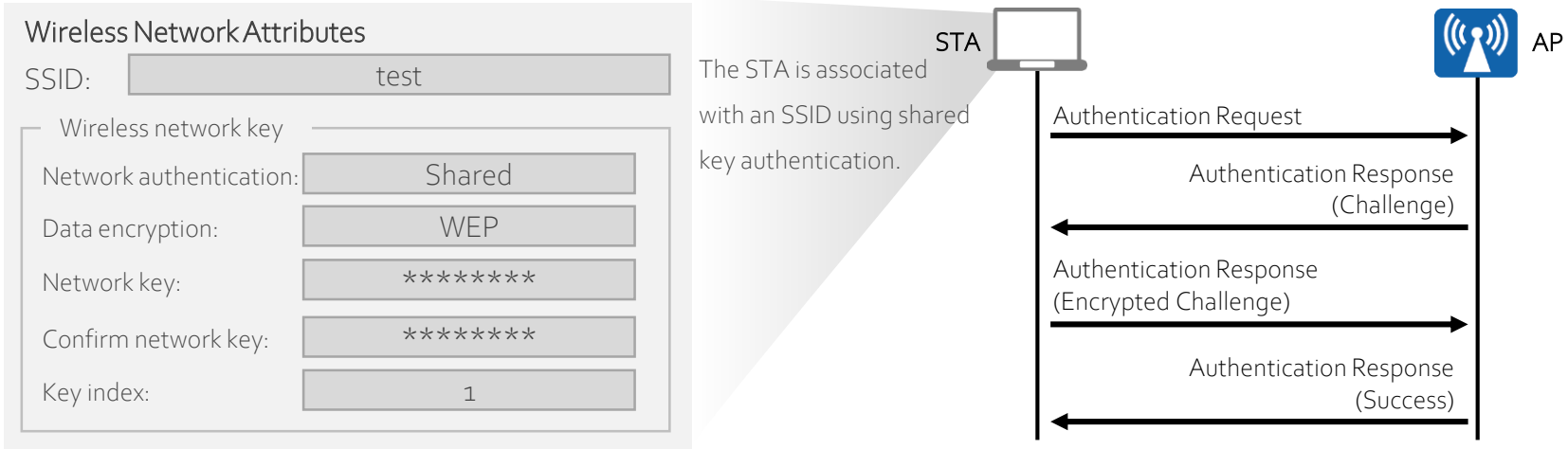
- L'authentification des clés partagées exige qu'un STA et un AP aient la même clé préconfigurée.
- Dans ce mode d'authentification, l'AP vérifie si sa clé est la même que celle sur le STA lors de l'authentification des liens. Si c'est le cas, l'authentification est réussie. Sinon, le STA échoue à l'authentification.



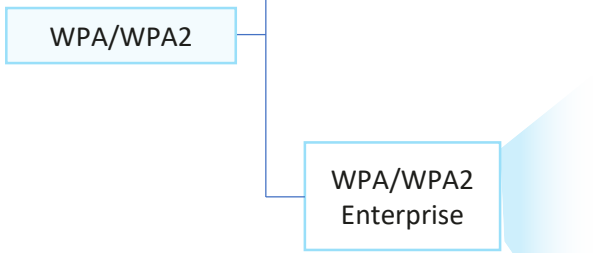
Politique de sécurité d'authentification d'accès : WEP

- Wired Equivalent Privacy (WEP) est un mécanisme de sécurité défini dans IEEE 802.11 pour empêcher l'interception des données transmises par les utilisateurs autorisés sur un WLAN.

- WEP utilise l'algorithme Rivest Cipher 4 (RC4) et une clé statique pour chiffrer les données. Toutes les STA associées à la même SSID utilisent la même clé pour adhérer à un WLAN.



Politique de sécurité d'authentification d'accès

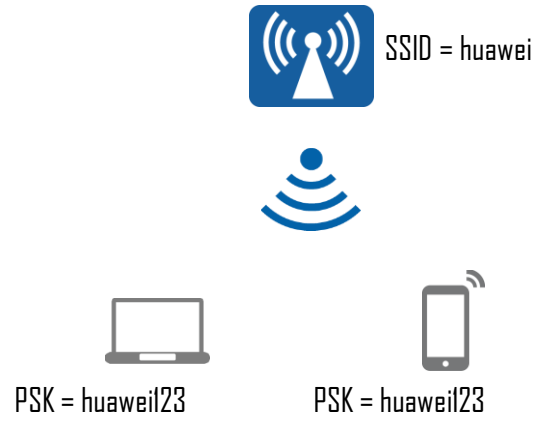


- Pour les WLAN de petite ou moyenne taille, le déploiement d'un serveur d'authentification dédié est coûteux et difficile à maintenir.
- WPA/WPA2-Personal utilise des clés pré-partagées (WPA/WPA2-PSK) pour une mise en œuvre et une gestion plus simples.
- Aucun serveur d'authentification dédié n'est requis. Seule une clé pré-partagée doit être saisie à l'avance sur chaque nœud WLAN (comme le serveur WLAN, le routeur sans fil et l'adaptateur réseau). Un client WLAN peut accéder au WLAN si sa clé pré-partagée est la même que celle configurée sur le nœud WLAN.
- La clé pré-partagée n'est utilisée que pour l'authentification, mais pas pour le chiffrement; par conséquent, il n'apportera pas de risques de sécurité que l'authentification 802.11 clé partagée.

- Le mode authentification WPA/WPA2-802.1X est utilisé.
- Le serveur RADIUS et le protocole d'authentification extensible (PAE) sont utilisés pour l'authentification.
- Les utilisateurs fournissent les informations requises pour l'authentification, y compris le nom d'utilisateur et le mot de passe, et sont authentifiés par un serveur d'authentification (généralement un serveur RADIUS).
- Les WLAN d'entreprise à grande échelle utilisent généralement WPA/WPA2-Enterprise pour l'authentification.

Authentification PSK et PPSK

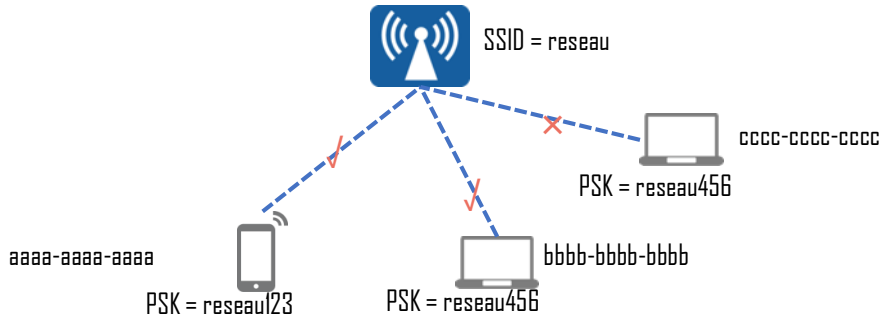
PSK



- L'authentification WPA/WPA2-PSK exige que la même clé pré-partagée soit configurée sur un client sans fil et un serveur sans fil (comme un AP).
- Tous les clients connectés à un SSID spécifié utilisent la même clé, ce qui peut entraîner des risques de sécurité.

PPSK

MAC	Password
aaaa-aaaa-aaaa	reseau123
bbbb-bbbb-bbbb	reseau456



- L'authentification WPA/WPA2-PPSK hérite des avantages de l'authentification WPA/WPA2-PSK et est facile à déployer.
- En outre, l'authentification WPA/WPA2-PPSK fournit différentes clés pré-partagées pour différents clients, améliorant ainsi la sécurité du réseau.
- Les utilisateurs du même SSID peuvent avoir des clés différentes.

PARTIE 3

METTRE EN ŒUVRE LE ROUTAGE D'UN RÉSEAU D'ENTREPRISE

CHAPITRE 1

ROUTAGE D'UN RÉSEAU D'ENTREPRISE

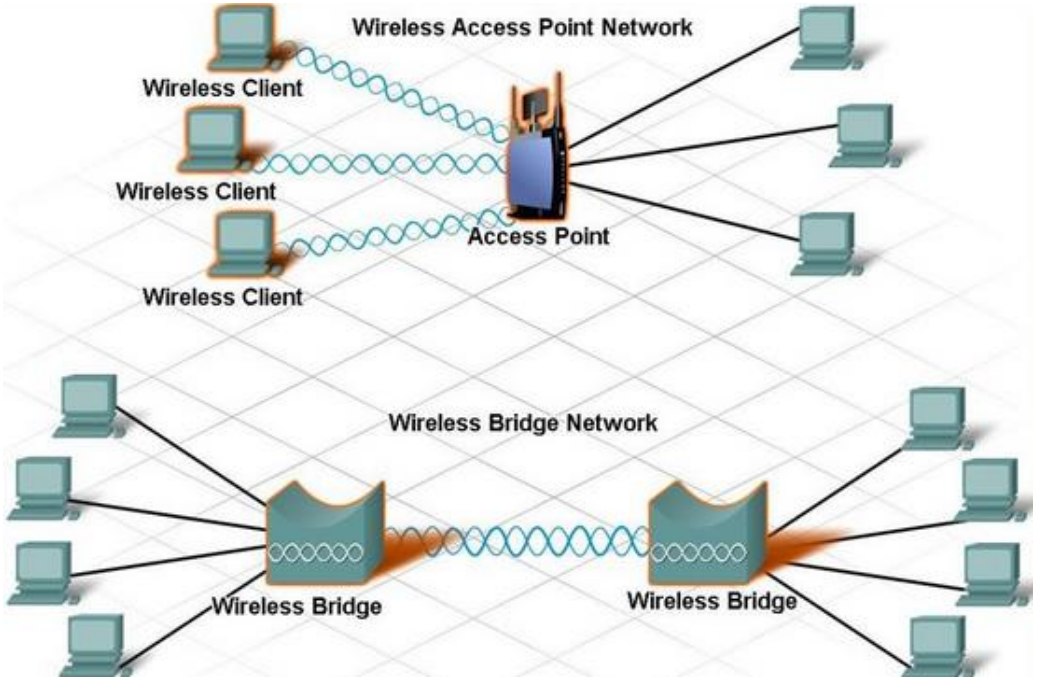
1 - Composants de WLAN

2 - Fonctionnement d'un réseau LAN

Composants de WLAN

Autonomous Solutions		Lightweight Solutions
Autonomous access points	Access Points	Lightweight access points
Wireless Domain Services (WDS)	Control	WLAN Controller
WLAN Solution Engine (WLSE)	WLAN Management	WLAN Control System (WCS)
PoE switches, routers	Network Infrastructure	PoE switches, routers
DHCP, DNS, AAA	Network Services	DHCP, DNS, AAA

Composants de WLAN



CHAPITRE 1

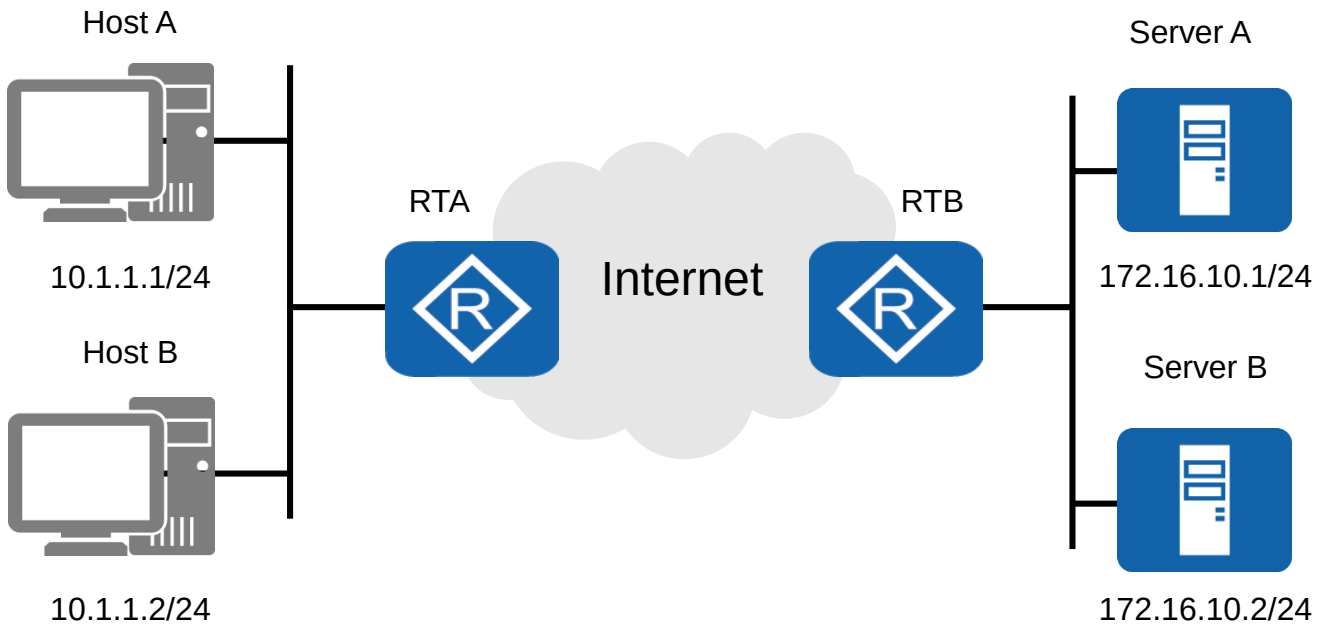
ROUTAGE D'UN RÉSEAU D'ENTREPRISE

1 - Composants de WLAN

2 - Fonctionnement d'un réseau LAN

Fonctionnement d’un réseau LAN

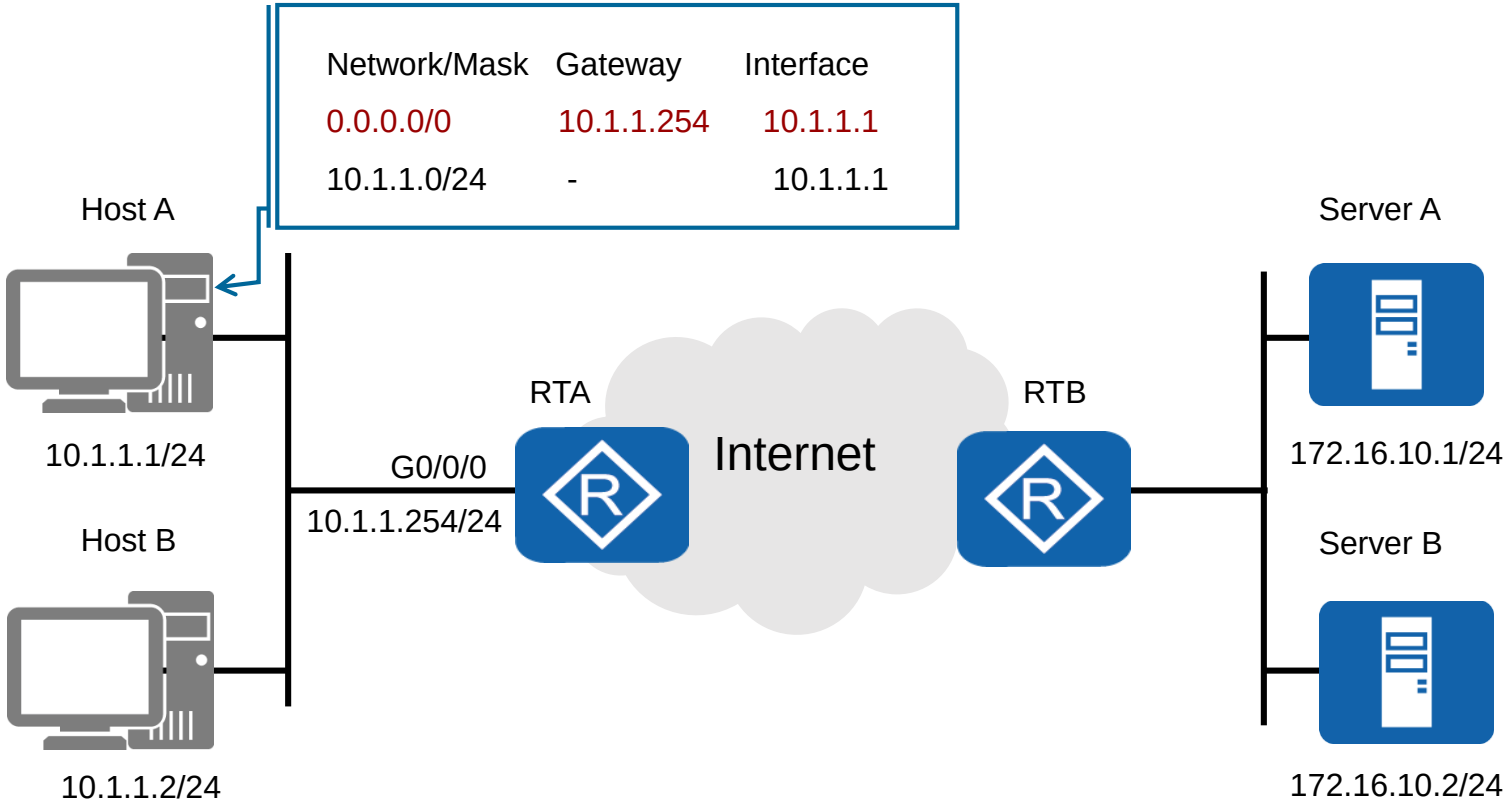
Scénario



Le transfert de données peut être local ou distant, mais le processus général de transfert est le même

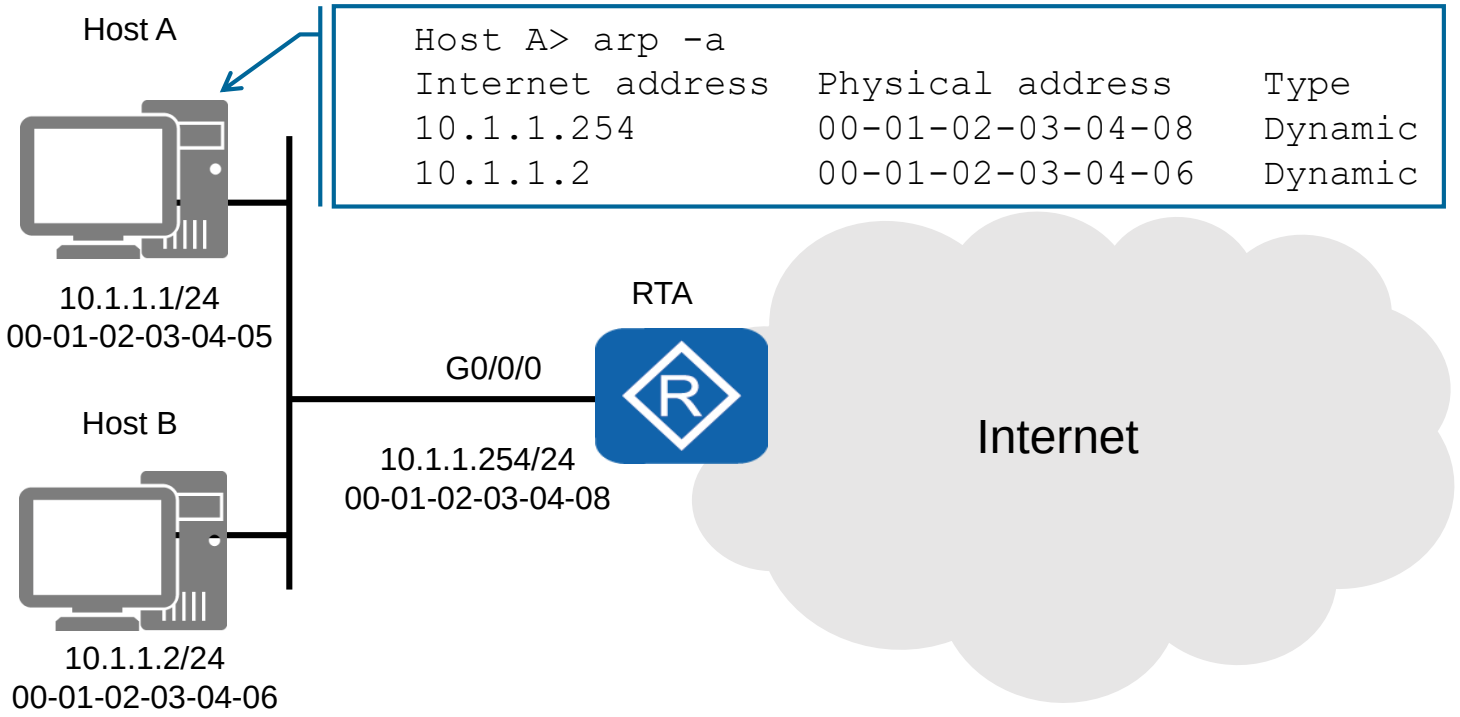
Fonctionnement d’un réseau LAN

Phase 1: découverte de chemin



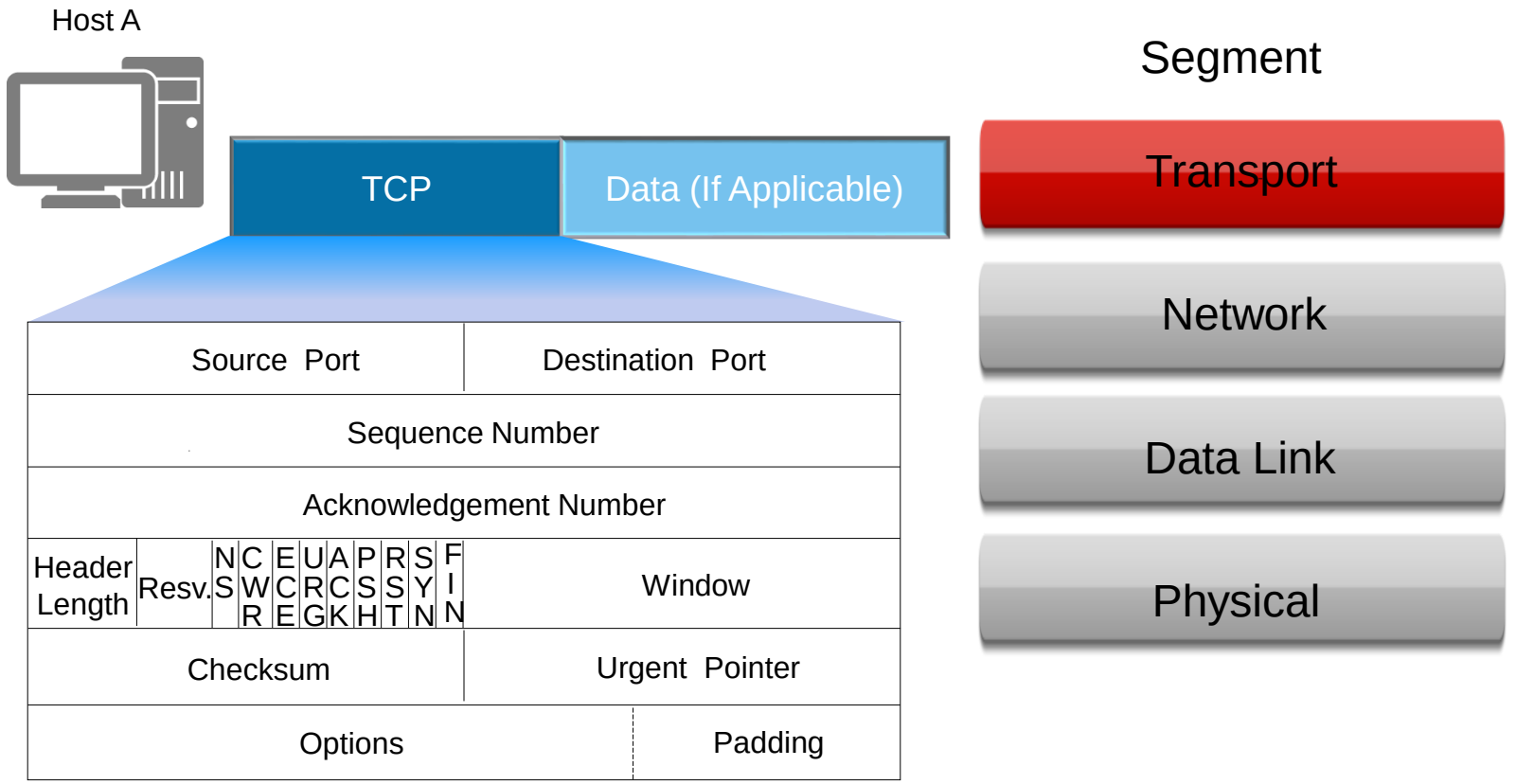
Fonctionnement d’un réseau LAN

Phase 2: ARP



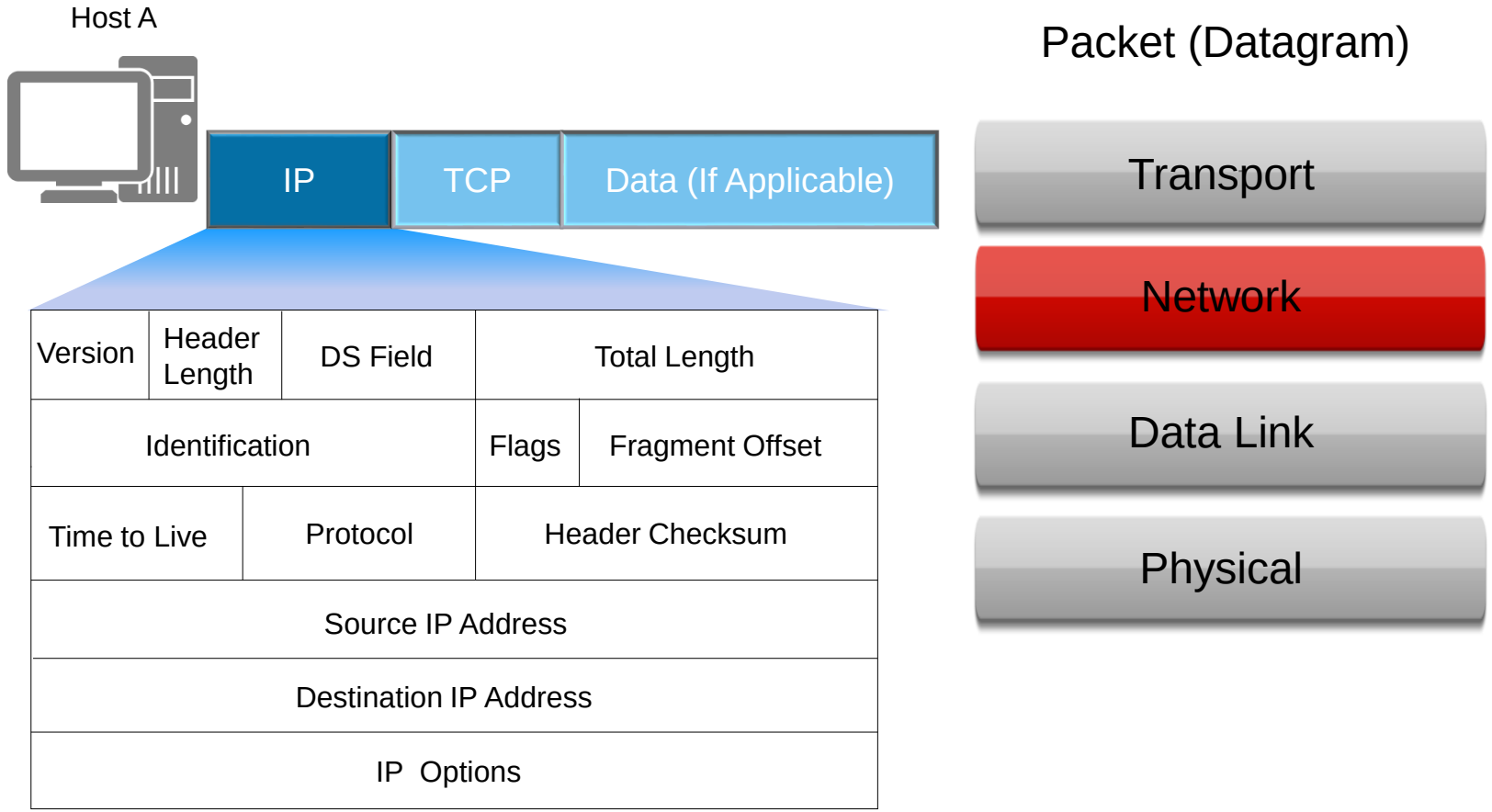
Fonctionnement d’un réseau LAN

Phase 3: encapsulation TCP



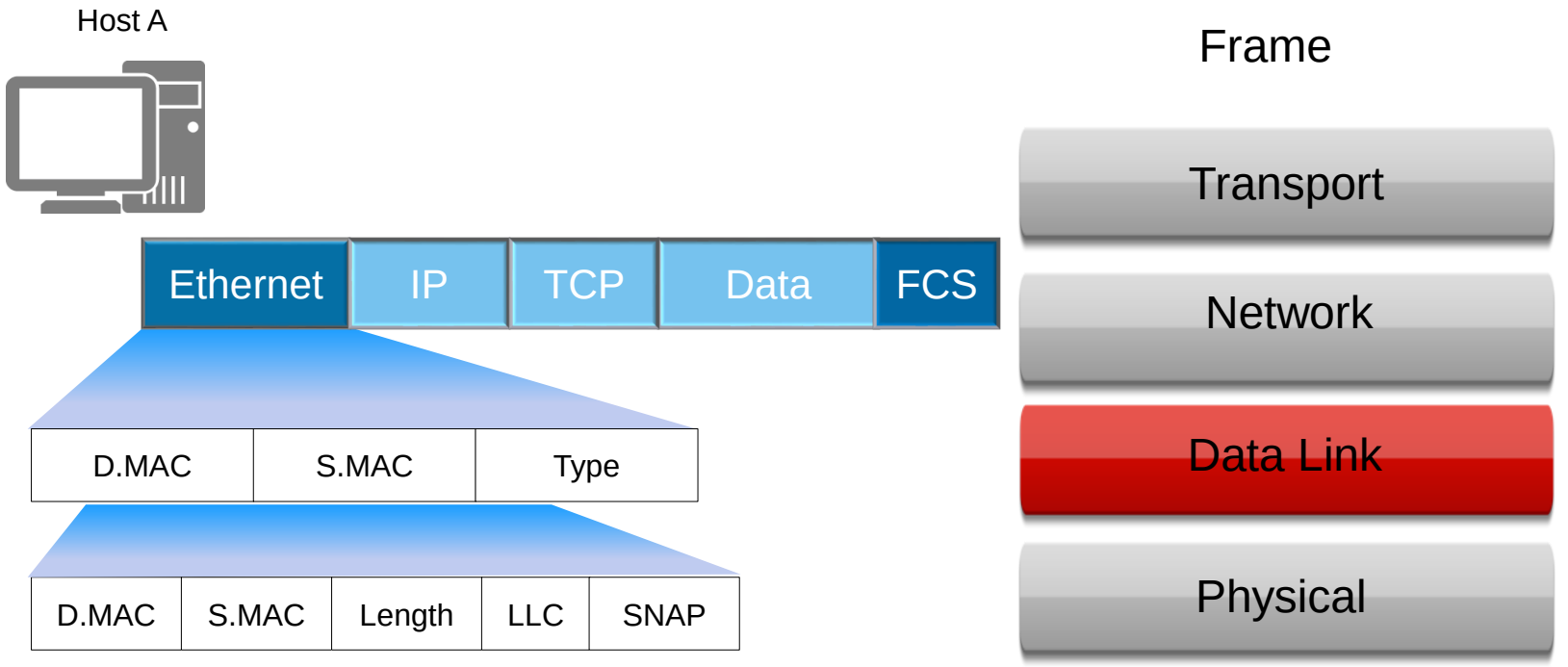
Fonctionnement d’un réseau LAN

Phase 4: encapsulation IP



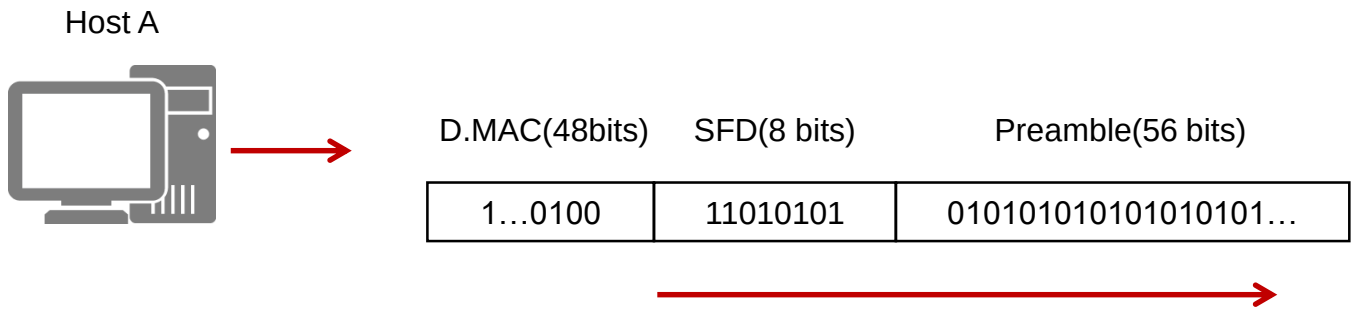
Fonctionnement d’un réseau LAN

Phase 5: encapsulation Ethernet



Fonctionnement d’un réseau LAN

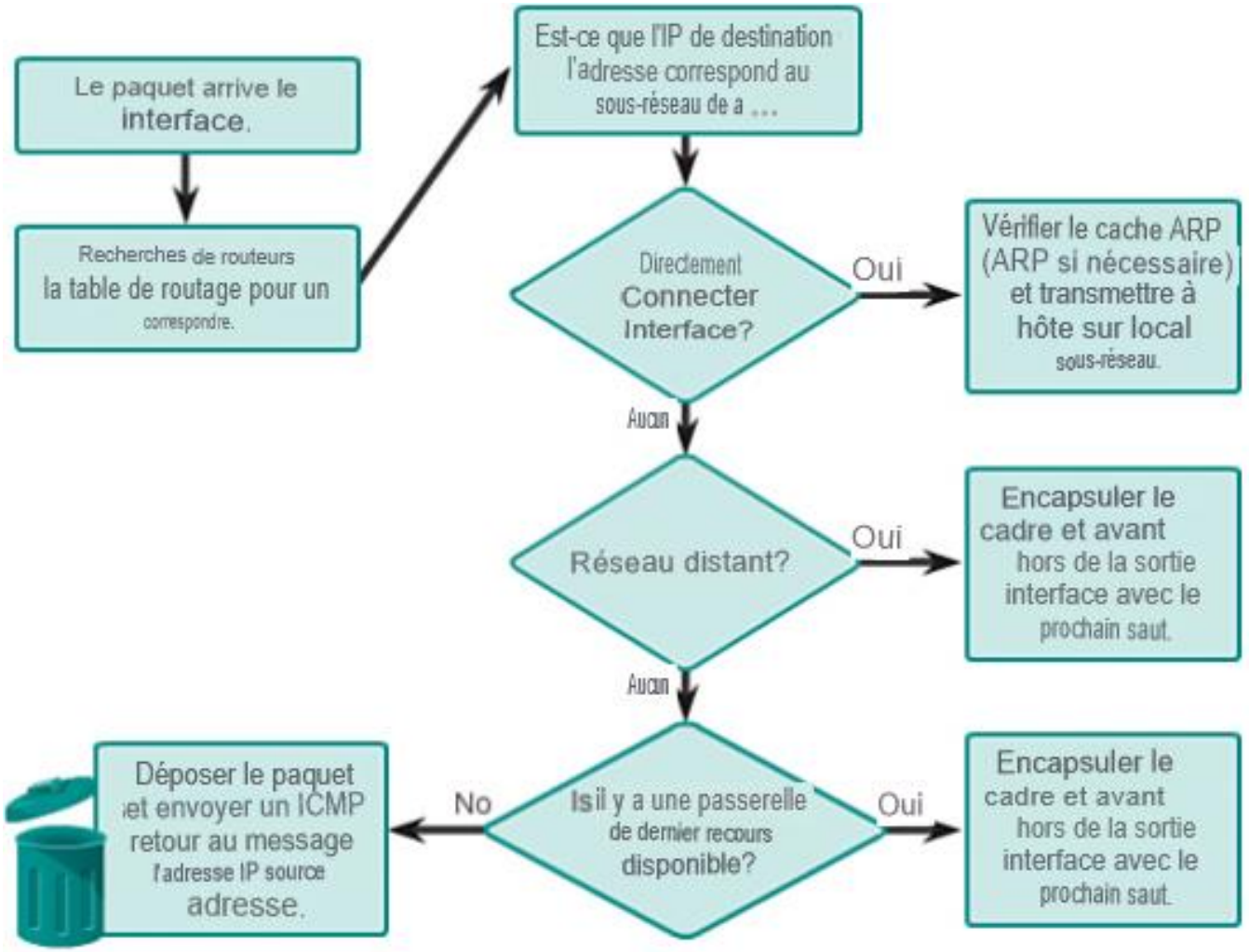
Phase 6: transmission des trames



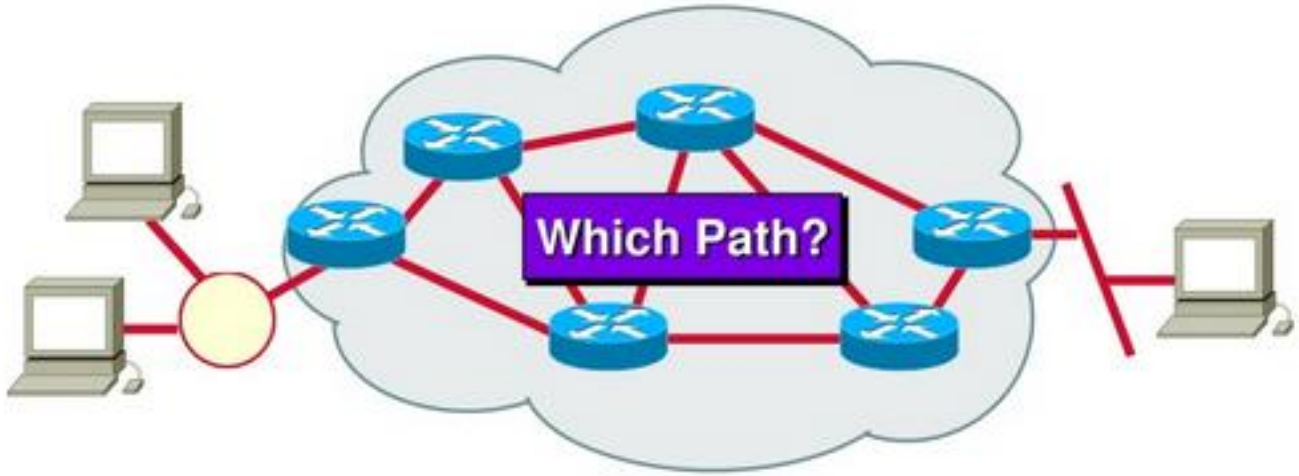
CHAPITRE 2

PROTOCOLES DE ROUTAGE

Détermination du chemin



Détermination du chemin



- La couche réseau est responsable de la recherche du meilleur chemin.
- Les routeurs sont chargés de retrouver la bonne route.

CHAPITRE 2

PROTOCOLES DE ROUTAGE

1 – Détermination du chemin

2 – Transmission de paquets

3 - Fonctions d’un routeur

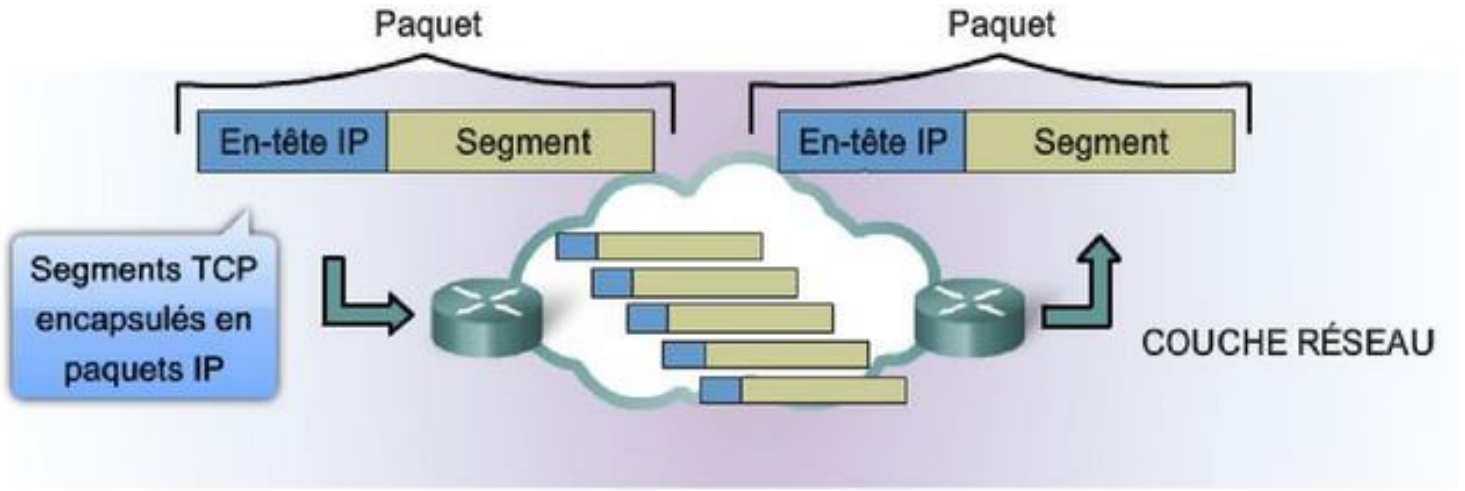
4 – Configuration de base d’un routeur

5 - Principes de routage

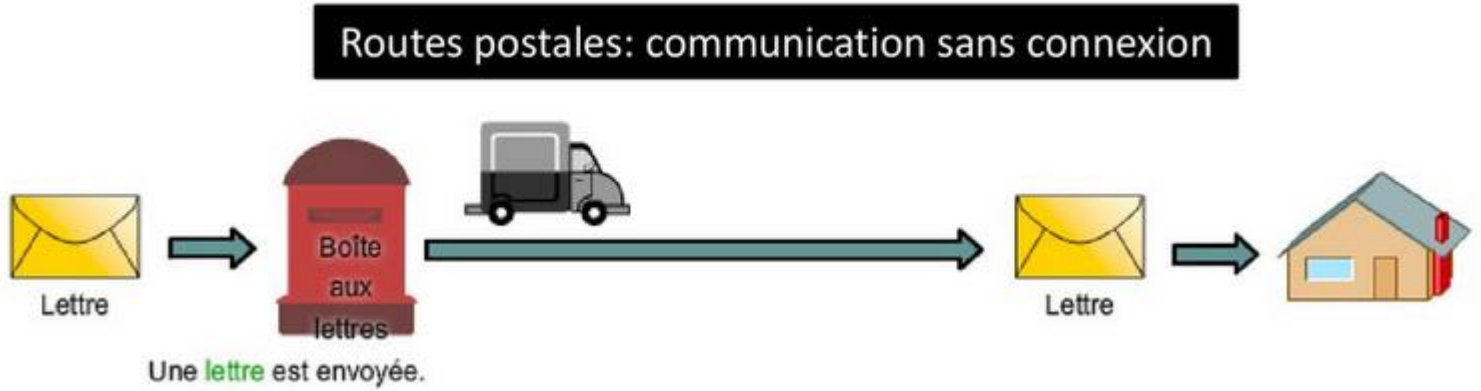
6 - Routage IP statique

Transmission de paquets

- Caractéristiques de base du protocole IPv4 :
  - Sans connexion : aucune connexion n'est établie avant l'envoi de paquets de données.
  - Au mieux (peu fiable) : aucune surcharge n'est utilisée pour garantir la transmission des paquets.
  - Indépendant des médias : fonctionne indépendamment du média transportant les données.



Transmission de paquets



L'expéditeur ne sait pas :

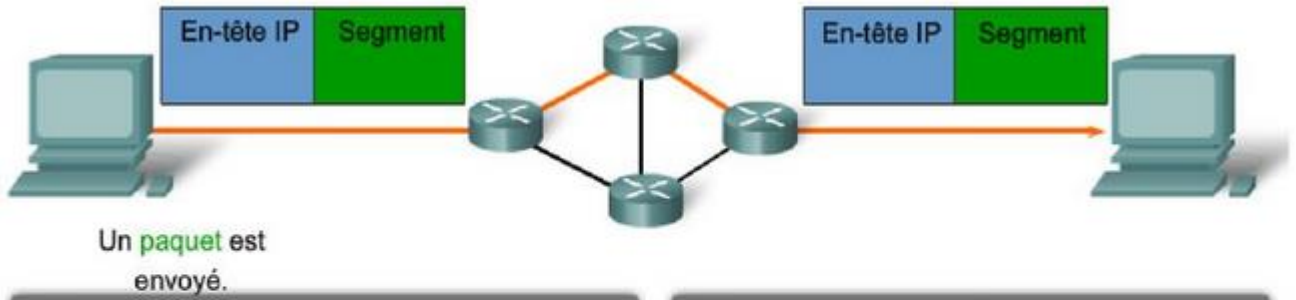
- si le destinataire est présent
- si la lettre est arrivée
- si le destinataire peut lire la lettre

Le destinataire ne sait pas :

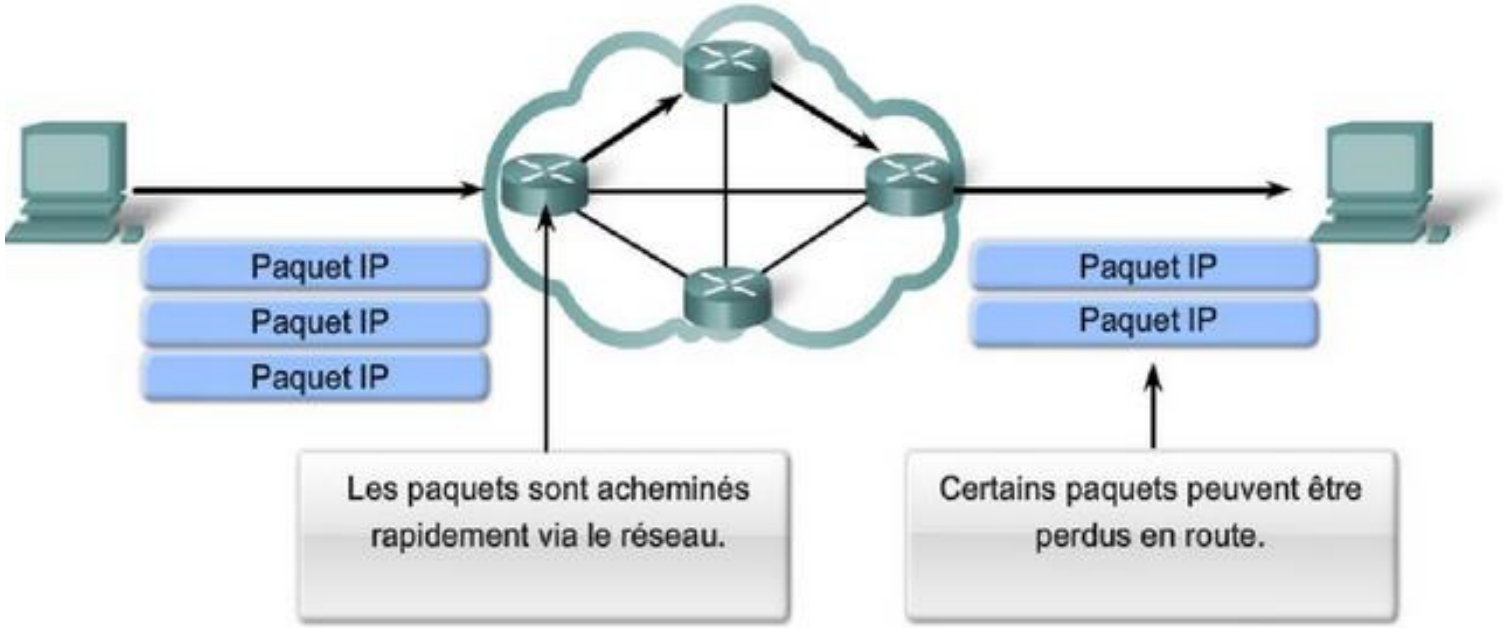
- quand elle arrive

Transmission de paquets

- Le protocole IP étant sans connexion :
  - il ne nécessite aucun échange initial d'informations de contrôle pour établir une connexion de bout en bout avant le transfert des paquets, ni de champs supplémentaires dans l'en-tête d'unité de données de protocole pour maintenir cette connexion.



Transmission de paquets



Protocole de couche réseau peu fiable, IP ne garantit pas que tous les paquets envoyés seront reçus.

D'autres protocoles gèrent le processus de suivi des paquets et garantissent leur acheminement.

CHAPITRE 2

PROTOCOLES DE ROUTAGE

1 – Détermination du chemin

2 – Transmission de paquets

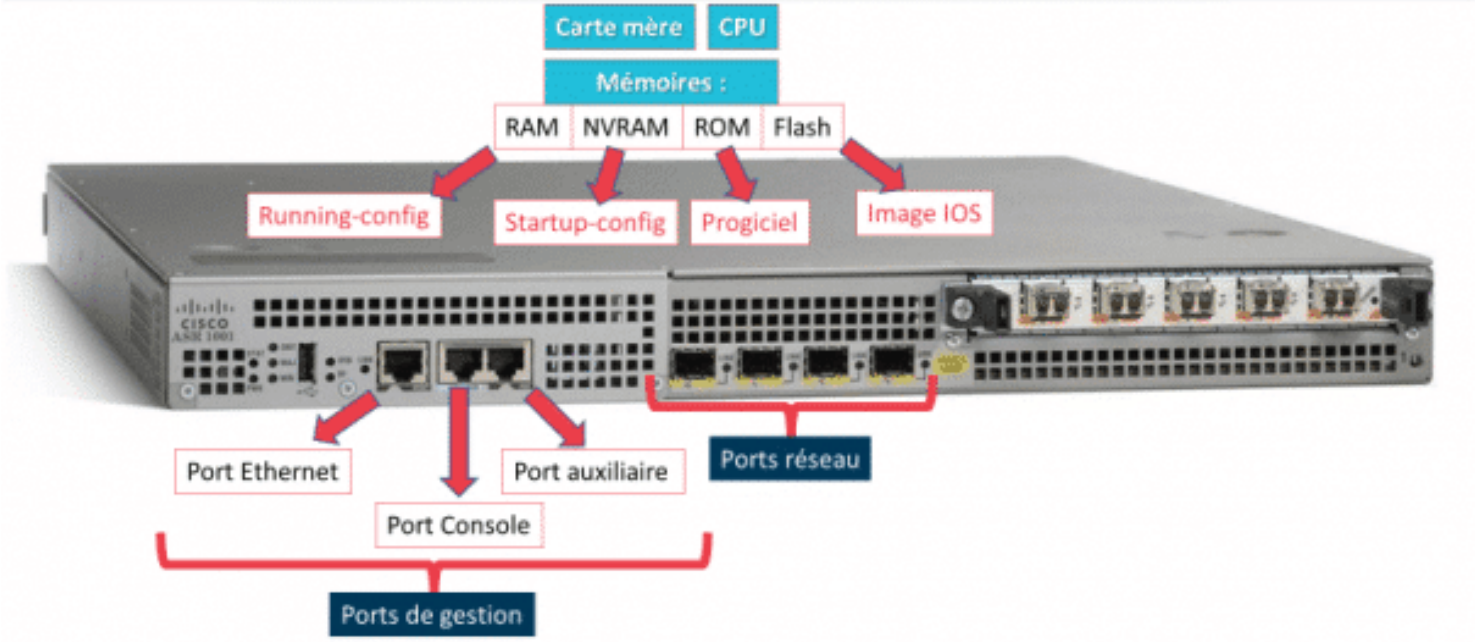
3 - Fonctions d’un routeur

4 – Configuration de base d’un routeur

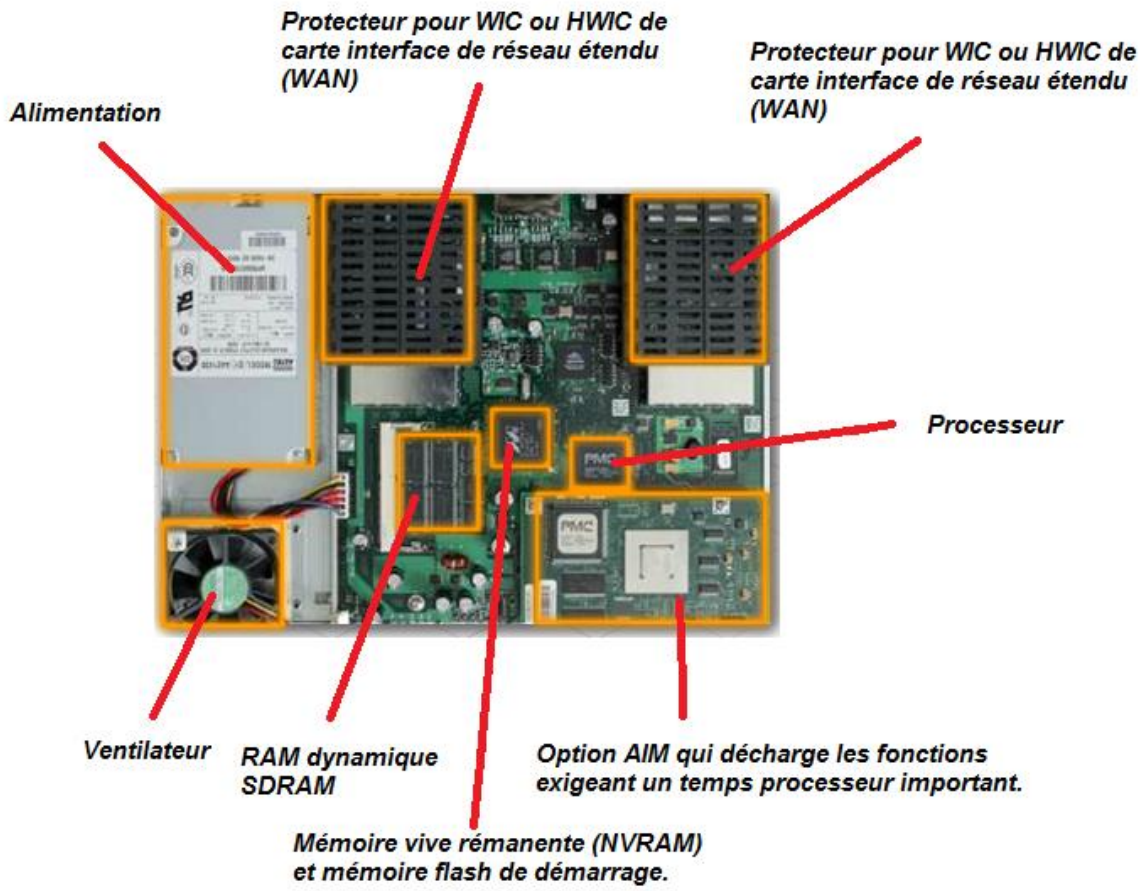
5 - Principes de routage

6 - Routage IP statique

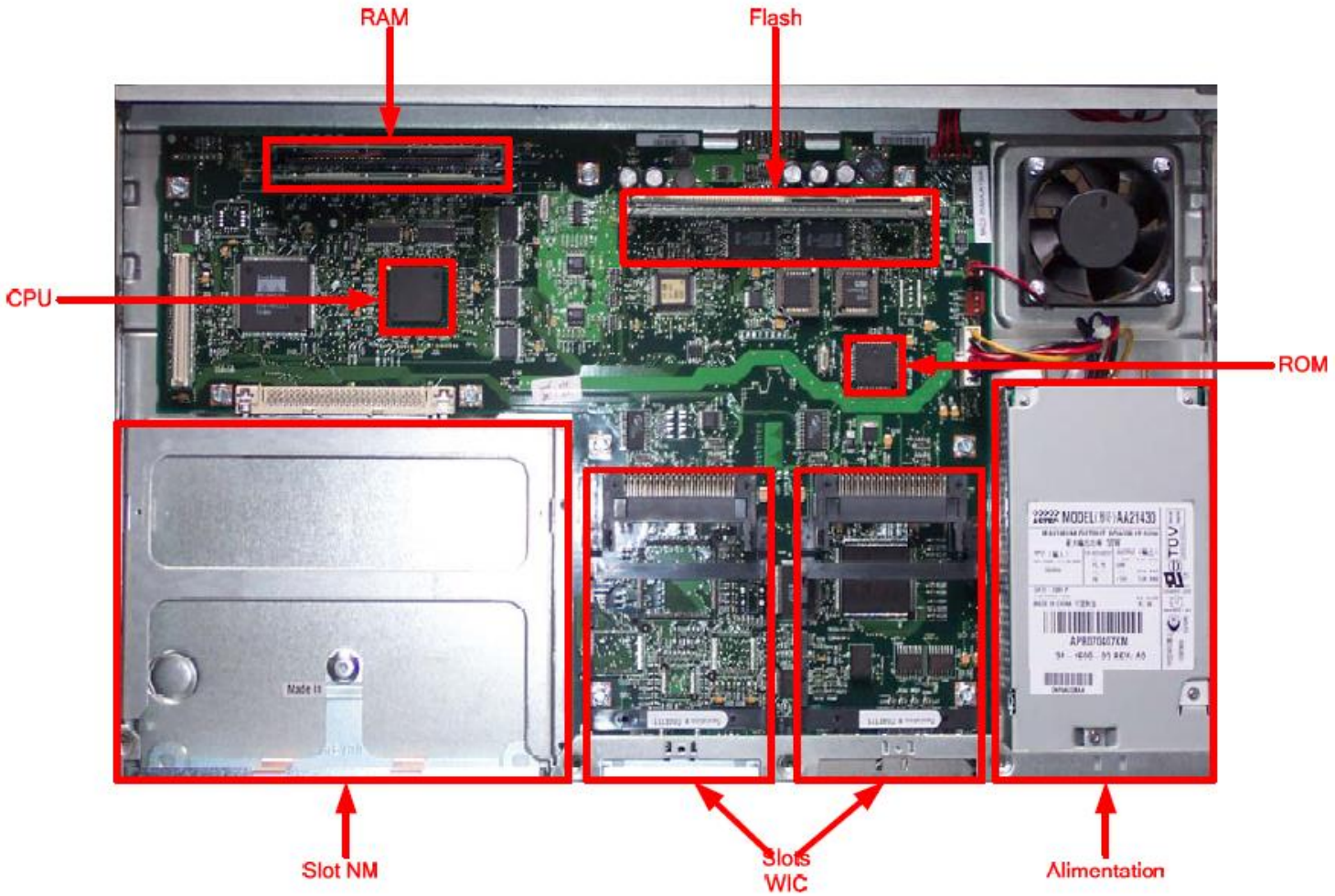
Les composants d’un routeur



Les composants d’un routeur



Les composants d’un routeur



Vue interne d’un routeur Cisco 2620XM

Les composants d'un routeur

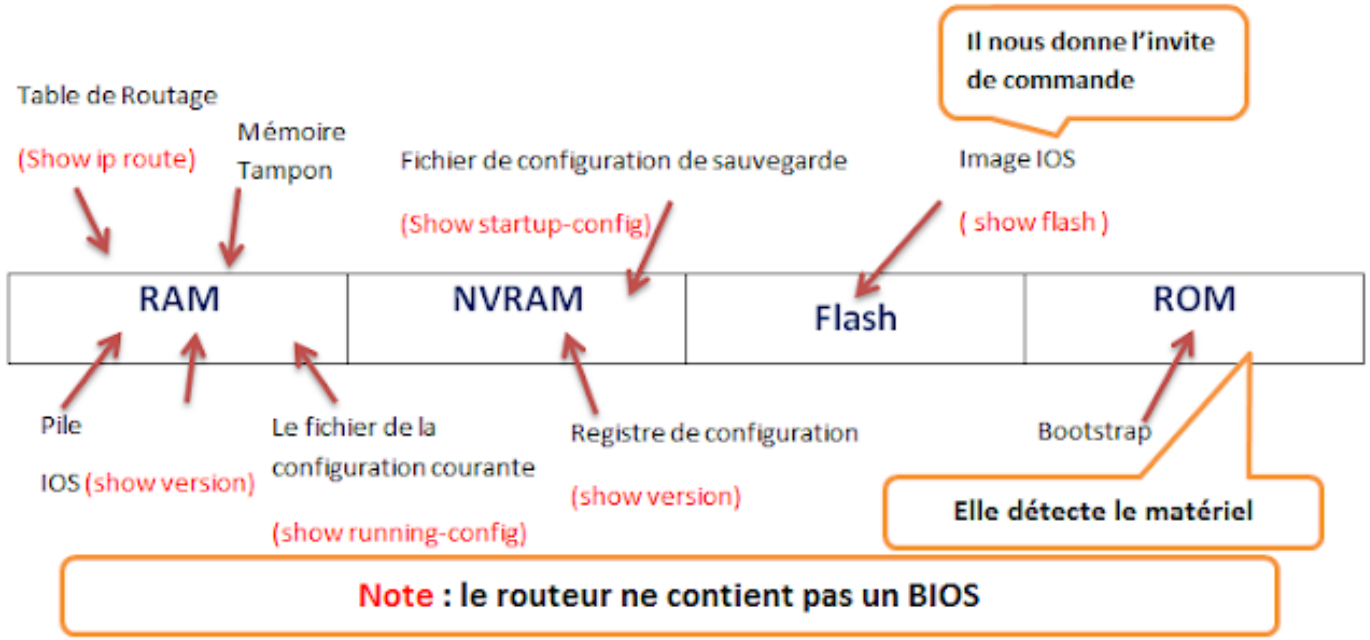


Table de routage

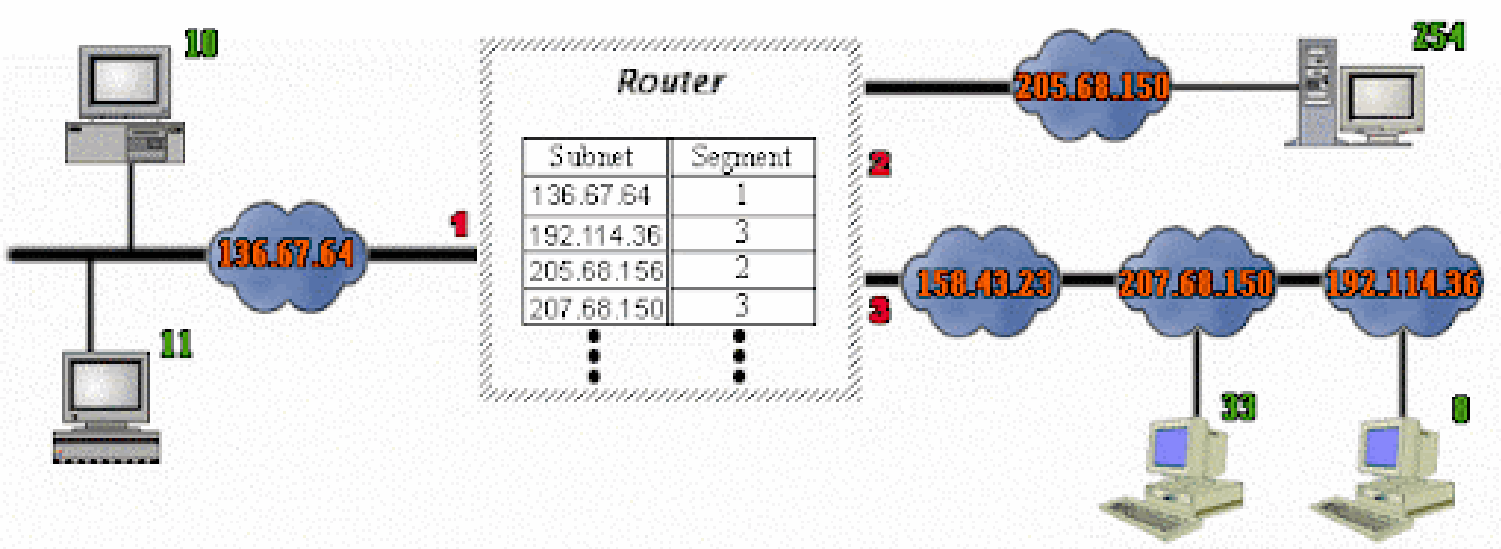
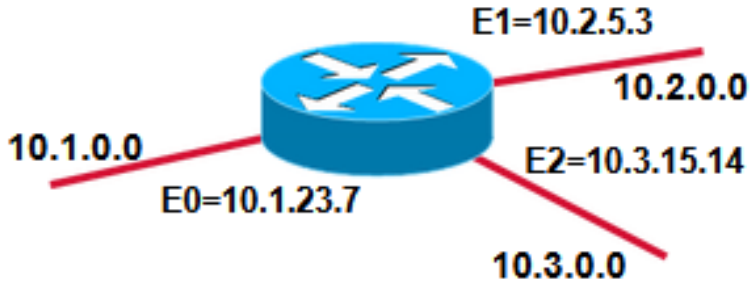


Table de routage

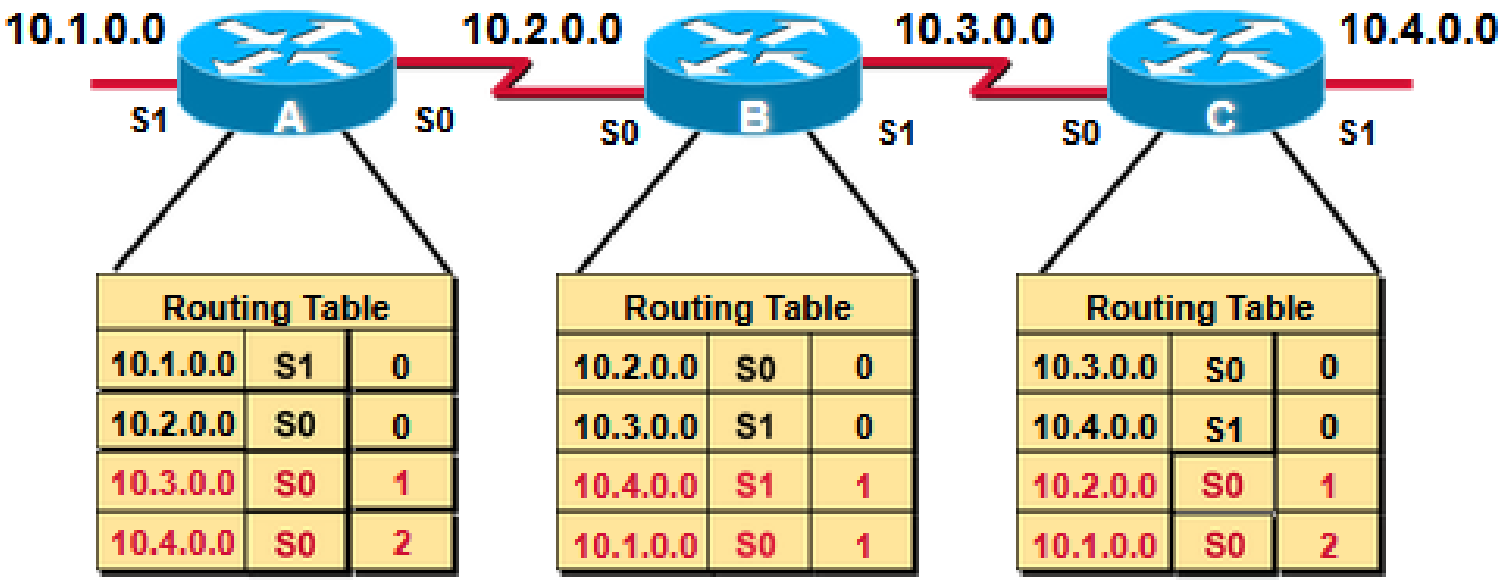
- La table de routage contient les réseaux ainsi que les interfaces de sortie correspondants.



Destination Network	Router Port	Router Address
10.1.0.0	E0	10.1.23.7
10.2.0.0	E1	10.2.5.3
10.3.0.0	E2	10.3.15.14

- **Network portion of address used to make path selections**

Table de routage



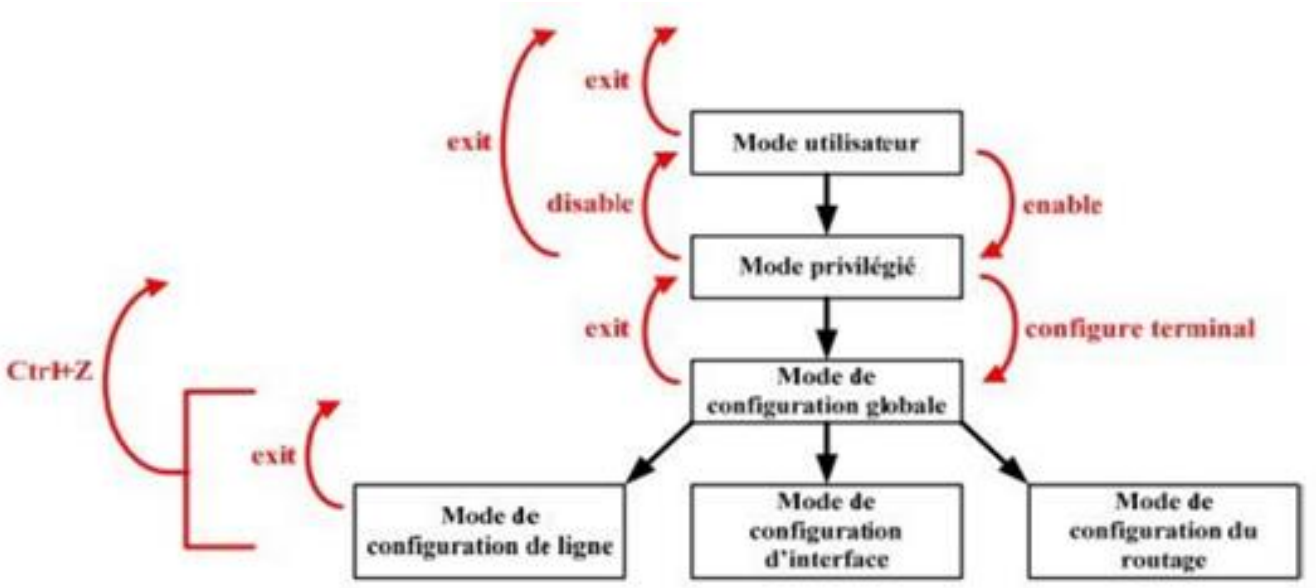
- La table de routage permet au routeur de retrouver les chemins vers la destination.

CHAPITRE 2

PROTOCOLES DE ROUTAGE

Configuration de base d’un routeur

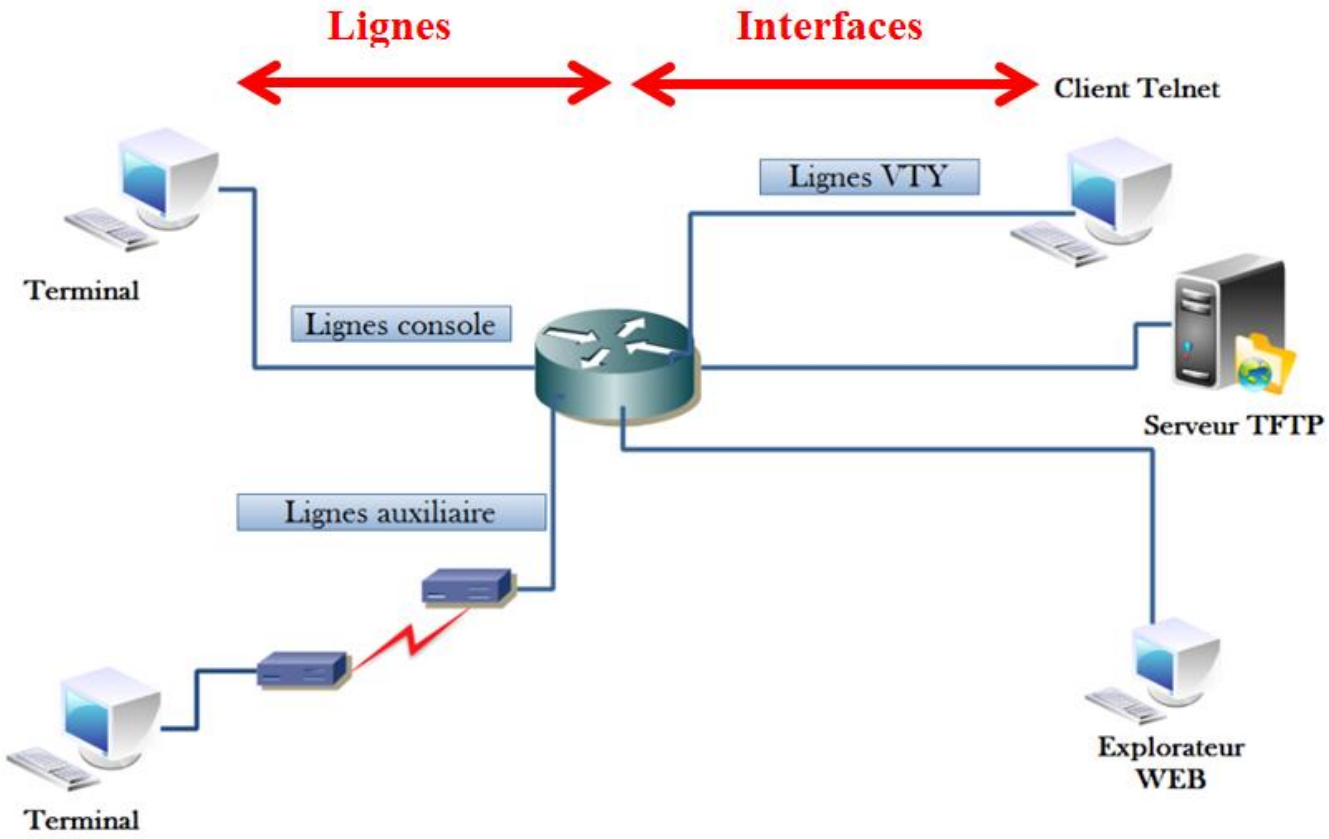
Exemple de configuration CISCO



Mode	Invite de Commande
Utilisateur	Router>
Privilégié	Router#
Configuration Globale	Router (config)#
Interface	Router (config-if)#
Ligne	Router (config-ligne)#
Routage	Router (config-router)#

Configuration de base d’un routeur

Exemple de configuration CISCO (modes d’accès au routeur)



Configuration de base d’un routeur

Configuration du nom d’un routeur

```
Router(config)#hostname RouteurTest
RouteurTest(config)#
```

L’une des premières tâches de configuration consiste à attribuer au routeur un nom unique

```
RouteurTest#sh run
Building configuration...

Current configuration : 440 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouteurTest
!
```

Configuration de base d’un routeur

Exemple de configuration CISCO (Interface série)

```
RouterX# configure terminal
RouterX(config)# interface Serial 0/0/0
RouterX(config-if)# ip address 172.18.0.1 255.255.0.0
RouterX(config-if)# no shutdown
```

Configuration de base d’un routeur

Affichage des informations IP des interfaces et leurs état

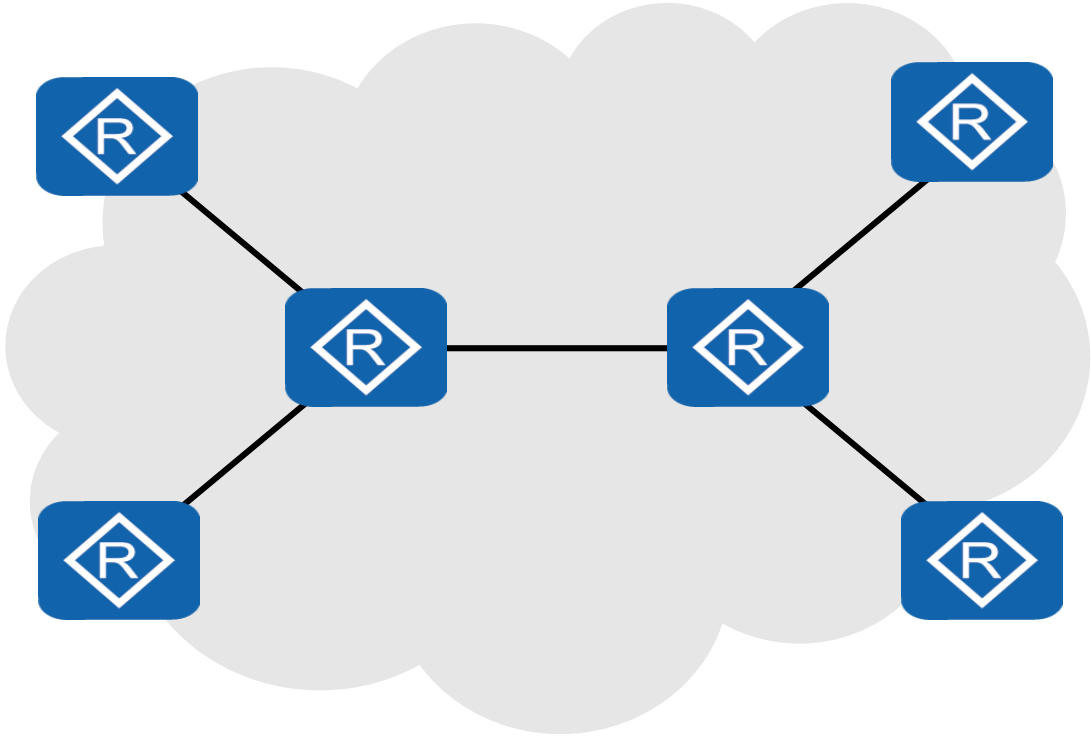
```
RouterY# show ip  interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.1.1        YES unset  up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  up                    up
Serial0/1/0                unassigned      YES unset  up                    up
Serial0/1/1                unassigned      YES unset  administratively down down
```

CHAPITRE 2

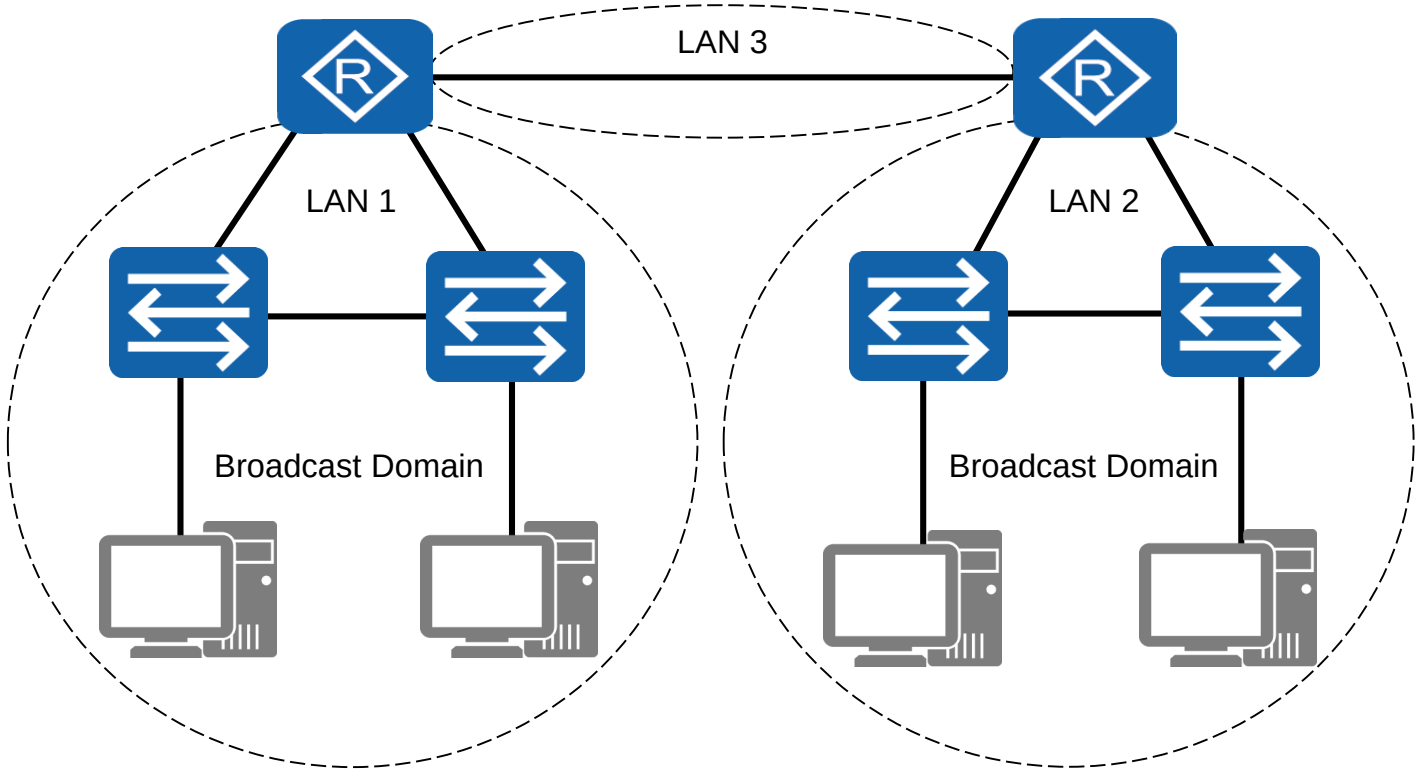
PROTOCOLES DE ROUTAGE

Système autonome

Un réseau IP, ou réseaux, contrôlé par un ou plusieurs opérateurs avec une politique claire qui régit la façon dont les décisions de routage sont prises



Domaine de diffusion



Décision de routage

Les routeurs sont responsables du processus décisionnel qui détermine le chemin par lequel les paquets sont transmis

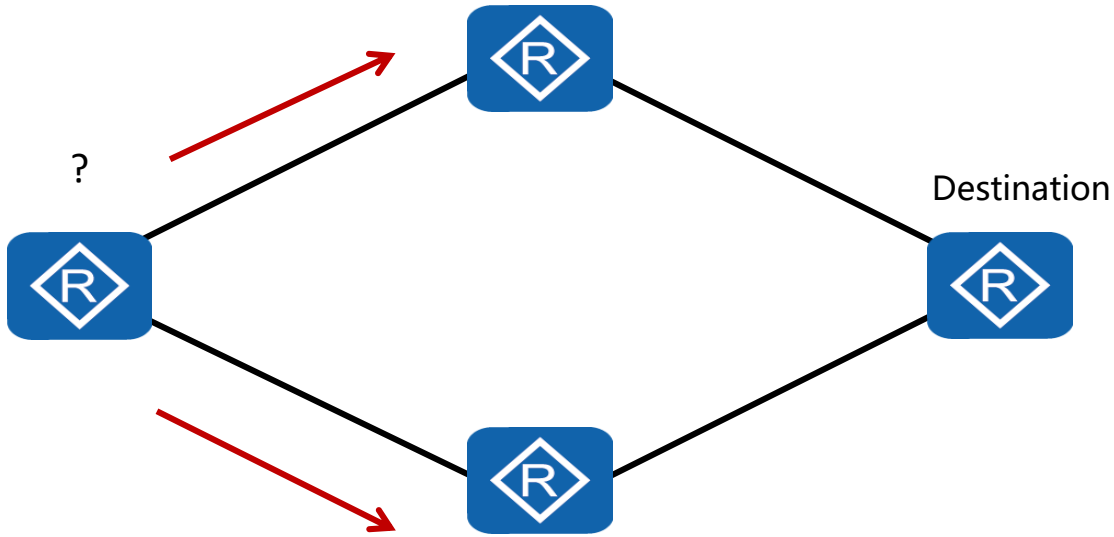
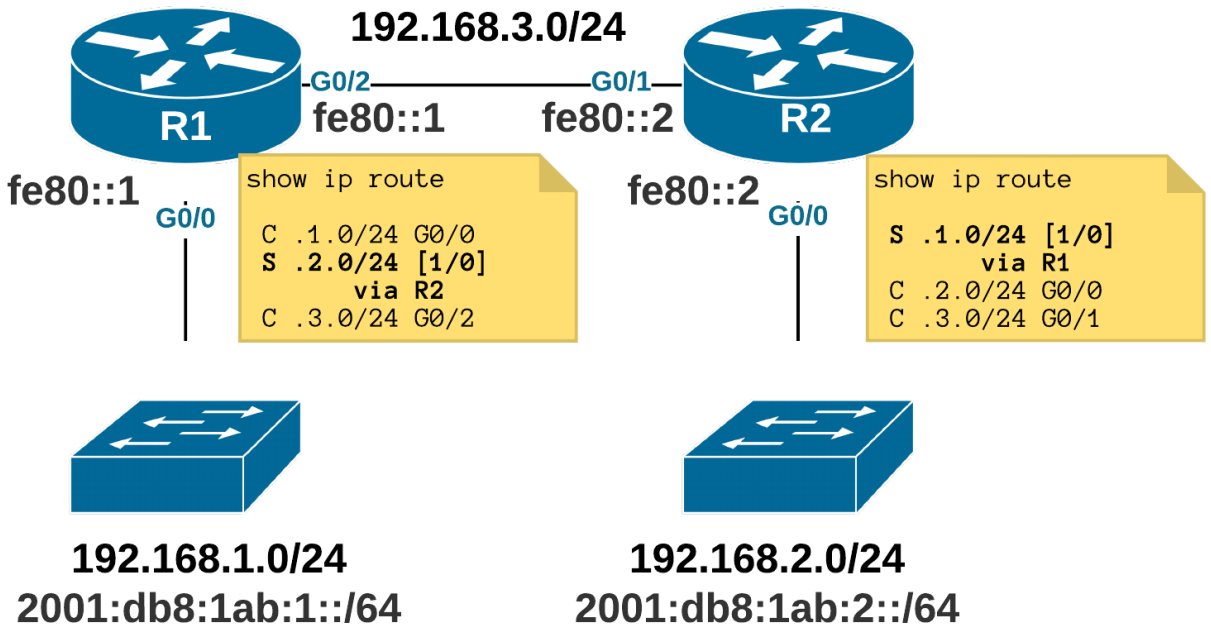
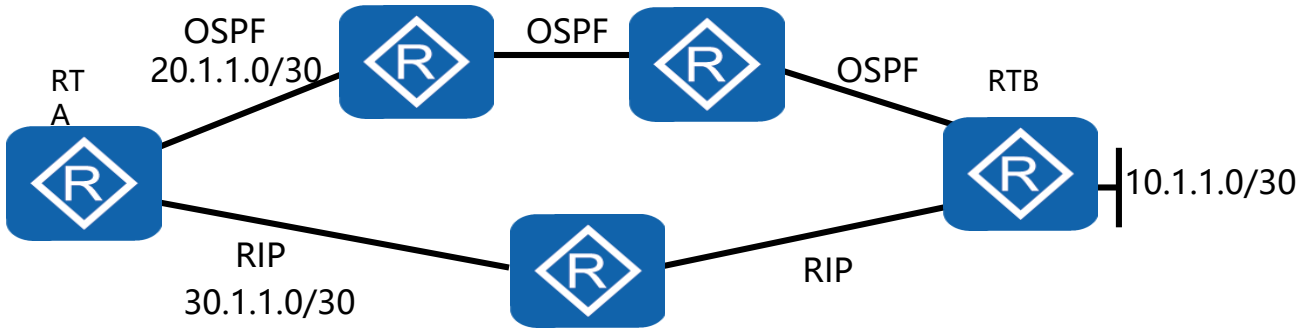


Table de routage

Le tableau de routage répertorie les réseaux accessibles via le routeur. Les paquets qui n'ont pas d'itinéraire sont par la suite jetés.



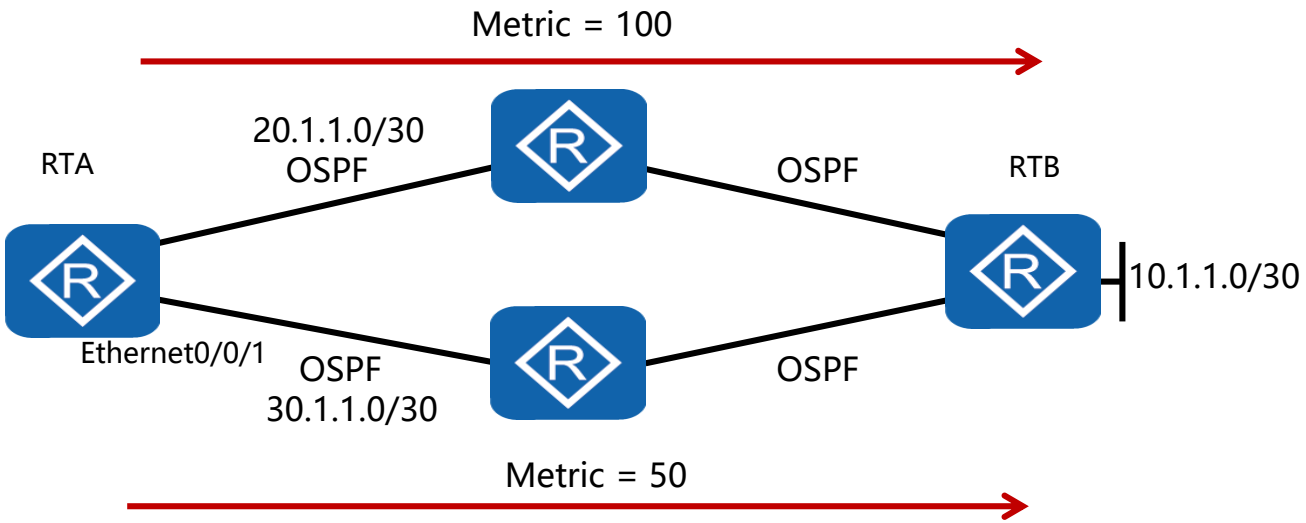
Préférence de routage




```
[RTA]display ip routing-table
Destination/Mask   Proto   Pre  Cost  Flags NextHop         Interface
10.1.1.0/30        OSPF    10   60    RD    20.1.1.2
Ethernet0/0/0
……
```

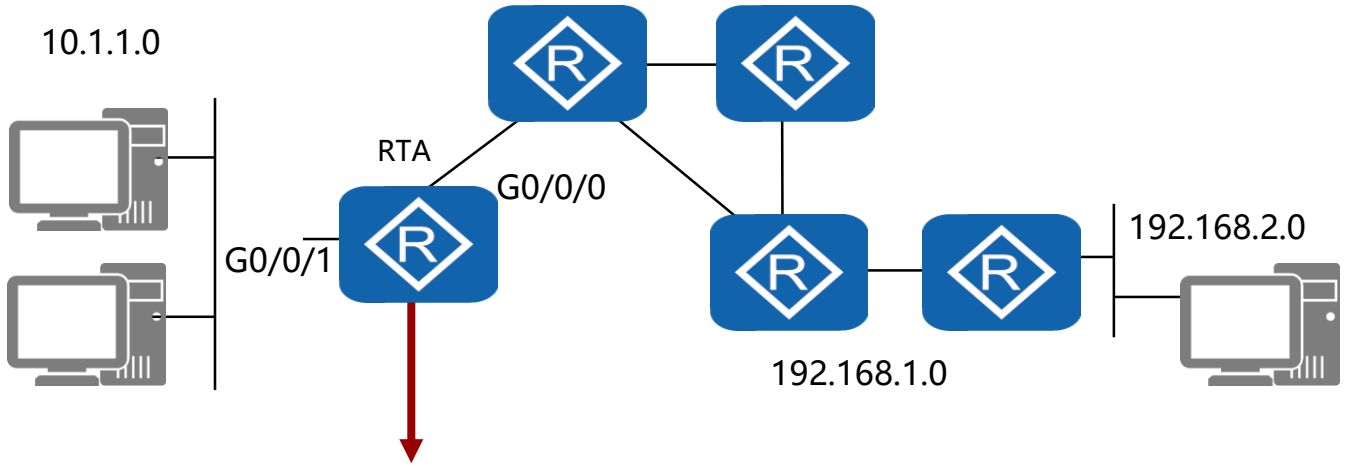
Route	Direct	OSPF	Static	RIP
Preference	0	10	60	100

Métrique




```
[RTA]display ip routing-table
Destination/Mask   Proto   Pre  Cost      Flags NextHop         Interface
10.1.1.0/30        OSPF    10   50        RD    30.1.1.2
Ethernet0/0/1
```

Etablir une table de routage



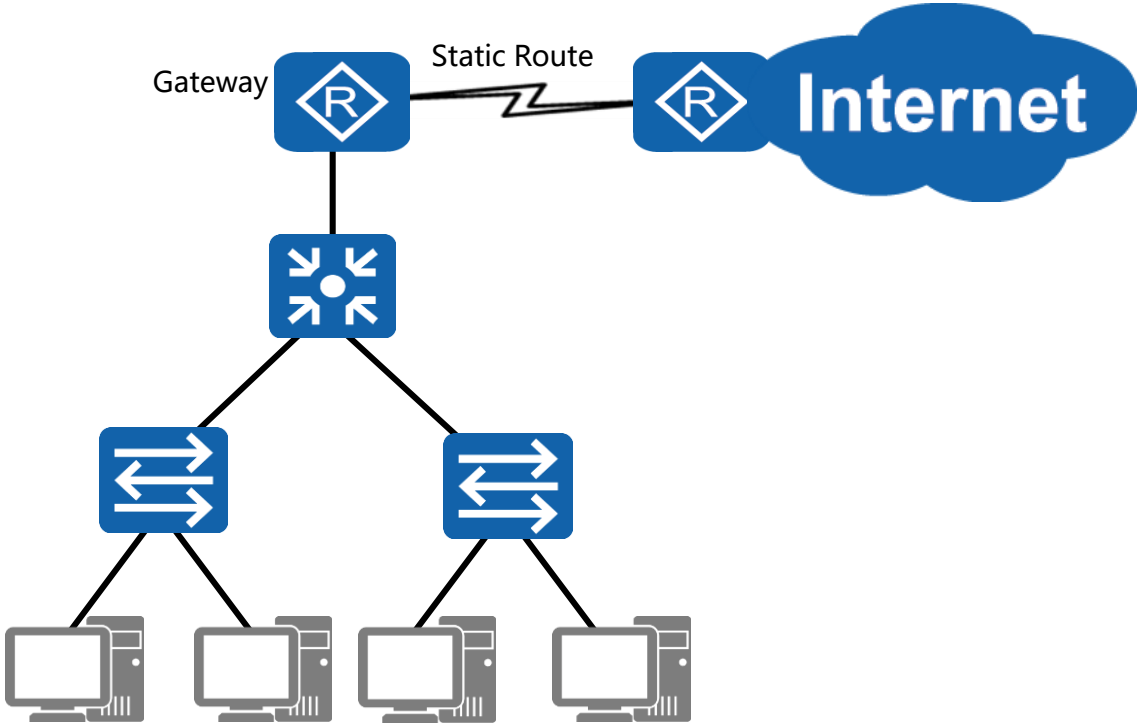
La source de l' itinéraire	Le réseau cible Interface	Interface
Direct	10.1.1.0	G0/0/1
Static	192.168.1.0	G0/0/0
OSPF	192.168.2.0	G0/0/0

CHAPITRE 2

PROTOCOLES DE ROUTAGE

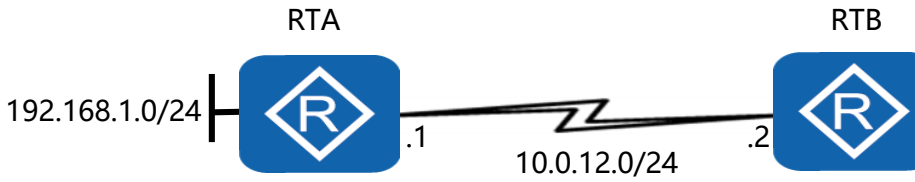
Routage IP statique

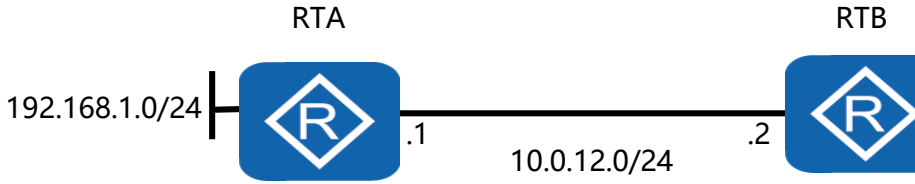
Les routes statiques définissent un moyen de sélection de chemin vers d'autres réseaux



Routage IP statique

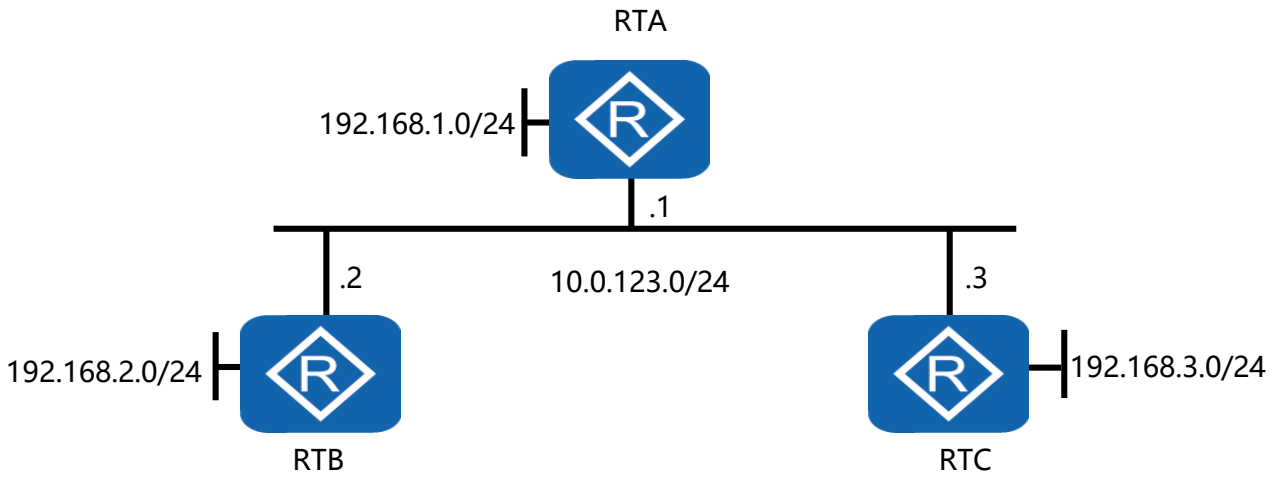
La transmettre de paquets sur la base d'une interface sérielle exige que l'interface sortante soit définie



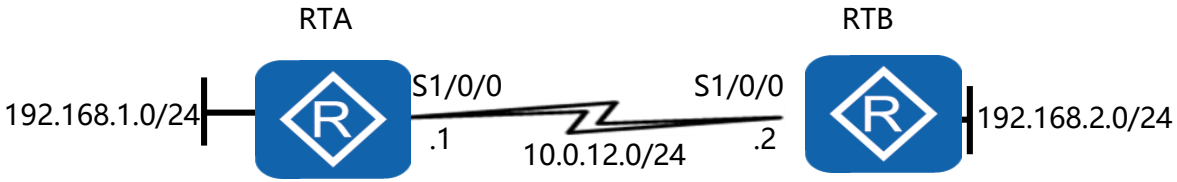


Routage IP statique

Le transfert de paquets sur des réseaux de diffusion tels qu'Ethernet, nécessite que le prochain saut soit défini.



Exemple de configuration

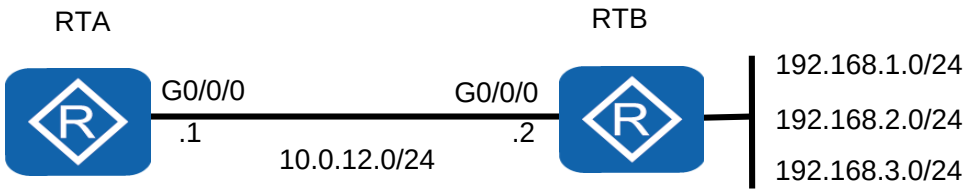



```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1
[RTB]ip route-static 192.168.1.0 255.255.255.0 Serial 1/0/0
[RTB]ip route-static 192.168.1.0 24 Serial 1/0/0
```

Une route statique peut être configurée en fonction de l'une des trois variantes.

Route par défaut

Les routes par défaut fournissent une forme d'itinéraire de dernier recours dans le cas où aucune autre correspondance la plus longue ne se trouve dans la table de routage.

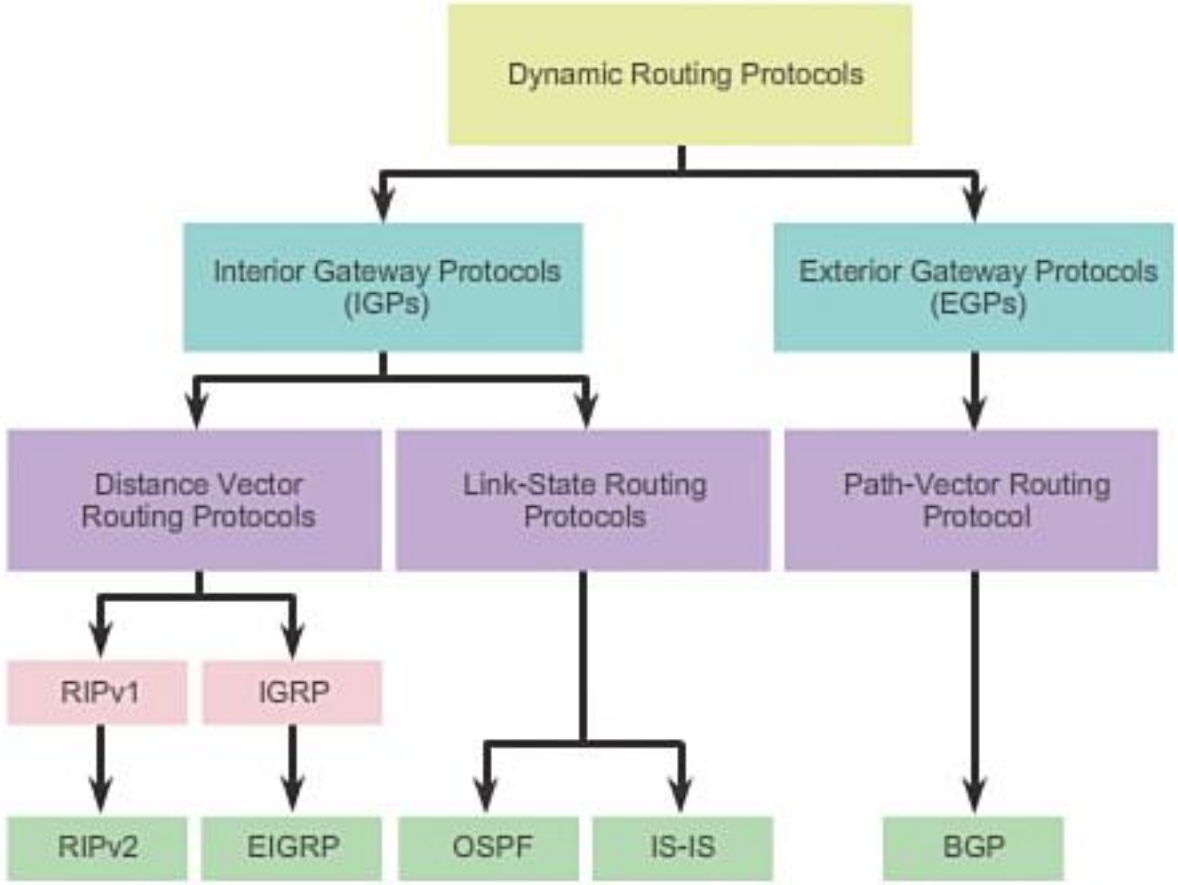



```
[RTA]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
```

CHAPITRE 3

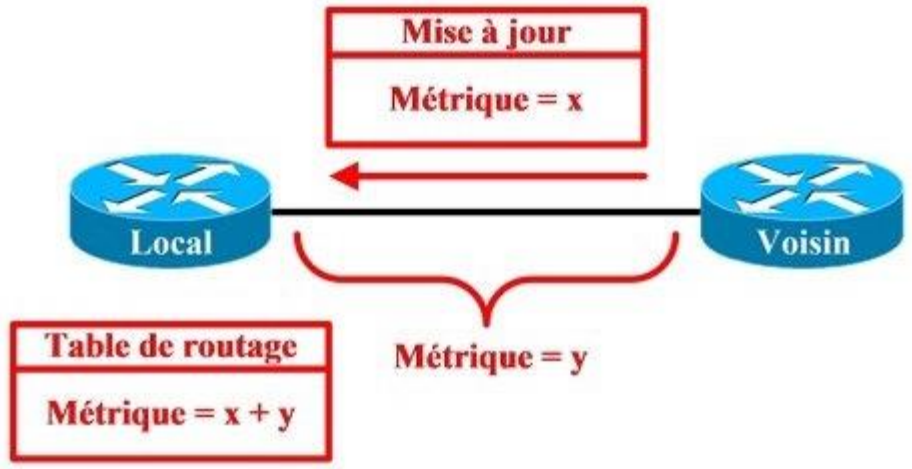
ROUTAGE DYNAMIQUE

Routage à vecteur de distance



Routage à vecteur de distance métrique

- **Convergence** : Tous ont la même vue de la topologie
- **Temps de convergence** : Temps après une modification topologique pour nouvelle convergence
- **Convergence rapide recommandée** : Réduire le temps d'incohérence
- Mises à jour sont envoyées périodiquement
- Elles contiennent la table de routage des voisins
- Emises en broadcast Sauf exceptions (RIPv 2 et EIGRP)
- Algorithme de Bellman Ford
- Métrique = Nombre de sauts n Sauf exceptions (IGRP & EIGRP)



CHAPITRE 3

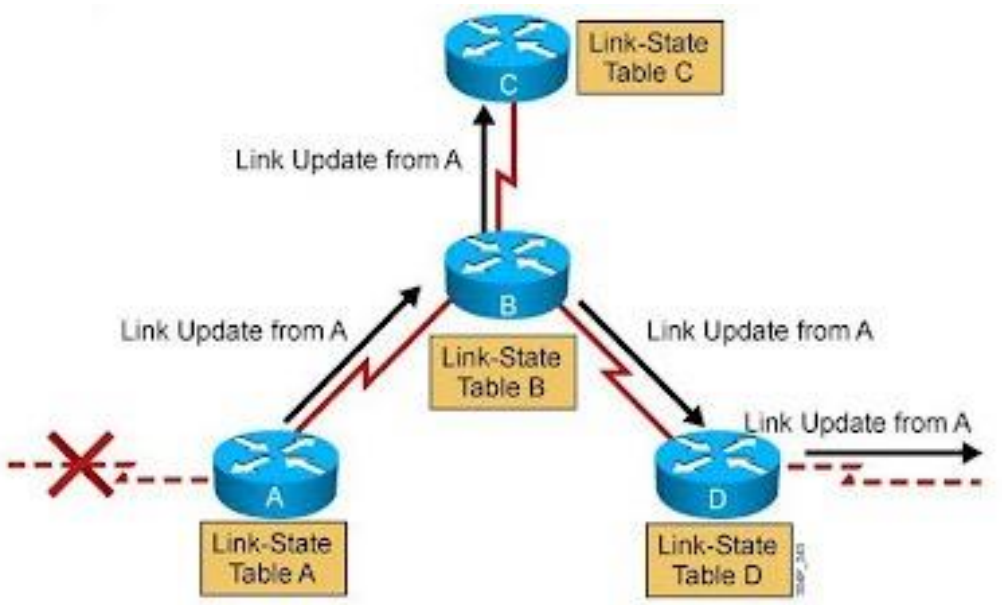
ROUTAGE DYNAMIQUE

Routage à état de liaison

Vecteur de distance	État de lien
Vue de la topologie de réseau à partir de la perspective des voisins	Vue commune de l'ensemble de la topologie de réseau
Ajout de vecteurs de distance d'un routeur à l'autre	Calcul du chemin le plus court menant aux autres routeurs
Mises à jour périodiques fréquentes : Convergence lente	Mises à jour déclenchées par événement : Convergence plus rapide
Transmission des copies des tables de routage aux routeurs voisins	Transmission des mises à jour de routage à état de liens aux autres routeurs

Routage à état de liaison

- Algorithme plus efficace (autre que RIP, comme “Dijkstra” ou “Shortest Path First”).
- Les routeurs construisent de leur point de vue l’arbre de tous les chemins possibles.
- Les meilleures routes sont alors intégrées à la table de routage.
- Exemple de protocole : OSPF et IS-IS.
- Ils convergent très rapidement.
- Les routeurs entretiennent des relations de voisinage maintenues.



CHAPITRE 3

ROUTAGE DYNAMIQUE

Protocole RIP

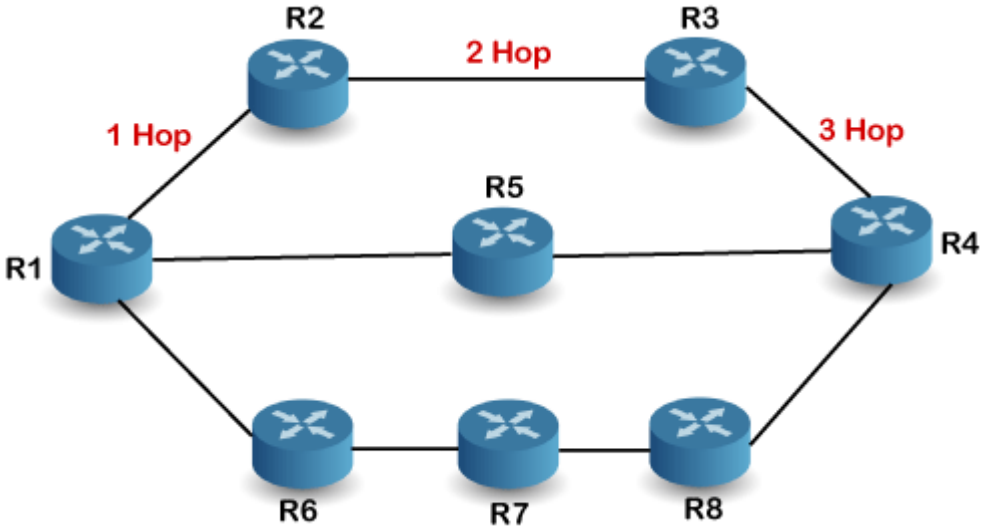
- RIP est un protocole de routage intérieur à vecteur de distance de l'IETF.

- Il est disponible en trois versions :

    1. RIPv1 (1988) : Broadcast 255.255.255.255, classful, UDP520, RFC 1058

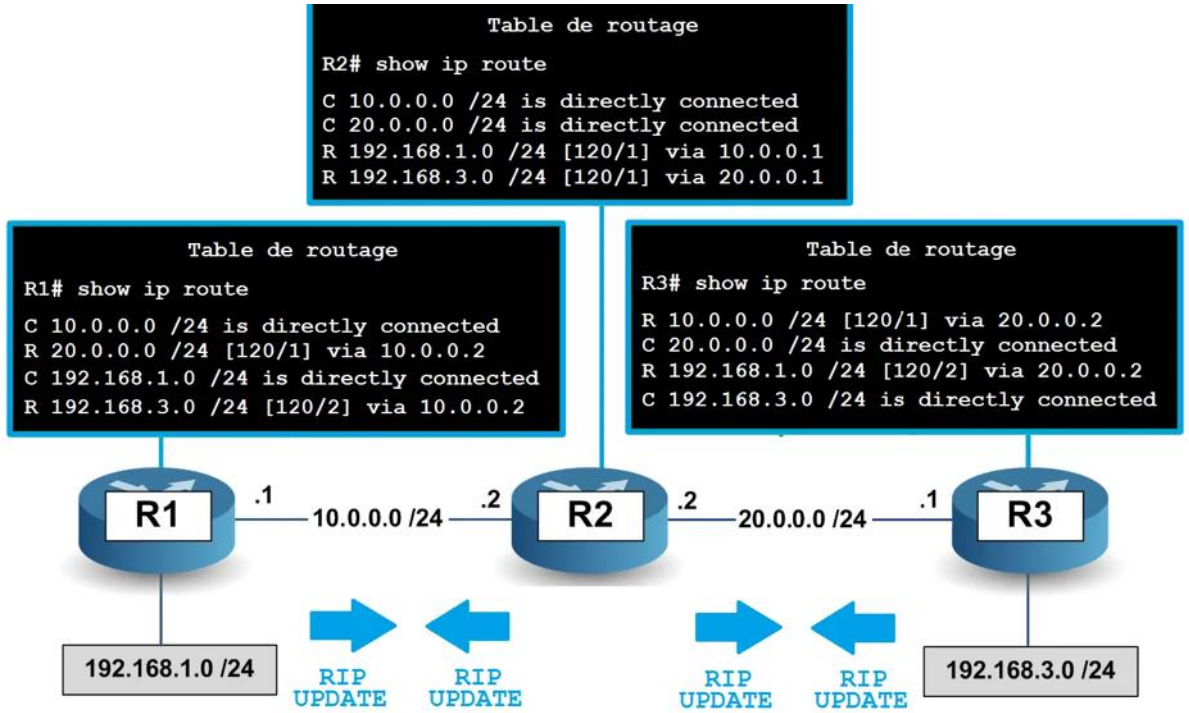
    2. RIPv2 (1993-1998) : Multicast 224.0.0.9, authentification, classless, UDP520, RFC2453

    3. RIPng : Support IPv6, authentification IPSEC, Multicast FF02::9, UDP 521, RFC2080



Protocole RIP

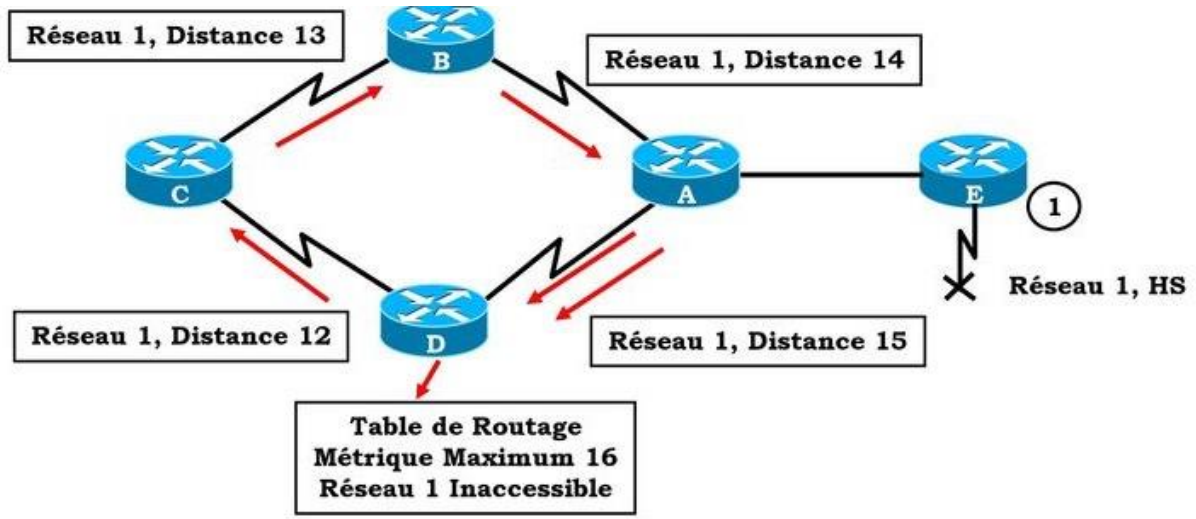
- Les mises à jour s'effectuent de routeurs en routeurs.
- Les mises à jour s'effectuent périodiquement, toutes les 30 secondes.
- Les mises à jour consistent en des envois des tables de routage entières.
- Les mises à jour sont envoyées à l'adresse de diffusion (Broadcast) 255.255.255.255 en RIPv1
- Les mises à jour sont envoyées à l'adresse Multicast 224.0.0.9 en RIPv2



L’algorithme Bellman-Ford

RIP utilise l’algorithme Bellman-Ford pour calculer les meilleures routes

- La distance administrative de RIP est de 120 par défaut.
- La métrique est basée sur le nombre de sauts.
- La métrique maximale est 15.
- La métrique infinie est 16. Empoisonne une route.



Le diamètre maximum du réseau est de 15 sauts

CHAPITRE 3

ROUTAGE DYNAMIQUE

1 - Principes de routage à vecteur de distance

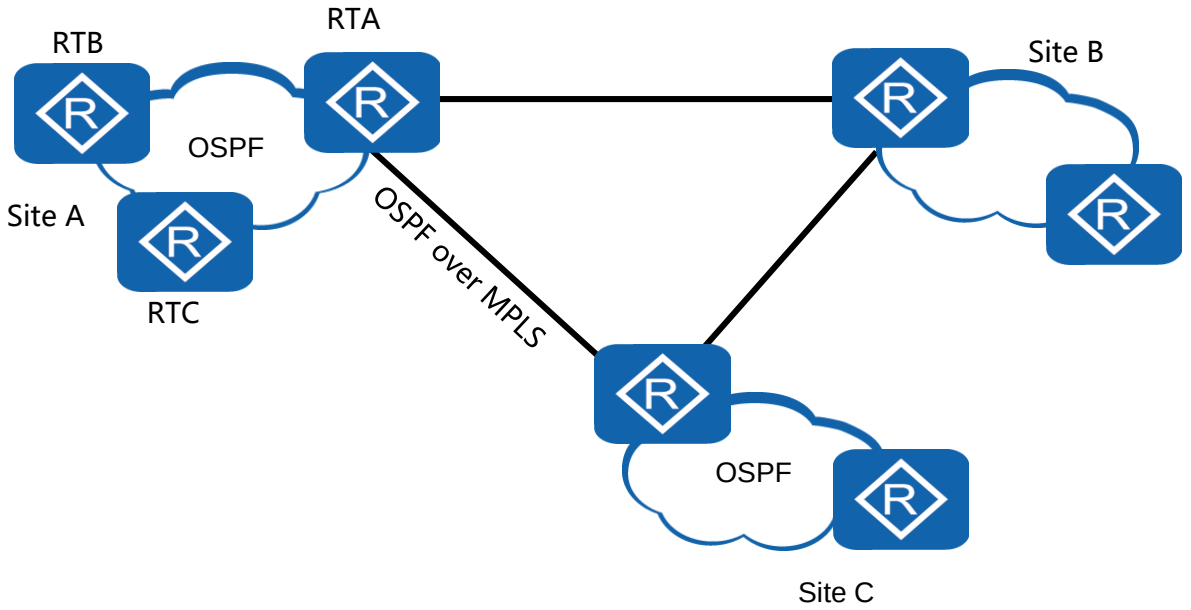
2 - Principes de routage à état de liaison

3 - Protocole RIP

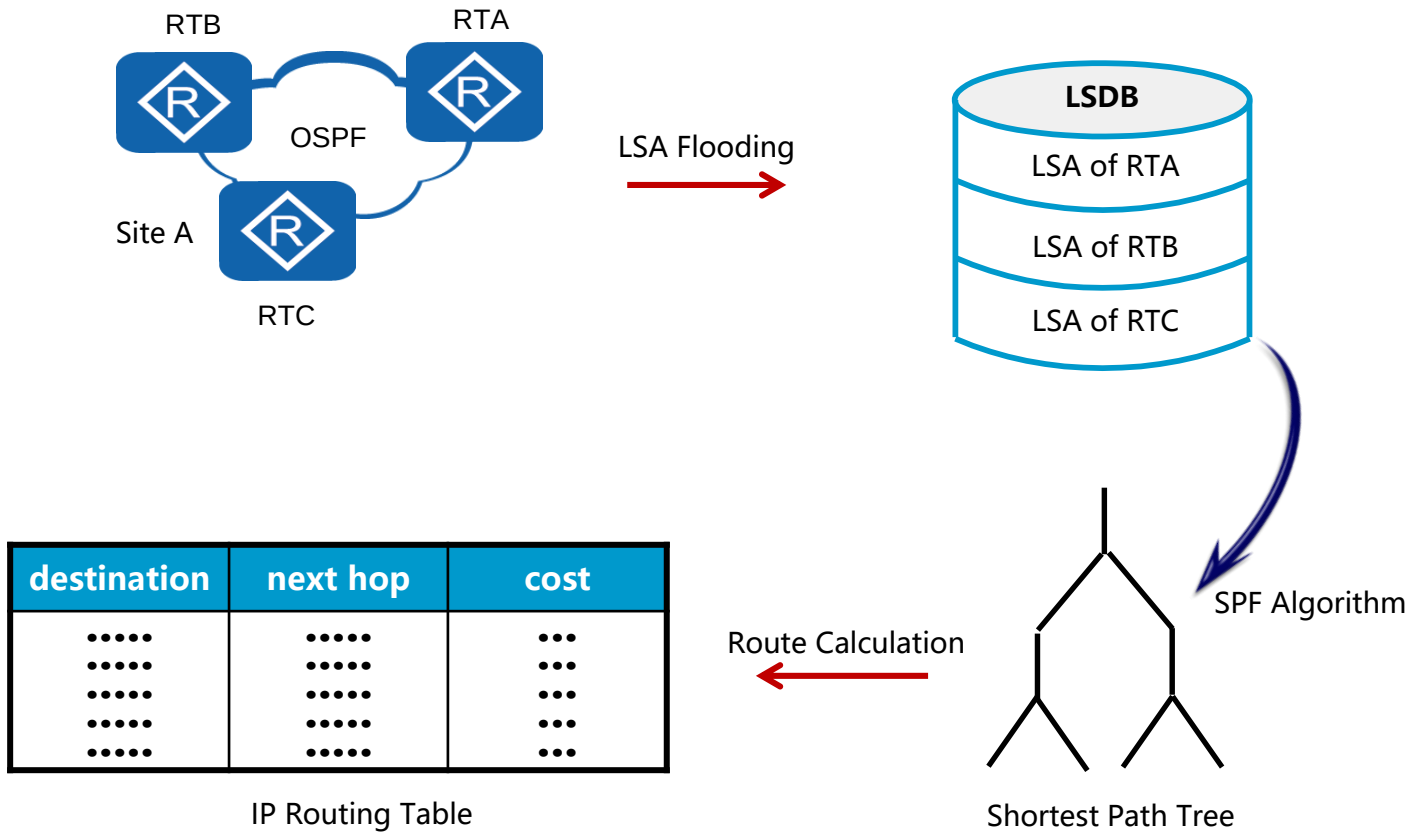
4 - Protocole OSPF

Protocole OSPF

- Minimal Routing Traffic
- Rapid Convergence
- Scalable
- Accurate Route Metrics

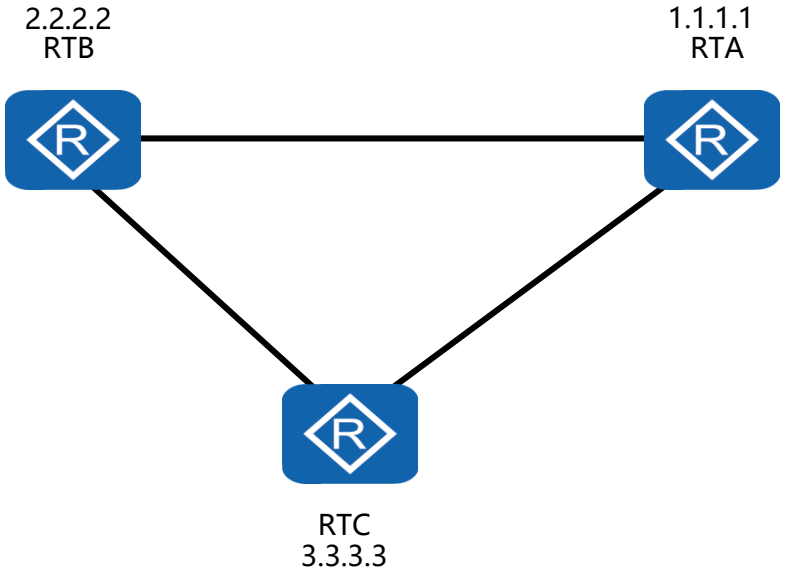


Comportement de convergence



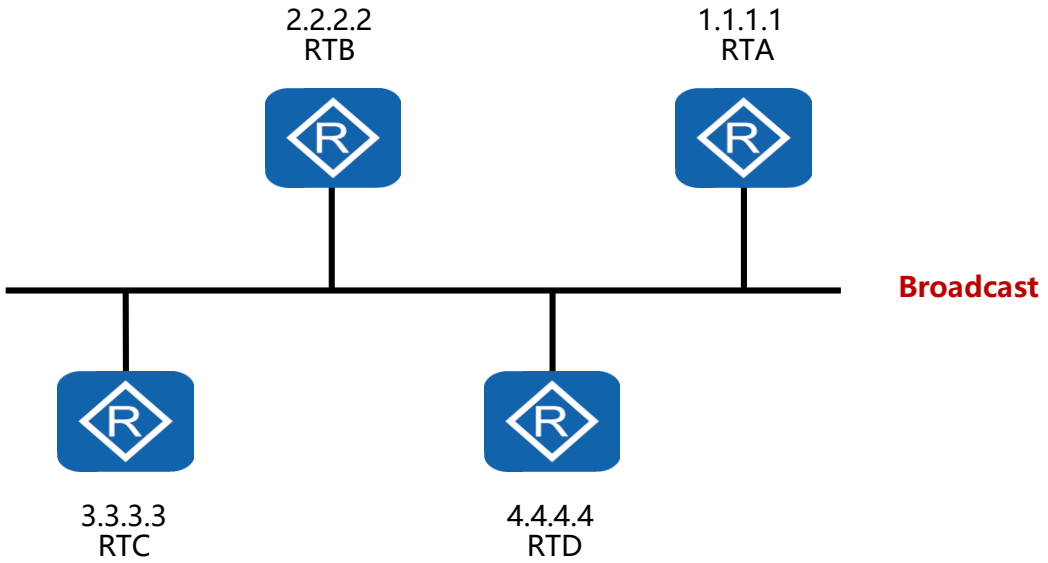
Router ID

Un id routeur est une valeur de 32 bits utilisée pour identifier chaque routeur exécutant le protocole OSPF.



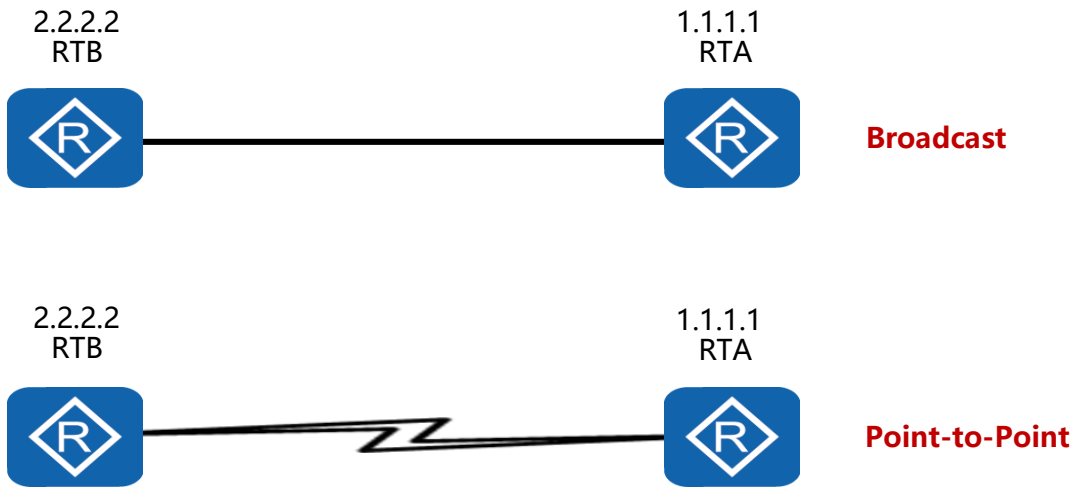
Types des réseaux

Les réseaux basés sur Ethernet adoptent le type de réseau de diffusion par défaut.



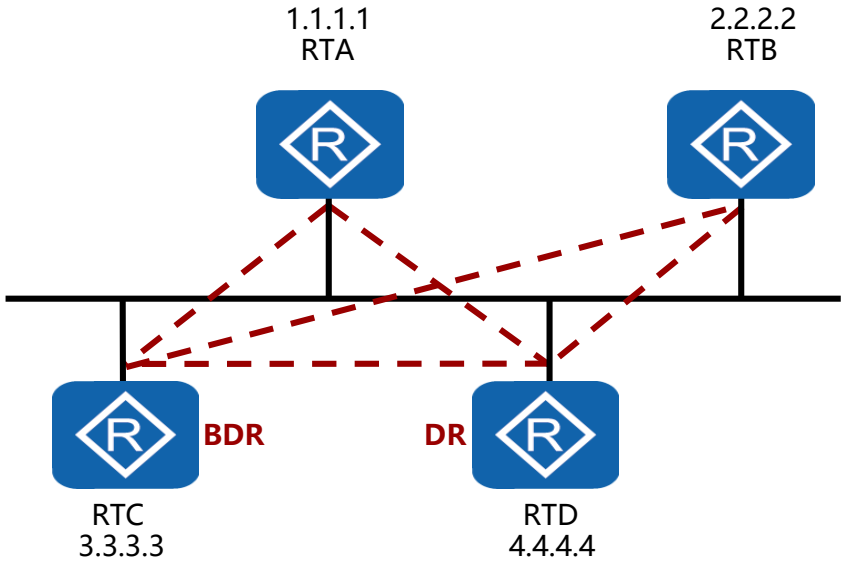
Types des réseaux

Les technologies en série telles que PPP et HDLC seront par défaut au type de réseau Point-to-Point.



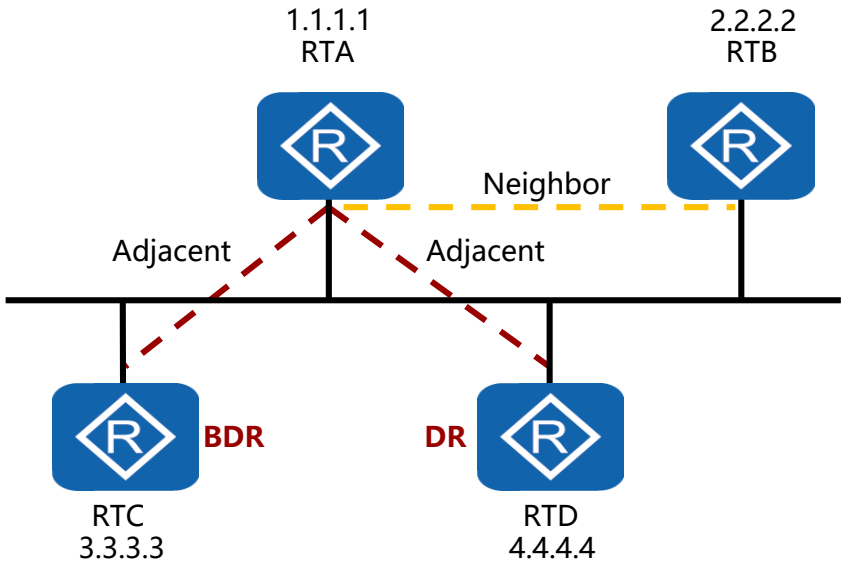
DR et BDR

Les routeurs désignés limitent le nombre de contiguïtés nécessaires dans les réseaux de diffusion (Ethernet).



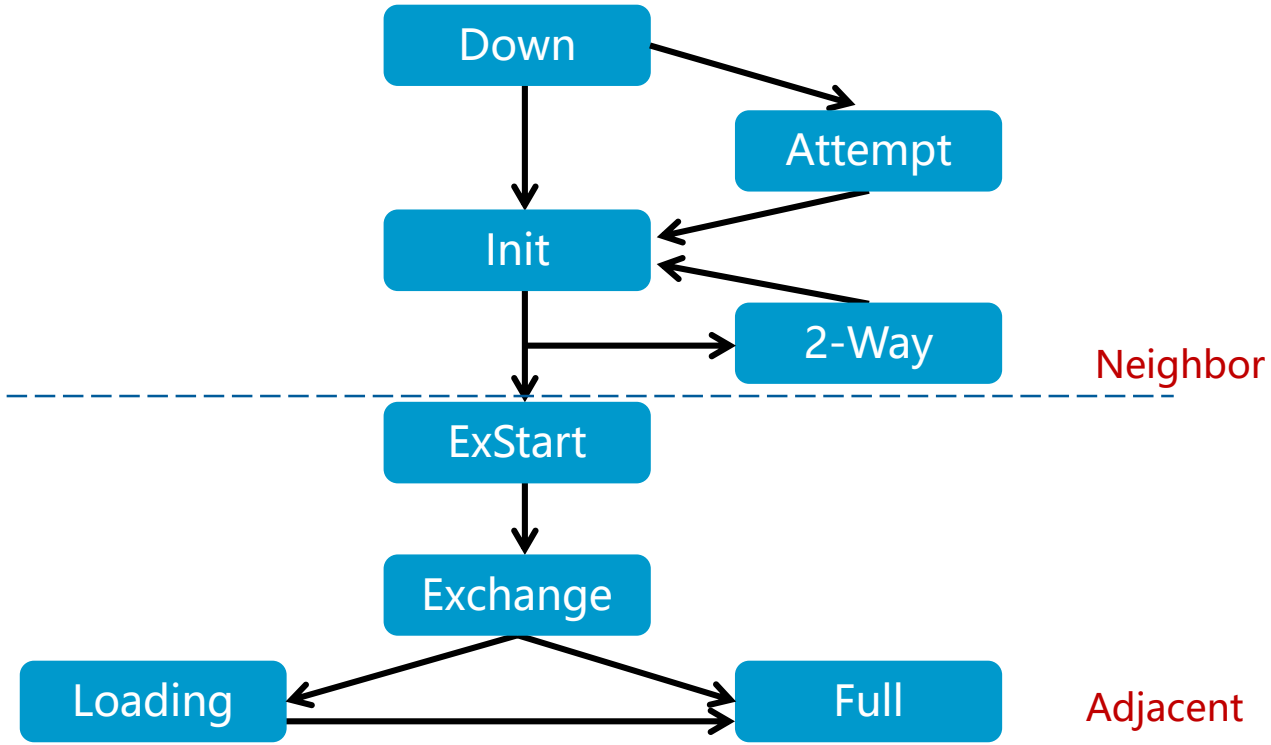
Etat des voisins

- Définit la forme de la relation entre voisins.
- Deux États voisins sont possibles, voisin et adjacent.



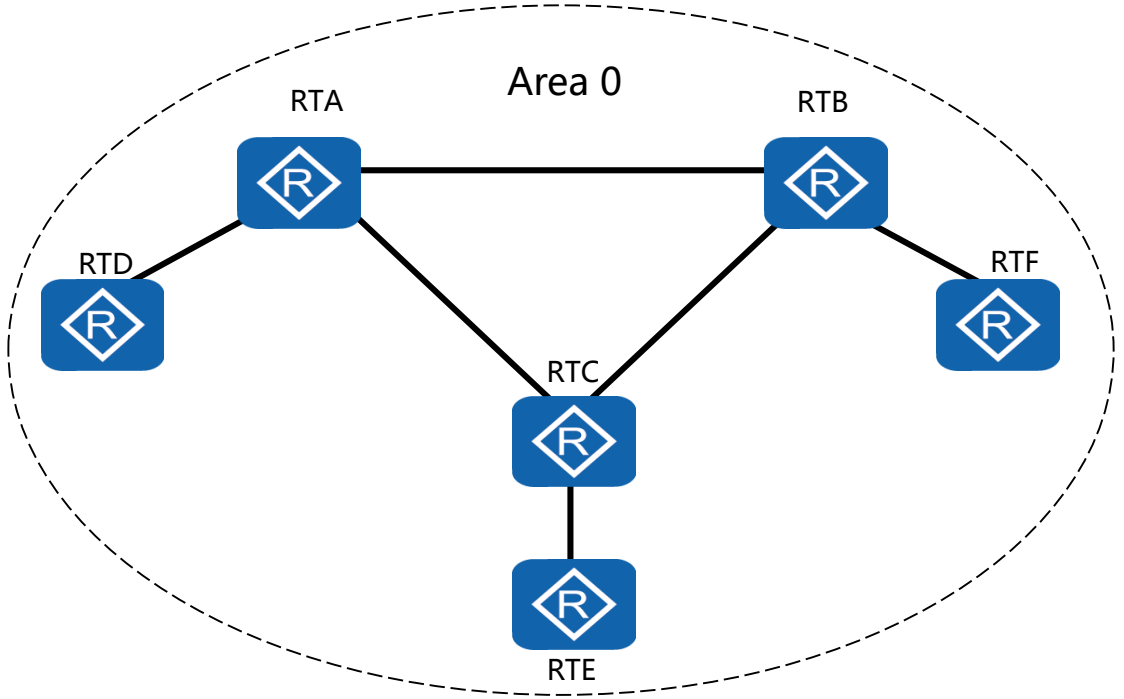
Etat des liaisons

Les changements d'État permettent d'atteindre les relations avec les voisins



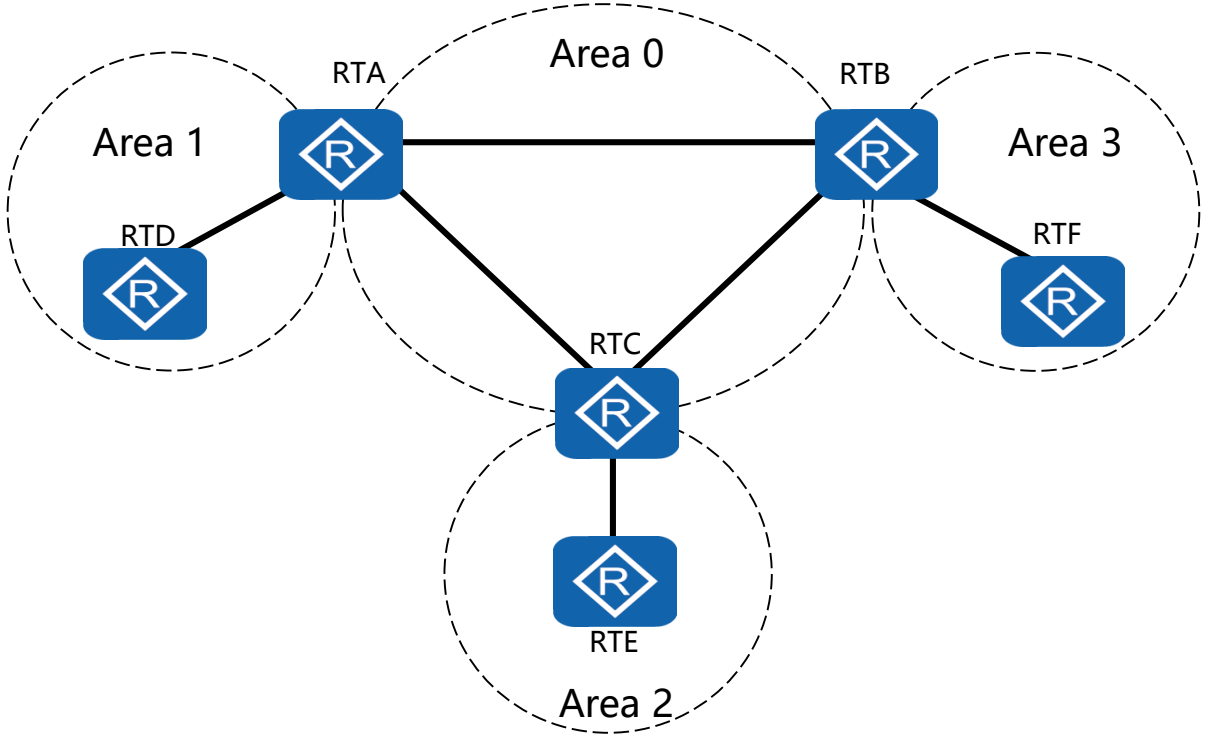
OSPF à zone unique

- Une base de données d'état des liens unique pour le domaine administratif
- N'importe quel numéro de zone peut être attribué, mais la zone 0 est recommandée.



OSPF à zones multiples

- Les zones construisent des bases de données LS distinctes, minimisent l'impact du changement.



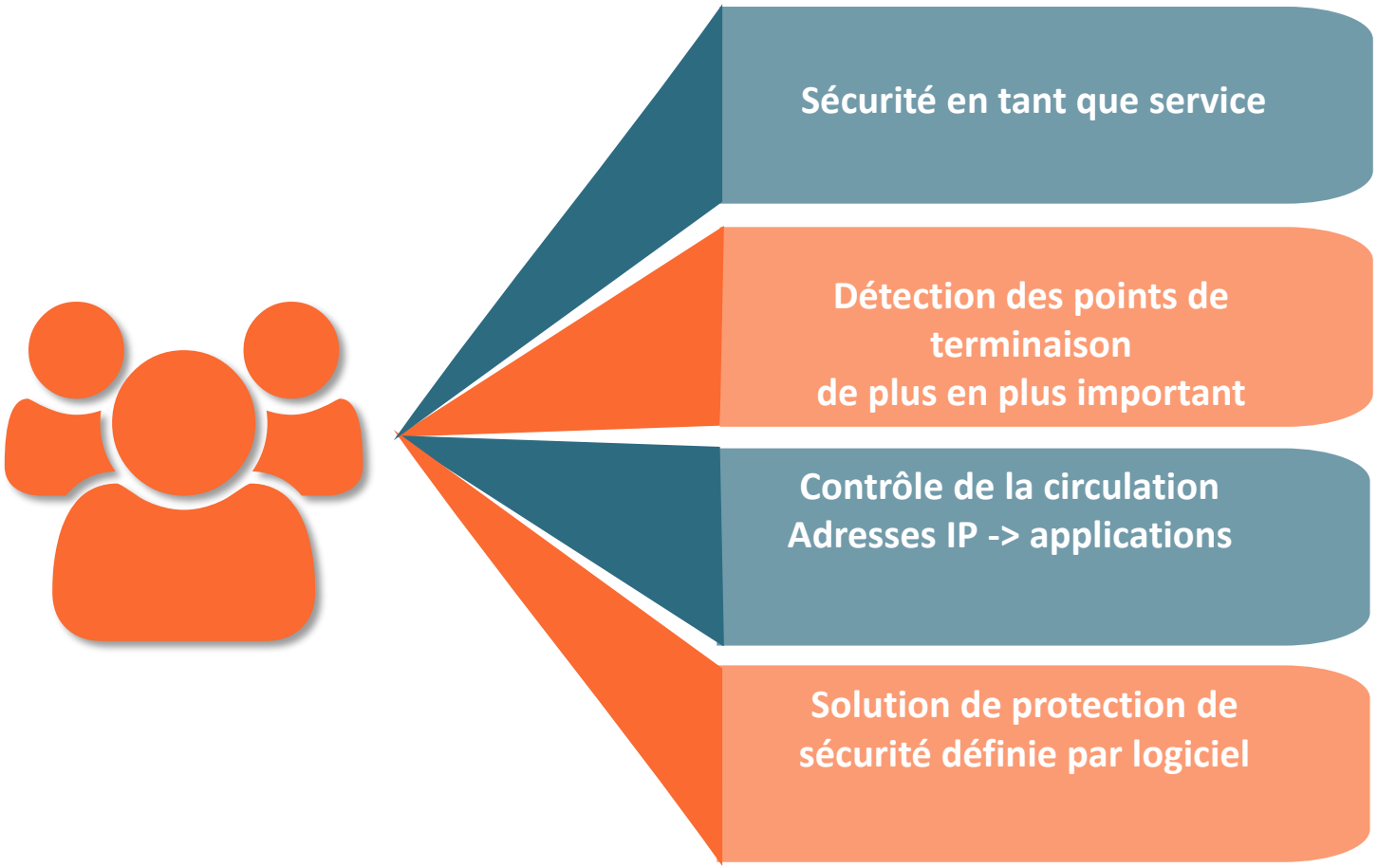
PARTIE 4

SÉCURISER UN RÉSEAU D'ENTREPRISE

CHAPITRE 1

RENFORCER LA SÉCURITÉ DU RÉSEAU

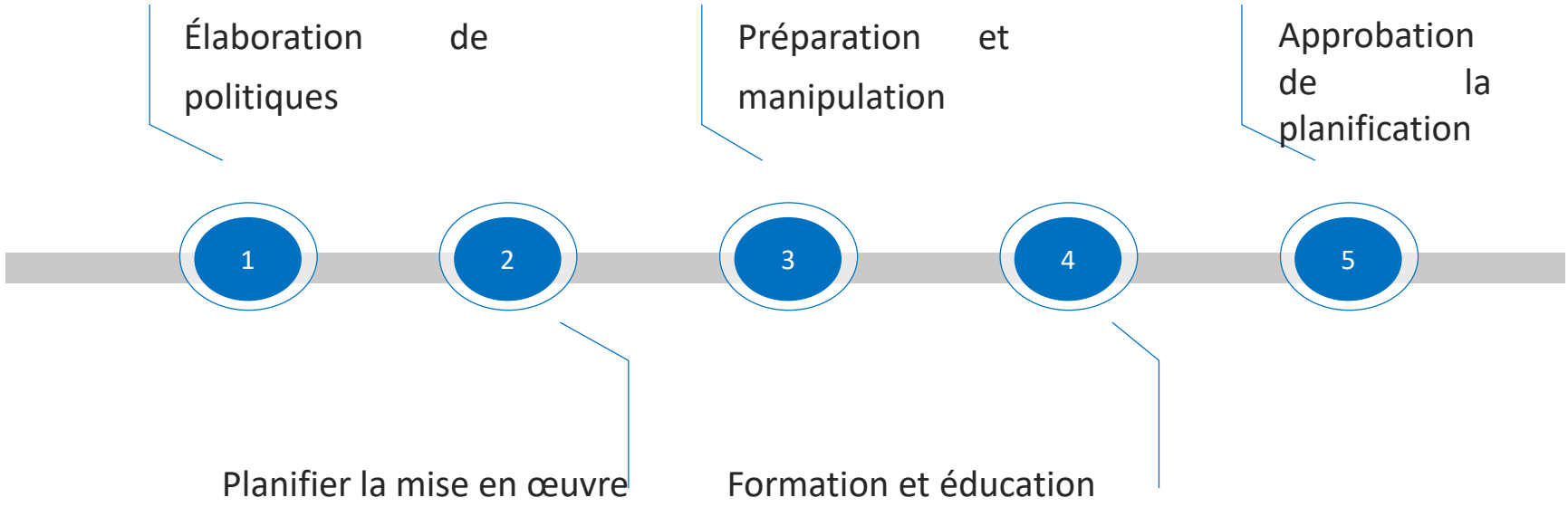
Principes de sécurité du réseau



Principes de sécurité du réseau

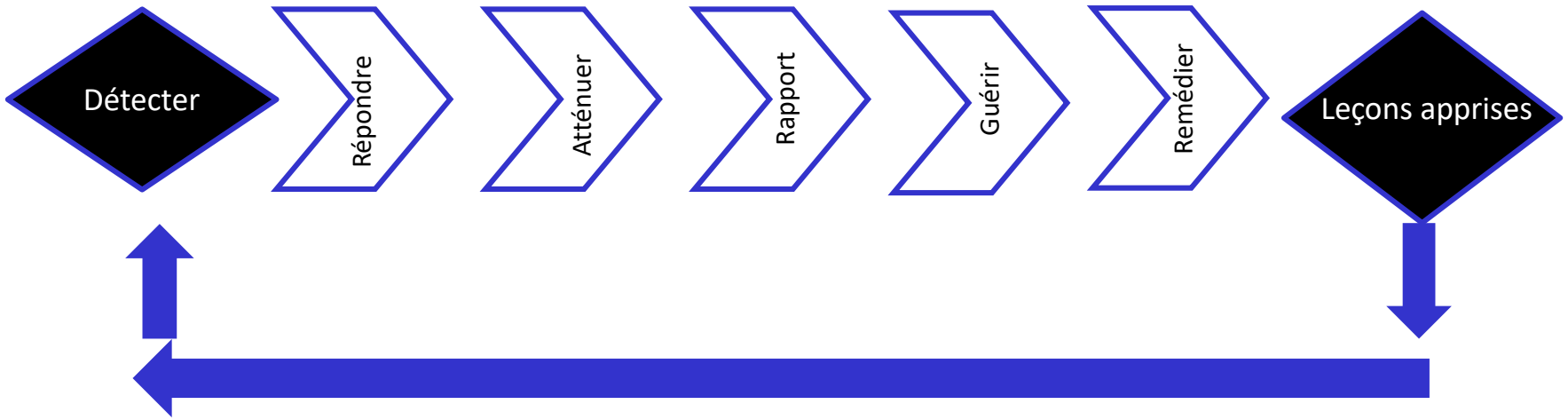
Rester vigilant en ligne est un moyen efficace de se défendre contre les escroqueries liées à la cybersécurité

Principes de sécurité du réseau



Principes de sécurité du réseau

Toutes les menaces ne peuvent pas être évitées, mais BCP (Business Continuity Planning) fournit des conseils de processus pour gérer les urgences et répondre aux incidents de menace dès que possible afin de minimiser les impacts sur les organisations.



CHAPITRE 1

RENFORCER LA SÉCURITÉ DU RÉSEAU

1 - Principes de sécurité du réseau

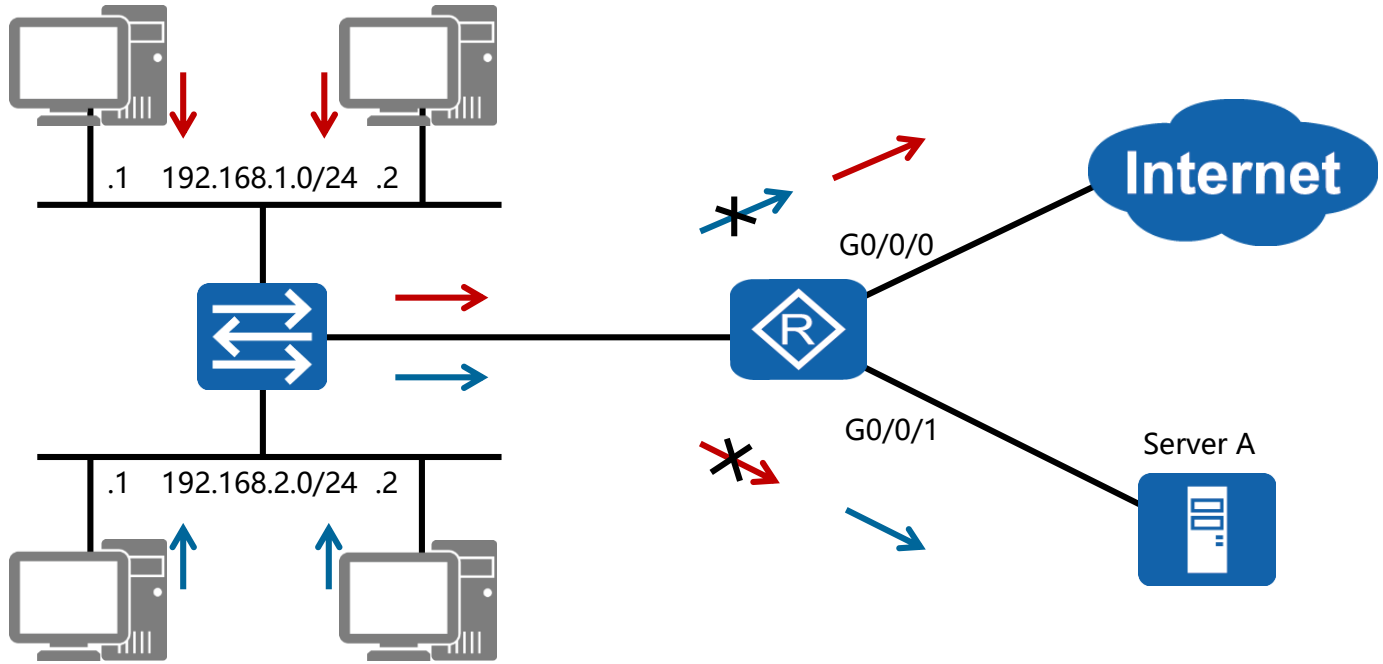
2 - Listes de contrôle d'accès

3 - Firewall et le proxy

Listes de contrôle d'accès

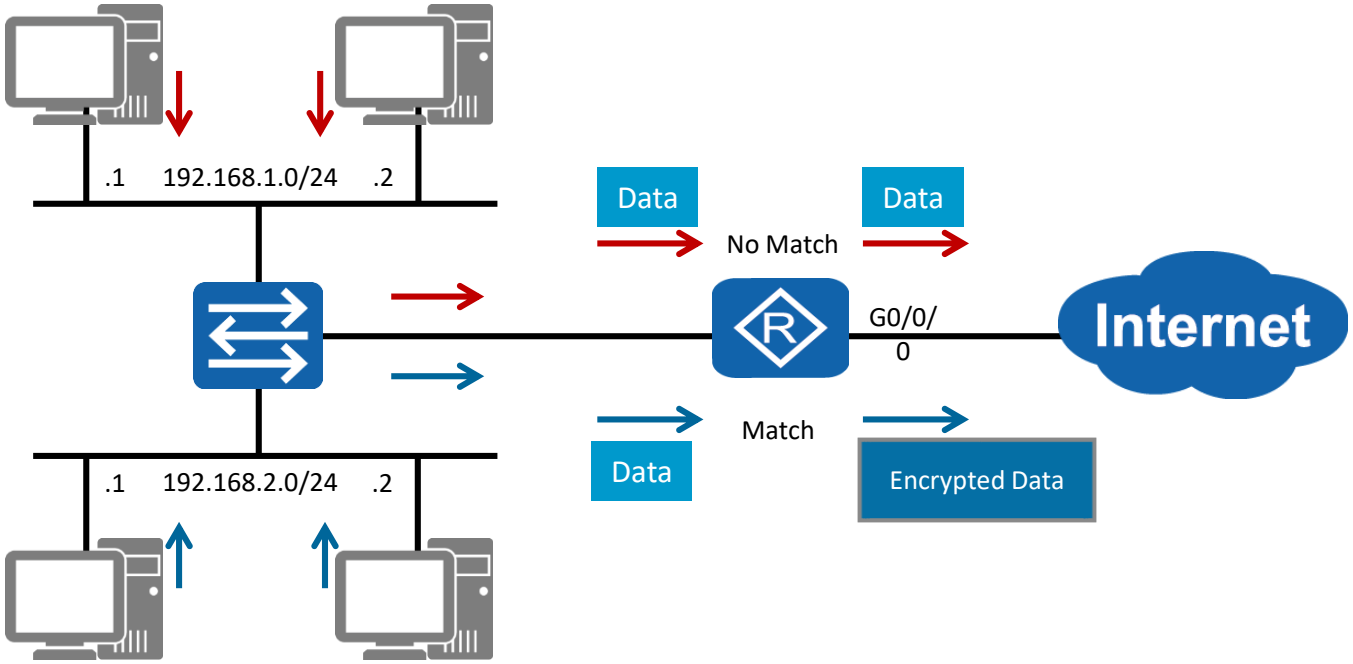
- Les paquets sont filtrés en fonction des adresses et des paramètres.

Les règles permettent de permettre ou de refuser les paquets.



Listes de contrôle d'accès

- Les paquets peuvent être filtrés pour manipuler le comportement et les actions.
- Les paramètres et le comportement de transmettre peuvent être modifiés.



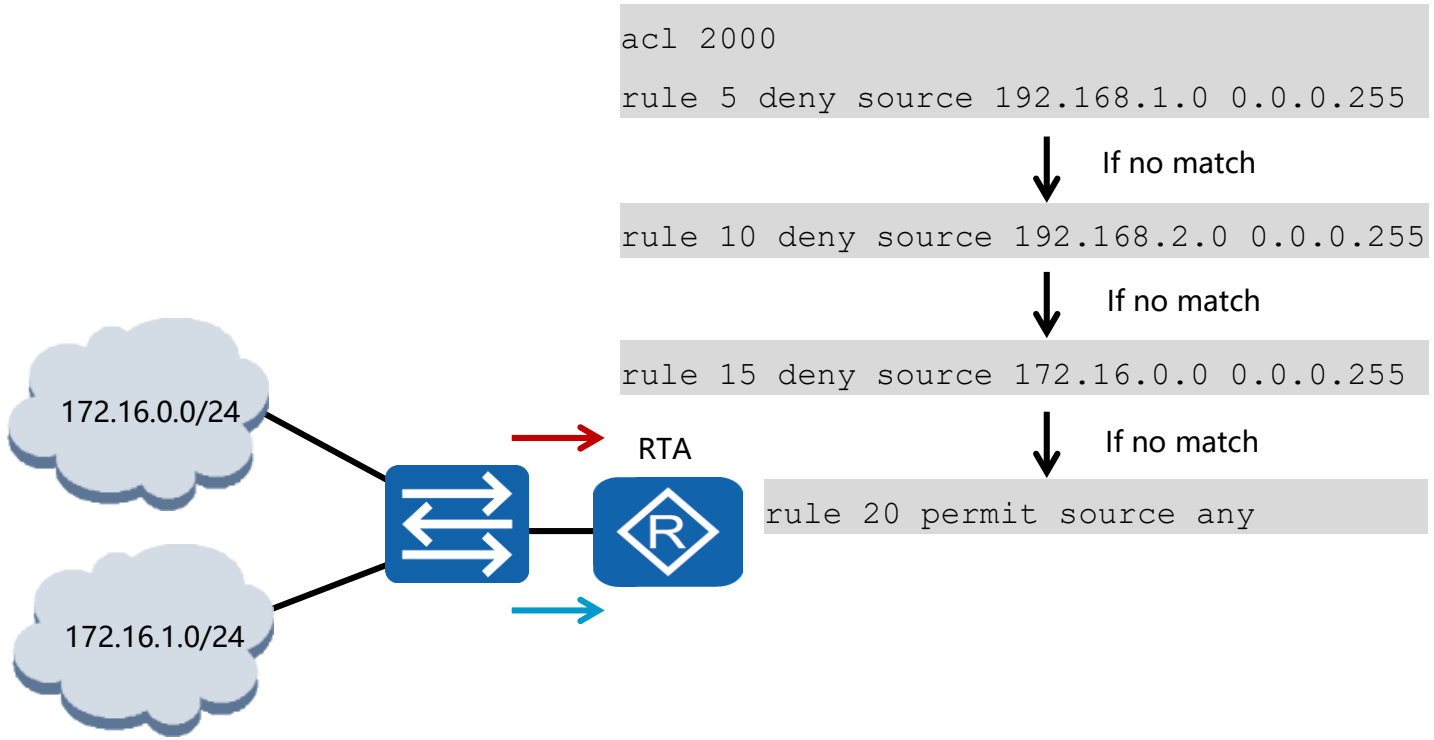
Types d’ACL

- Trois formes d’ACL peuvent être appliquées aux routeurs.
- Les paramètres de filtrage des paquets varient pour chaque type d’ACL.

Types	Value Ranges	Parameters
Basic	2000-2999	Source IP
Advanced	3000-3999	Source & Destination IP, Protocol, Source & Destination Port
Layer 2 ACL	4000-4999	MAC Address

Gestion des règles

Les règles sont utilisées pour gérer le processus de décision de chaque ACL.

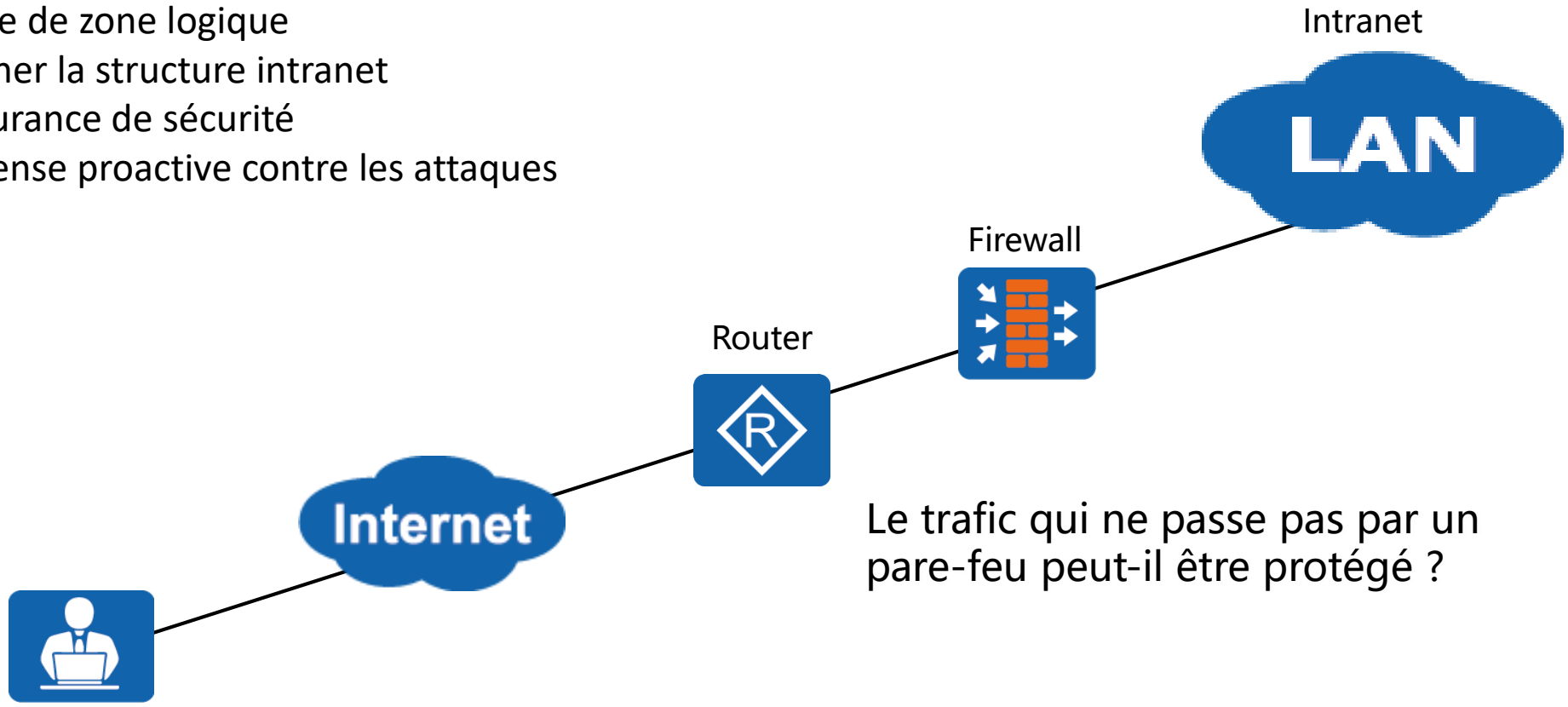


CHAPITRE 1

RENFORCER LA SÉCURITÉ DU RÉSEAU

Firewall et le proxy

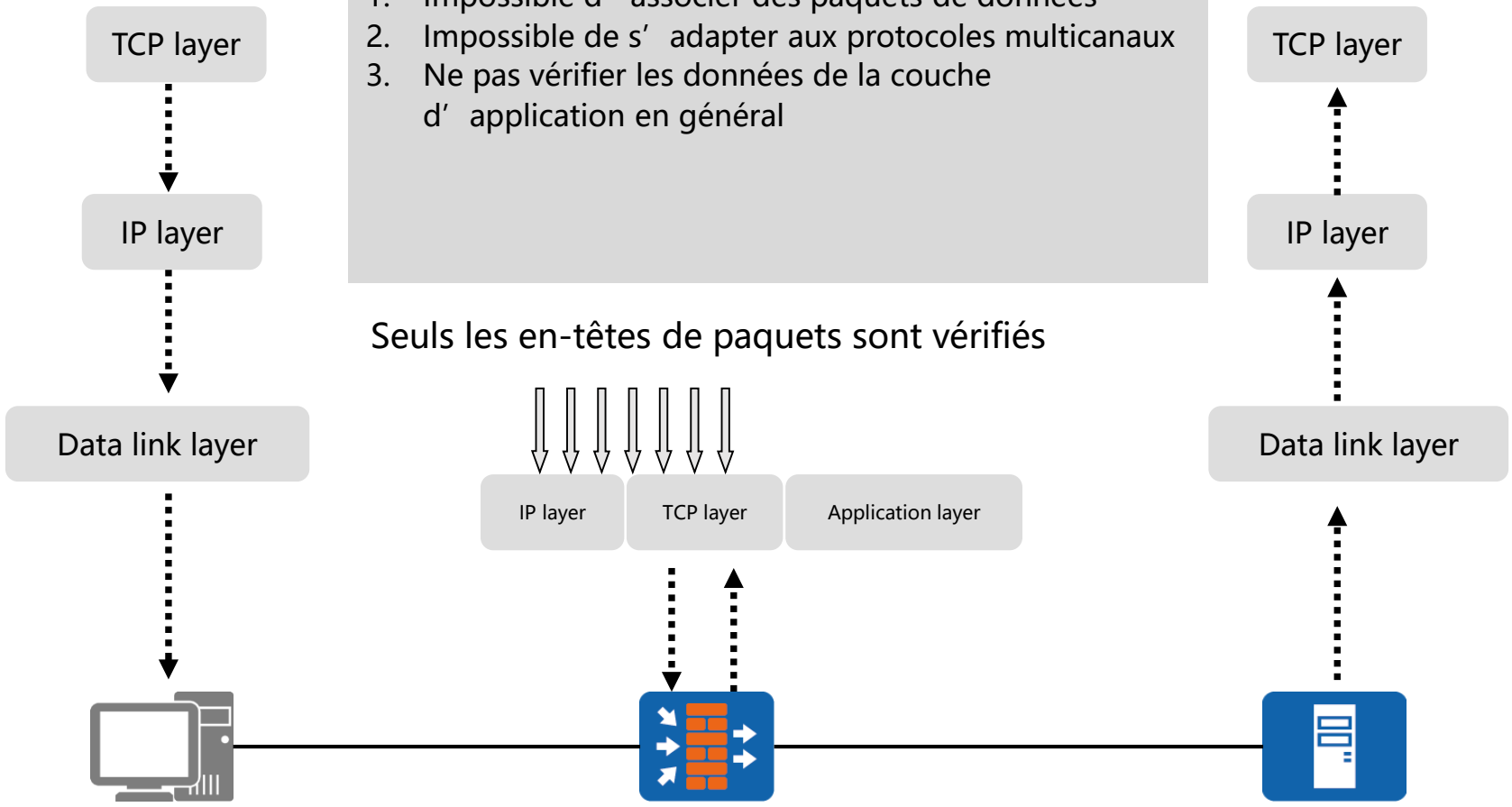
- Filtre de zone logique
- Cacher la structure intranet
- Assurance de sécurité
- Défense proactive contre les attaques



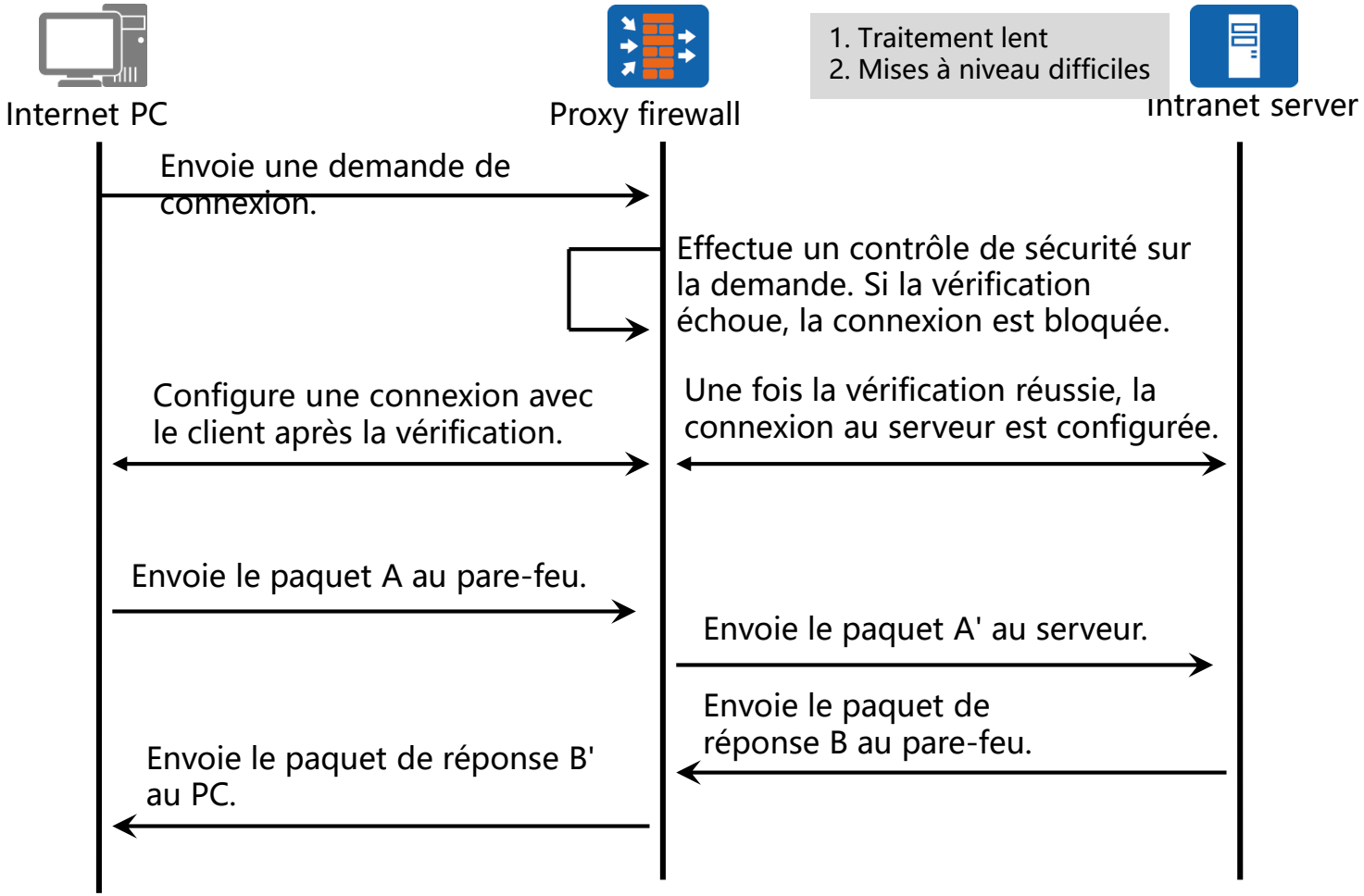
Le trafic qui ne passe pas par un pare-feu peut-il être protégé ?

Pare-feu filtrant les paquets

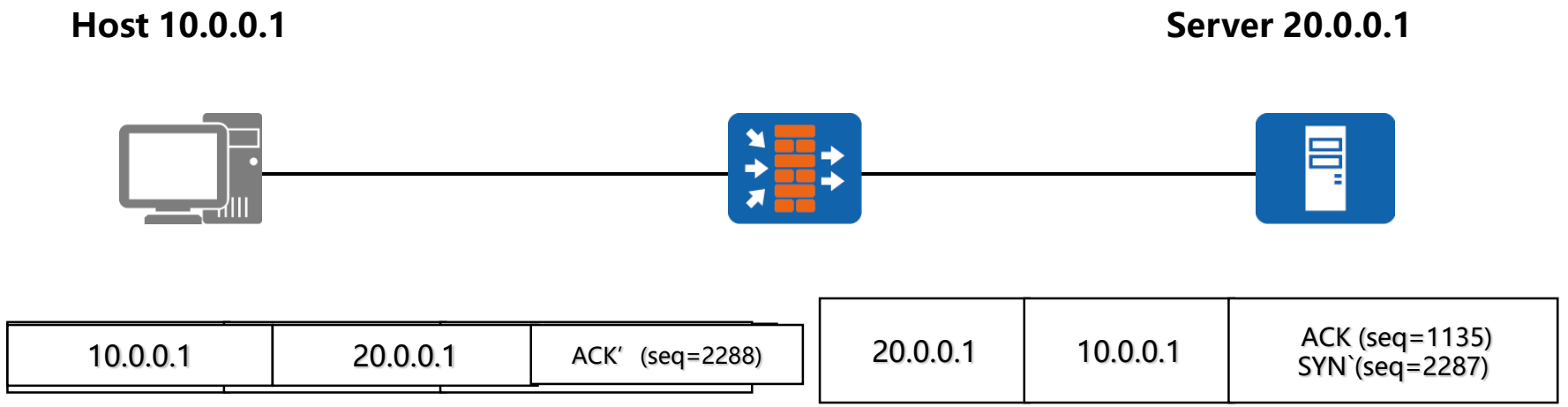
1. Impossible d’ associer des paquets de données
2. Impossible de s’ adapter aux protocoles multicanaux
3. Ne pas vérifier les données de la couche d’ application en général



Pare-feu proxy



Pare-feu d’inspection « stateful »



État incorrect, ignoré

Vérification de la stratégie de sécurité

Enregistrement des informations de session

1. Traitement rapide des paquets suivants
2. Haute sécurité

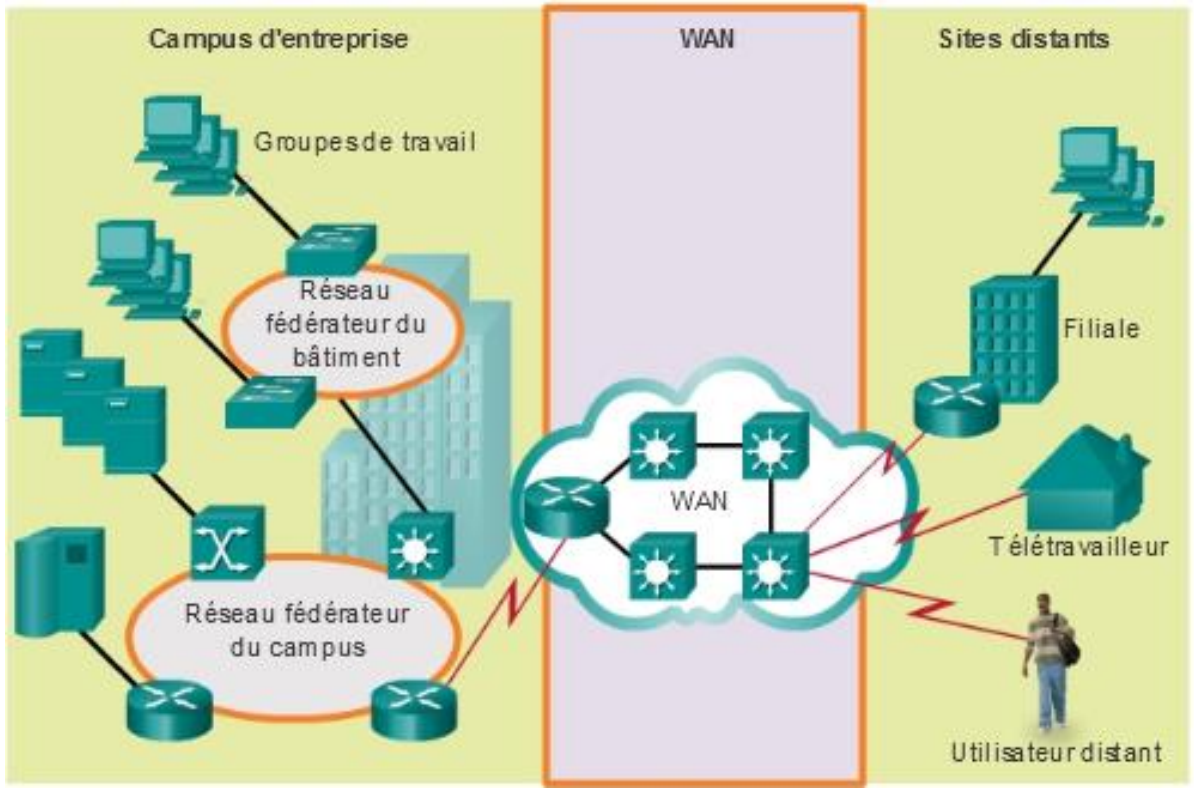
CHAPITRE 2

METTRE EN ŒUVRE UN WAN

Principes de sécurité du réseau

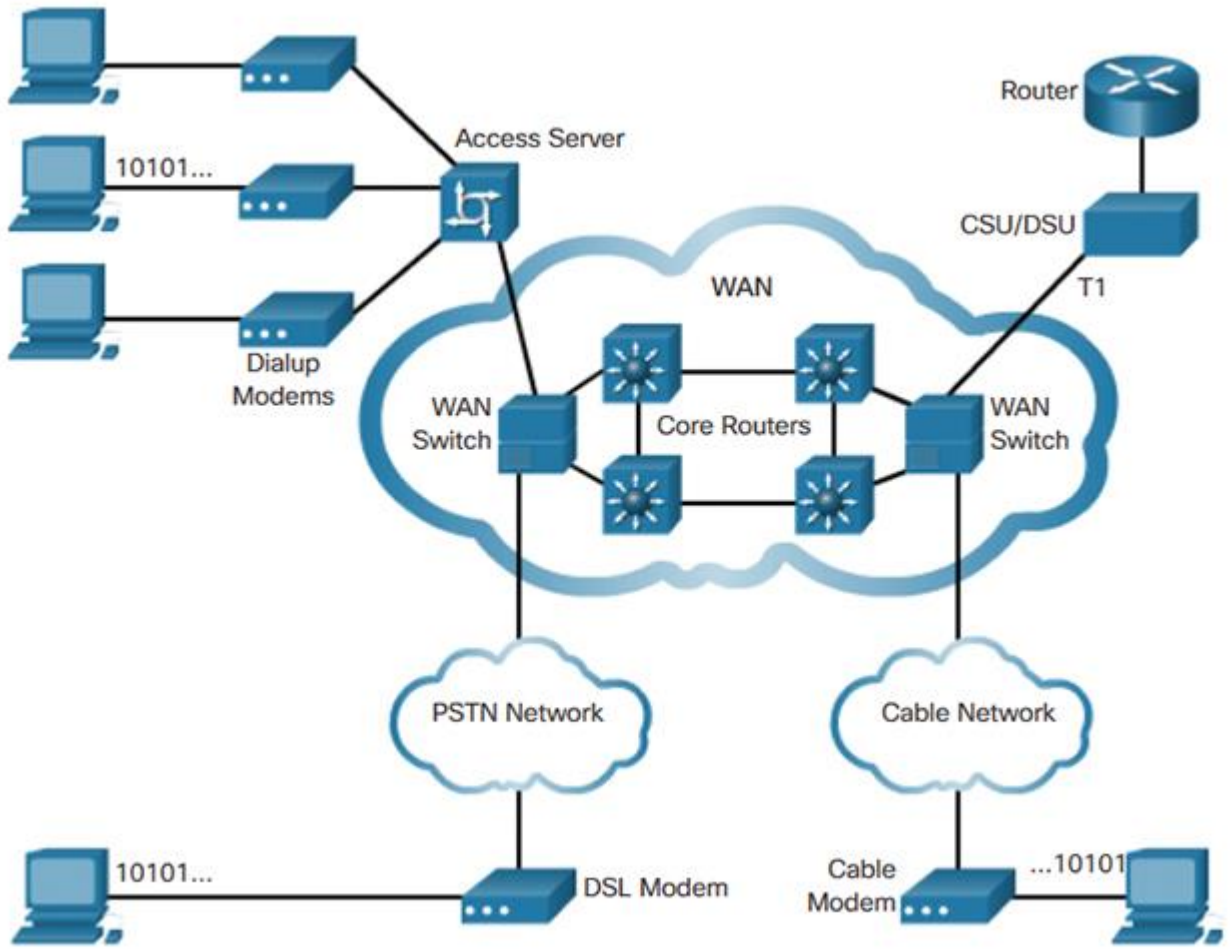
Introduction aux technologies WAN

- Le WAN est la propriété du fournisseur de services.
- L'organisation doit payer pour utiliser les services de réseau du fournisseur pour connecter des sites distants.
- Les fournisseurs de services WAN comprennent les opérateurs de réseau téléphonique, de réseau câblé ou de service par satellite.



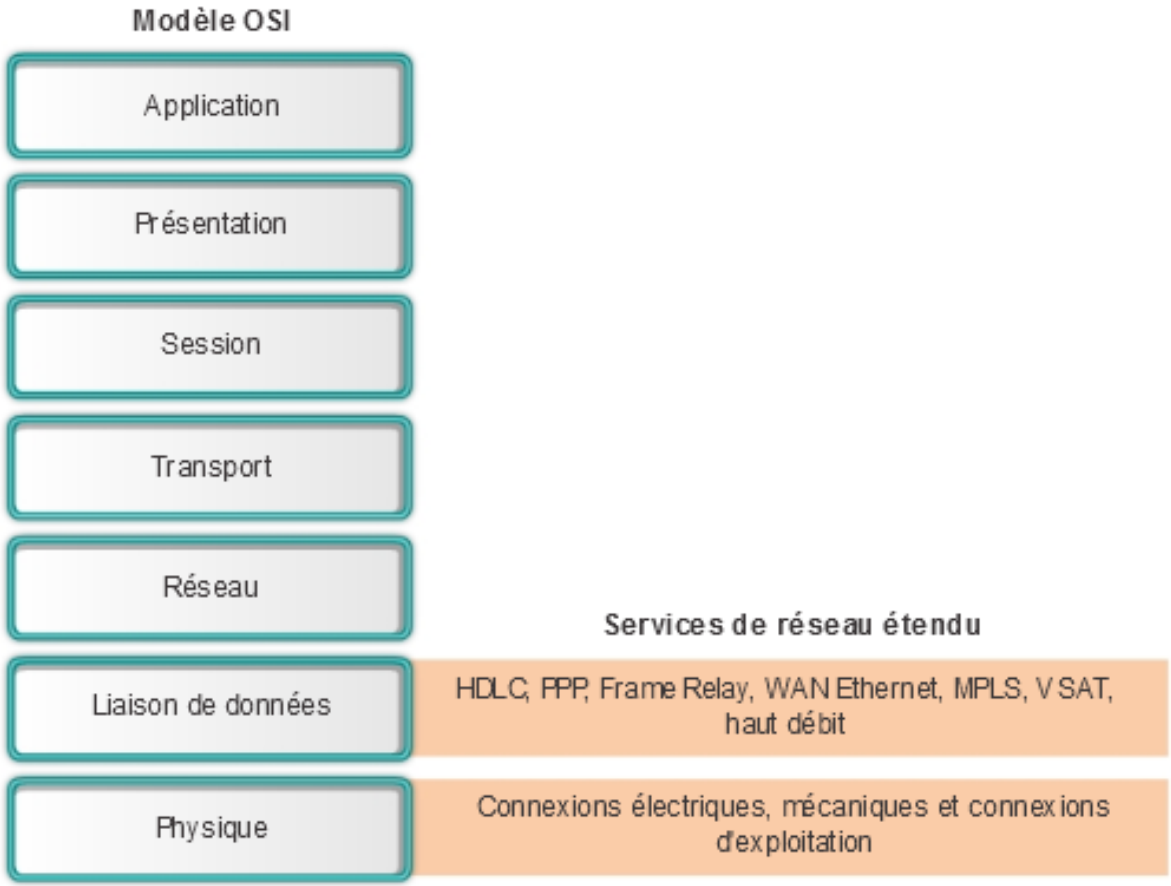
Principes de sécurité du réseau

Périphériques WAN



Principes de sécurité du réseau

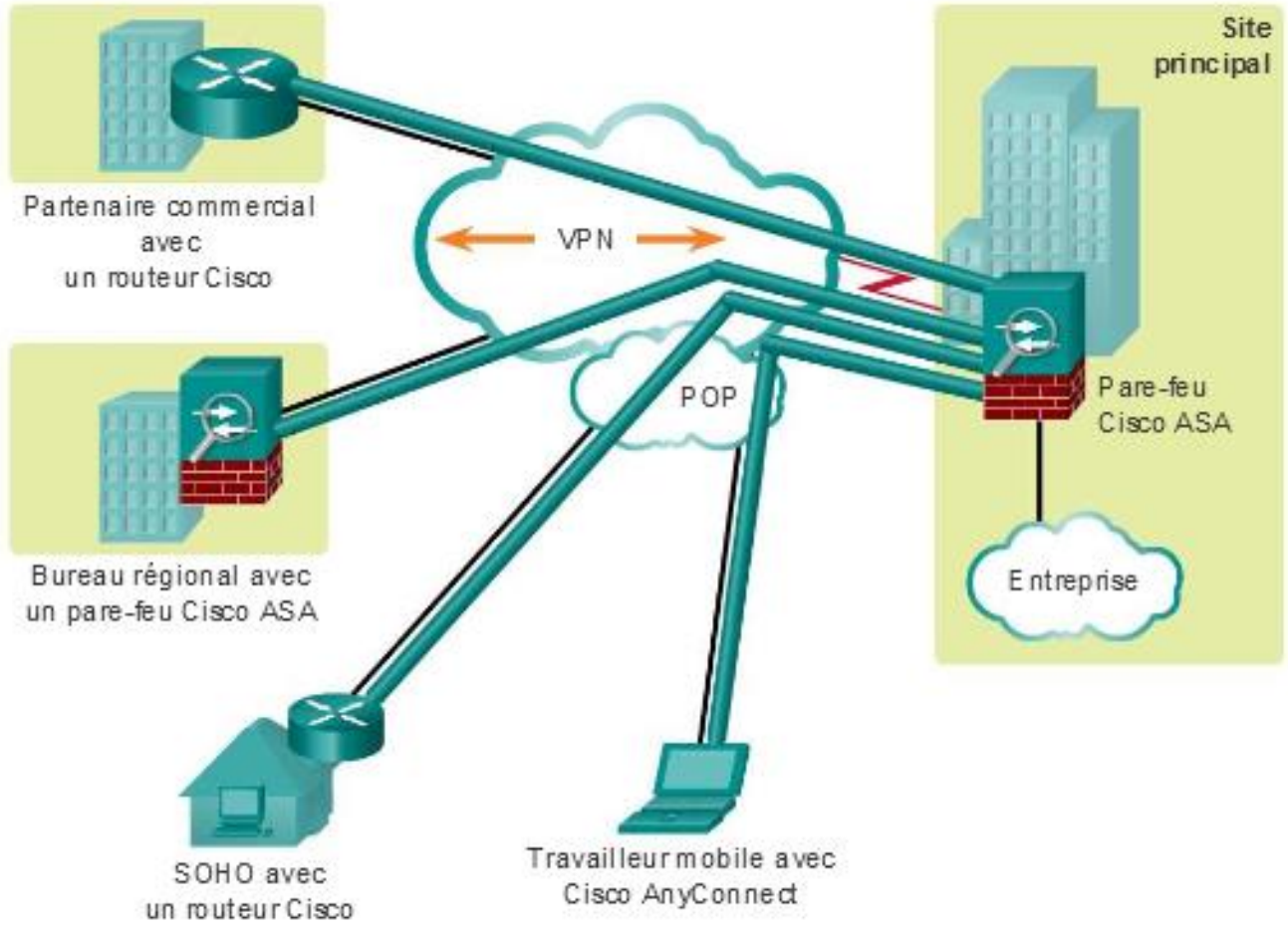
Le fonctionnement du WAN



Principes de sécurité du réseau

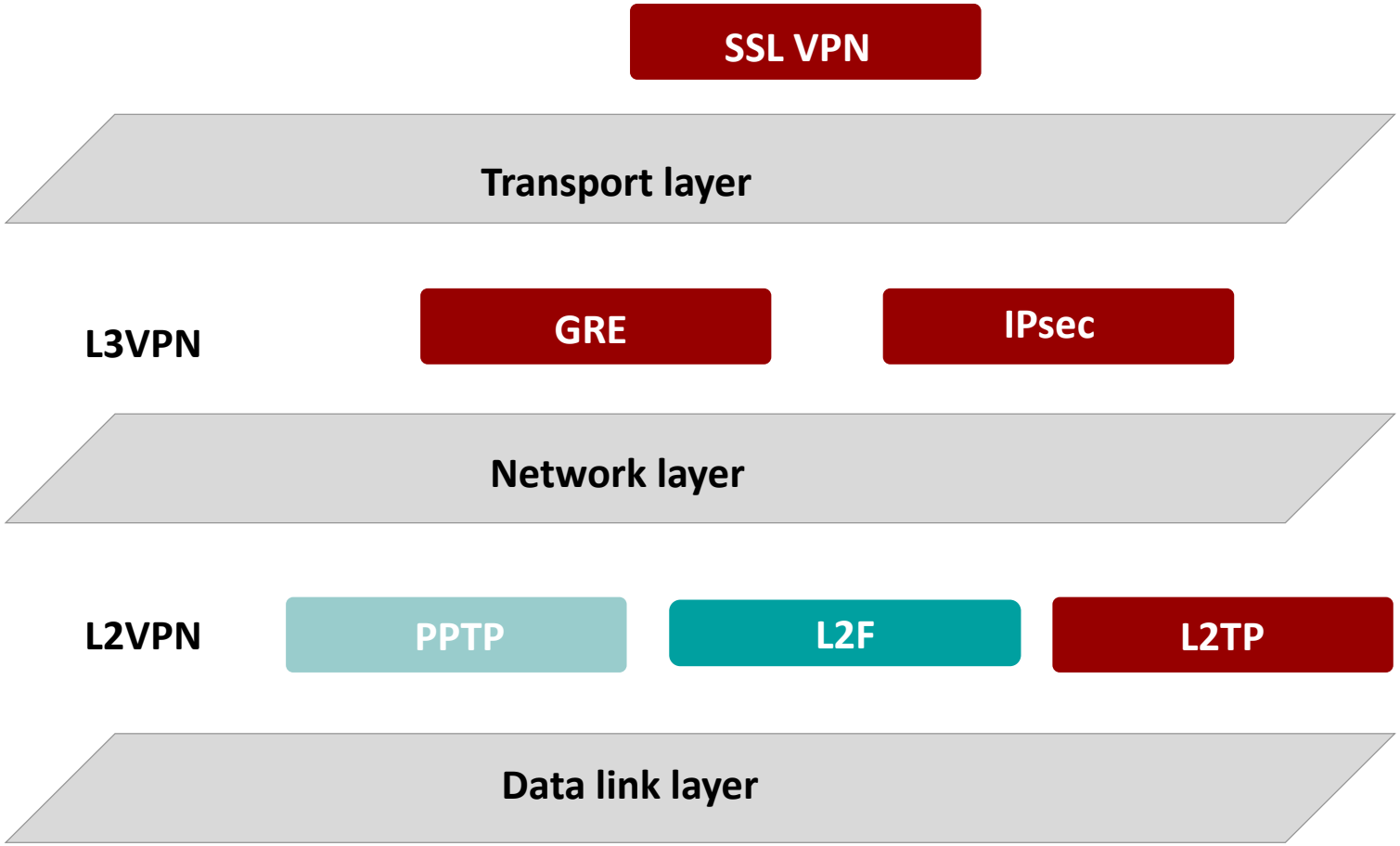
Réseaux privés virtuels (VPN)

- Les entreprises utilisent des VPN pour créer une connexion sécurisée de bout en bout par réseau privé sur des réseaux tiers, comme Internet ou des extranets.
- Le tunnel supprime la barrière de distance et permet aux utilisateurs distants d'accéder aux ressources réseau du site central.
- Un VPN est un réseau privé créé par tunneling sur un réseau public, généralement Internet.



Principes de sécurité du réseau

Principes VPN et IPsec



Principes de sécurité du réseau

Scénarios d'application des VPN

Site-to-Site VPN

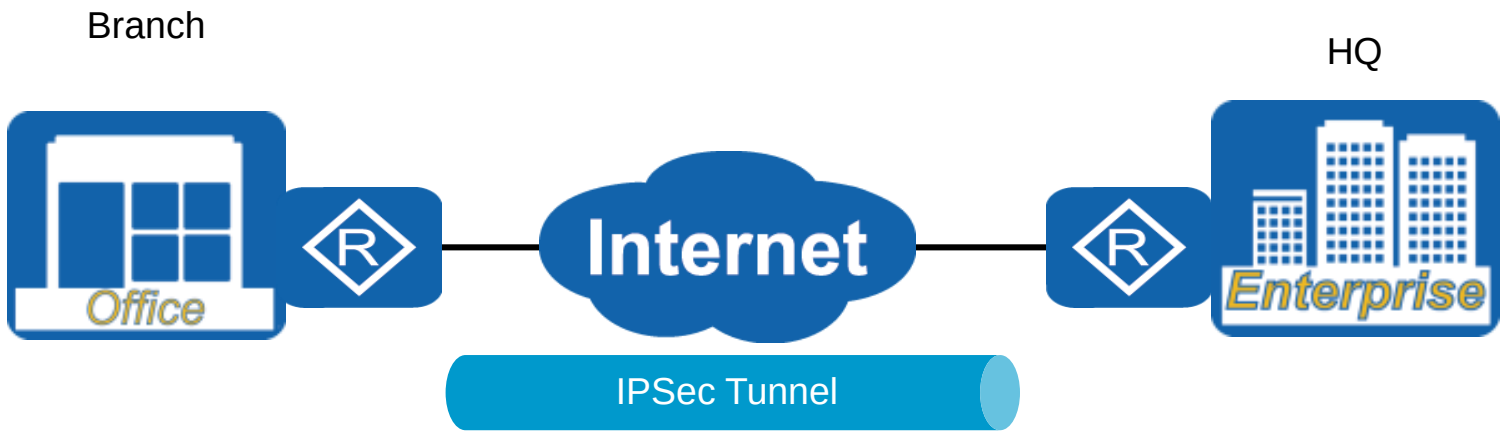
- Connexion entre deux LAN
- Technologies VPN applicables : IPsec, L2TP, L2TP over IPsec, GRE over IPsec, et IPsec over GRE

Client-to-Site VPN

- Connexion entre les clients et un intranet d'entreprise
- Technologies VPN applicables : SSL, IPsec, L2TP et L2TP sur IPsec

Principes de sécurité du réseau

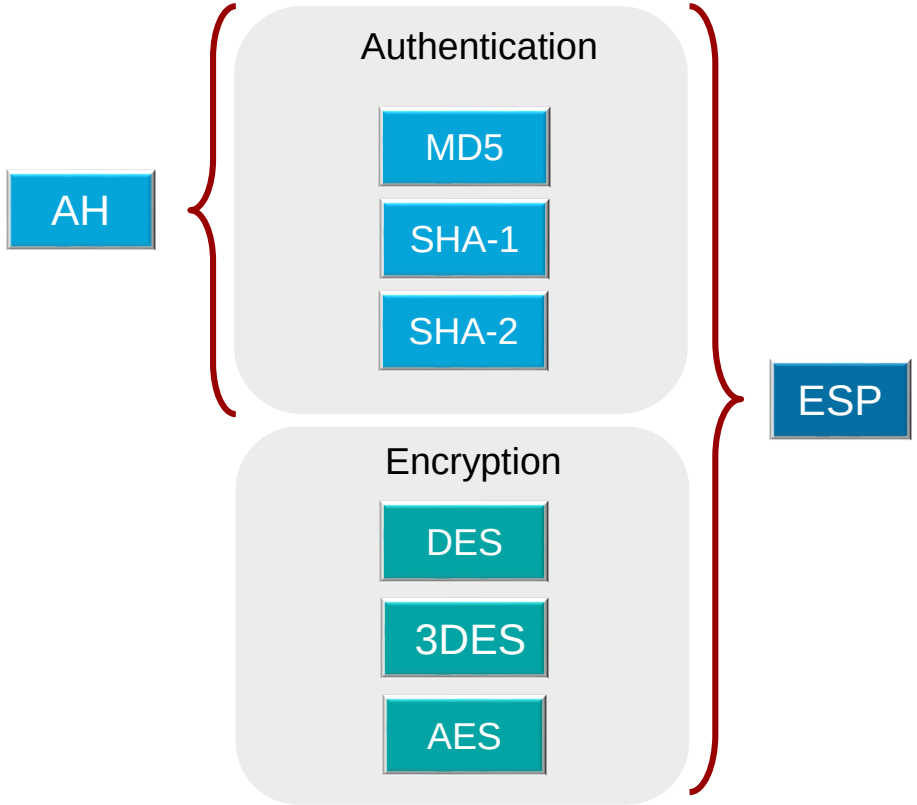
Application IPSec VPN



Facilite l'établissement d'une communication de réseau privé sur une infrastructure de réseau public

Principes de sécurité du réseau

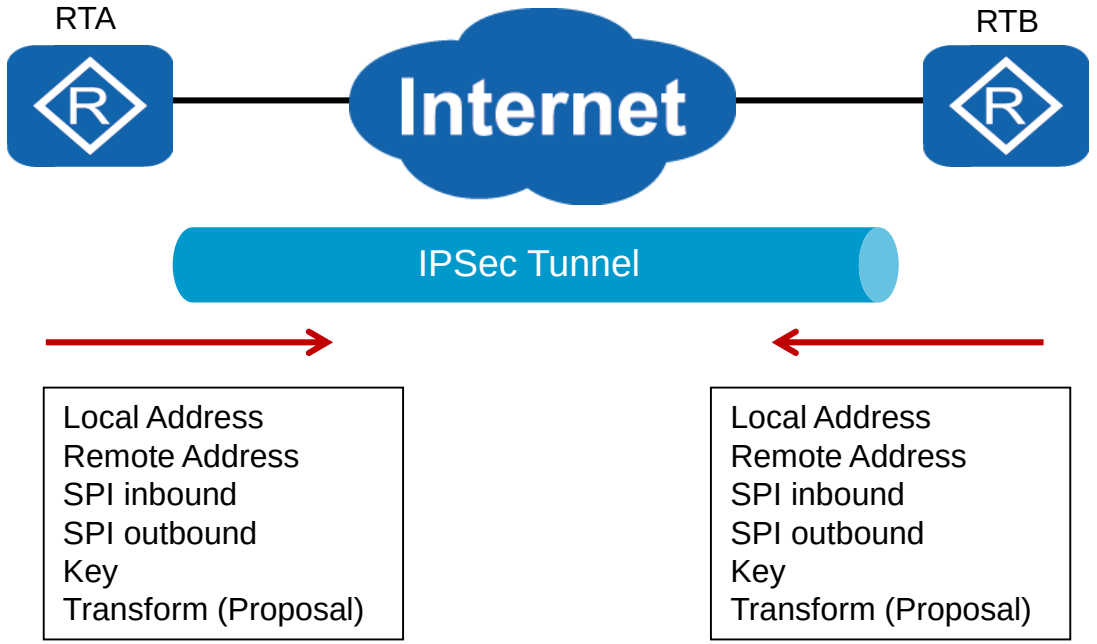
Architecture IPSec VPN



La confidentialité et l'intégrité des services sont prises en charge par des protocoles basés sur l'authentification et le cryptage

Principes de sécurité du réseau

Association de sécurité



- Spécifie les paramètres d'établissement de la connexion.
- Une association de sécurité définit des paramètres dans une seule direction

CHAPITRE 2

METTRE EN ŒUVRE UN WAN

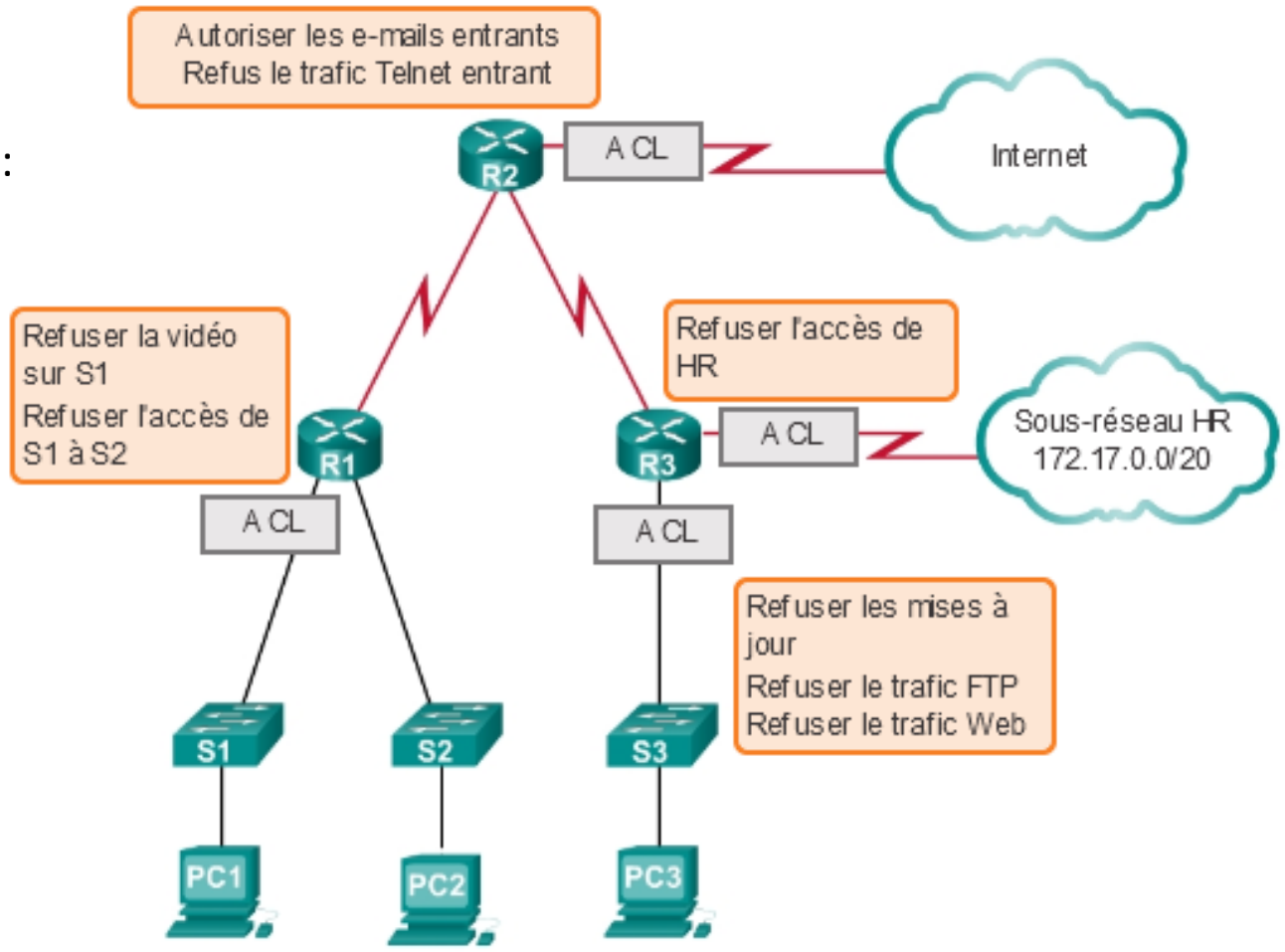
1 - Principes de sécurité du réseau

2 - Listes de contrôle d'accès

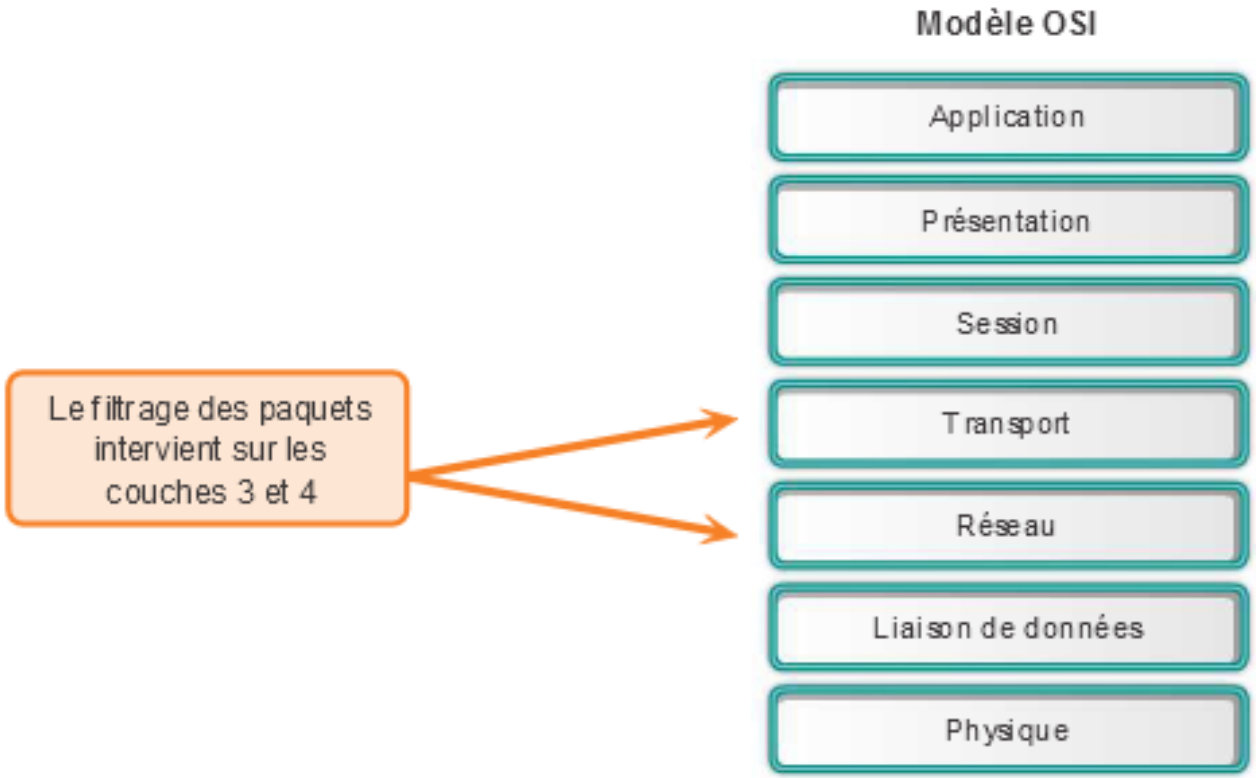
3 - Optimisation de l’adressage IP

Listes de contrôle d'accès

- les listes de contrôle d'accès assurent les tâches suivantes :
  - Elles limitent le trafic réseau pour accroître les performances réseau.
  - Elles contrôlent le flux de trafic.
  - Elles fournissent un niveau de sécurité de base pour l'accès réseau.
  - Elles filtrent le trafic en fonction de son type.

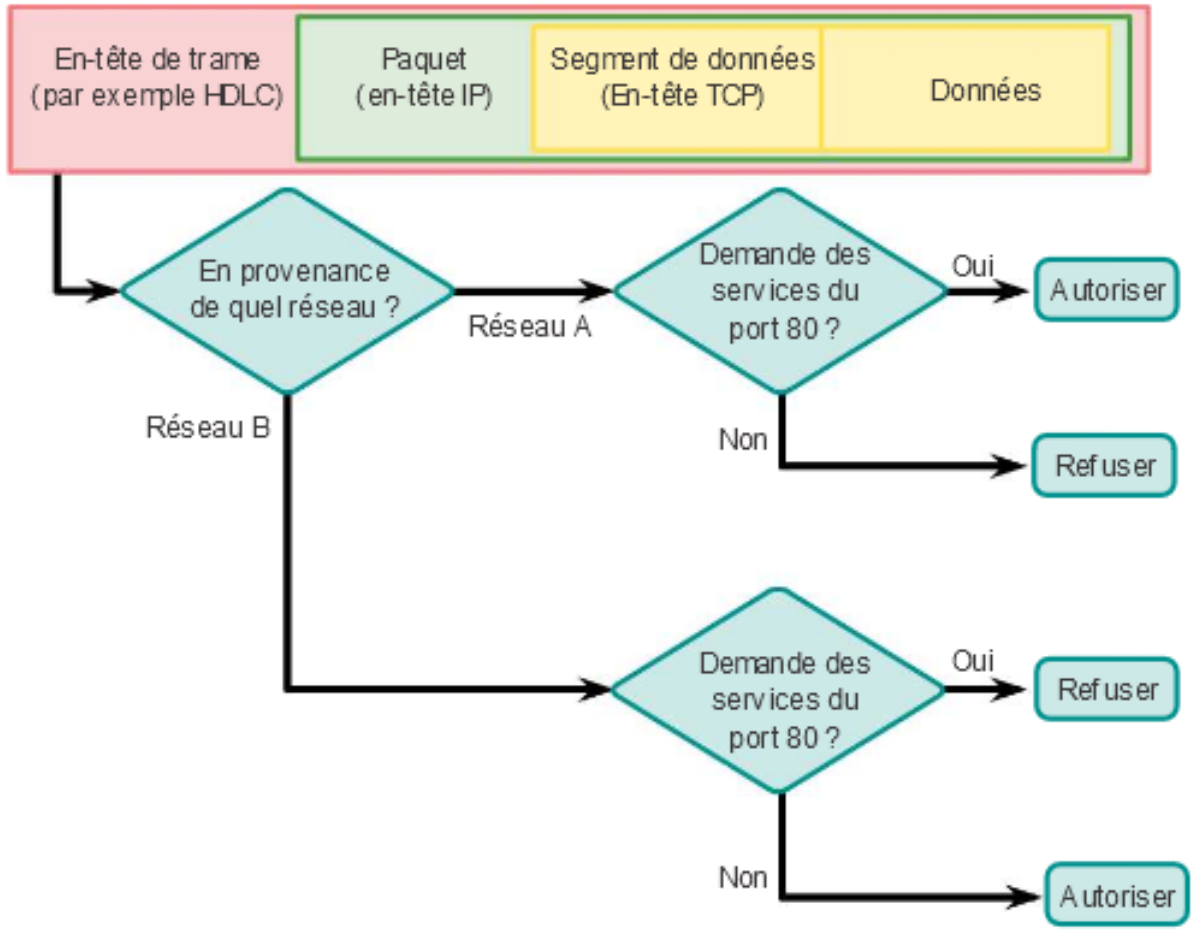


Listes de contrôle d'accès



Listes de contrôle d'accès

Exemple de filtrage des paquets



Listes de contrôle d'accès

Exemple de filtrage des paquets

Les listes de contrôle d'accès entrantes filtrent les paquets entrant dans une interface spécifique avant qu'ils ne soient acheminés vers l'interface de sortie.

Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.

CHAPITRE 2

METTRE EN ŒUVRE UN WAN

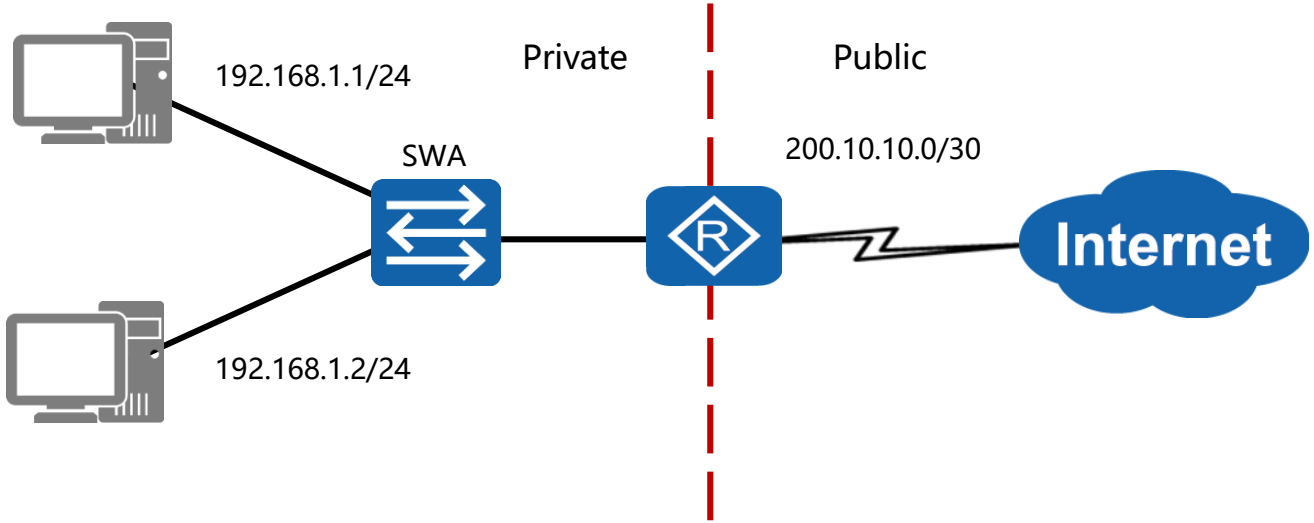
1 - Principes de sécurité du réseau

2 - Listes de contrôle d'accès

3 - Optimisation de l’adressage IP

Optimisation de l’adressage IP

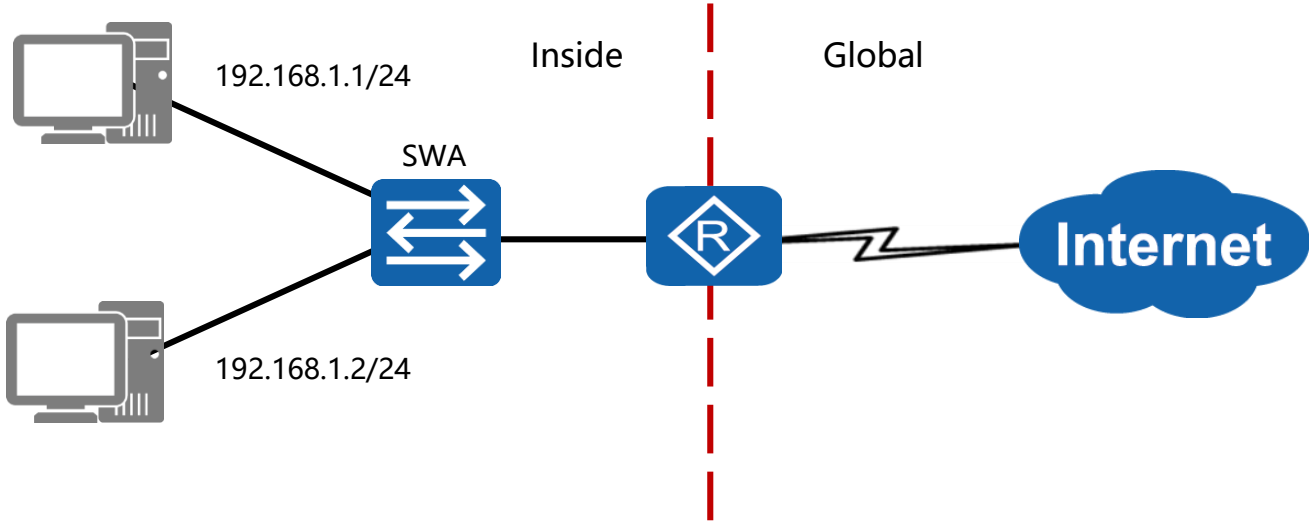
Réseaux privés et publics



- Une mesure prise contre l’épuisement rapide des adresses IP.
- Gateway fonctionne comme une limite d’adresse privée/publique.

Optimisation de l’adressage IP

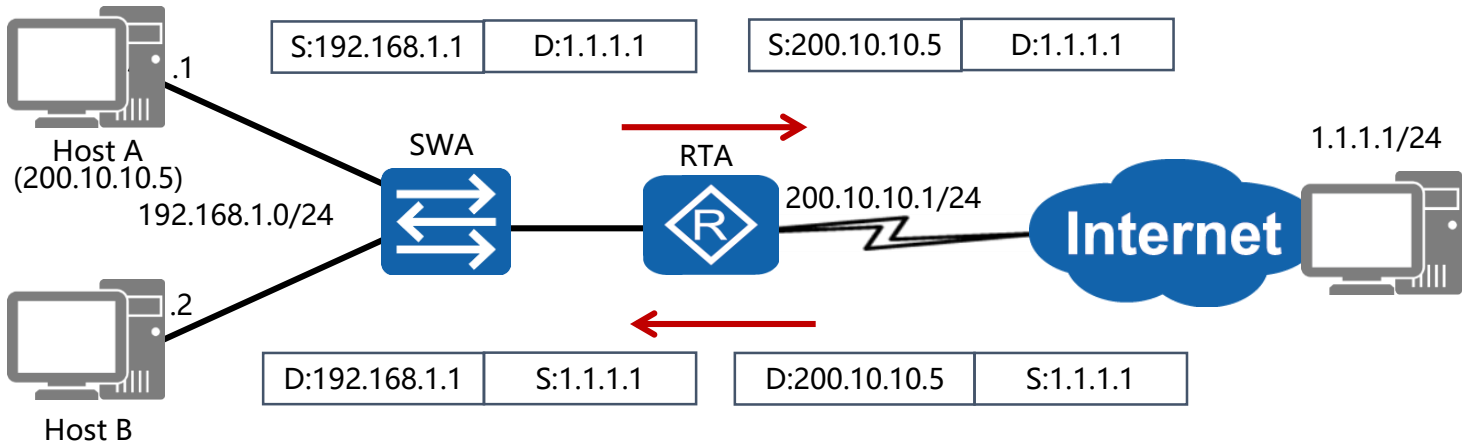
Comportement du NAT



- Les limites du NAT sont représentées à l’intérieur ou à l’échelle mondiale.
- La traduction des adresses se fait entre les limites.

Optimisation de l’adressage IP

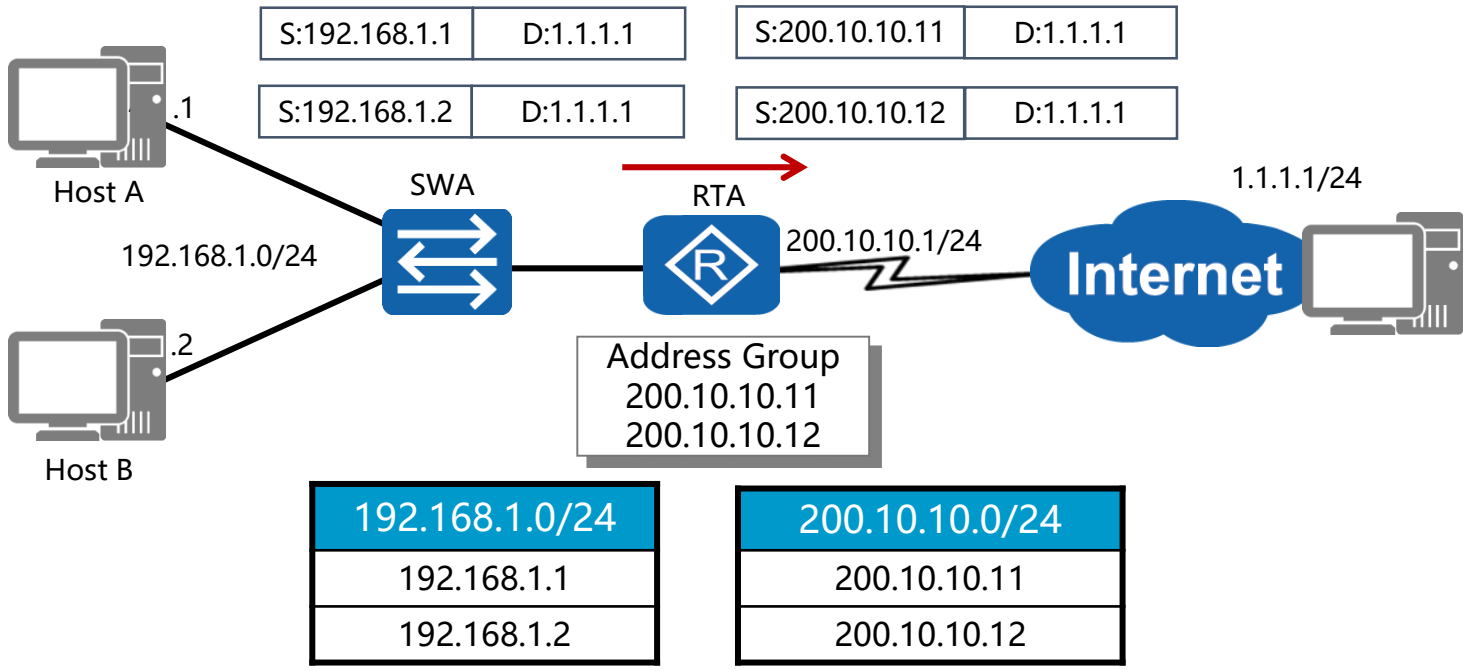
NAT statique



- One-to-one mapping d’adresses privées à publiques.
- Limite le besoin de gestion des adresses avec les flux de session

Optimisation de l’adressage IP

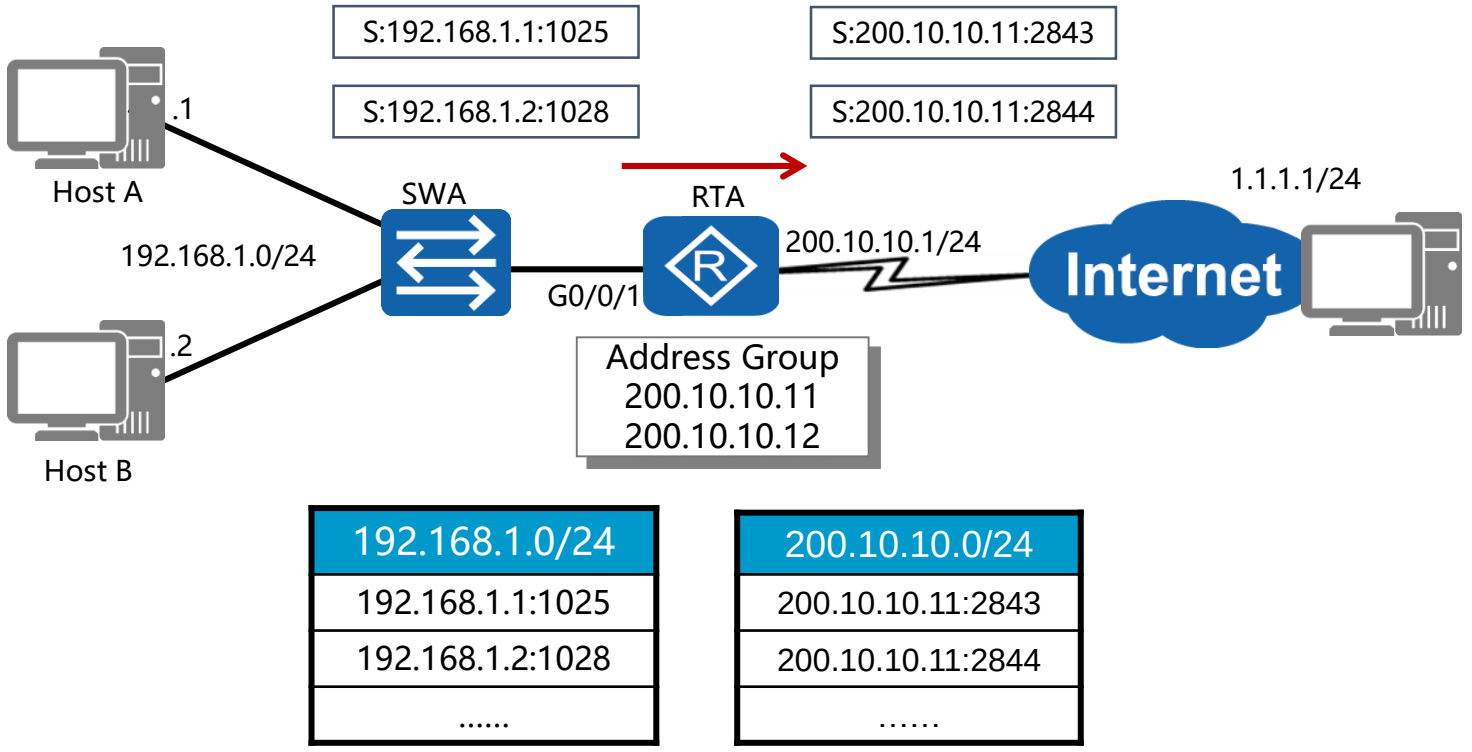
NAT dynamique



- Adresse privée mapping sur la base d’un pool d’adresses.
- Permet aux utilisateurs d’utiliser des adresses publiques en fonction des besoins

Optimisation de l’adressage IP

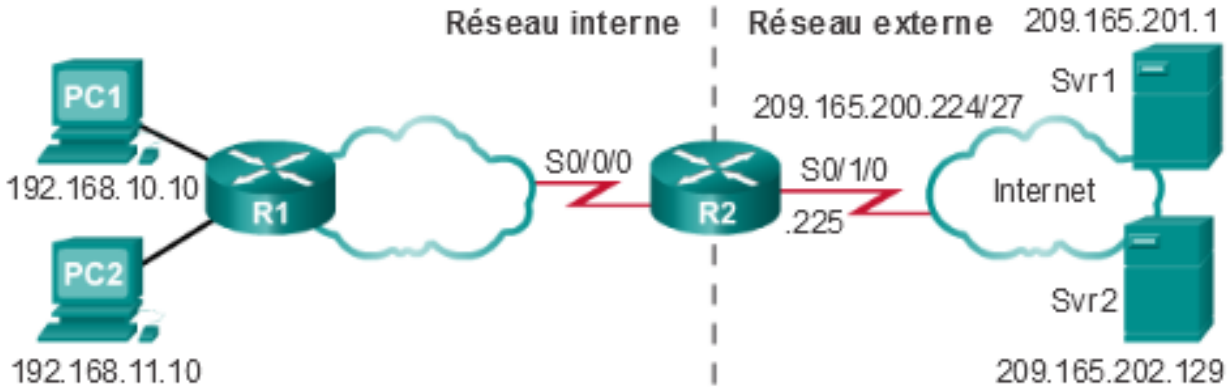
Network Address Port Translation



- Les numéros de port distinguent mapping de la même adresse publique

Optimisation de l’adressage IP

Exemple PAT



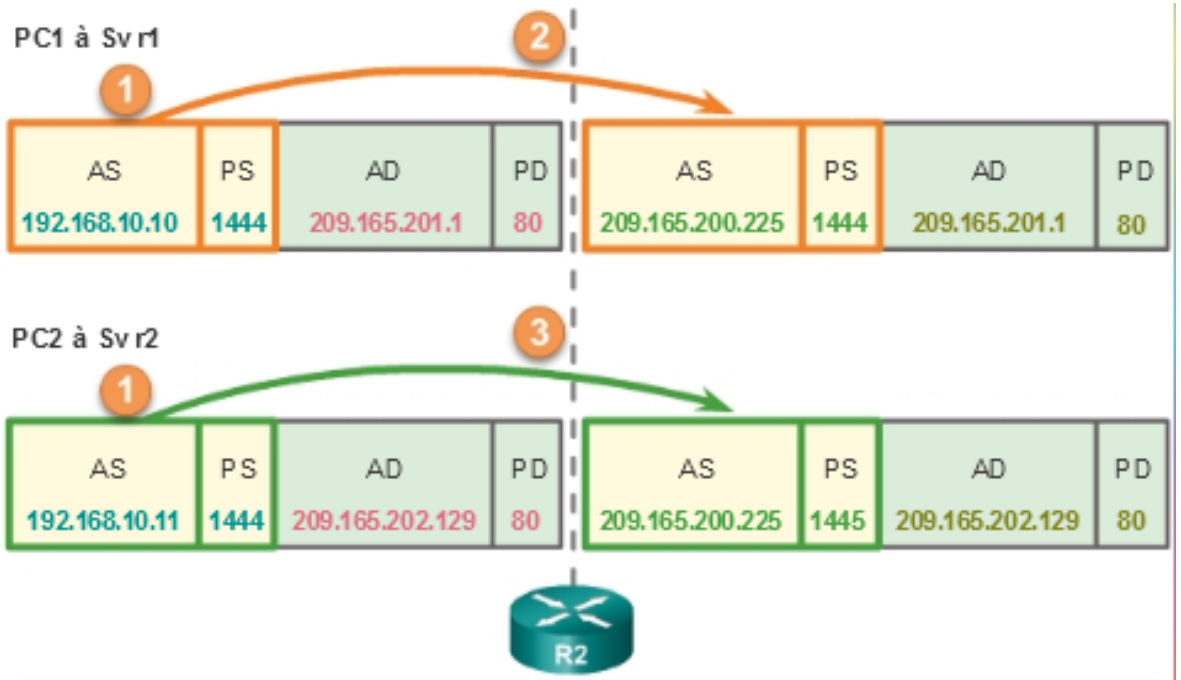


Table NAT

Adresse locale interne	Adresse globale interne	Adresse globale externe	Adresse locale externe
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

CHAPITRE 3

PLAN UN SYSTÈME DE GESTION ET DE SUPERVISION DES RÉSEAUX

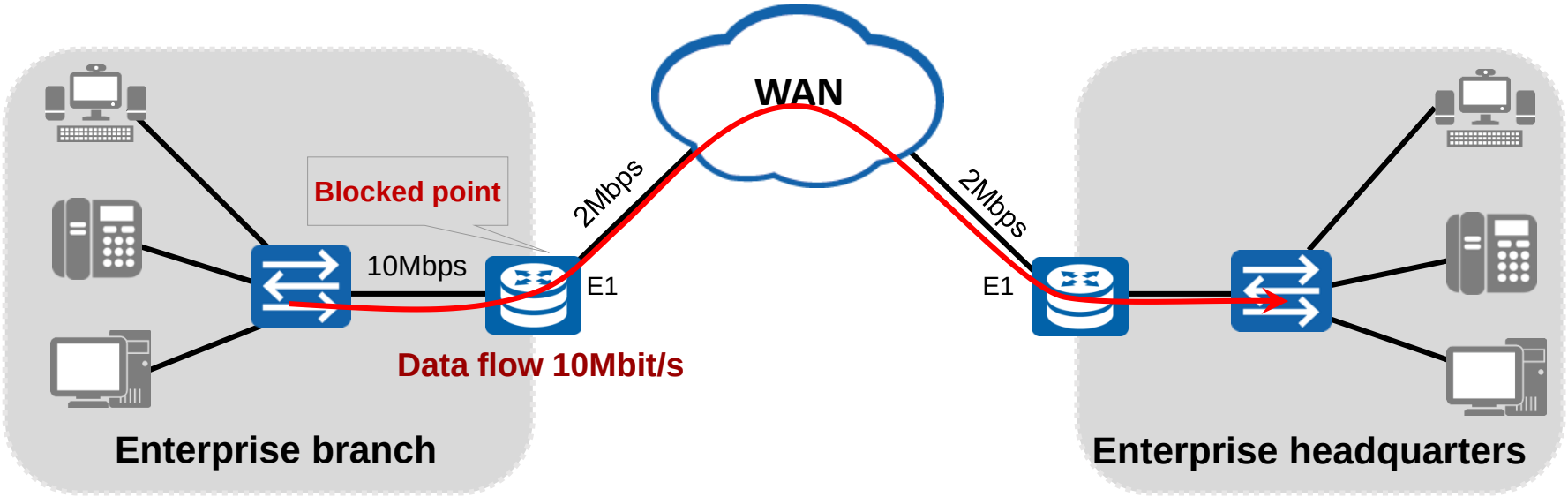
1 - Principes QOS

2 – Dépannage réseau

3 - Protocole d'administration des équipements réseaux SNMP

4 – Solutions d’administration

Principes QOS



- Les périphériques réseau traditionnels traitent les paquets en fonction de la séquence d'arrivée des paquets.
- C'est-à-dire que le paquet qui arrive en premier est transmis de préférence.
- Lorsque la congestion du réseau se produit, la qualité de communication de certains services clés ne peut pas être garantie (tels que le retard de la voix, le gel des images vidéo, l'échec du traitement des services clés). Cela affecte l'expérience utilisateur

Principes QOS

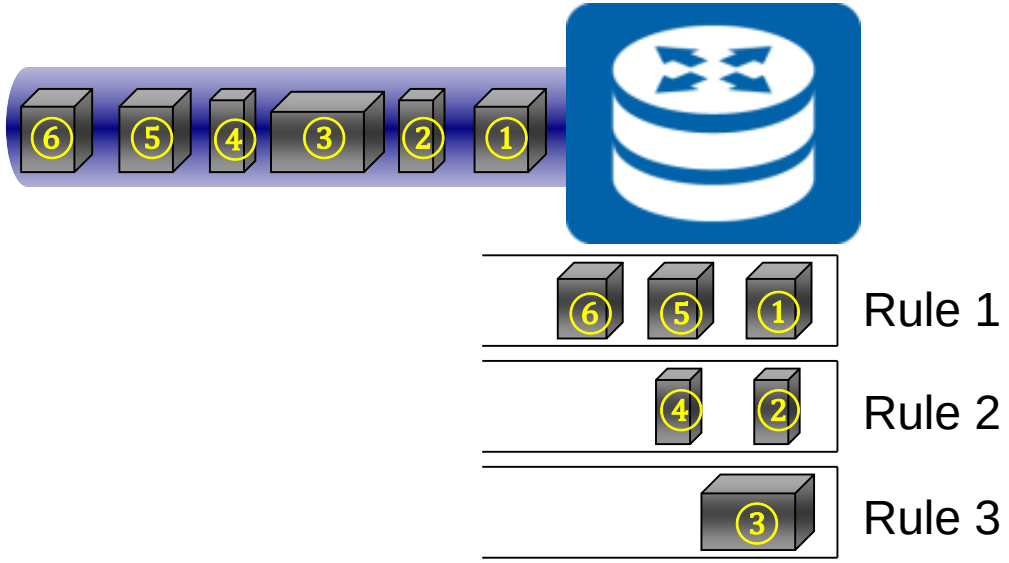
Exigences de qualité du réseau

Type de trafic	Bande passante	Retarder	Gigue	Taux de perte de paquets
Voice	Bas	Haut	Haut	Bas
Video	Haut	Haut	Haut	Bas
FTP	moyen, haut	Bas	Bas	Haut
Email, HTTP	Bas	Bas	Bas	moyen, haut

- Les exigences de réseau des différents services doivent être satisfaites pour assurer la qualité de la communication.
- Améliorer la qualité de la communication, c'est améliorer la bande passante et réduire le retard, la gigue et le taux de perte de paquets

Principes QOS

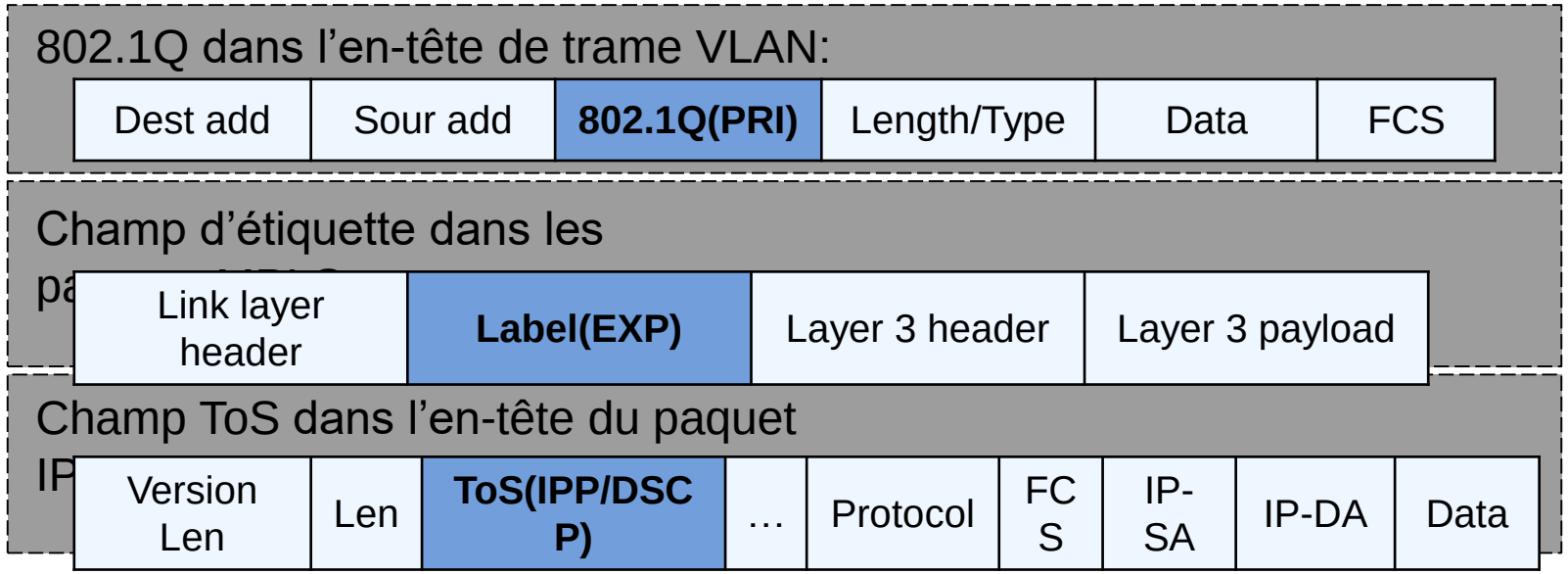
Classification des paquets



La classification du trafic est la base du déploiement de DiffServ QoS.

Principes QOS

Classification des paquets



La technologie de classification des paquets peut transmettre différents types de paquets en fonction des types de liens et des champs de priorité QoS dans les paquets

CHAPITRE 3

PLAN UN SYSTÈME DE GESTION ET DE SUPERVISION DES RÉSEAUX

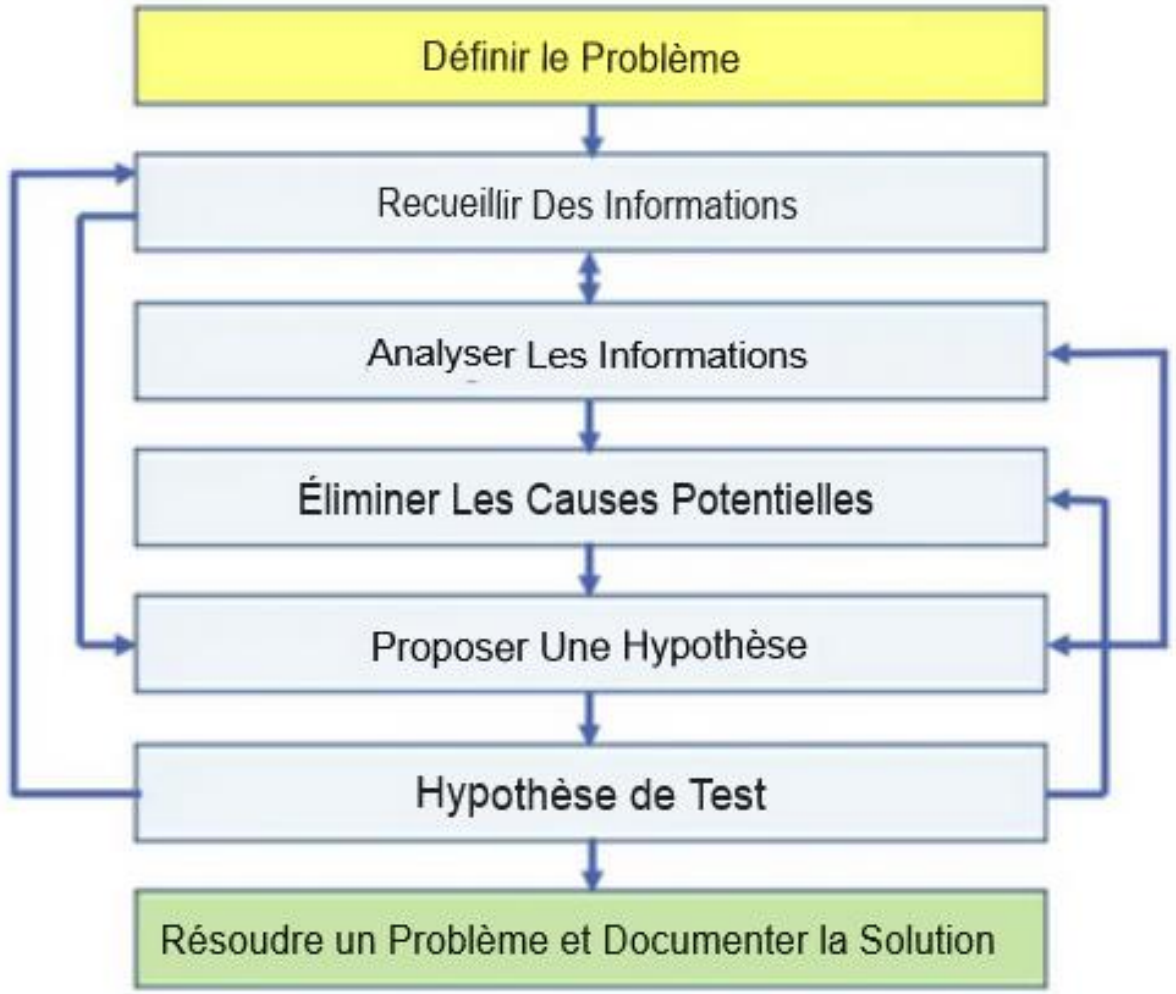
1 - Principes QOS

2 – Dépannage réseau

3 - Protocole d'administration des équipements réseaux SNMP

4 – Solutions d’administration

Dépannage réseau



Dépannage réseau

Méthodes de dépannage de la connectivité

1. Ping
2. Traceroute
3. SSH

- Les commandes courantes pour dépanner la connectivité, une commande vraiment super commune à utiliser est **ping**.

- Cela vérifie la connectivité entre deux appareils. Lorsque vous envoyez un ping, il utilise ICMP et envoie un paquet de la source à la destination.

- La destination enverra ensuite une réponse ping à nouveau. Ainsi, ping vérifie la connectivité bidirectionnelle.

Dépannage réseau

Méthodes de dépannage de la connectivité

1. Ping
2. Traceroute
3. SSH

- La prochaine commande que nous utiliserons probablement après un **ping** est un traceroute.

- Si vous avez plusieurs routeurs entre la source et la destination, ce que vous pouvez faire, c'est que vous pouvez le dépanner de la source à la destination.

Dépannage réseau

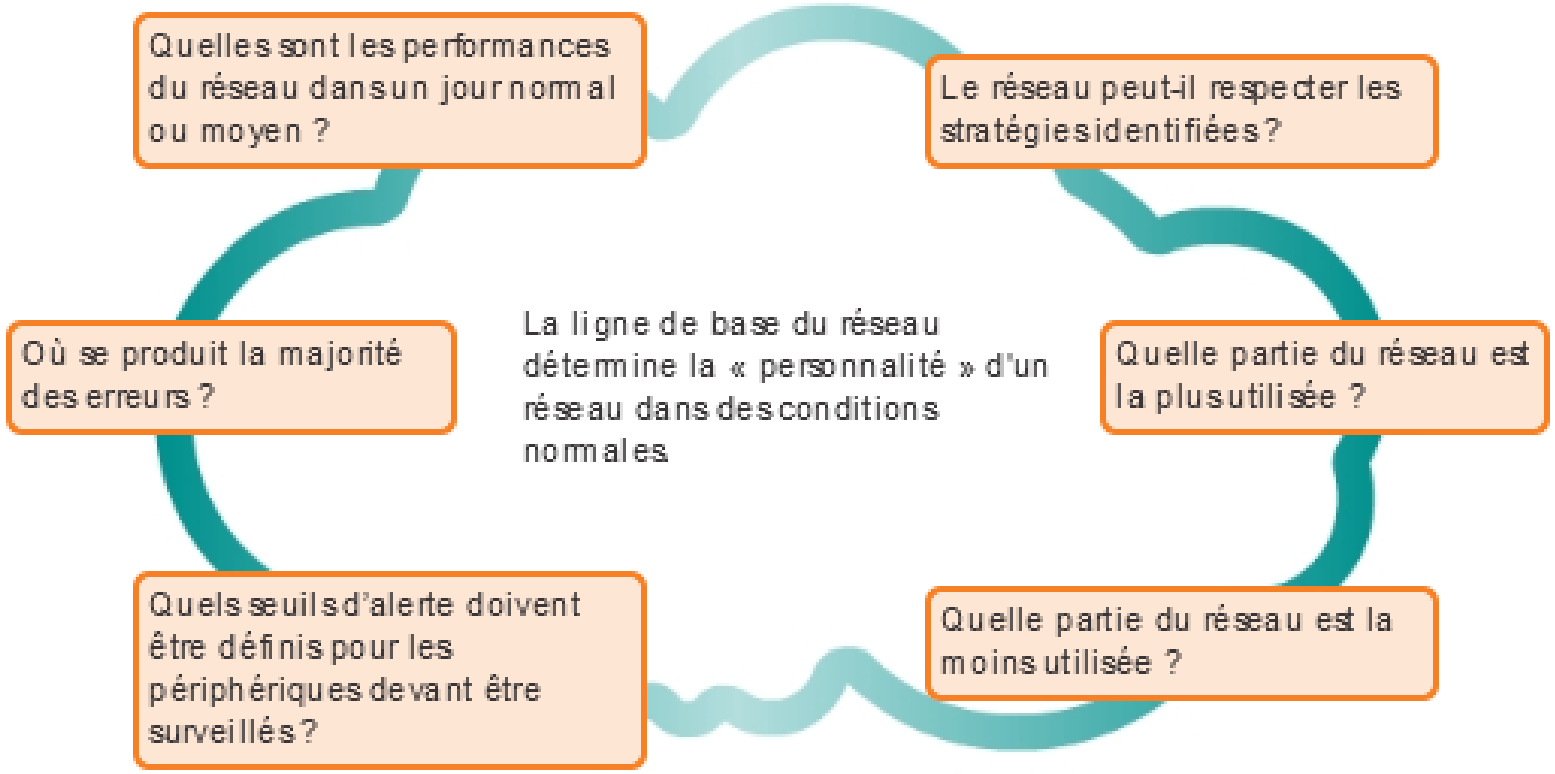
Méthodes de dépannage de la connectivité

1. Ping
2. Traceroute
3. SSH

- Enfin, nous pouvons utiliser **SSH**. **SSH** est normalement utilisé pour gérer vos périphériques d'infrastructure réseau, tels que vos routeurs et commutateurs.

- Nous pouvons l'utiliser pour accéder à une ligne de commande sur l'appareil d'une façon sécurisée.

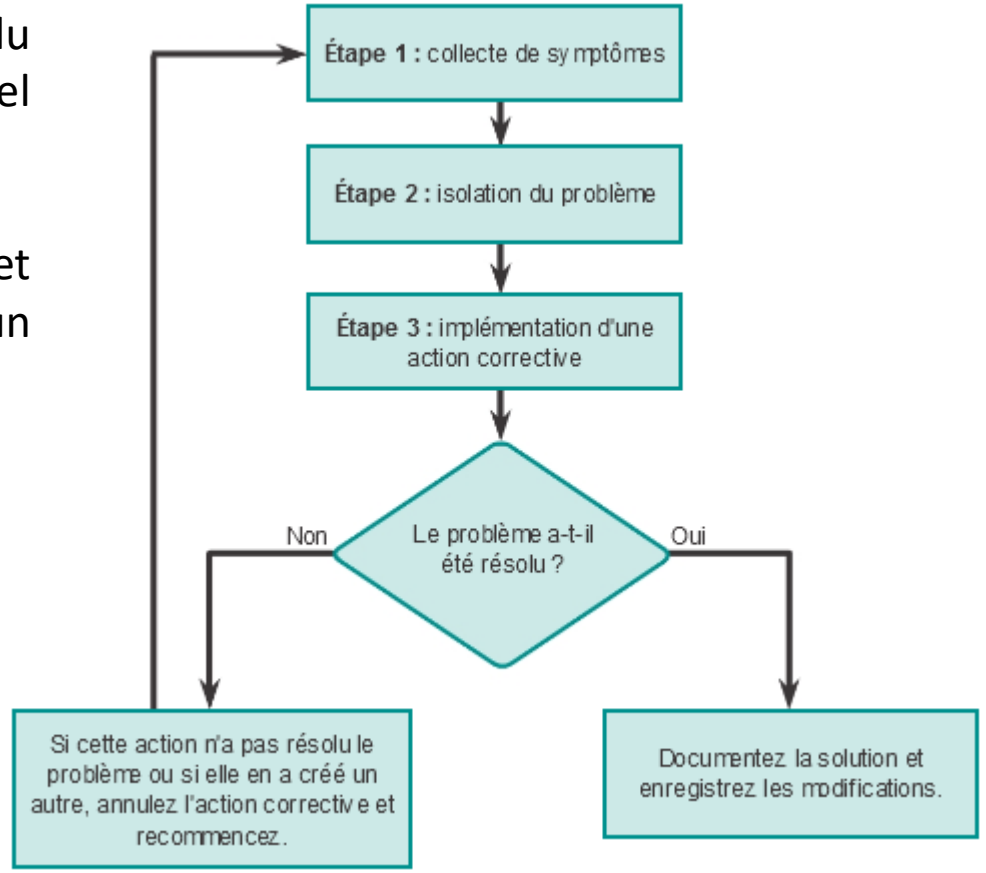
Dépannage réseau



Dépannage réseau

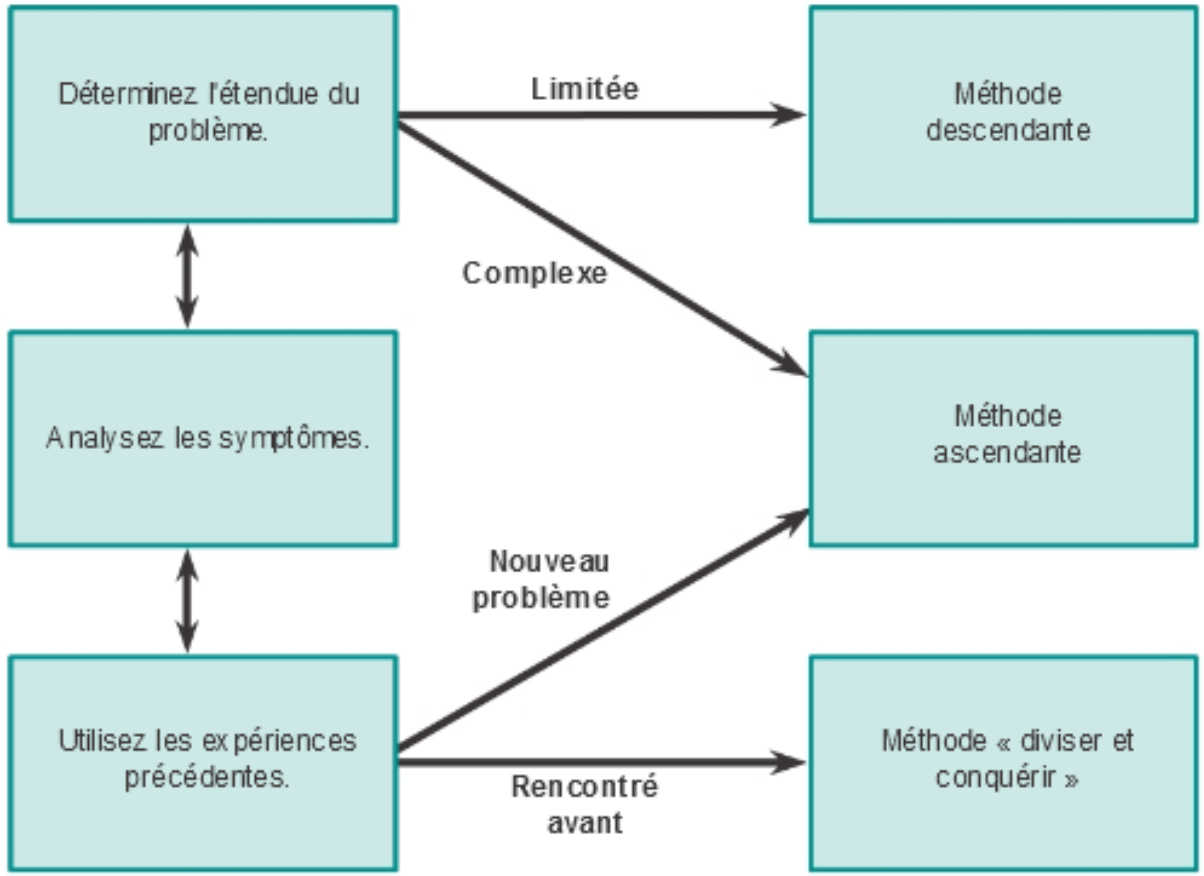
- Les tâches de dépannage occupent une grande partie du temps des administrateurs réseau et du personnel d'assistance.

- L'utilisation de techniques de dépannage efficaces permet de diminuer le temps de dépannage global dans un environnement de production.



Dépannage réseau

- Afin de résoudre rapidement les problèmes réseau, prenez le temps de sélectionner la méthode de dépannage réseau la plus efficace.



Dépannage réseau

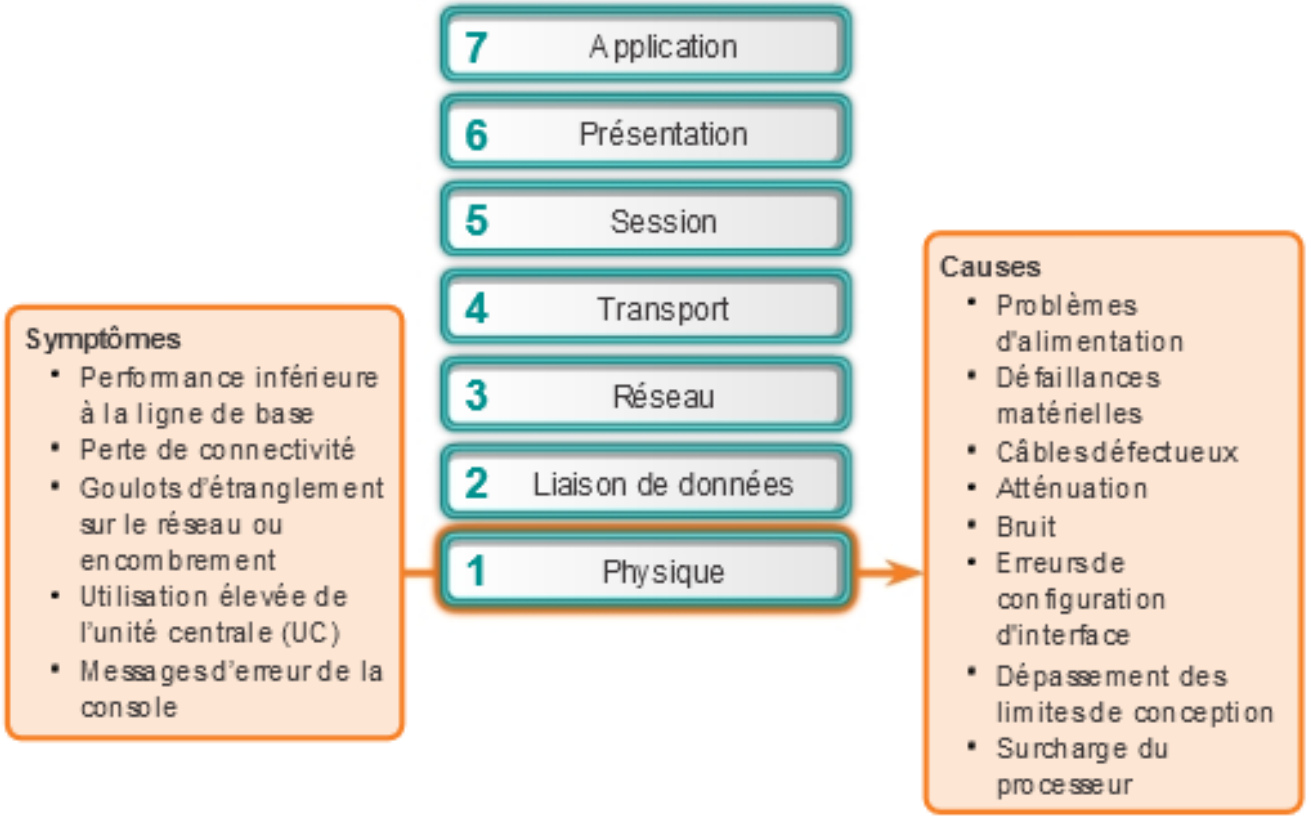
- Le protocole Syslog est un protocole simple utilisé par un périphérique IP faisant office de client Syslog, afin d'envoyer des messages textuels de journal vers un autre périphérique IP, à savoir le serveur Syslog.

- L'implémentation d'une méthode de journalisation est une partie importante de la sécurité du réseau et du dépannage réseau.

	Niveau	Mot-clé	Description	Définition
Niveau le plus élevé	0	urgences	Système inutilisable	LOG_EMERG
	1	alertes	Action immédiate requise	LOG_ALERT
	2	critique	Existence de conditions critiques	LOG_CRIT
	3	erreurs	Existence de conditions d'erreur	LOG_ERR
	4	avertissements	Existence de conditions d'avertissement	LOG_WARNING
	5	notifications	Événement normal mais important	LOG_NOTICE
	6	informatif	Message d'information uniquement	LOG_INFO
Niveau le plus bas	7	débogage	Messages de débogage	LOG_DEBUG

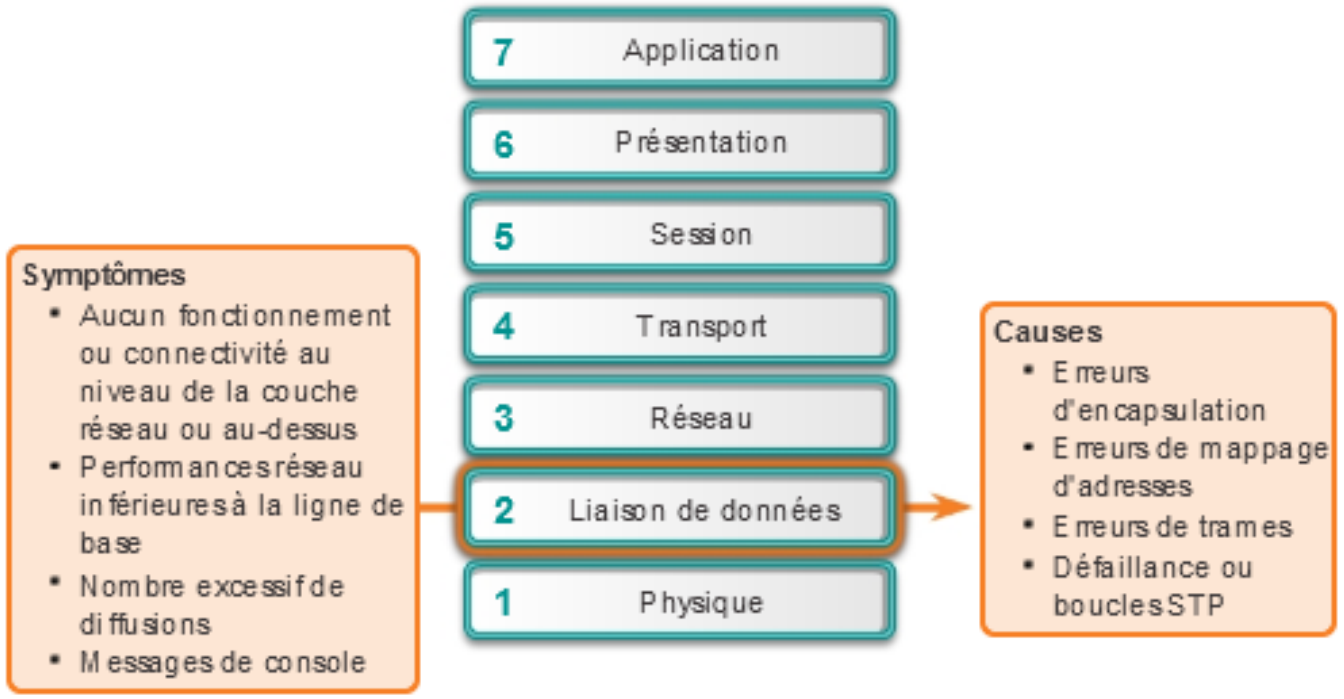
Dépannage réseau

Dépannage de la couche physique



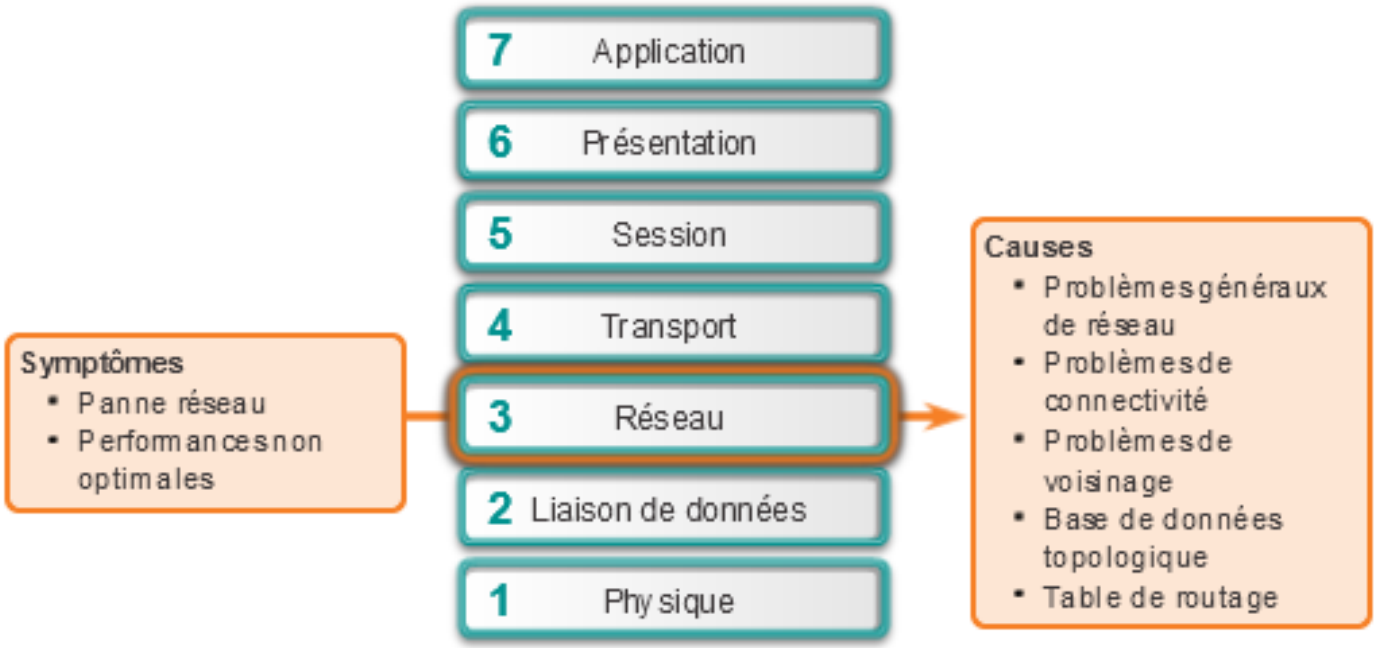
Dépannage réseau

Dépannage de la couche liaison de données



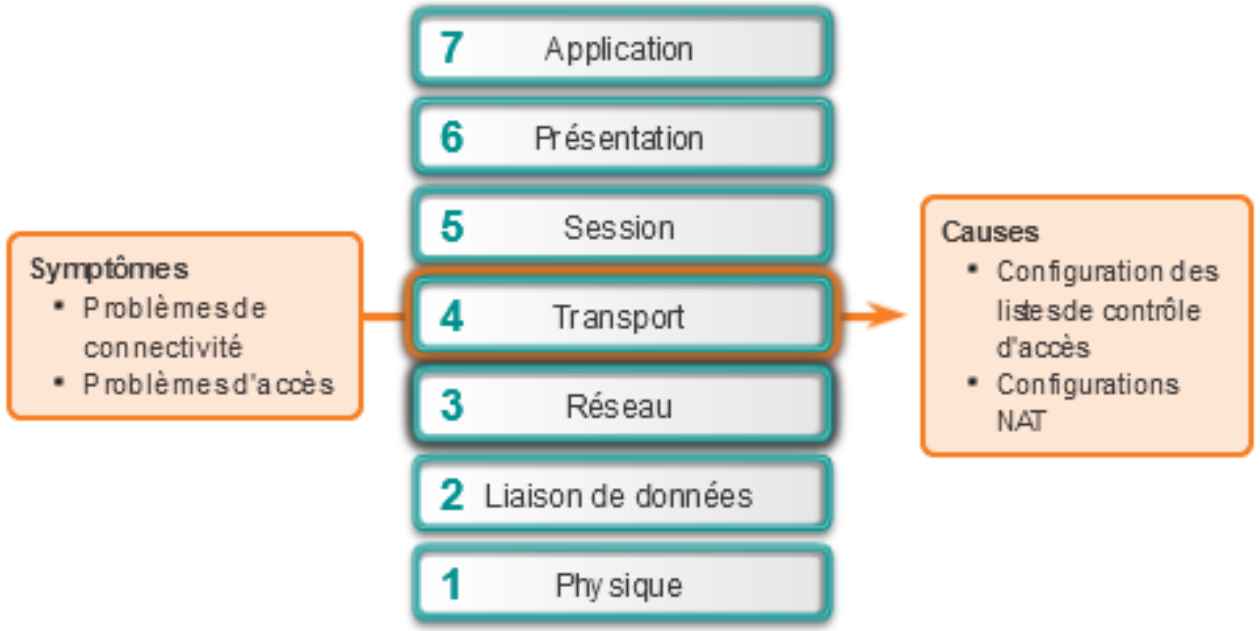
Dépannage réseau

Dépannage de la couche réseau



Dépannage réseau

Dépannage de la couche transport



CHAPITRE 3

PLAN UN SYSTÈME DE GESTION ET DE SUPERVISION DES RÉSEAUX

1 - Principes QOS

2 – Dépannage réseau

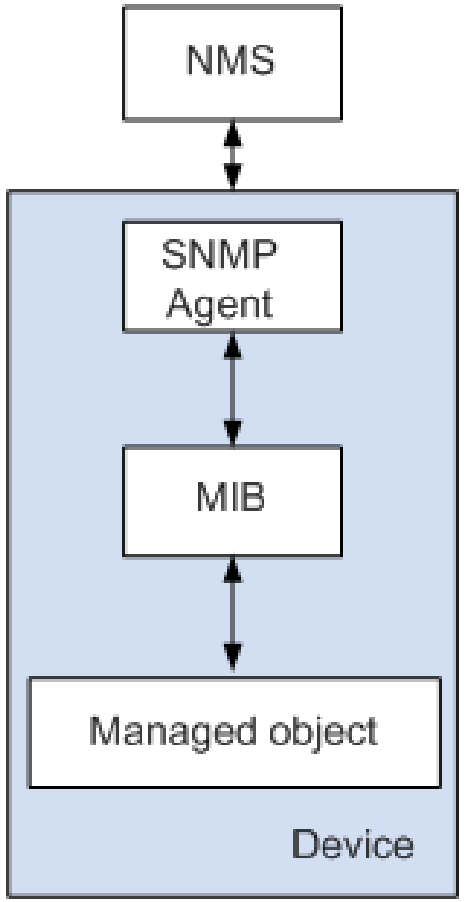
3 - Protocole d'administration des équipements réseaux SNMP

4 – Solutions d’administration

Protocole d'administration des équipements réseaux SNMP

- Un système SNMP se compose de quatre composants clés :
  - système de gestion de réseau (NMS),
  - agent SNMP,
  - objet géré et base d'informations de gestion (MIB).

- Le NMS gère les éléments de réseau sur un réseau.



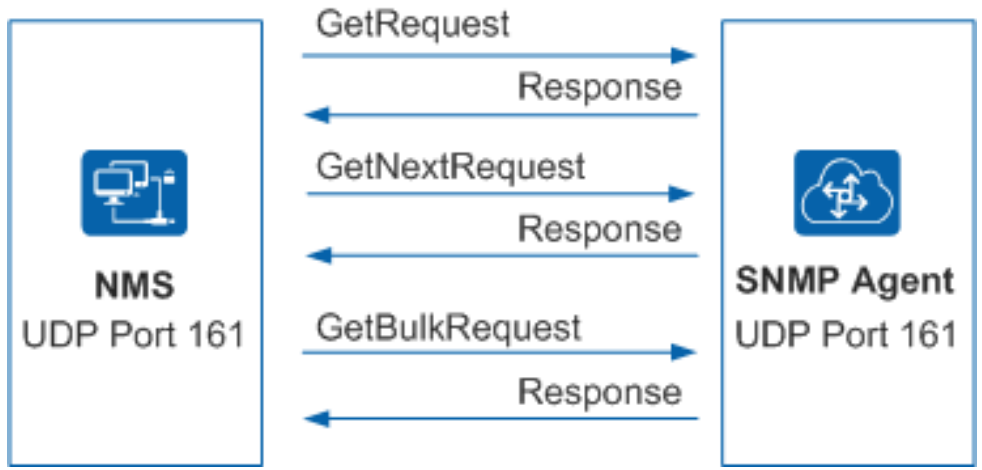
SNMP Get

Le NMS peut envoyer des demandes **get** à un agent SNMP pour obtenir des données.

L'agent SNMP exécute l'instruction correspondante dans la MIB et envoie le résultat au NMS.

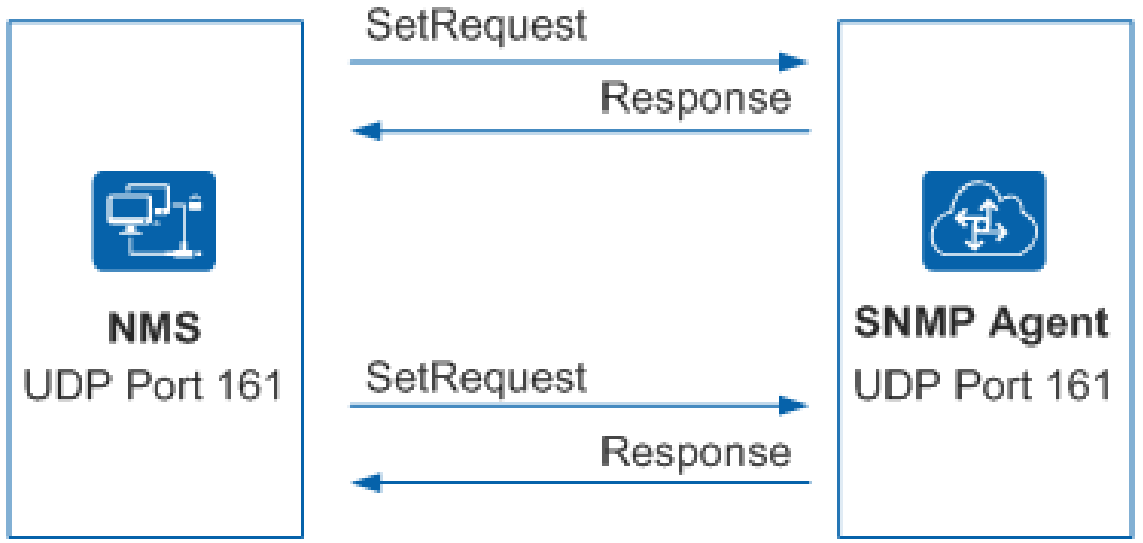
Les opérations d'obtenir SNMP incluent Get, GetNext et GetBulk. SNMPv1 ne prend pas en charge l'opération GetBulk.

1. **Get**: Cette opération permet au NMS d'obtenir une ou plusieurs variables de l'agent SNMP.
2. **GetNext**: Cette opération permet au NMS d'obtenir une ou plusieurs variables ultérieures de l'agent SNMP.
3. **GetBulk**: Cette opération est égale aux opérations GetNext consécutives.



SNMP Set

- Le NMS peut envoyer des demandes de set à un agent SNMP pour effectuer des configurations sur le périphérique géré.
- Après avoir reçu une demande Set, l'agent SNMP exécute l'instruction correspondante dans la MIB et envoie le résultat au NMS.
- À l'aide de l'opération SNMP Set, le NMS peut configurer un ou plusieurs paramètres pour un agent SNMP.



CHAPITRE 3

PLAN UN SYSTÈME DE GESTION ET DE SUPERVISION DES RÉSEAUX

1 - Principes QOS

2 – Dépannage réseau

3 - Protocole d'administration des équipements réseaux SNMP

4 – Solutions d’administration

Solutions d’administration

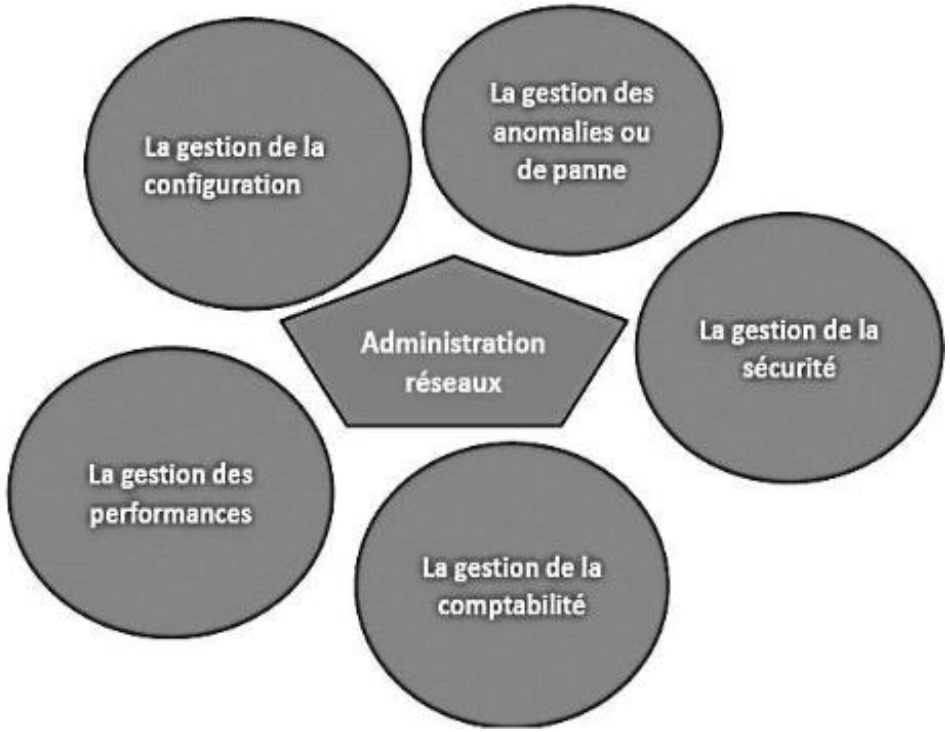
Les objectifs (les finalités) de l’administration des réseaux pour un administrateur :

- Supervision du fonctionnement des réseaux ;
- Optimisation pour l’utilisation des ressources ;
- Détection et prévision des erreurs ;
- Signalisation des pannes ;
- Calculs de facturations à l’utilisation des ressources ;
- Le support technique pour utilisateurs.

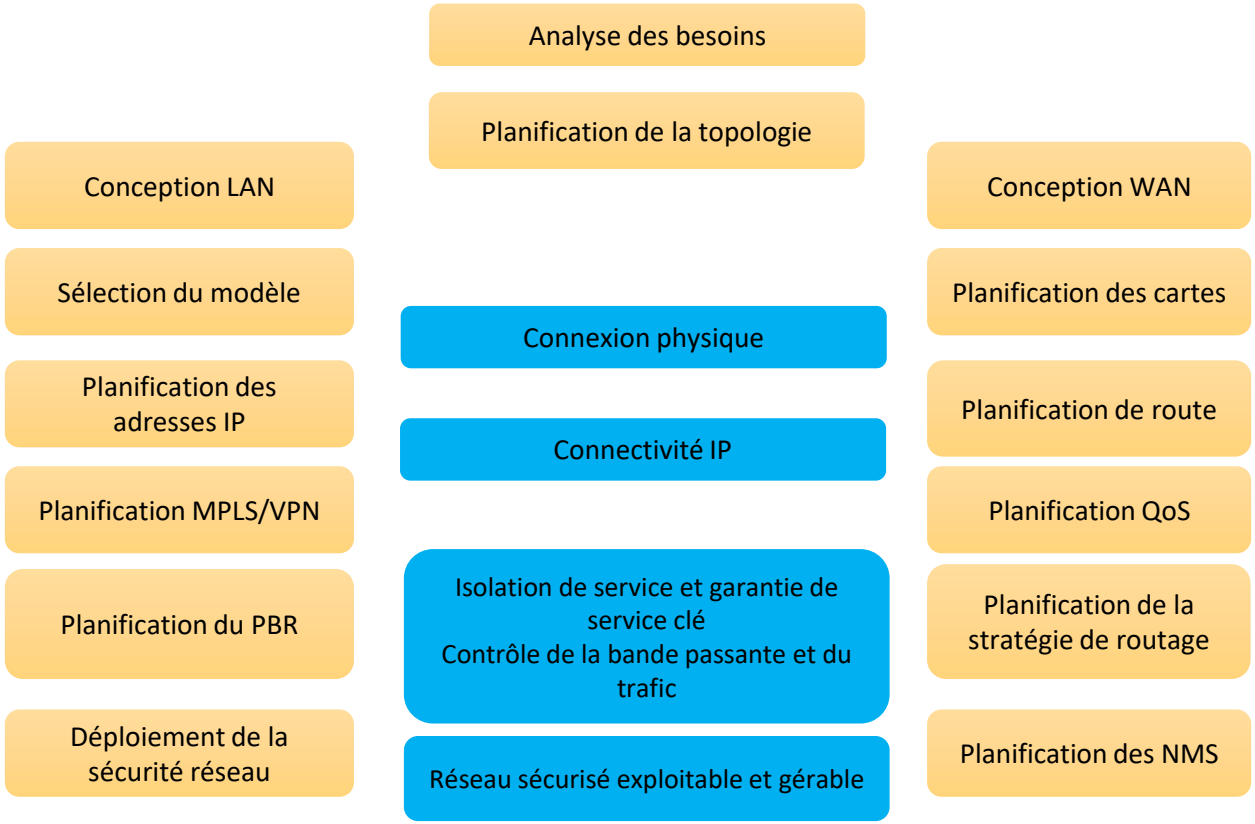
Solutions d’administration

L’OSI a regroupé les activités d’administration en cinq groupes fonctionnels :

1. Gestion de configuration
2. Gestion de performance
3. Gestion de panne
4. Gestion de compatibilité
5. Gestion de sécurité



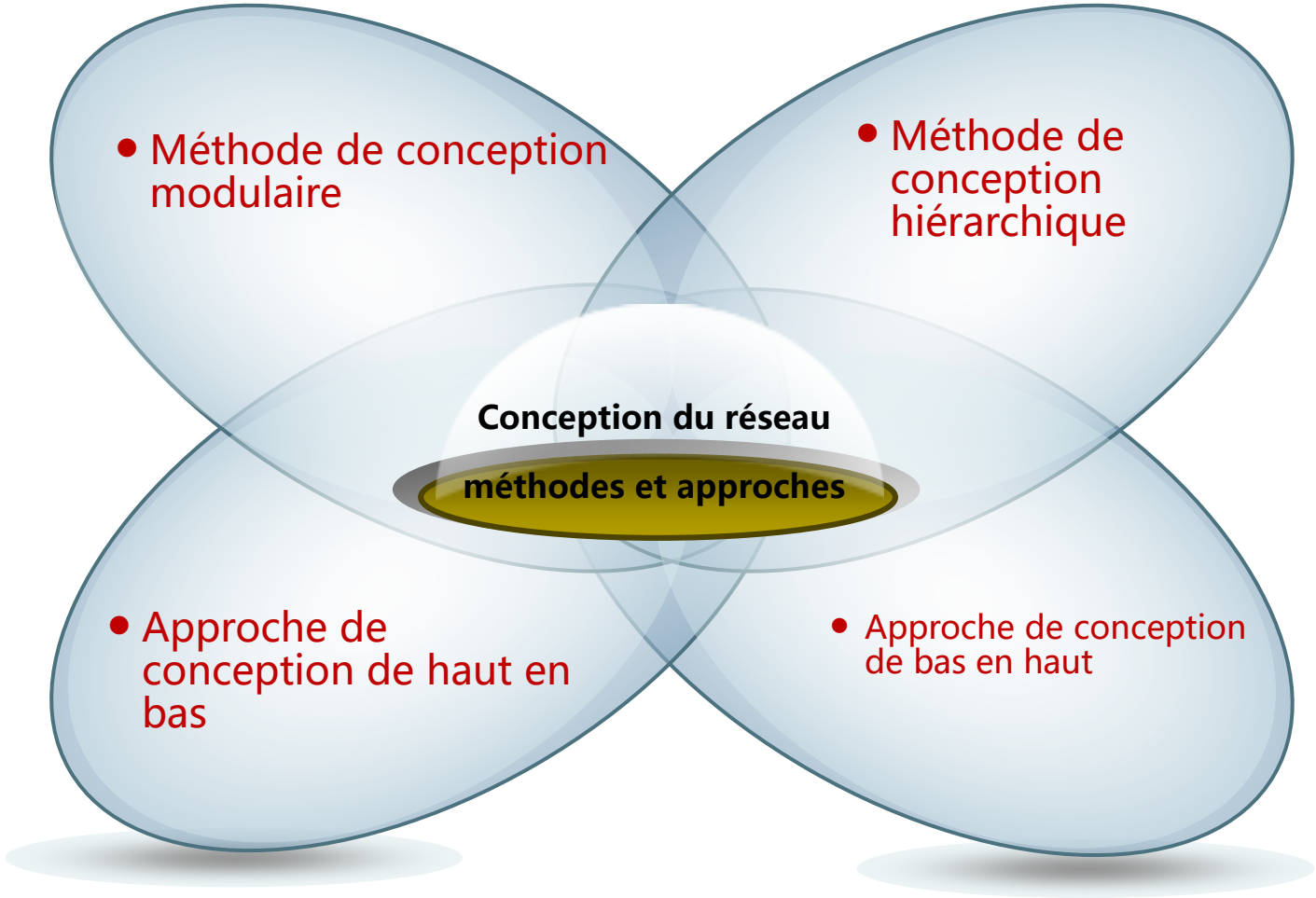
Solutions d’administration



Solutions d’administration

- Moteur de supervision d’un SI complet
- Outil d’administration complet
- Mesure de performances réseau et système
- Capture et visualisation des flux sur le réseau
- Consultation d’état d’hôtes et services sur des cartes
- Création rapports et Dashboard
- Performances sous forme PDF
- Sauvegarde

Solutions d’administration



Nagios

Nagios surveille le réseau pour les problèmes causés par des liaisons de données ou des connexions réseau surchargées, ainsi que des routeurs…