CCNA

SWITCHING & ROUTING

Déroulé de la formation

Première semaine

1. **Introduction aux réseaux :**
   - Couches OSI, ARP, IOS, CDP, LLDP, DHCP, Architecture …
2. **LAN & commutation :**
   - Trame Ethernet, collision, CSMA/CD, table d'@ Mac, Port Security, VLAN, VTP, Routage inter VLAN, Management, STP, Etherchannel, HSRP …
3. **IPv6 :**
   - Adressage, routage, techniques de transition …

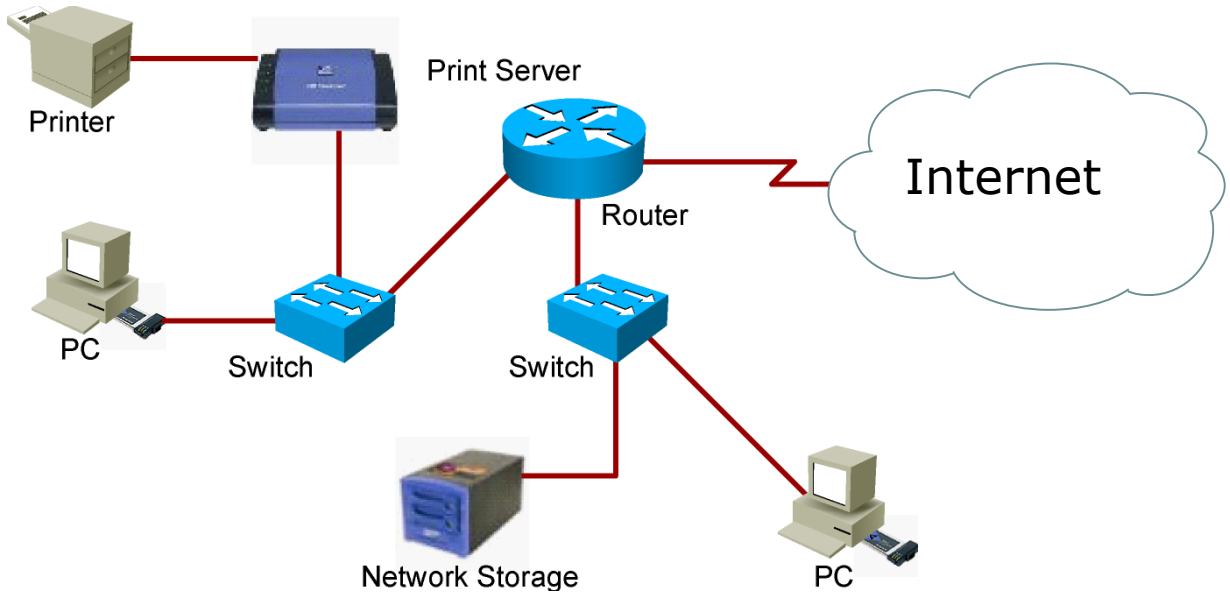
Seconde semaine

4. **Routage :**
   - Subnetting, statique, dynamique, DV, LS RIP, OSPF, EIGRP, BGP …
5. **WAN :**
   - Technologies, topologies, équipements Protocoles HDLC, PPP PAP CHAP, VPN …
6. **Sécurité & administration :**
   - ACL, NAT, SNMP, Logging, NetFlow, QoS, IP SLA …

Introduction aux réseaux

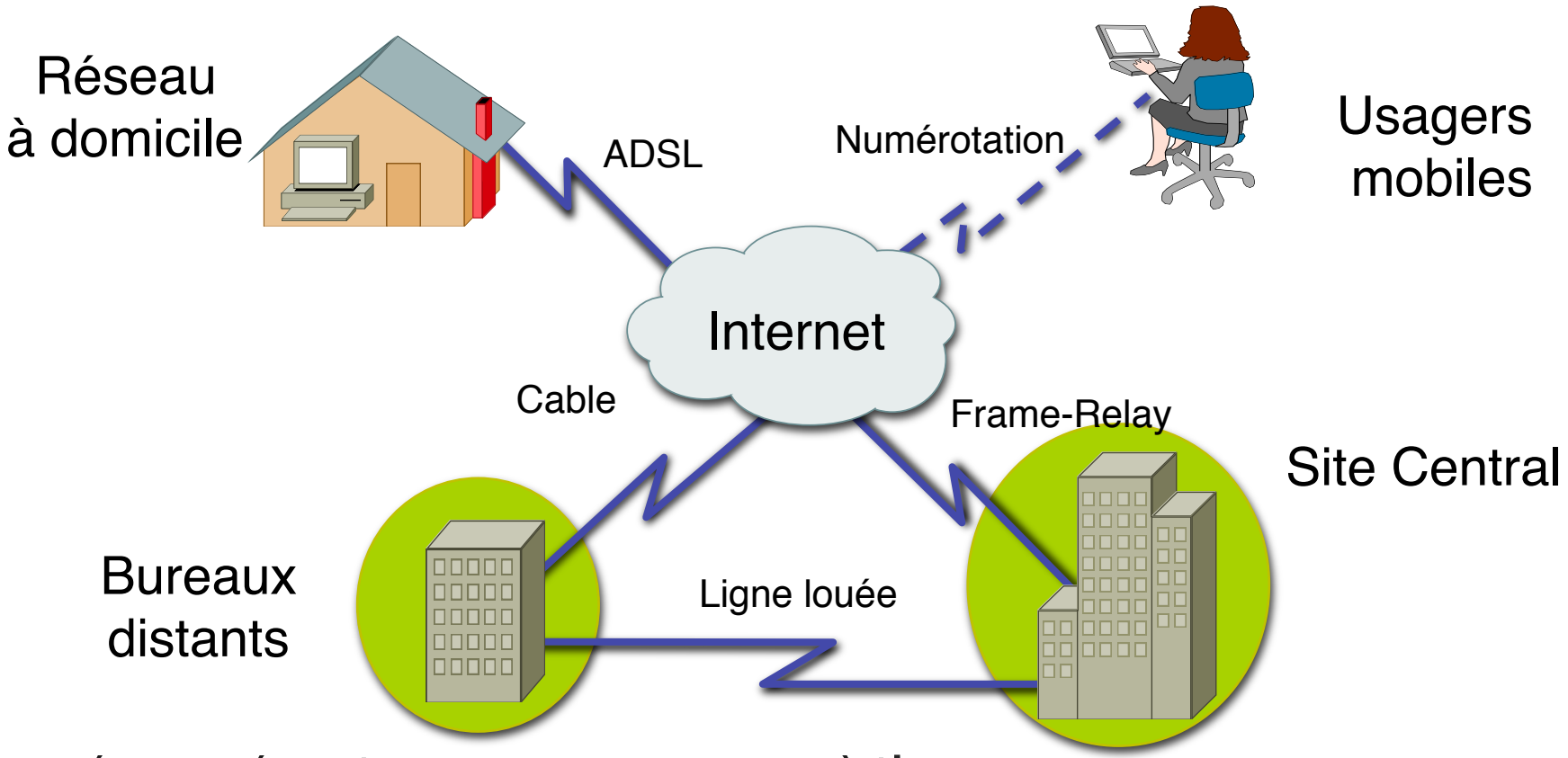
Présentation générale

LAN : Partage des ressources locales



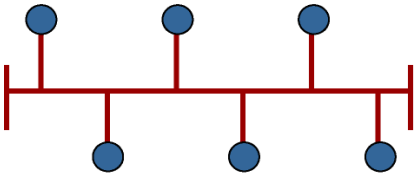
- Réseaux Locaux (LAN)
  - Partage d'applications et de données
  - Stockage
  - Accès à l'Internet

WAN : Accès aux réseaux étendus

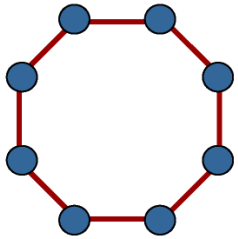


- Les réseaux étendus (WAN) connectent à l'Internet
- Ils peuvent aussi interconnecter des sites
- Il existe de nombreuses technologies d'accès : DSL, Cable…

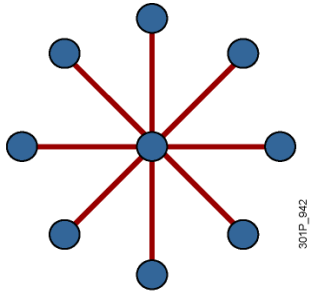
Les topologies d'accès



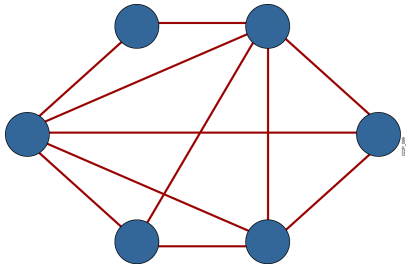
Topologie en bus
Ethernet



Anneaux
Token Ring



Topologie en étoile
Hub and Spoke



Topologie maillée
Circuits virtuels

Réseaux locaux (LAN)

Réseaux étendus (WAN)

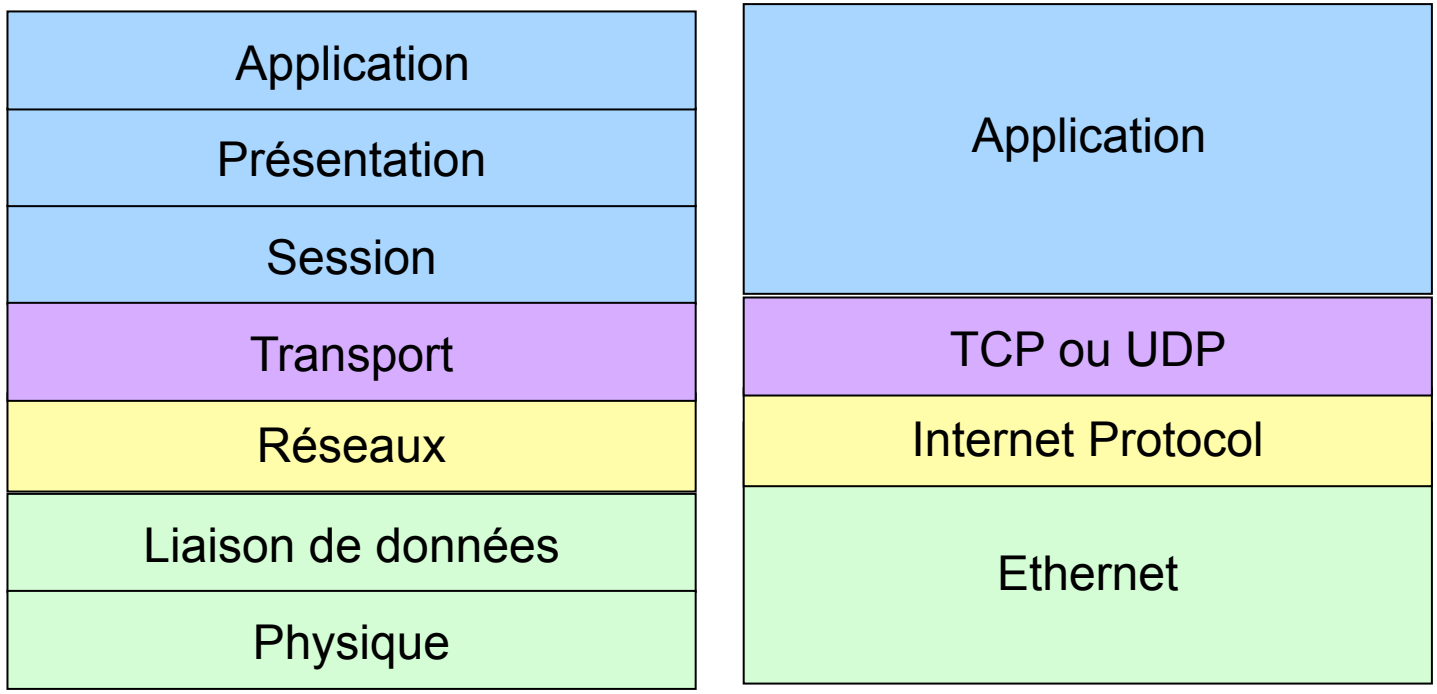
Les modèles OSI et TCP/IP

Le modèle OSI

- **OSI** (Open Systems Interface) est une suite de protocoles standards. Cependant, **TCP/IP** est devenu, de fait, le standard.Toutefois, l'invocation du modèle **OSI** subiste et facilite la compréhension.
- Il permet de **spéficier** séparément chaque couche et de définir les messages échangés à chaque niveau
- Il permet aussi d' associer un **dispositif** à une couche du modèle OSI qu' il utilise

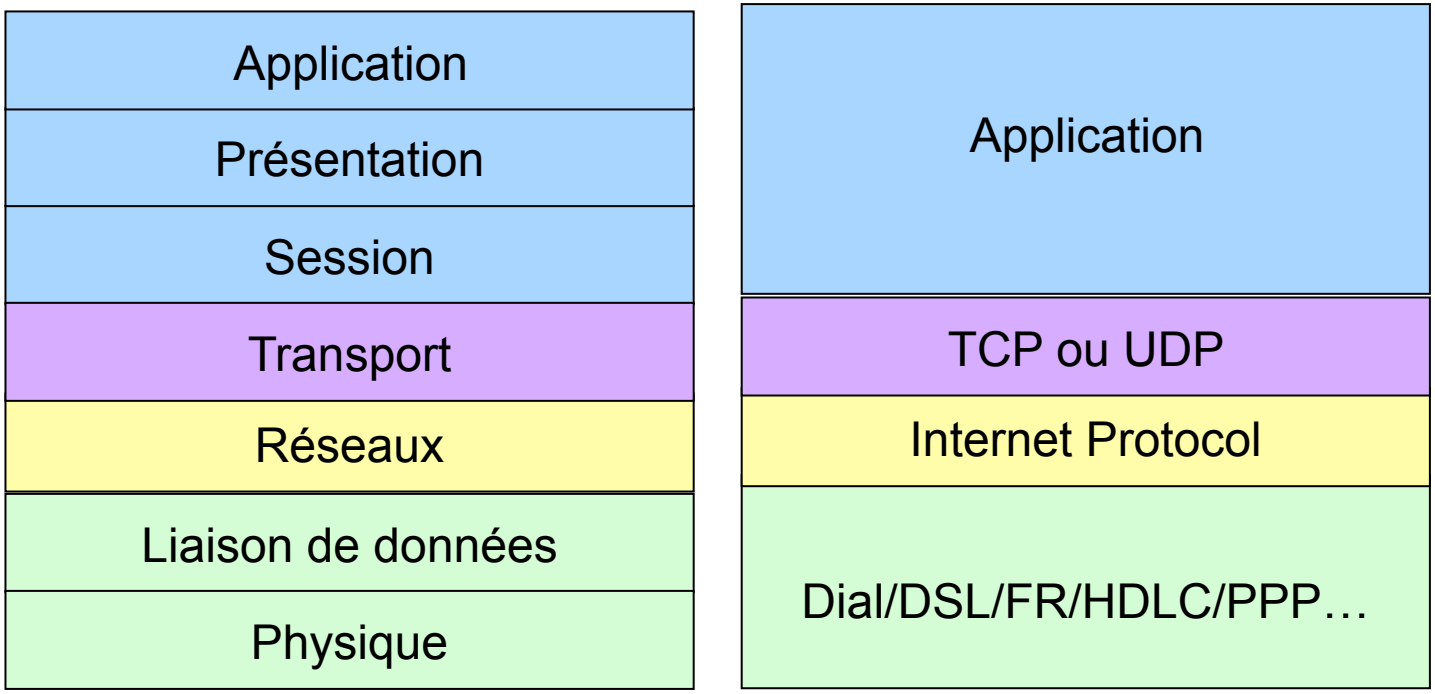
Comparaison de OSI et TCP/IP dans le LAN

TCP/IP sur Ethernet est le modèle qui s'est imposé dans les réseaux locaux



Comparaison de OSI et TCP/IP dans le WAN

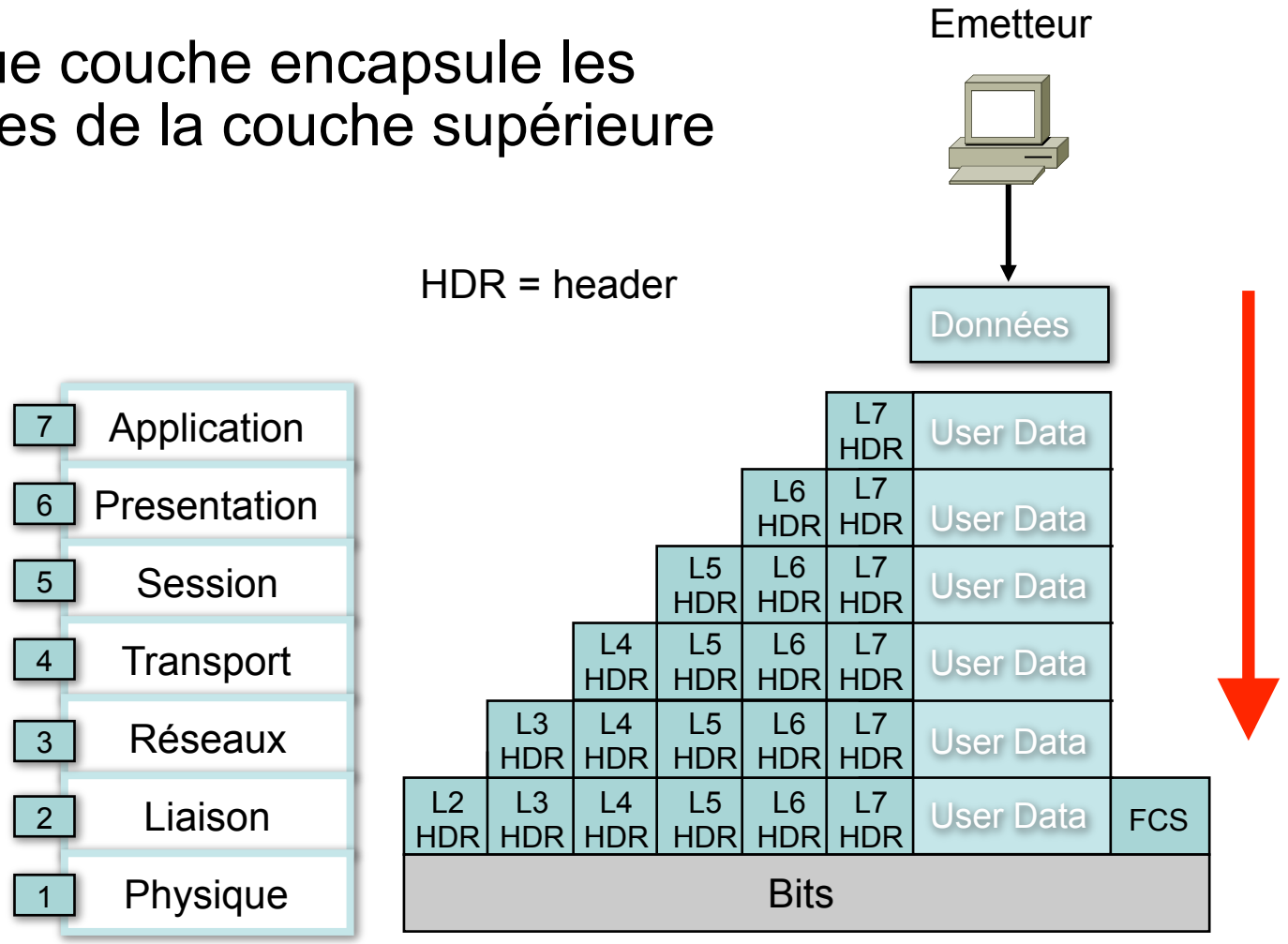
Le réseau étendu est caractérisé par les deux premières couches



Encapsulation et dé-encapsulation

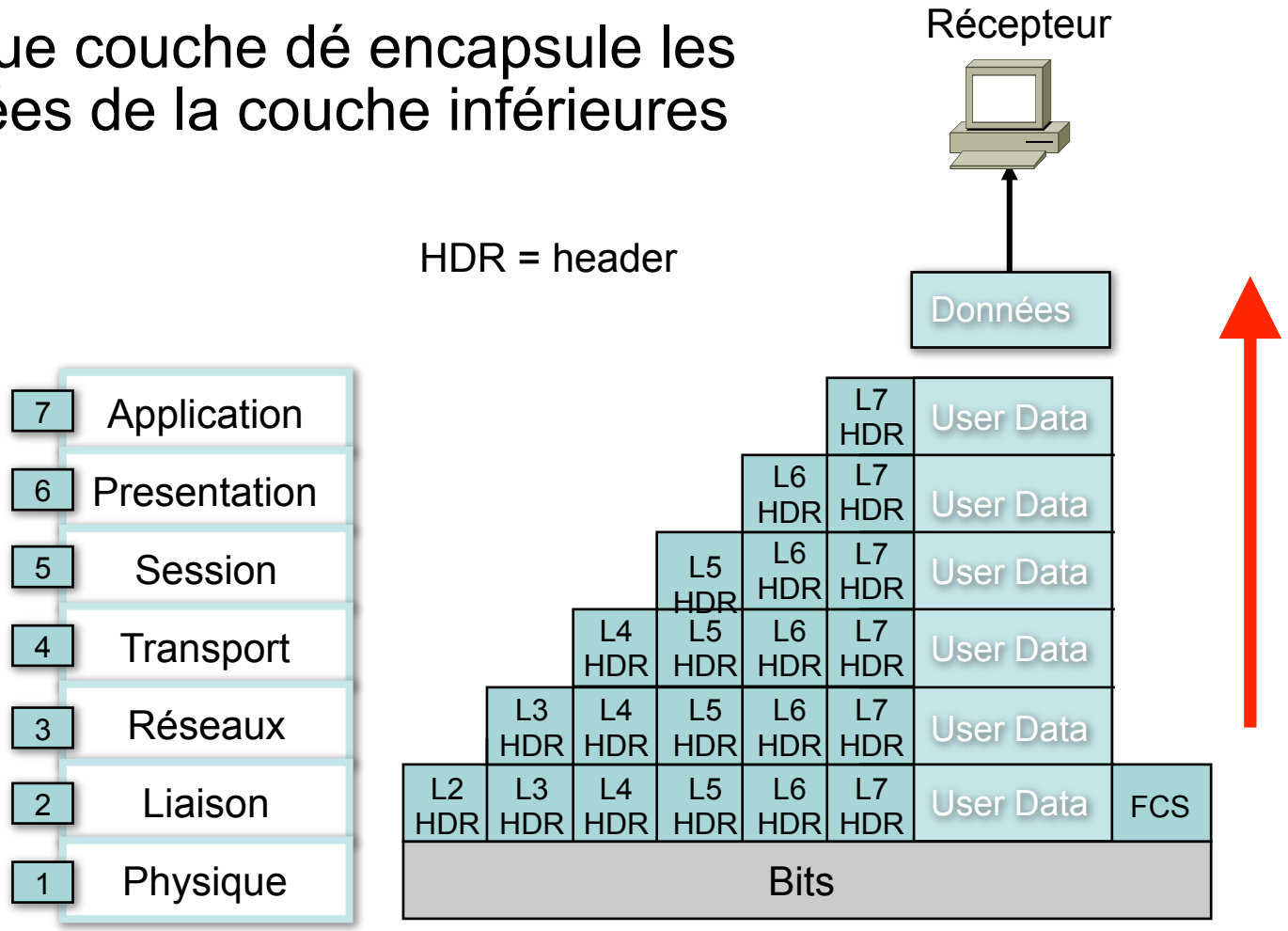
L'encapsulation des données

- Chaque couche encapsule les données de la couche supérieure



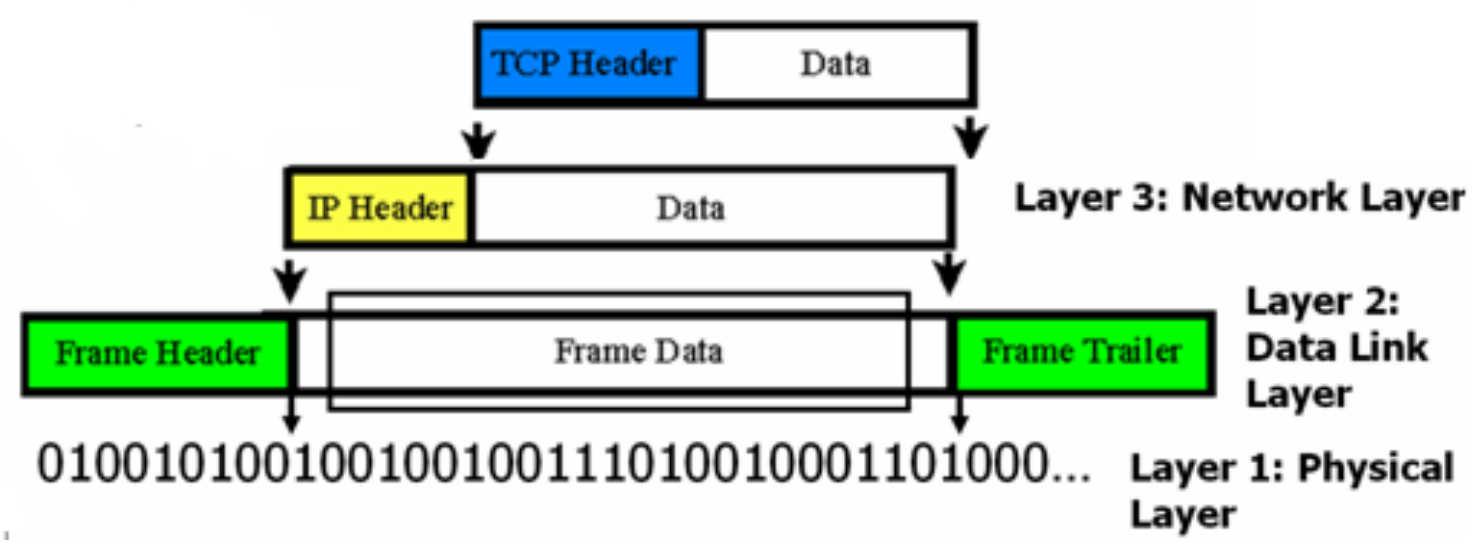
Dé-encapsulation des données

- Chaque couche dé encapsule les données de la couche inférieures

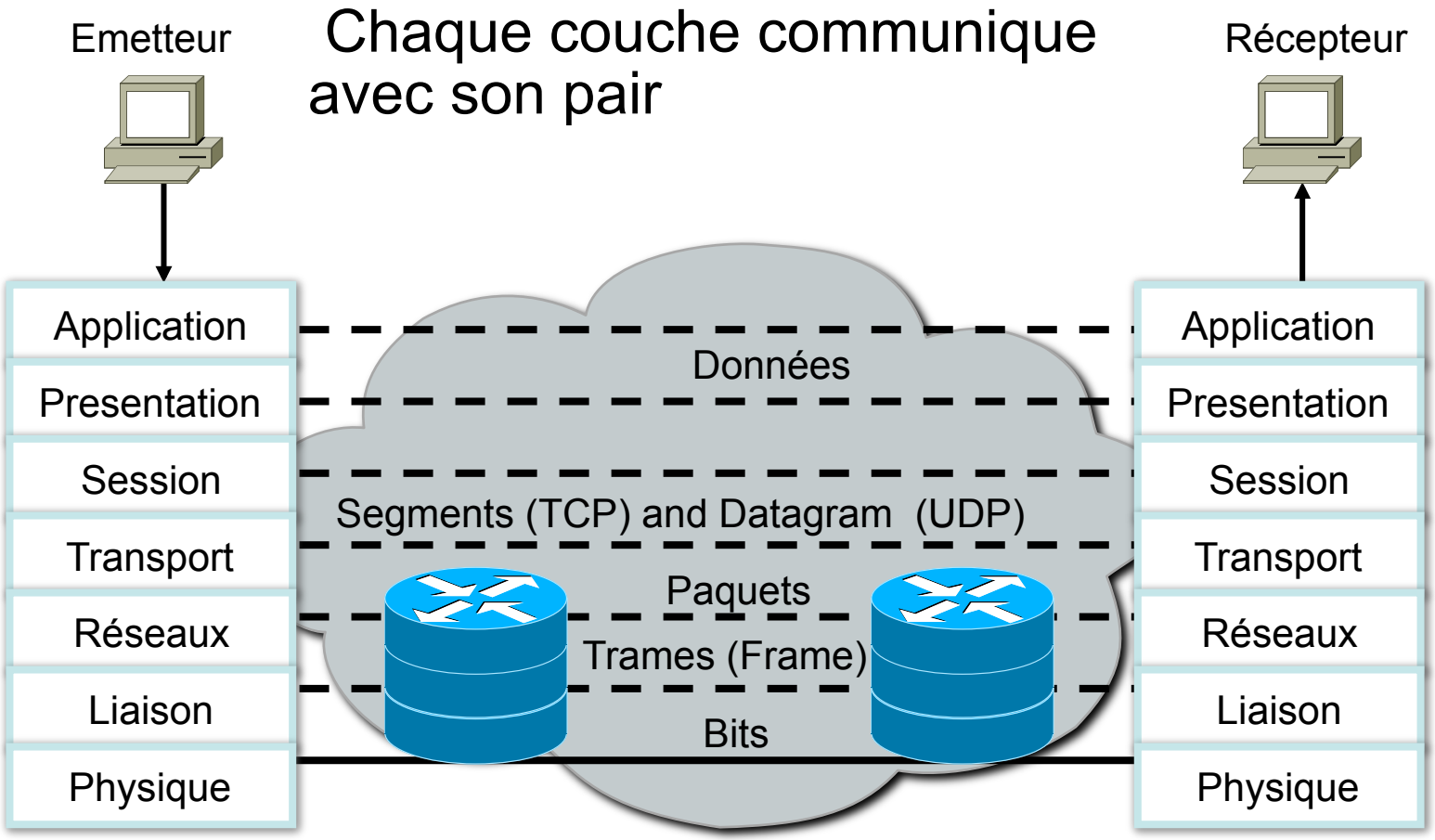


Data encapsulation avec TCP/IP

Les données de l'usager sont encapsulées dans un **segment** TCP qui lui-même est encapsulé dans un **paquet** IP. Ce paquet est encapsulé dans une **trame** Ethernet qui est découpée en bits et envoyée sur le réseau



Communication pair à pair



OSI couche 1 : la couche physique

OSI couche 1 - Couche physique

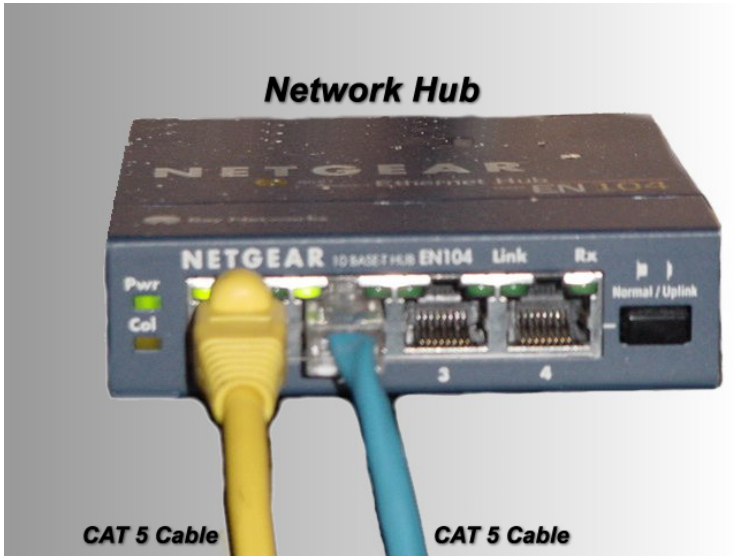
- Définit les spécifications techniques et fonctionnelles des jonctions entre dispositifs
- Le Protocol Data Unit est le **Bit**
- Les dispositifs sont :
  - Repeteurs (LAN)
  - Concentrateurs (LAN)
  - Modems (WAN)
  - DSU/CSU (WAN)

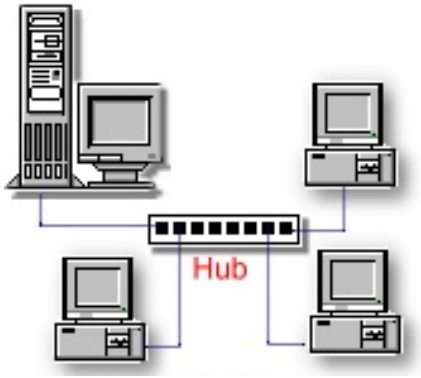
10110011110000101100 1

Le répéteur

- Equipement de couche 1 qui combat l'atténuation.
- Le répéteur:
  - Récupére le signal atténué
  - Le régénére (détection d'erreurs)
  - Le retransmet sur le réseau

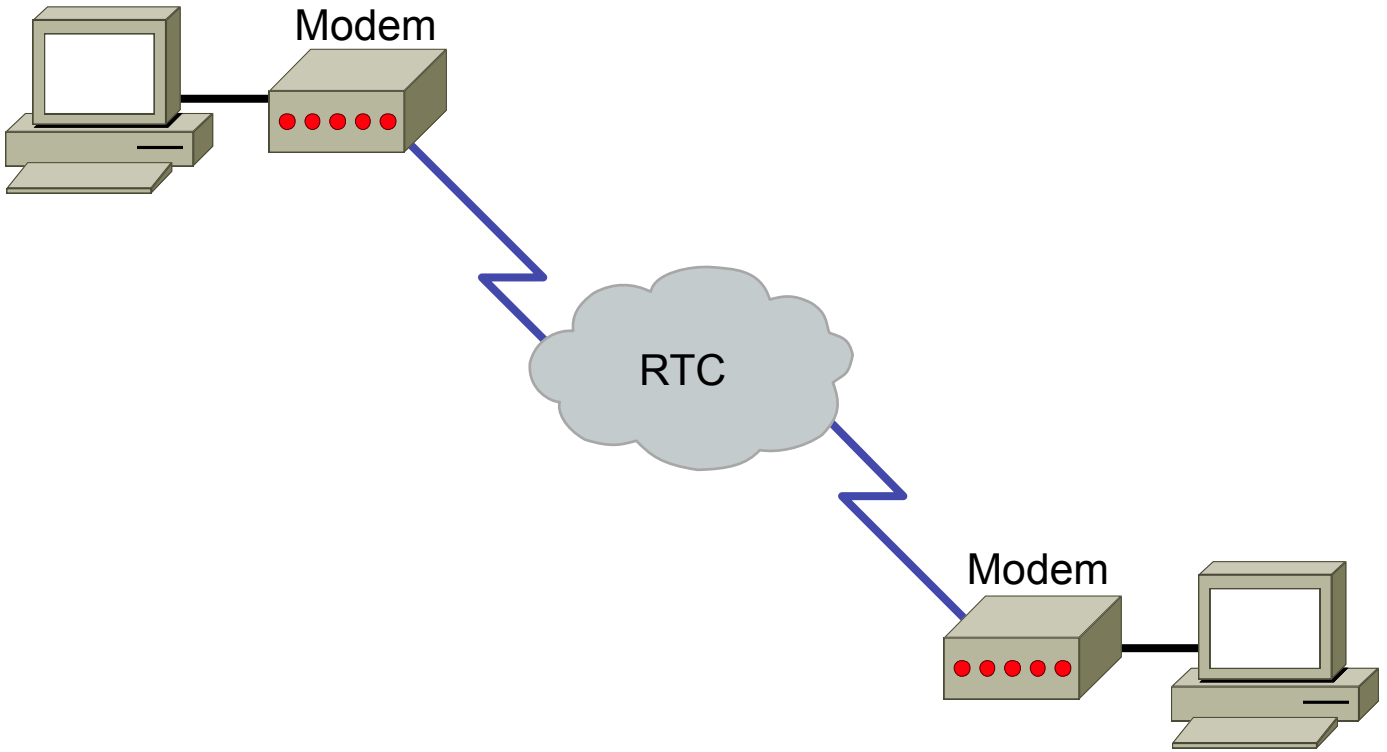
Le concentrateur





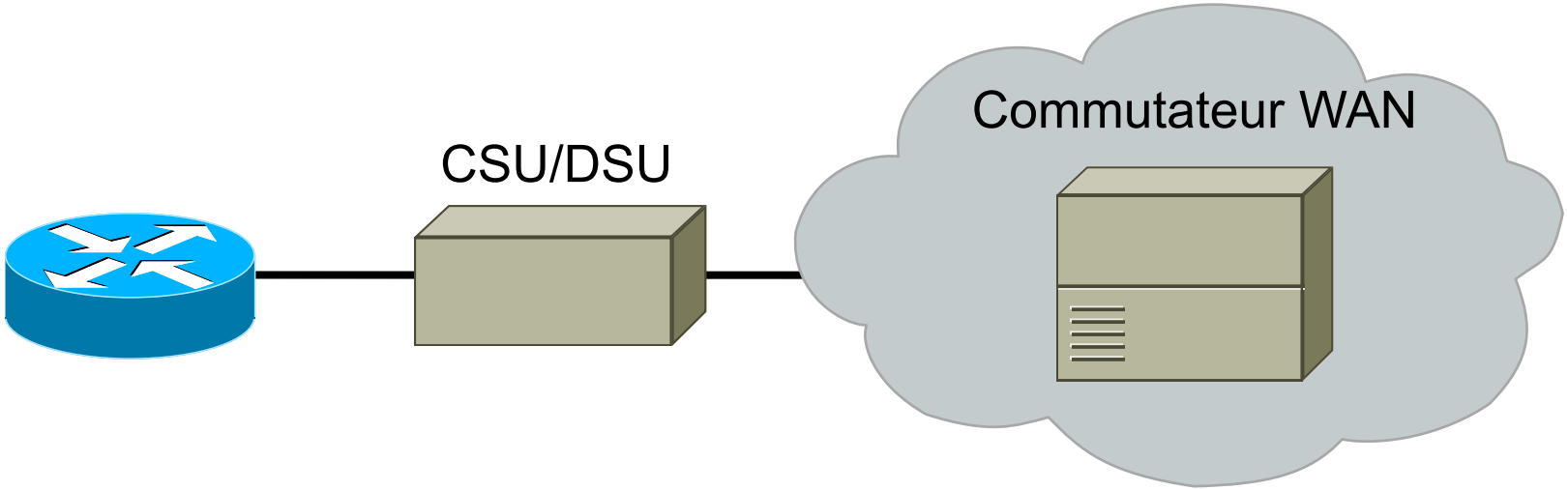
- Permet d'interconnecter plusieurs équipements
- Régénère le signal, comme le répeteur
- C'est un répeteur multiport

Le Modem



Un modem convertit le signal analogique du RTC en signal numérique pour le PC

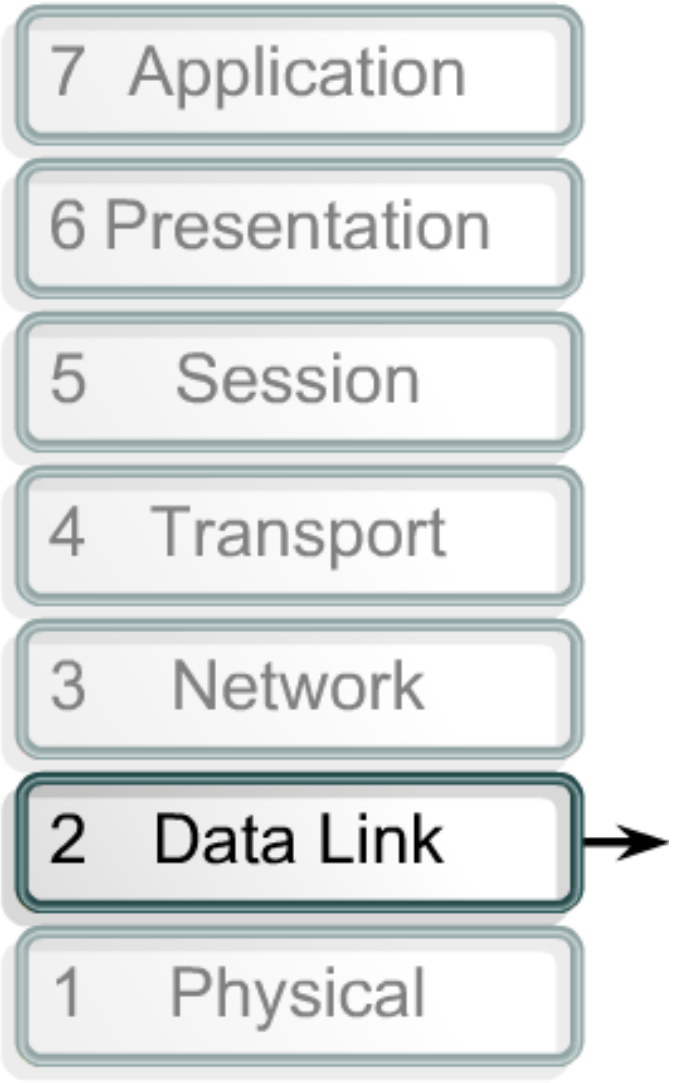
CSU/DSU ou ETTD/ETCD



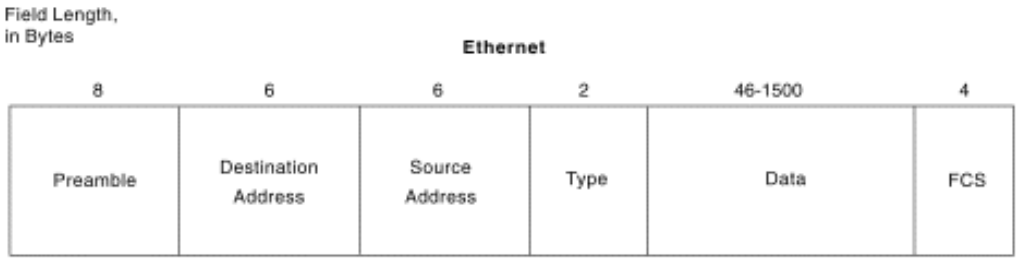
C'est un modem utilisé par les liaisons spécialisées et Frame-Relay

OSI couche 2 : Liaison de données

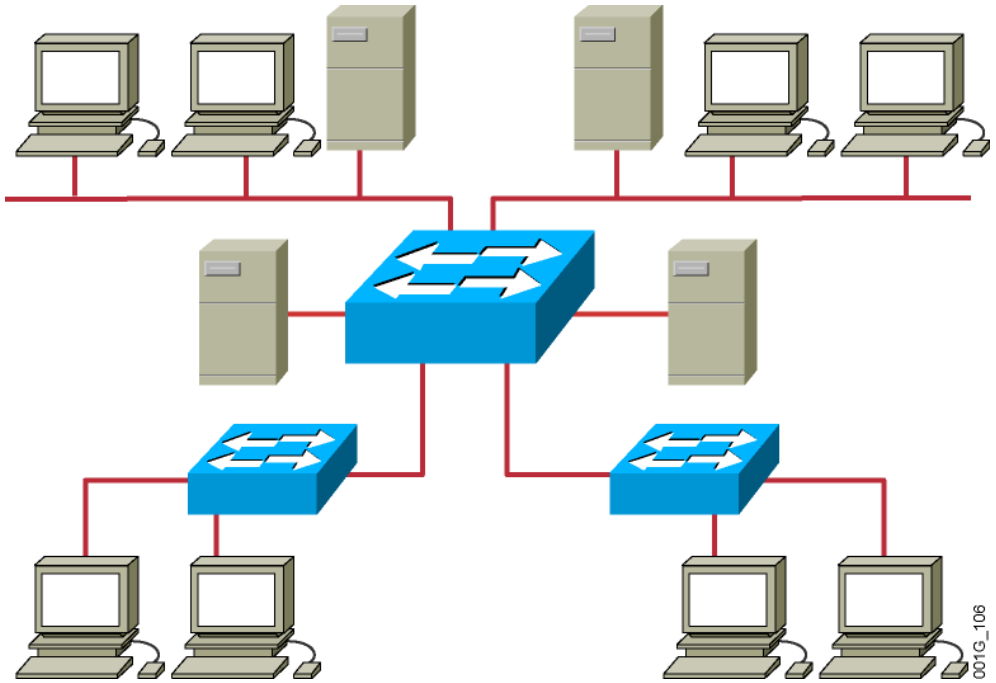
OSI couche 2 – Liaison des données



- La couche liaison de données fournit un conteneur de bits appelés Trames.
- Cette couche définit la méthode d'accès au média (Ethernet, Token Ring)
- Chaque équipement de couche 2 possède une adresse physique appelée aussi MAC



Equipements de couche 2 : le commutateur



- Le commutateur apprend les adresses MAC en silence
- Cet apprentissage permet, par la suite, de copier les trames uniquement sur le port concerné

Exemple de protocole couche 2 : Ethernet

DIX

Preambule	Destination	Source	Type	Data Upper Layers	FCS
8	6	6	2	46 - 1500	4

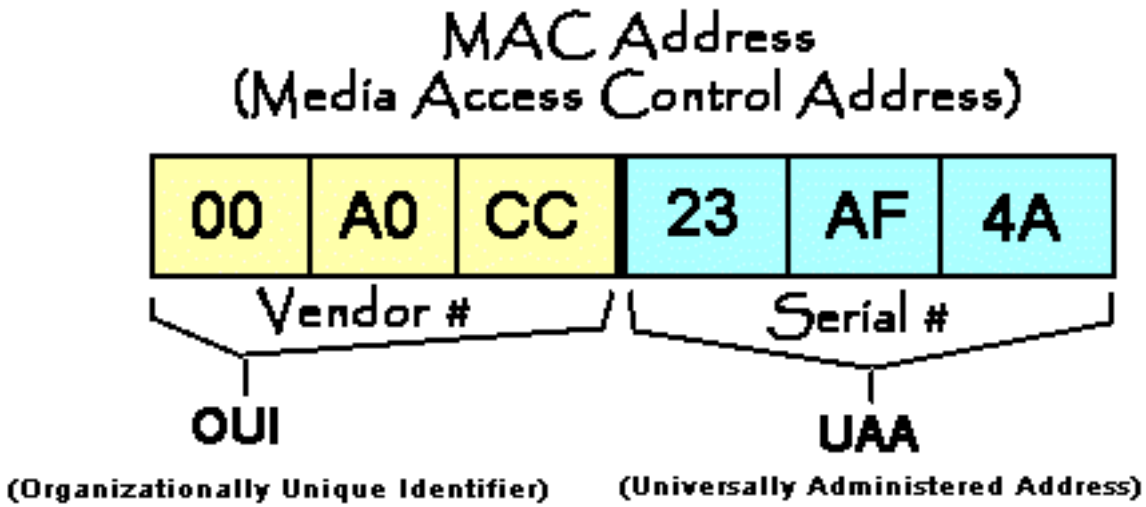
IEEE 802.3 original

Preambule	SFD	Destination	Source	Len.	Data Upper Layers	FCS
7	1	6	6	2	46 - 1500	4

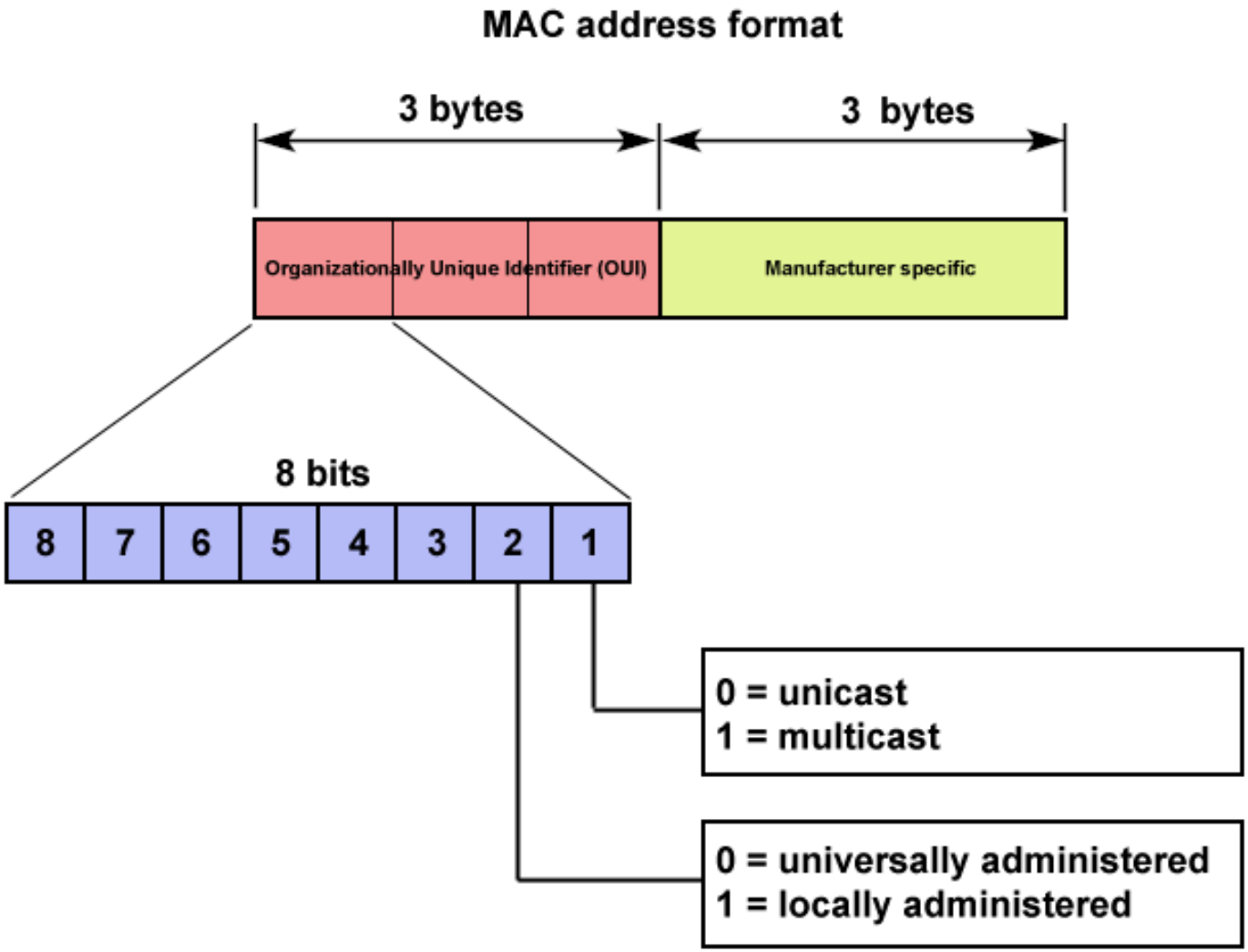
IEEE 802.3 révisé

Preambule	SFD	Destination	Source	L/T	Data Upper Layers	FCS
7	1	6	6	2	46 - 1500	4

L’adresse MAC



L’adresse MAC



Ethertype

Valeur	Signification
0x0800	IP
0x0806	ARP Address Resolution Protocol
0x8100	802.1Q pour interfaces trunk
0x86DD	IPv6

OSI couche 3 : la couche réseaux

OSI couche 3 – La couche réseaux

- La couche réseau introduit un nommage logique : l'adresse IP
- Des adresses IP sont regroupées en entités appelés réseaux et sous réseaux.
- Les réseaux sont annoncés par des protocoles de routage afin de déterminer le plus court chemin.
- La couche réseaux n'est pas fiable

Dispositif de la couche 3 : le Router

- Les équipements de la couche 3 sont des **routeurs**

Caractéristiques du Protocole IP

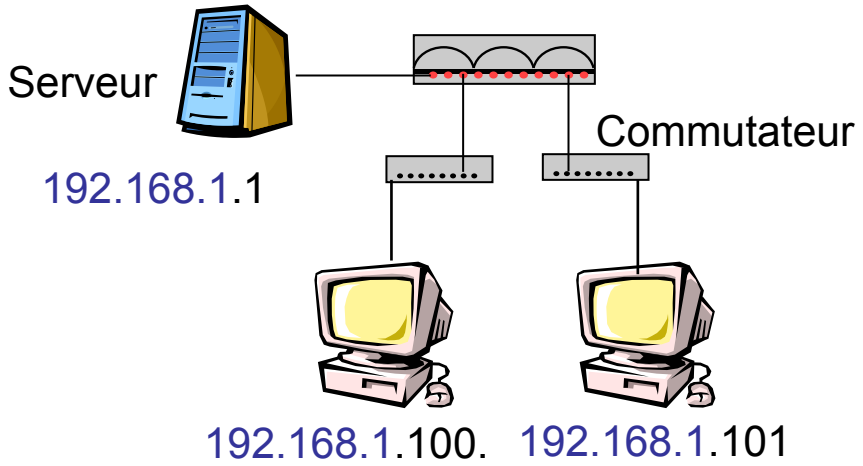
- Couche 3 du modèle OSI
- Non fiable (best effort) : pas de garantie que les paquets soient bien arrivés, ni qu'ils arrivent dans l'ordre dans lequel ils ont été envoyés
- Chaque paquet est traité indépendamment : 2 paquets dont les adresses source et destination sont identiques peuvent emprunter des chemins différents

Adressage IP

- Chaque hôte (PC, imprimante, périphérique…) doit posséder son adresse IP
- Une adresse IP est la combinaison d'une adresse de réseau et d'un complément de hôte
- L'adresse est représentés sur 4 octets en décimal

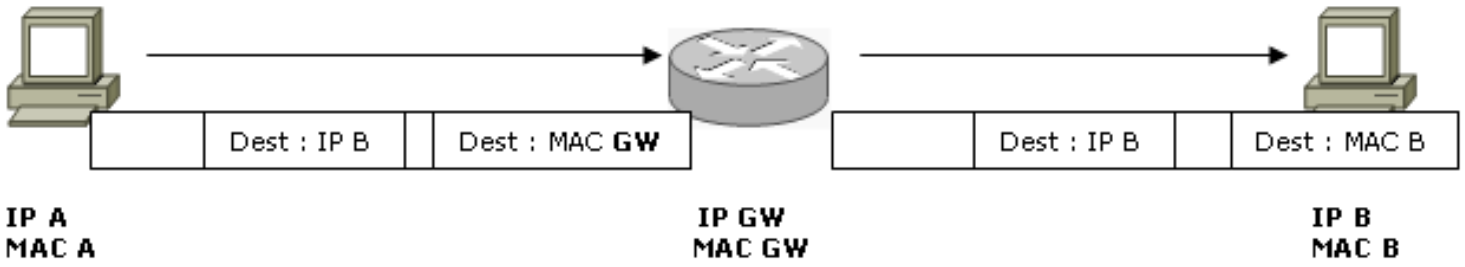
réseau.hôte

Réseau :
192.168.1.0/24
255.255.255.0

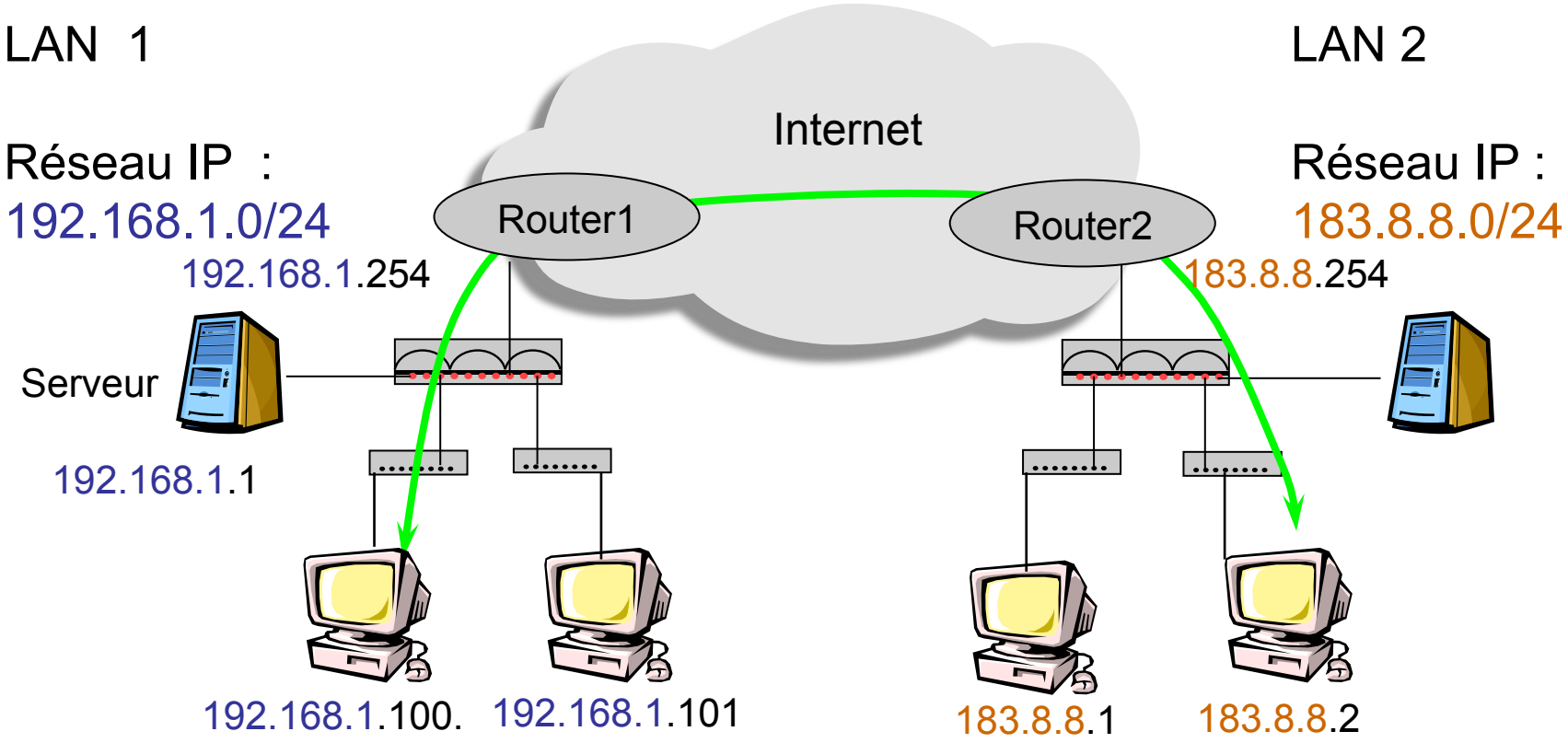


Le rôle du routeur

- Si deux PC ne sont pas sur le même réseau, ils sont séparés par un routeur.
  - Ce routeur est la passerelle de chaque PC
- Les entêtes IP ne sont **pas modifiées** par le routeur
- Les entêtes Ethernet sont **reconstruites** par le routeur

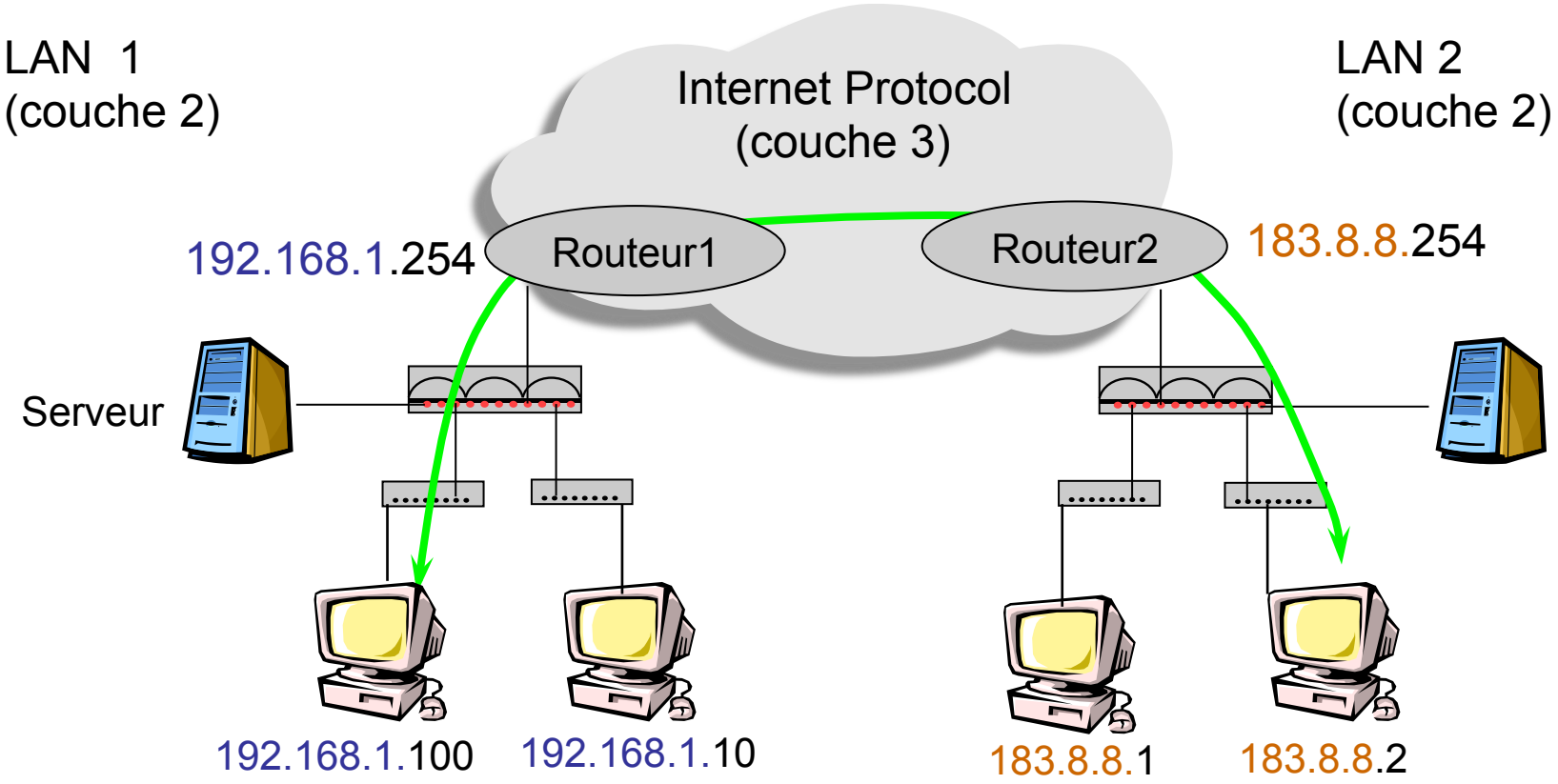


Un réseau local est associé à un réseau IP



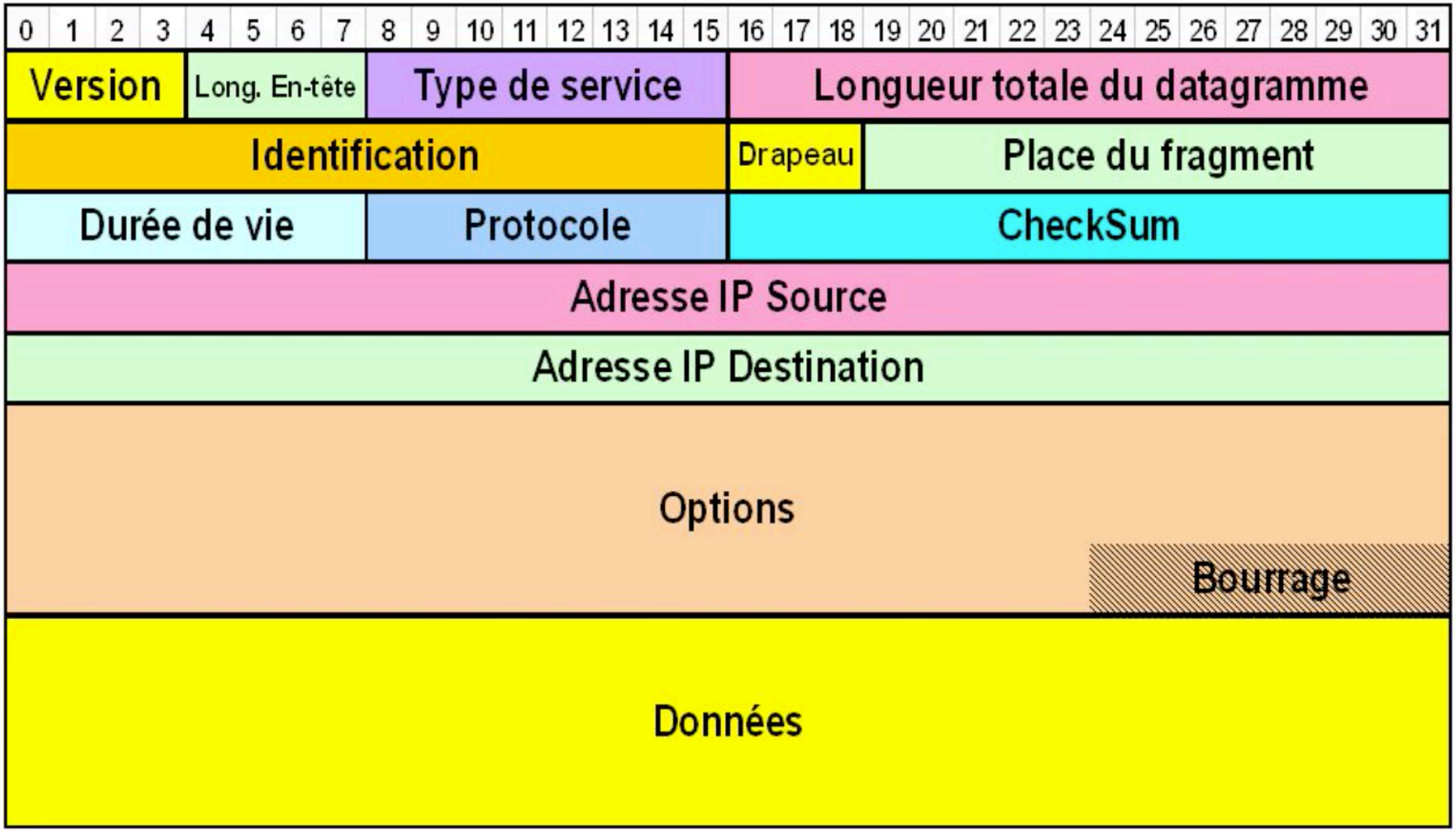
- Chaque host a une adresse IP
- Toutes les adresses IP d'un même site appartiennent au même réseau

Le routeur est la passerelle par défaut

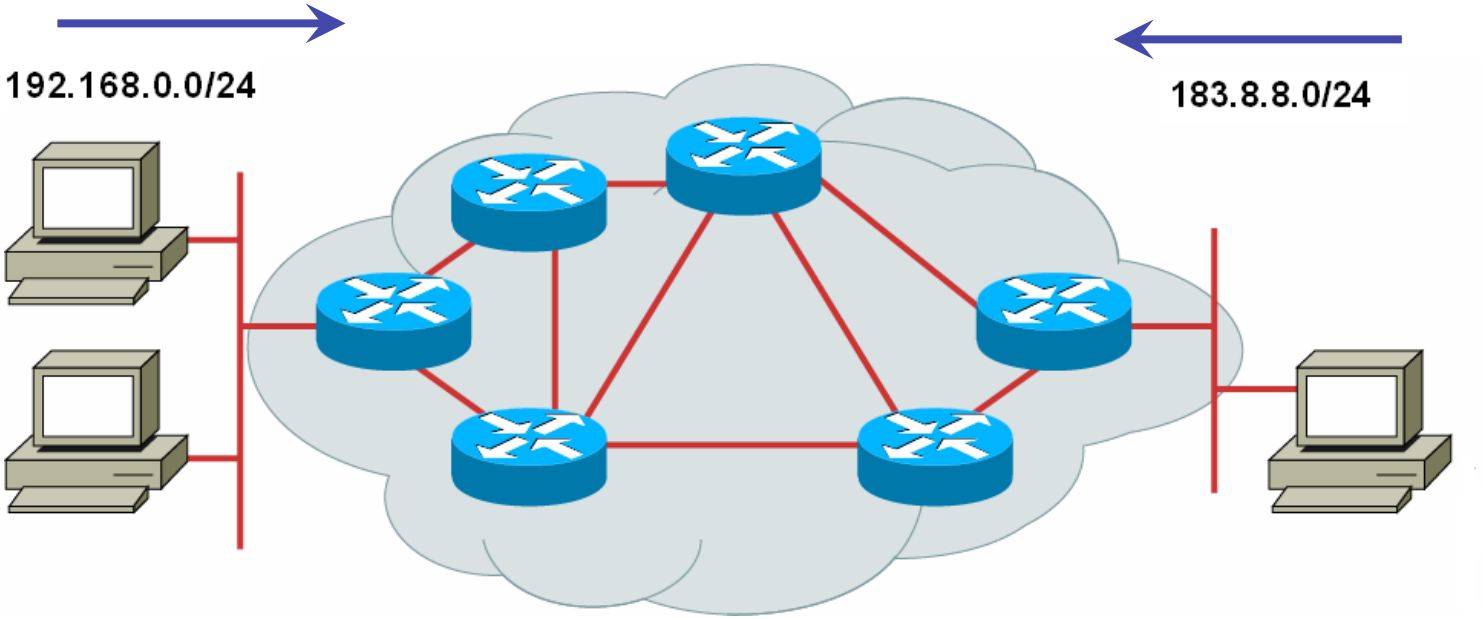


- Internet Protocol (IP) interconnect les LAN (Ethernet)
- Le routeur est la passerelle par défaut du LAN

L'entête IP


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
Long. En-tête
Type de service
Longueur totale du datagramme
Identification
Drapeau
Place du fragment
Durée de vie
Protocole
CheckSum
Adresse IP Source
Adresse IP Destination
Options
Bourrage
Données

Les protocoles de routage

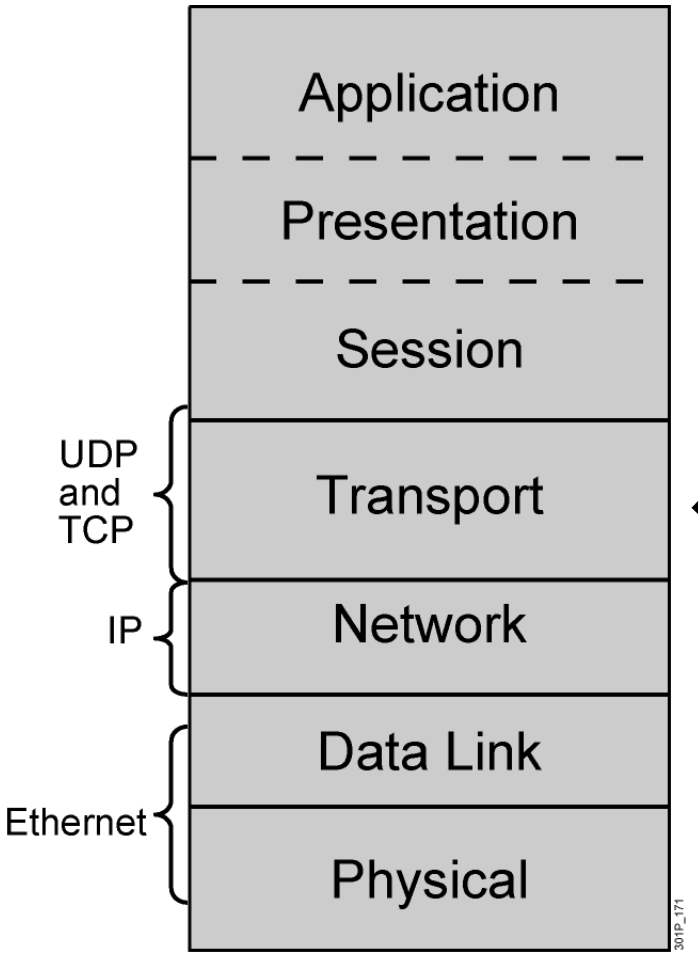


- Les protocoles de routage annoncent les routes de chaque site

- Chaque routeur tient compte de ces annonces pour déterminer le “Next hop” dans la perspective du meilleur chemin vers la destination

OSI couche 4 : la couche transport

La couche transport



- Multiplexage de session (UDP et TCP)
- Segmentation (TCP)
- Controle de flux (TCP)
- Orienté connexion (TCP)
- Fiabilité (TCP)

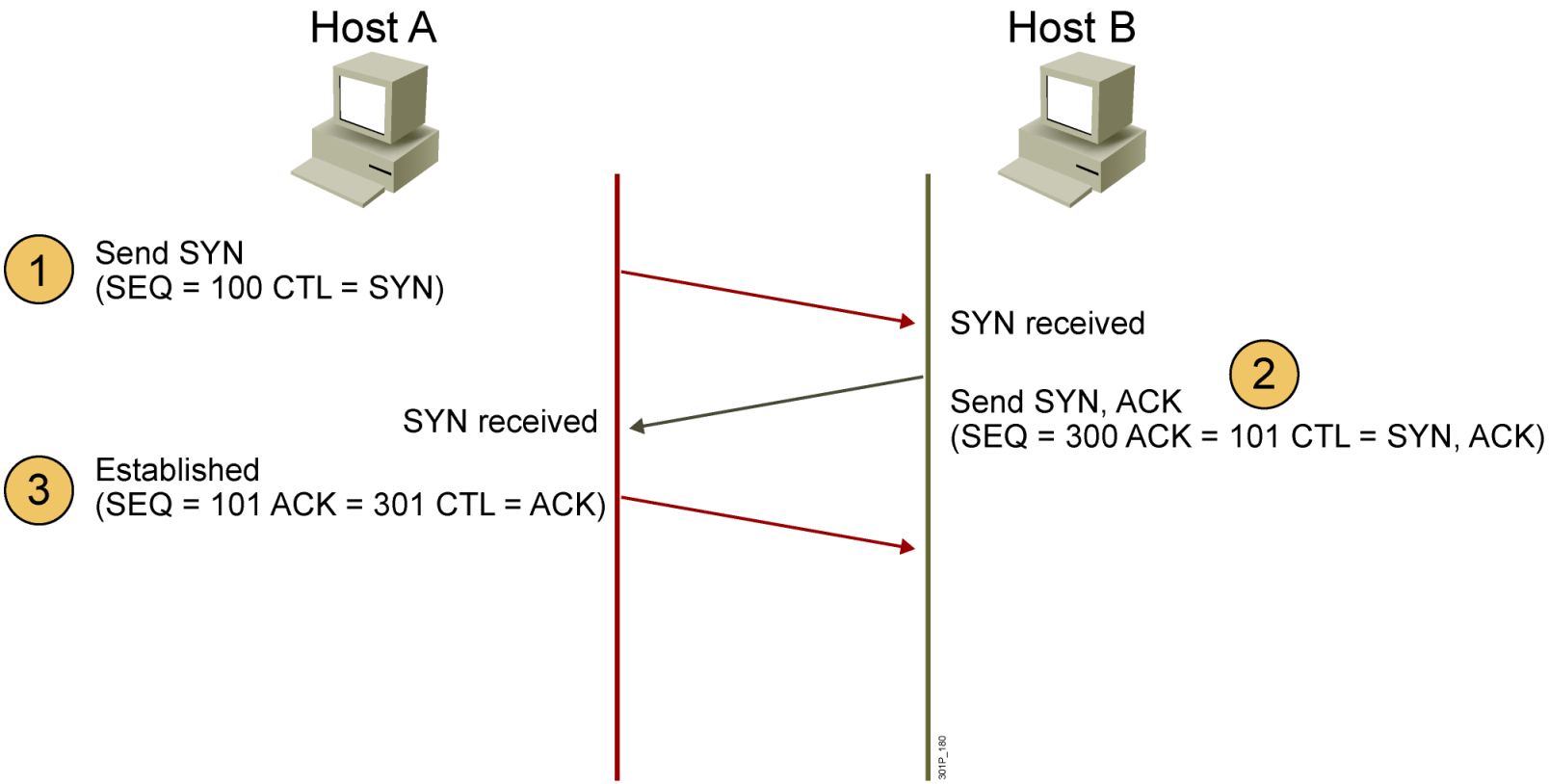
Caractéristiques de UDP

- Sans connexion
- Simplex
- Détection d’erreur
- Fait de son mieux (Best effort)
- Pas de correction d’erreur

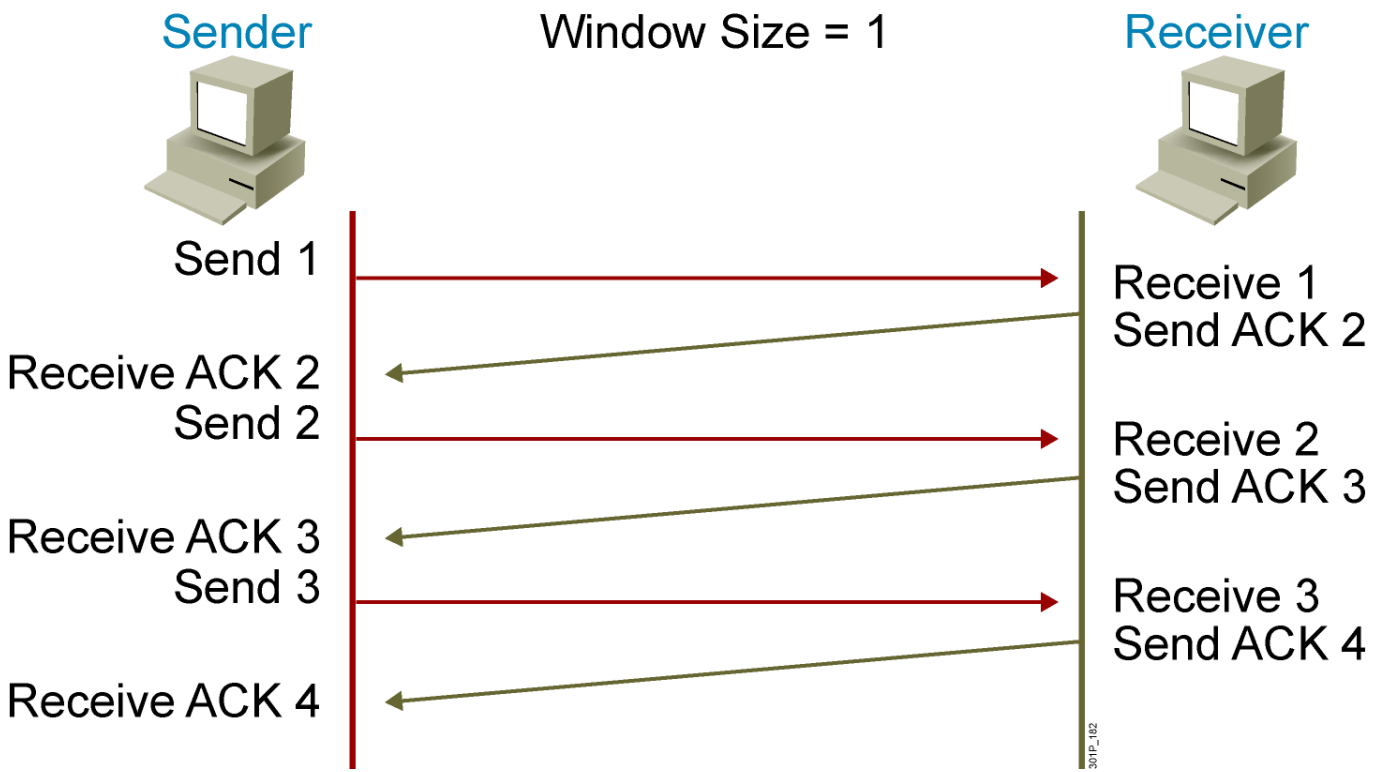
Caractéristiques de TCP

- Protocol orienté connexion
- Fonctionne en mode Full-duplex
- Détection d’erreur
- Sequencement et ordonnancement des paquets
- Acquittement des paquets reçus
- Retransmission des paquets perdus

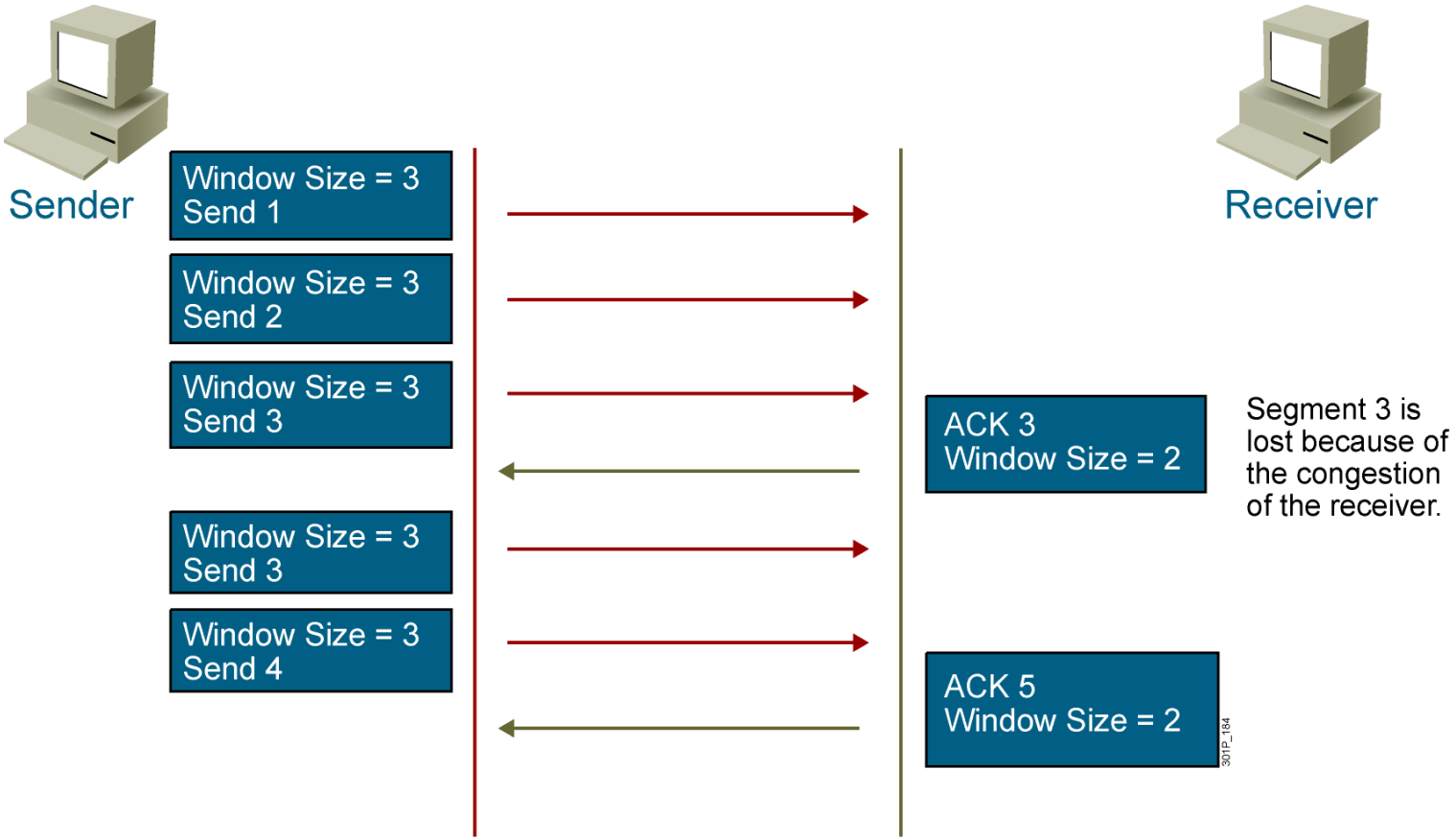
Protocol à trois poignées de main



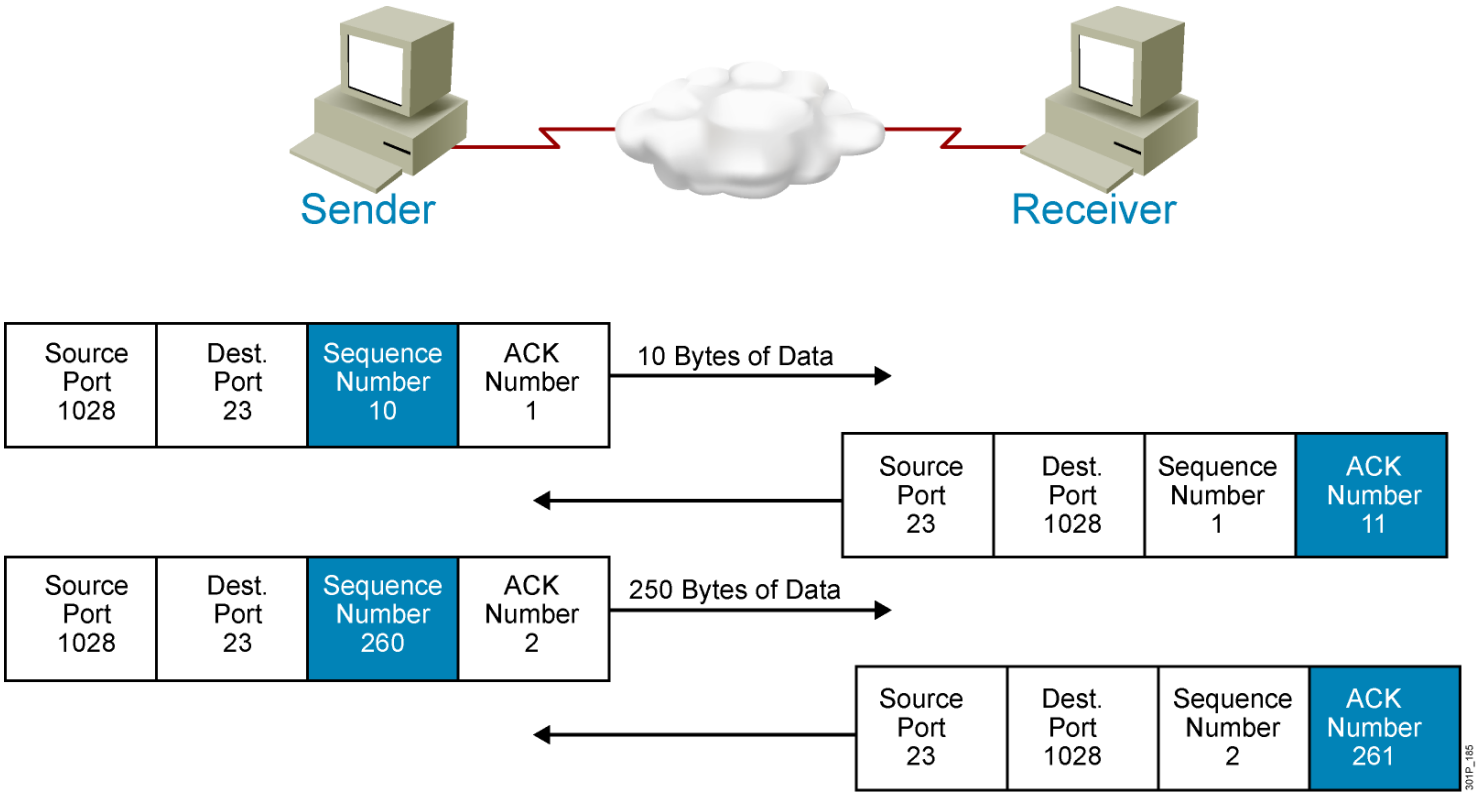
Acquittement TCP



La fenêtre glissante

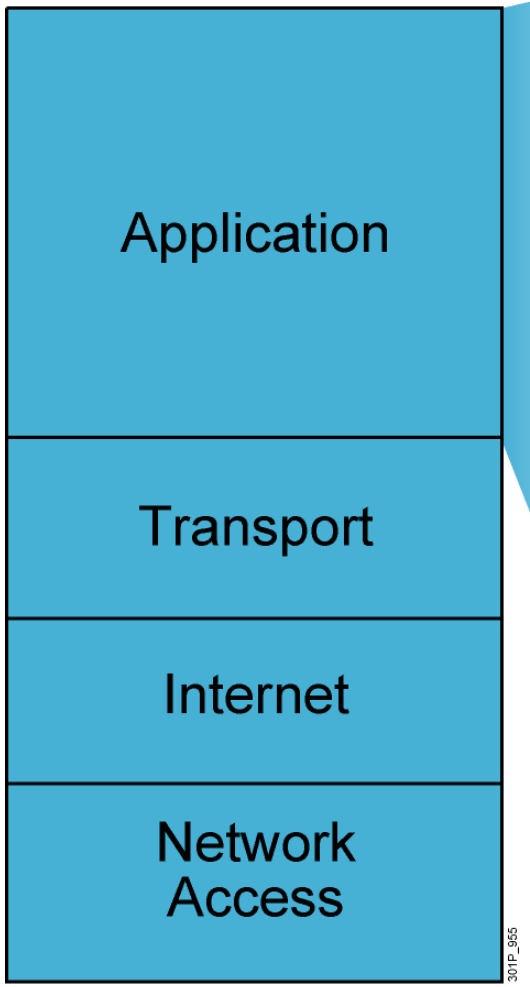


Numéros de séquence



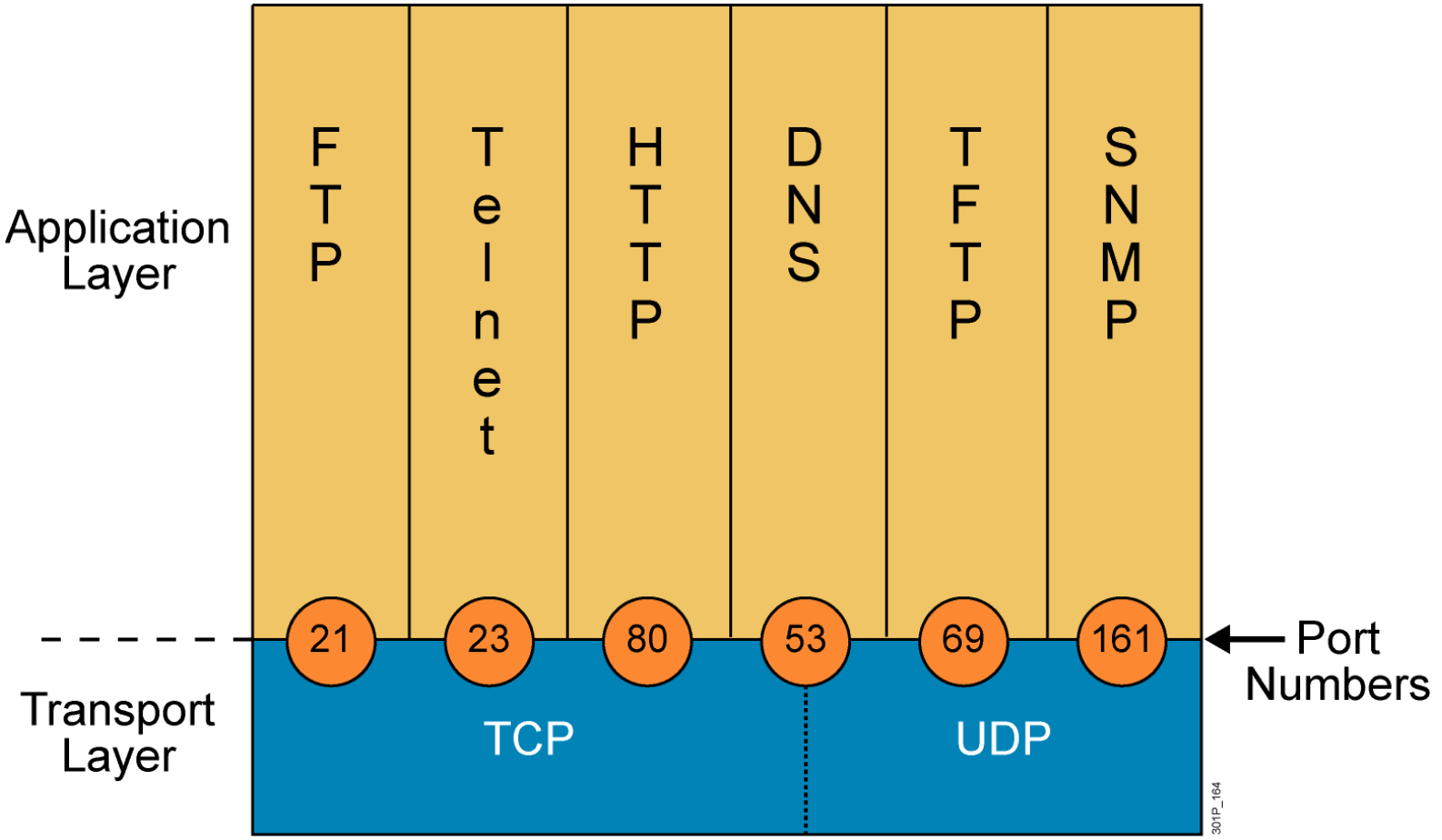
OSI couche 7 : Application

Les applications TCP/IP

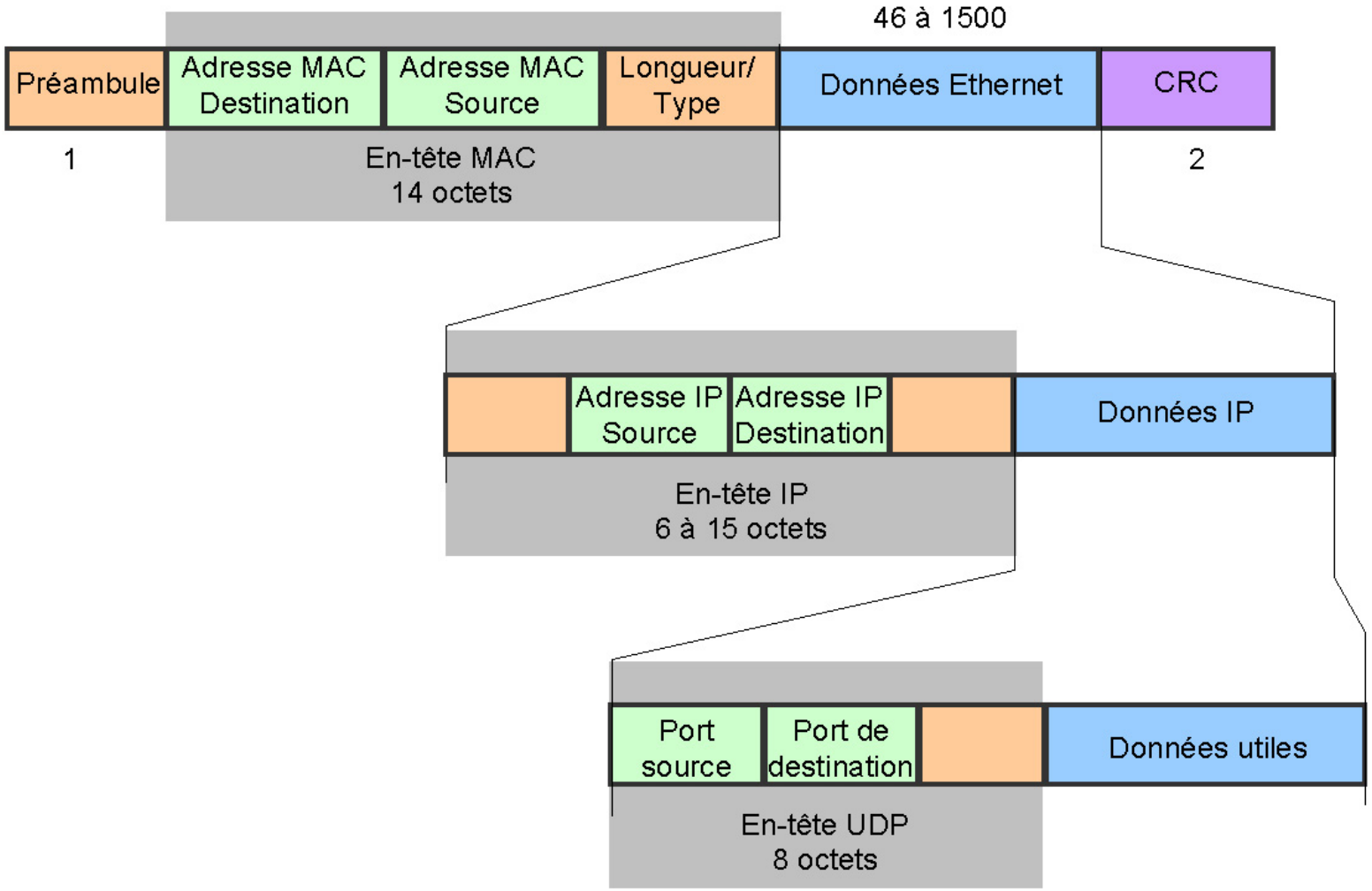


- Transferts de fichiers
  - FTP
  - TFTP
  - Network File System
- E-mail
  - Simple Mail Transfer Protocol
- Accès distant
  - Telnet
  - rlogin
- Gestion des réseaux
  - Simple Network Management Protocol
- Gestion des noms
  - Domain Name System

Les numéros de port des applications



Bilan des couches

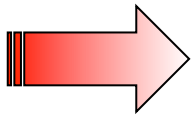


Subnetting

Première partie

Subnetting sur octet entier

L’adresse de couche 3:

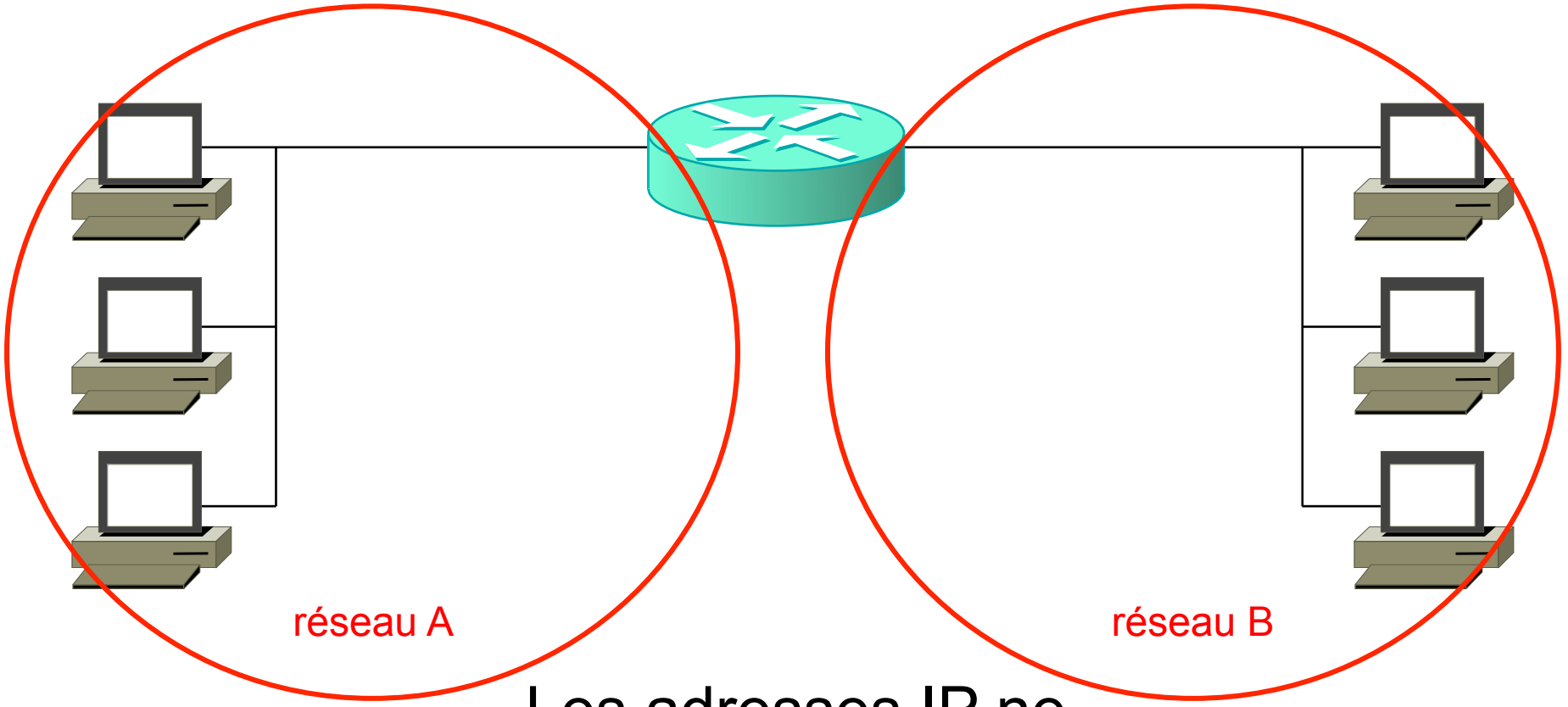


1. **L’adresse IP et son masque**
2. Les adresses réservées
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

L'adresse IP

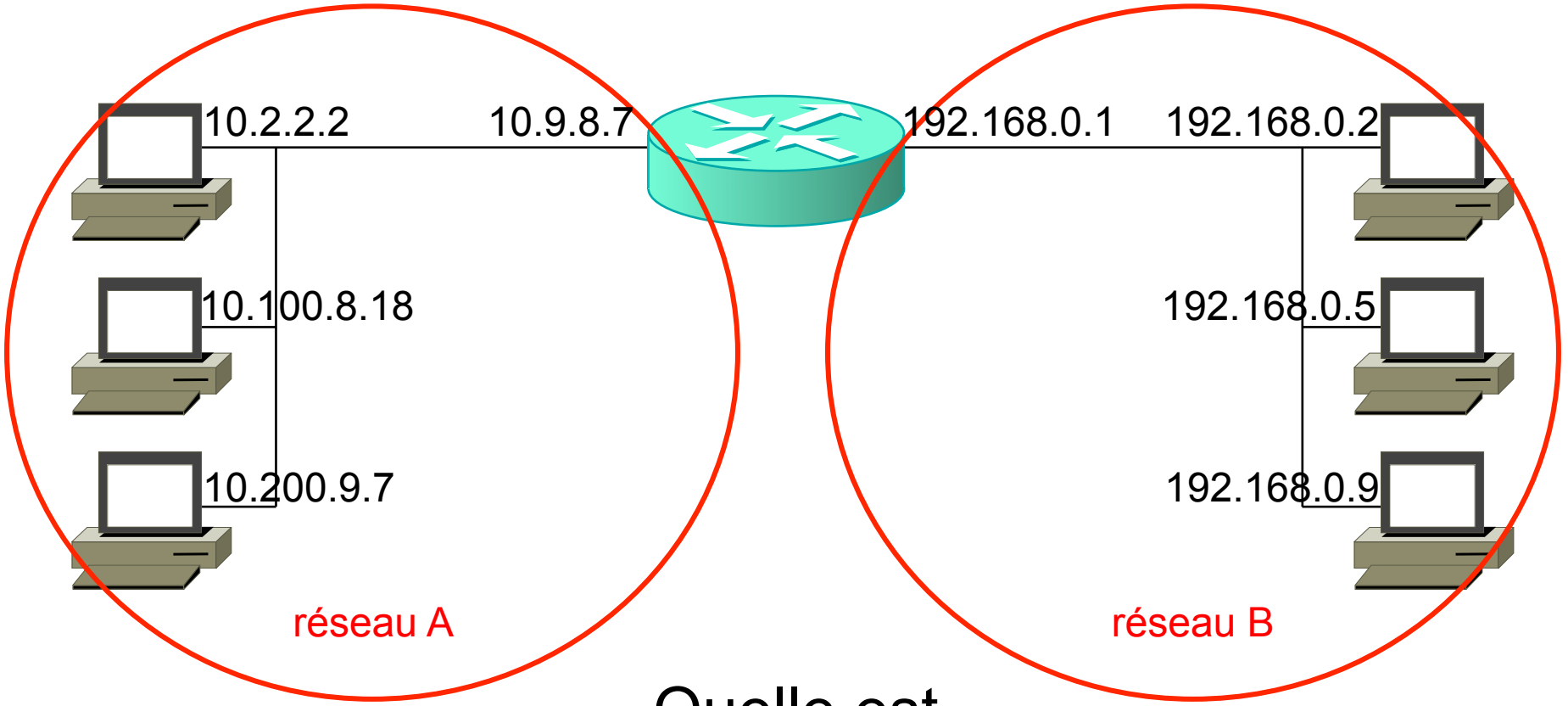
- Une adresse IP, c'est 4 octets : 192.168.4.6
  - 192 = 1er octet
  - 168 = 2ème octet
  - 4 = 3ème octet
  - 6 = 4ème octet
- Un octet = 8 bits
  - donc une adresse IP = 8 x 4 = 32 bits

Deux réseaux



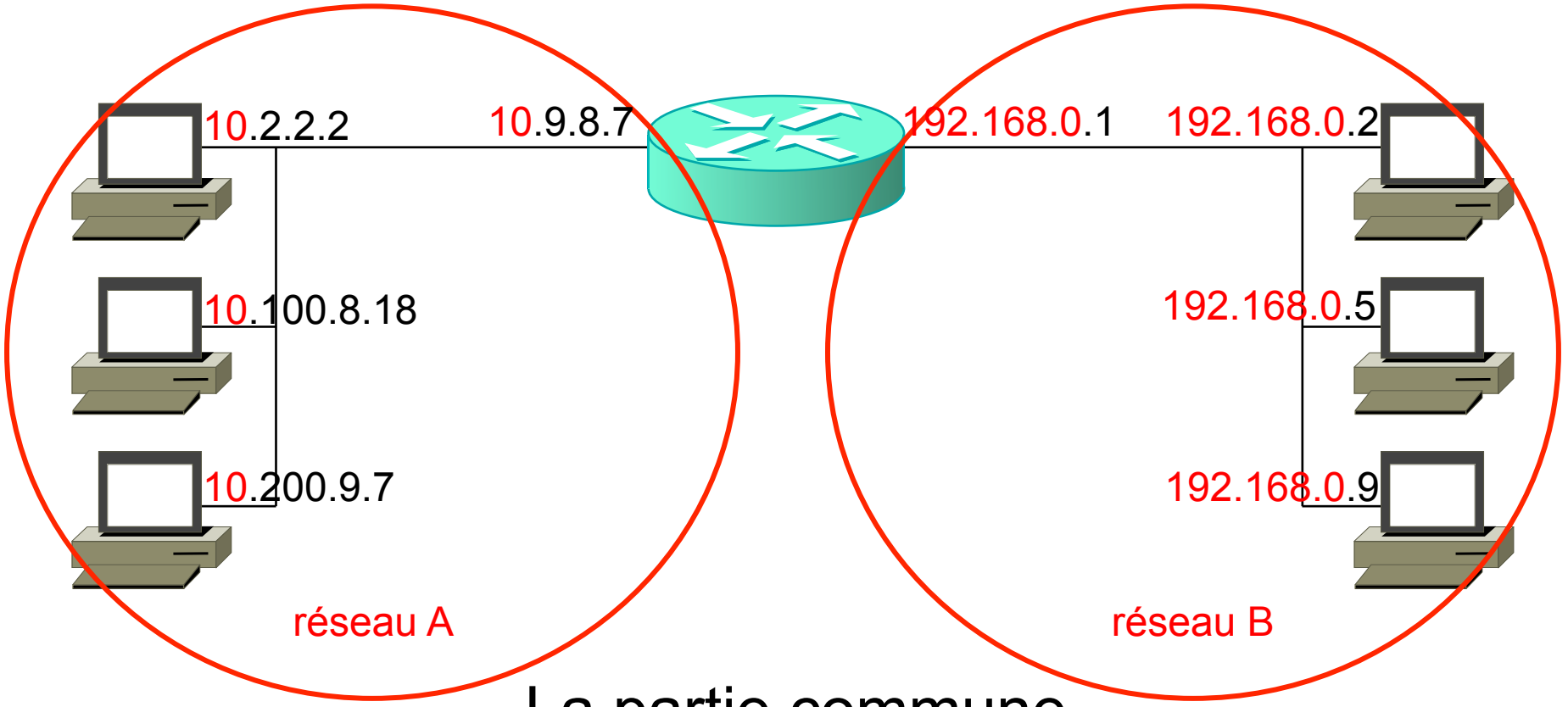
Les adresses IP ne pourront pas être attribuées de manière quelconque !

Identifiez la partie commune !



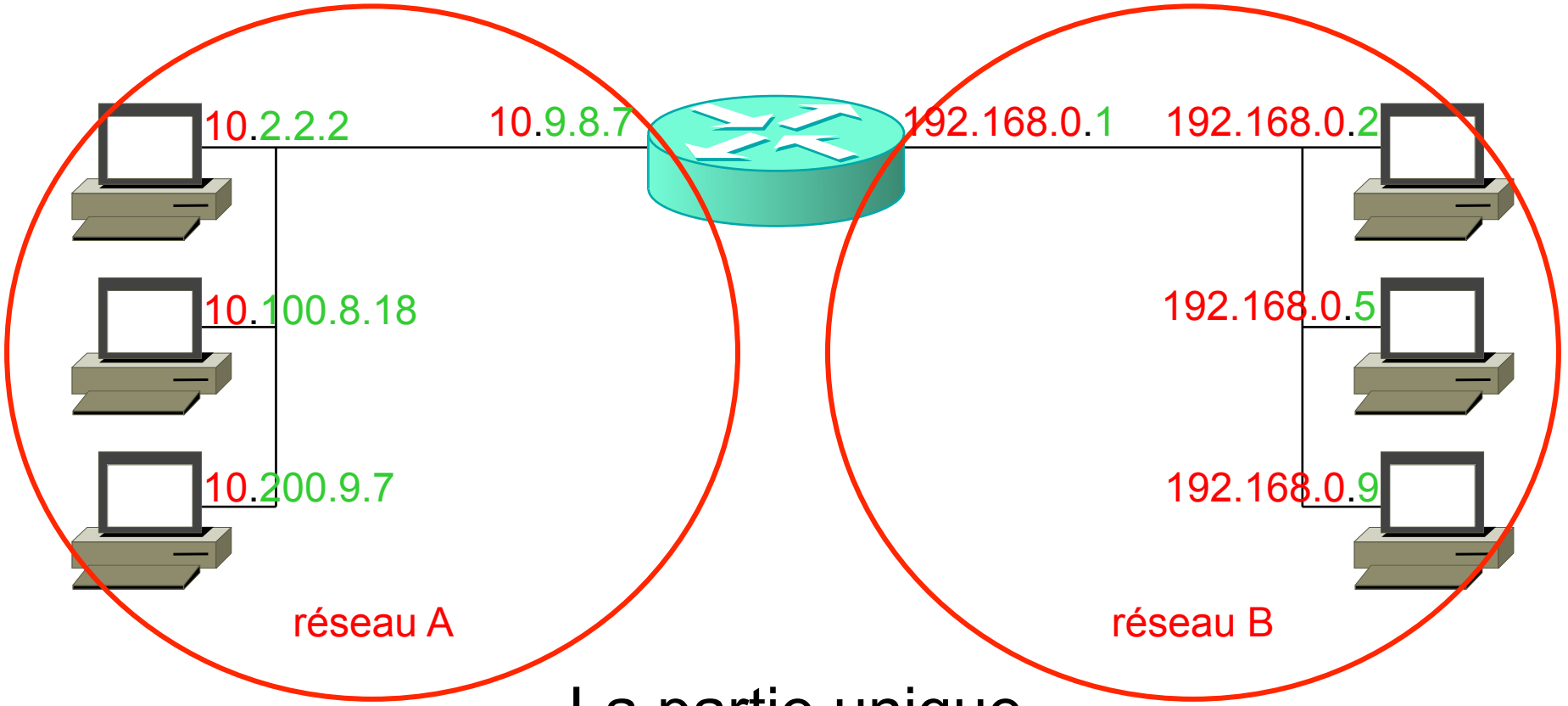
Quelle est
la partie **commune**
dans chaque réseau ?

La partie commune



La partie commune s’ appelle la partie réseau.

La partie unique



La partie unique
s’appelle la partie hôte.

L'adresse IP seule ne suffit pas !

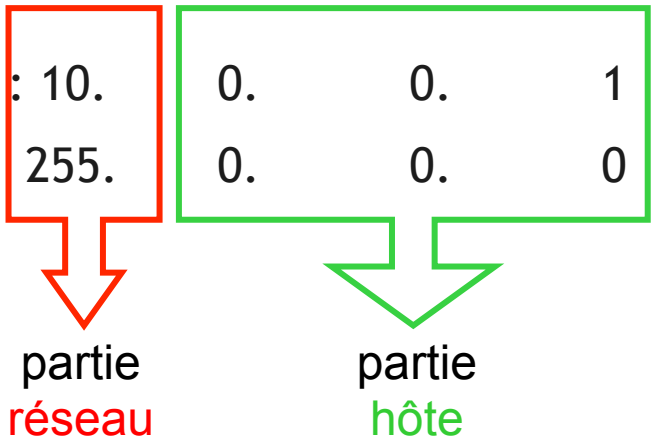
- Comment distinguer la partie 'réseau' de la partie 'hôte' ?
- ➔ à l'aide du masque

- Exemples de masques :
  - 255.0.0.0
  - 255.255.0.0
  - 255.255.255.0

Application du masque décimal

- On va **superposer** le masque et l'adresse IP.

- Exemple :
  - Adresse IP : 10. 0. 0. 1
  - Masque : 255. 0. 0. 0



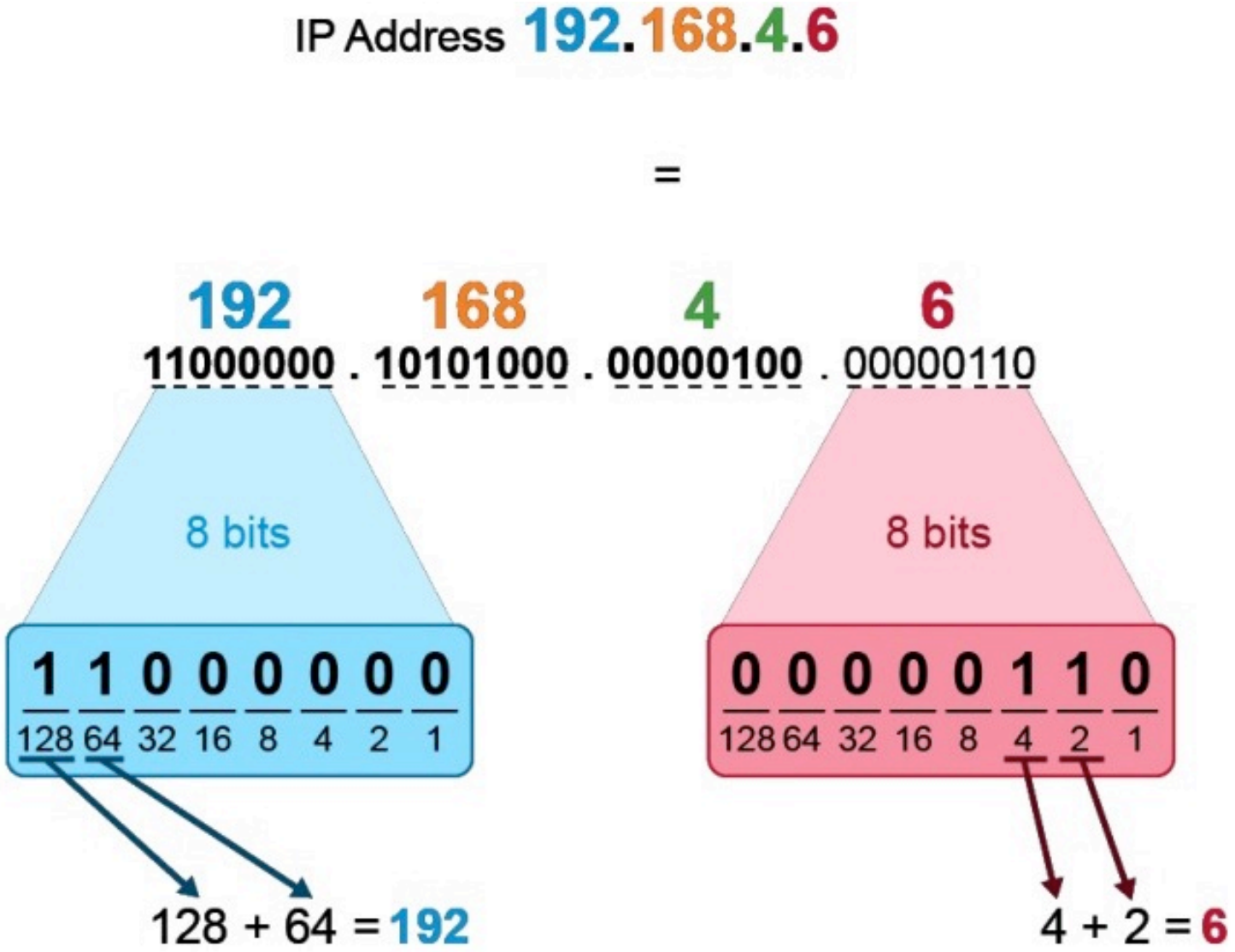
Exercice : identifiez la partie réseau

Adresse IP				Masque			
10	1	1	2	255	0	0	0
14	14	14	14	255	0	0	0
142	142	142	142	255	255	0	0
172	16	0	255	255	255	0	0
192	168	168	168	255	255	255	0
199	199	199	199	255	255	255	0

Solution

Adresse IP				Masque			
10	1	1	2	255	0	0	0
14	14	14	14	255	0	0	0
142	142	142	142	255	255	0	0
172	16	0	255	255	255	0	0
192	168	168	168	255	255	255	0
199	199	199	199	255	255	255	0

L’adresse IP peut aussi s’écrire en binaire



Les puissances de 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Ce tableau facilite les conversions

Binaire ⇔ Décimal

Exemples de conversion

128	64	32	16	8	4	2	1		en décimal
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
0	0	1	1	0	0	0	0	=	?
0	0	0	0	1	0	1	0	=	?
?	?	?	?	?	?	?	?	=	40

Exemples de conversion

128	64	32	16	8	4	2	1		en décimal
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
0	0	1	1	0	0	0	0	=	**48**
0	0	0	0	1	0	1	0	=	**10**
0	**0**	**1**	**0**	**1**	**0**	**0**	**0**	=	40

Comment écrire le masque en binaire ?

128	64	32	16	8	4	2	1		en décimal
?	?	?	?	?	?	?	?	=	255

1	1	1	1	1	1	1	1	=	255

Exemple :

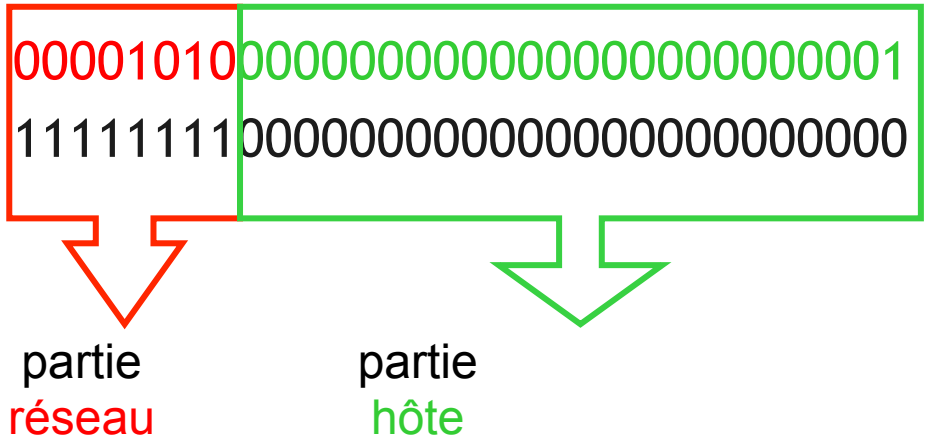
- 11111111.00000000.00000000.00000000
- 255 . 0 . 0 . 0

Le masque en binaire

- Le masque est une suite de 32 bits.
  - Dès qu'un bit est à **0**, tous les bits suivants sont à 0.
- Exemples :
  - **0**00000000000000000000000000000
  - 11**0**00000000000000000000000000
  - 11111111**0**0000000000000000000
  - 1111111111111111**0**000000000000
  - 111111111111111111111111**0**0000000
  - 11111111111111111111111111111111

Application du masque binaire

- Le masque est **superposé** à l'adresse IP.
  - Exemple :
    - Adresse IP : 00001010 00000000000000000000001
    - Masque : 11111111 00000000000000000000000



Ecriture simplifiée du masque

- Le masque est une suite de ‘1’ suivie par une suite de ‘0’ :
  - il suffit **d’indiquer le nombre de 1.**
- Exemples :
  - 00000000.00000000.00000000.00000000 s’écrira /0
  - 11111111.00000000.00000000.00000000 s’écrira /8
  - 11111111.11111111.00000000.00000000 s’écrira /16
  - 11111111.11111111.11111111.00000000 s’écrira /24
  - 11111111.11111111.11111111.11111111 s’écrira /32

Exercice : identifiez la partie réseau

Adresse IP				Masque
10	1	2	3	/8
19	19	19	19	/8
150	150	150	150	/16
200	201	202	203	/24

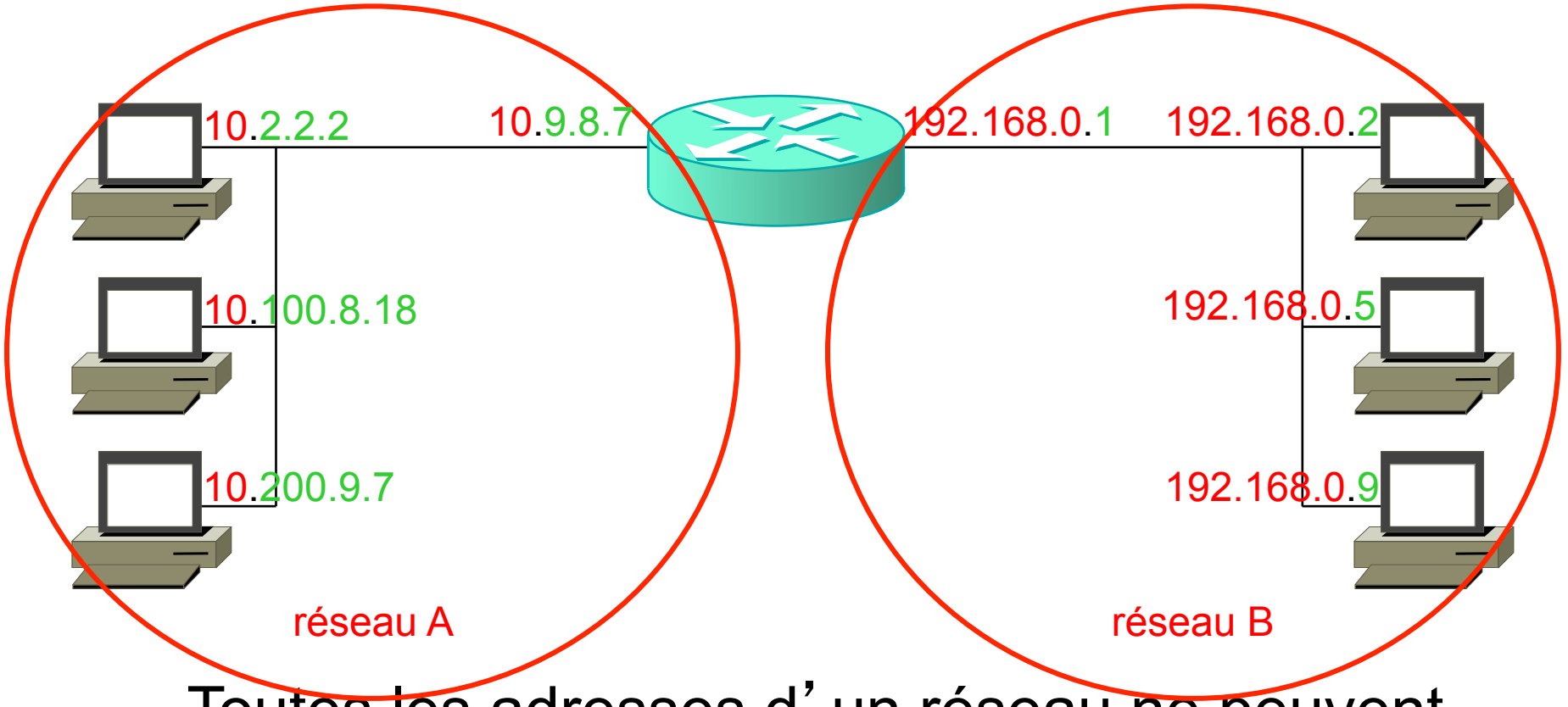
Solution

Adresse IP				Masque
10	1	2	3	/8
19	19	19	19	/8
150	150	150	150	/16
200	201	202	203	/24

L’adresse de couche 3:

1. **L’adresse IP et son masque**
2. **Les adresses réservées**
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

Quelle adresse attribuer à un PC ?



Toutes les adresses d'un réseau ne peuvent pas être attribuée aux équipements.

2 adresses sont réservées :
l'adresse RESEAU et l'adresse BROADCAST

Exemples d'adresses réseau

Adresse IP				Masque
10	0	0	0	/8
19	0	0	0	/8
150	150	0	0	/16
200	201	202	0	/24

Exemples d'adresses broadcast

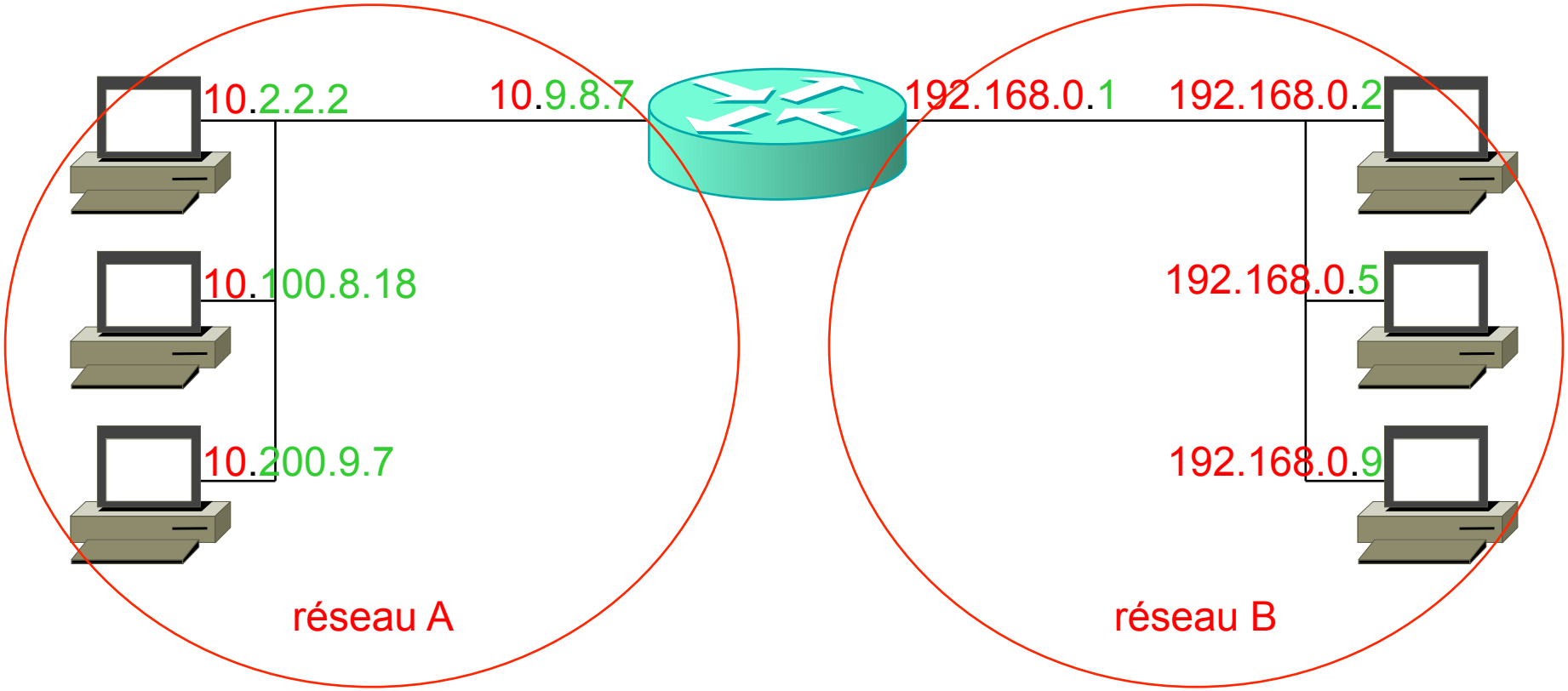
Adresse IP				Masque
10	255	255	255	/8
19	255	255	255	/8
150	150	255	255	/16
200	201	202	255	/24

Adresses réservées

- Si la partie hôte **ne contient que des 0** :
  - C'est l'adresse 'réseau'.
    - Elle ne peut pas être attribuée à un équipement.

- Si la partie hôte **ne contient que des 1** :
  - C'est l'adresse 'broadcast'.
    - Elle ne peut pas être attribuée à un équipement.

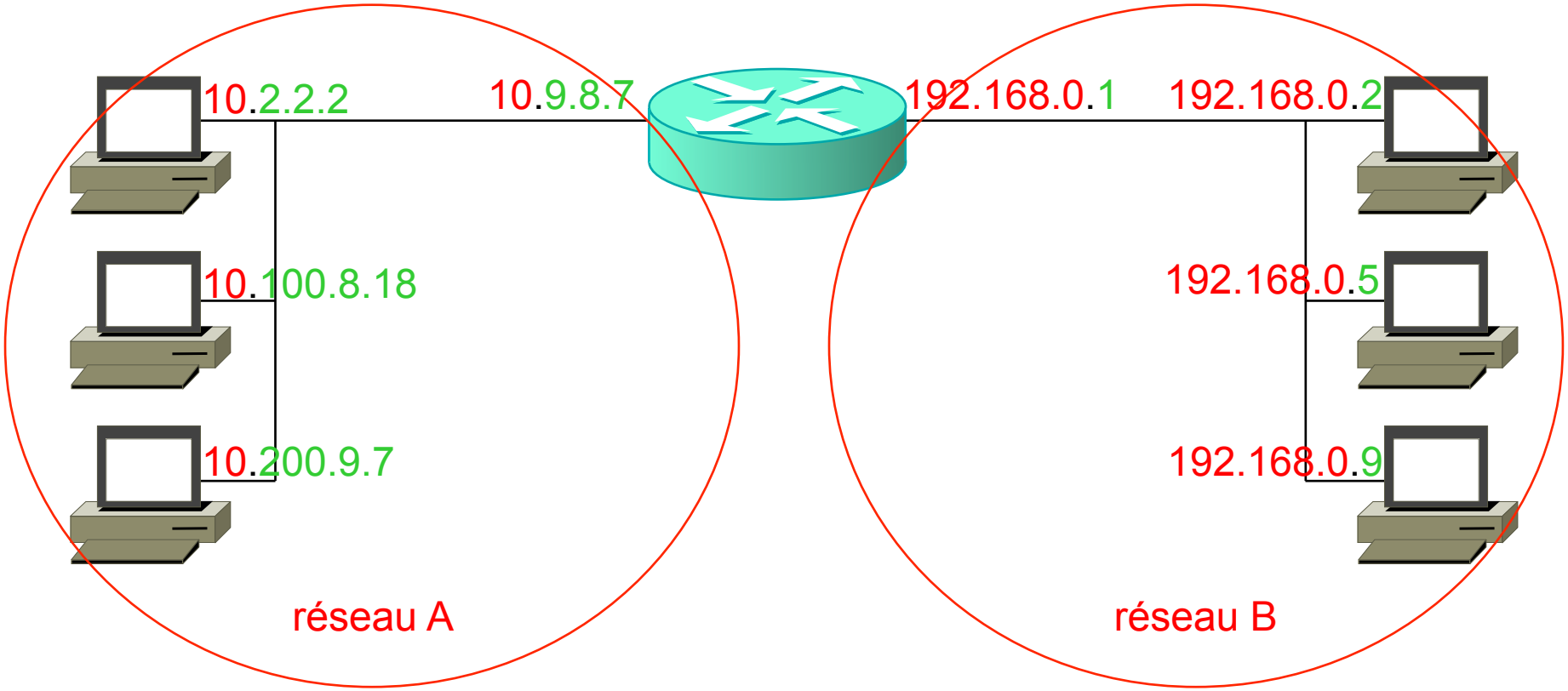
Adresse réseau de A et B



Adresse réseau de A
= 10.0.0.0

Adresse réseau de B
= 192.168.0.0

Adresse broadcast de A et B



Adresse broadcast de A = 10.255.255.255

Adresse broadcast de B = 192.168.0.255

Exercice : déterminez les adresses interdites

Adresse IP				Masque	Adresse réseau	Adresse broadcast
10	5	8	3	/8		
50	50	50	50	/8		
111	111	111	111	/16		
172	16	0	3	/16		
192	168	168	8	/24		
200	200	200	200	/24		

Solutions

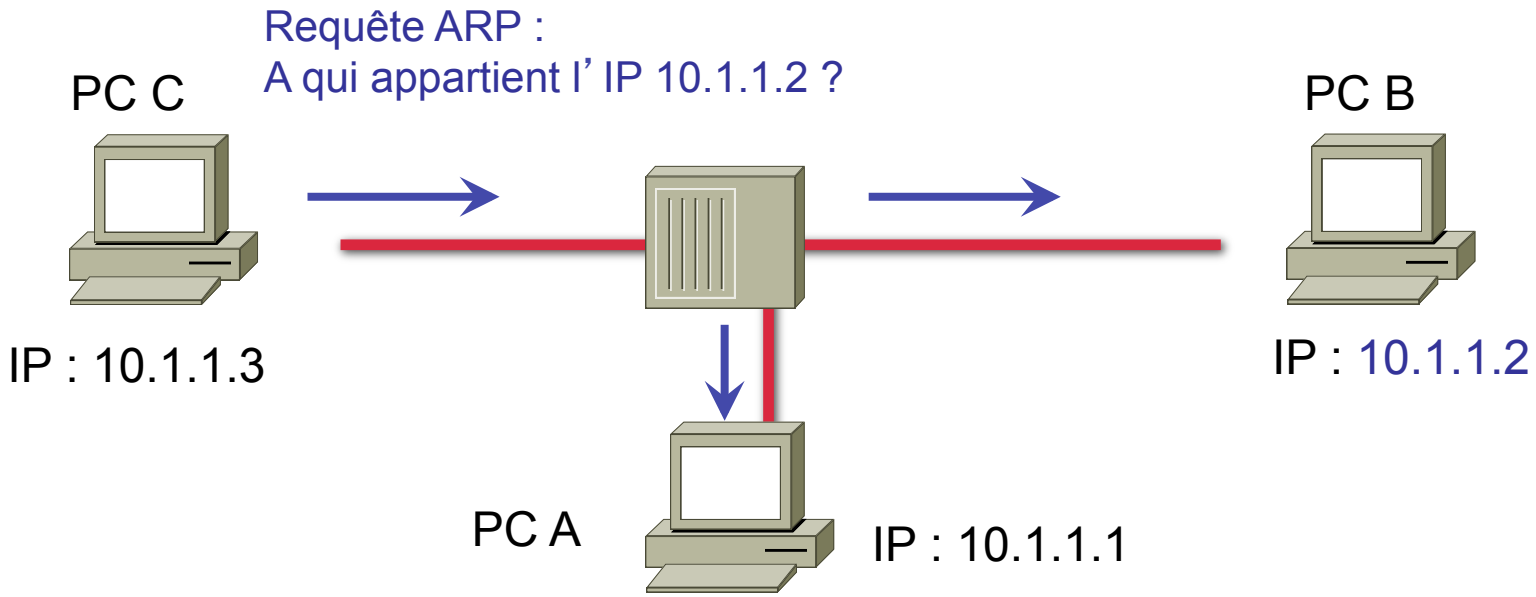
Adresse IP				Masque	Adresse réseau	Adresse broadcast
10	5	8	3	/8	10.0.0.0	10.255.255.255
50	50	50	50	/8	50.0.0.0	50.255.255.255
111	111	111	111	/16	111.111.0.0	111.111.255.255
172	16	0	3	/16	172.16.0.0	172.16.255.255
192	168	168	8	/24	192.168.168.0	192.168.168.255
200	200	200	200	/24	200.200.200.0	200.200.200.255

Address Resolution Protocol

Adresse physique et adresse logique

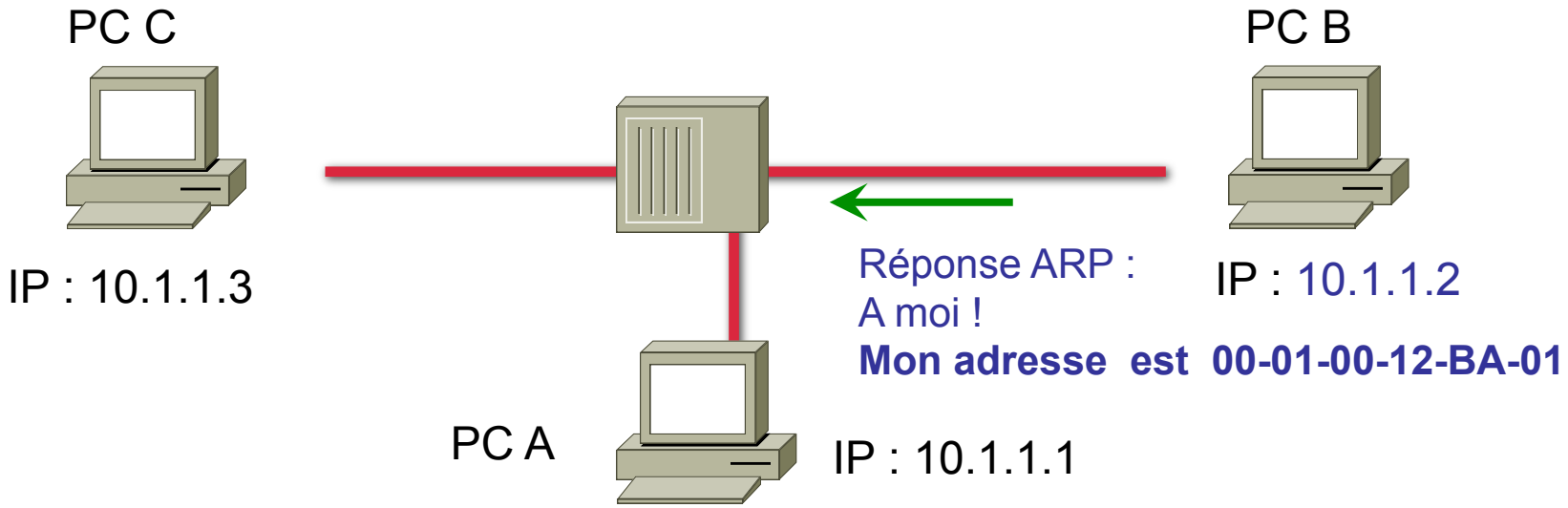
- Chaque noeud du réseau a deux adresses :
  - Une adresse physique appelée adresse MAC
  - Une adresse logique appelée adresse IP
- L'adresse MAC est gravée dans la carte réseau. Si l'on change cette carte, l'adresse MAC change
- L' adresse IP est configurée par l' administrateur et ne dépends pas du matériel, c' est une adresse logique
- ARP permet de trouver l'adresse MAC d'un équipement dont on connaît déjà l'adresse IP

Requête ARP



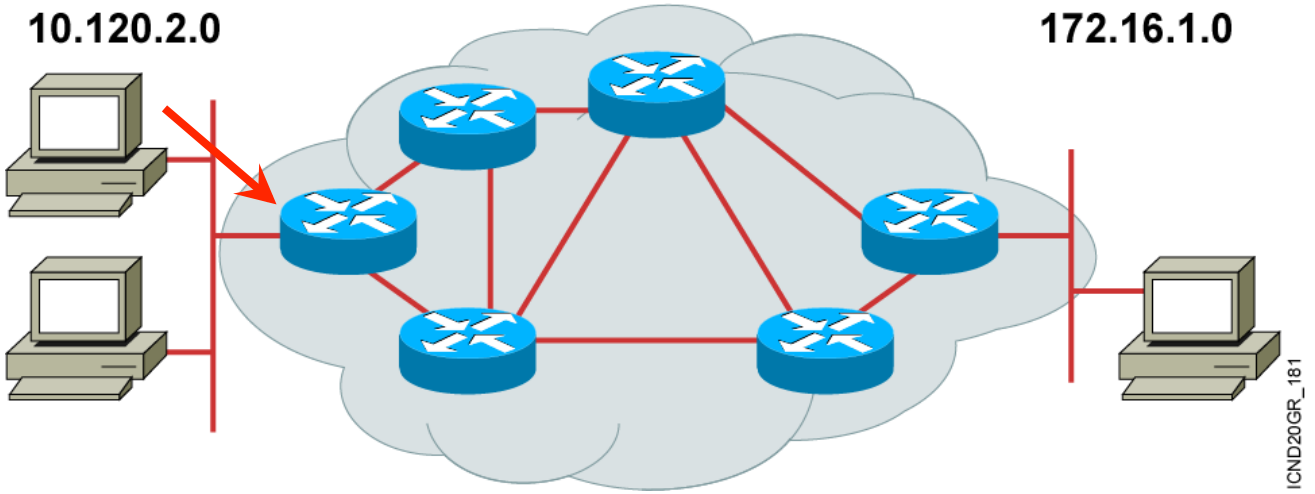
- Une requête ARP est un **broadcast** et tous les PCs du LAN le reçoivent

Réponse ARP



- Mais **seul** le PC B qui se reconnaît répond en unicast en envoyant son adresse MAC

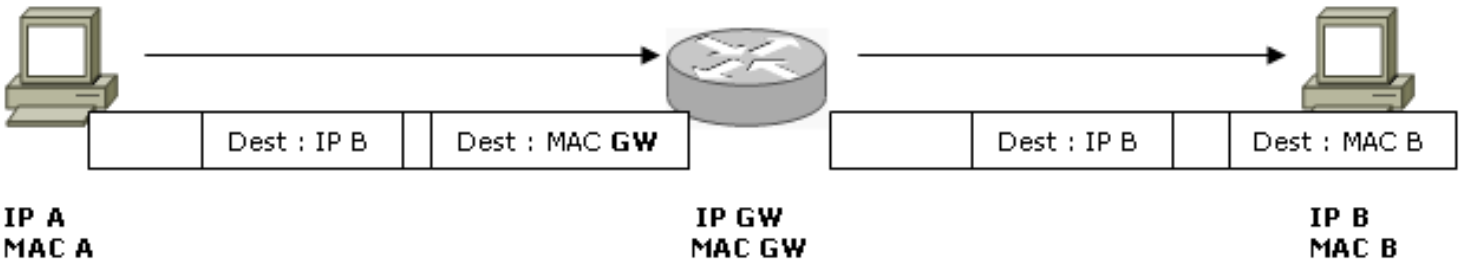
La requête ARP ne sort pas du LAN



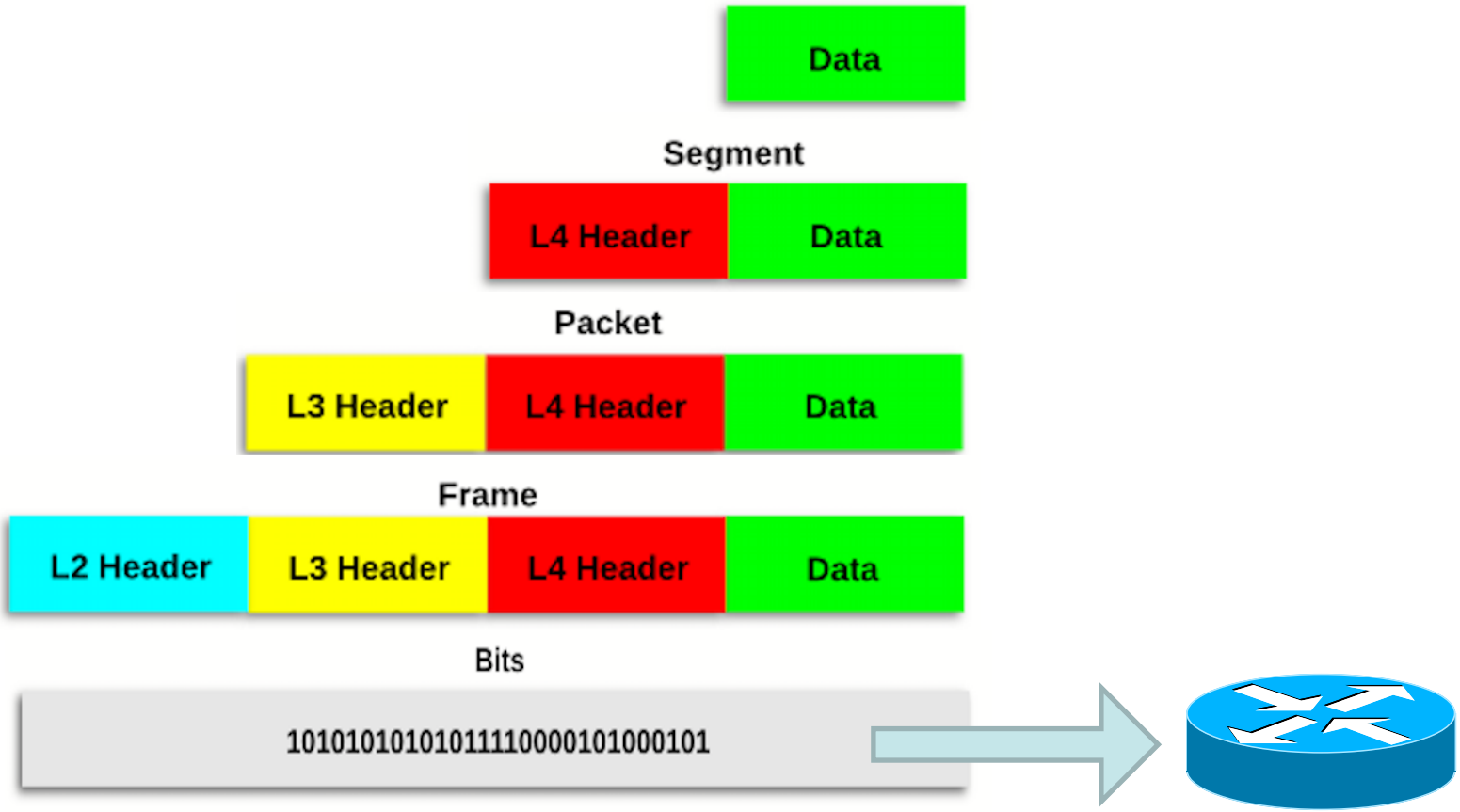
- Par défaut, les routeurs filtrent les broadcasts
- Si la destination nécessite de traverser des routeurs, ARP est inopérant

Rappel !

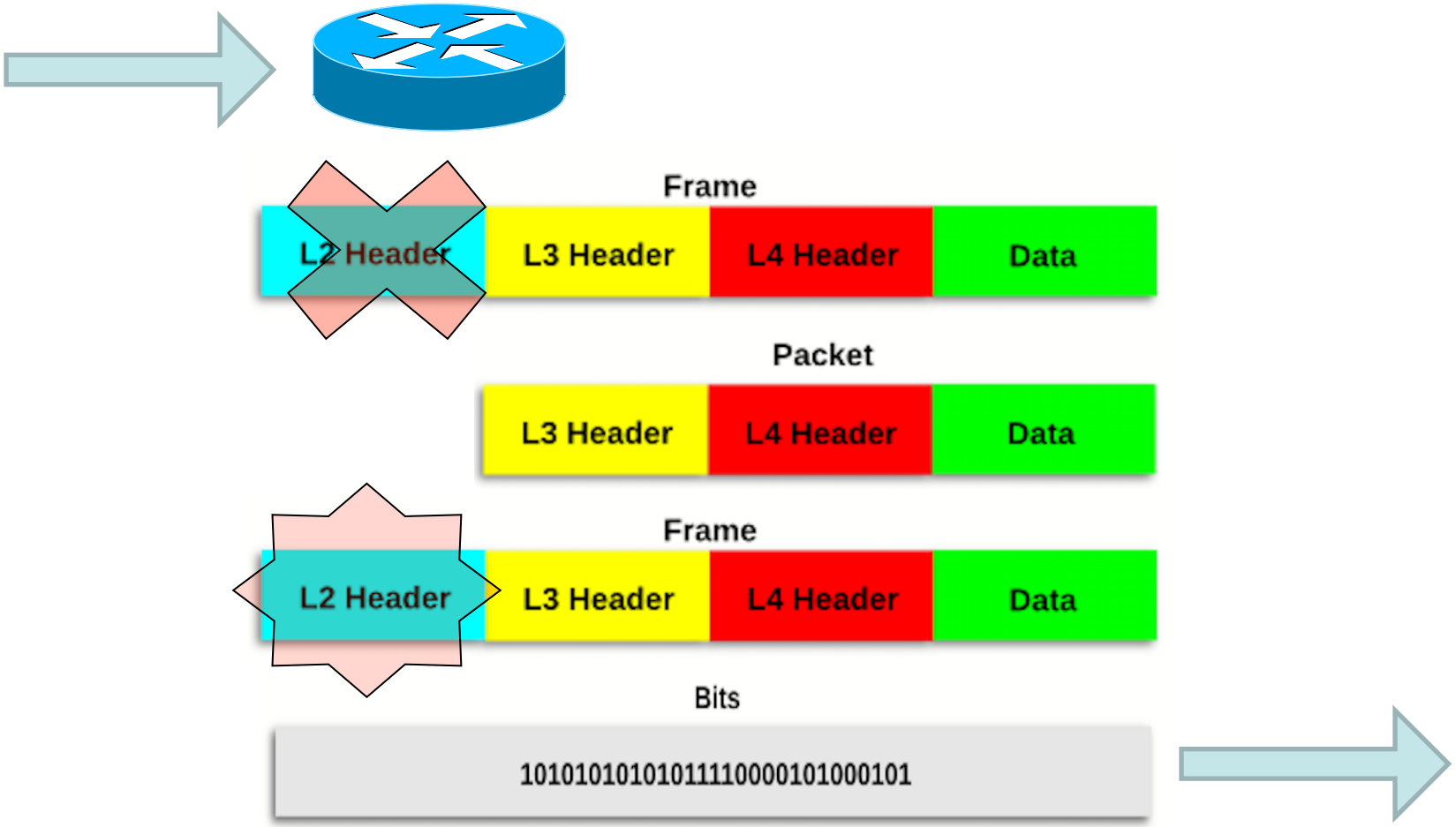
- Si deux PC ne sont pas sur le même réseau, ils sont séparés par un routeur.
  - Ce routeur est la passerelle de chaque PC
- Les entêtes IP ne sont **pas modifiées** par le routeur
- Les entêtes Ethernet sont **reconstruites** par le routeur



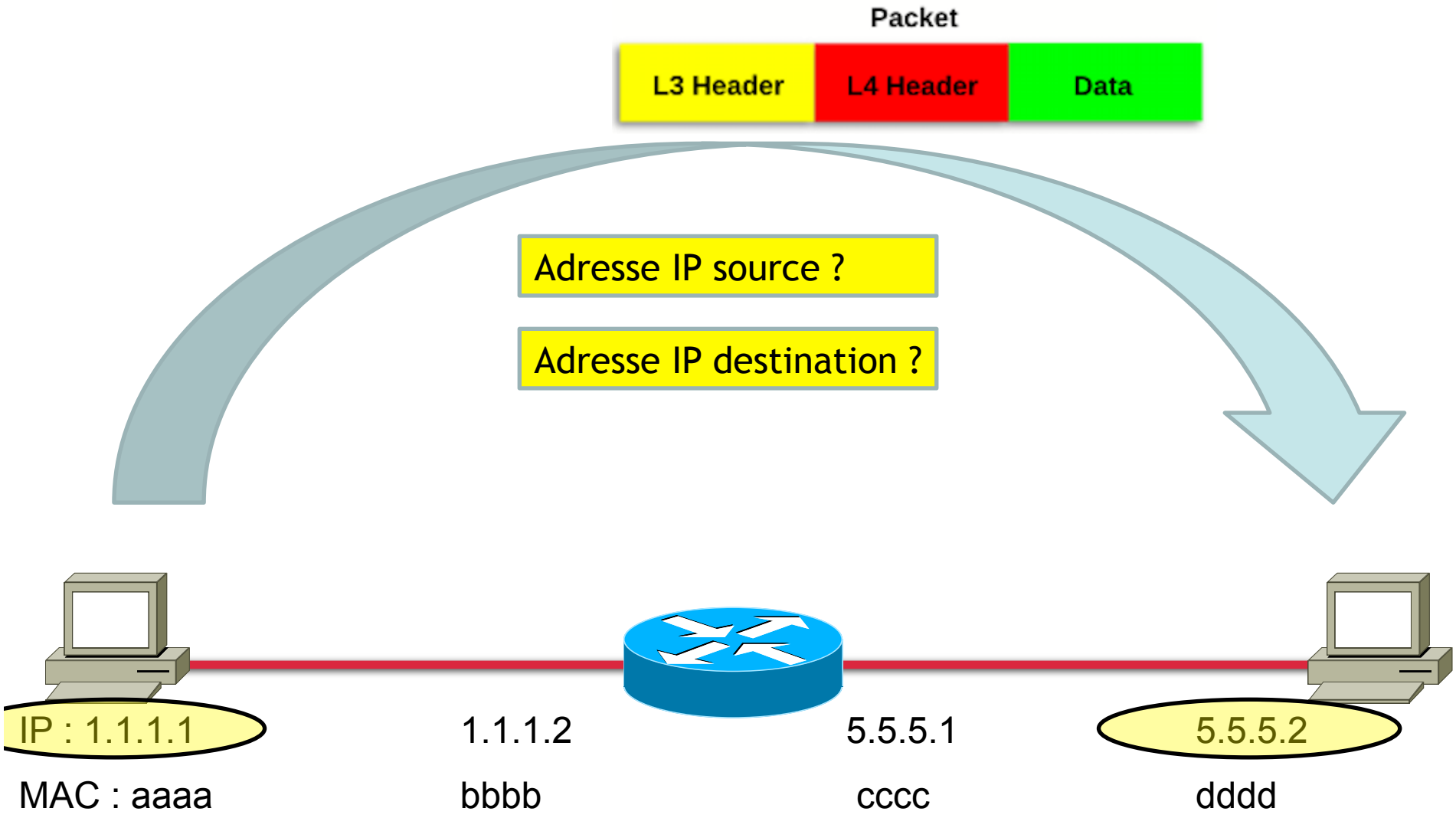
Rappel !


Data
Segment
L4 Header
Data
Packet
L3 Header
L4 Header
Data
Frame
L2 Header
L3 Header
L4 Header
Data
Bits
10101010101011110000101000101

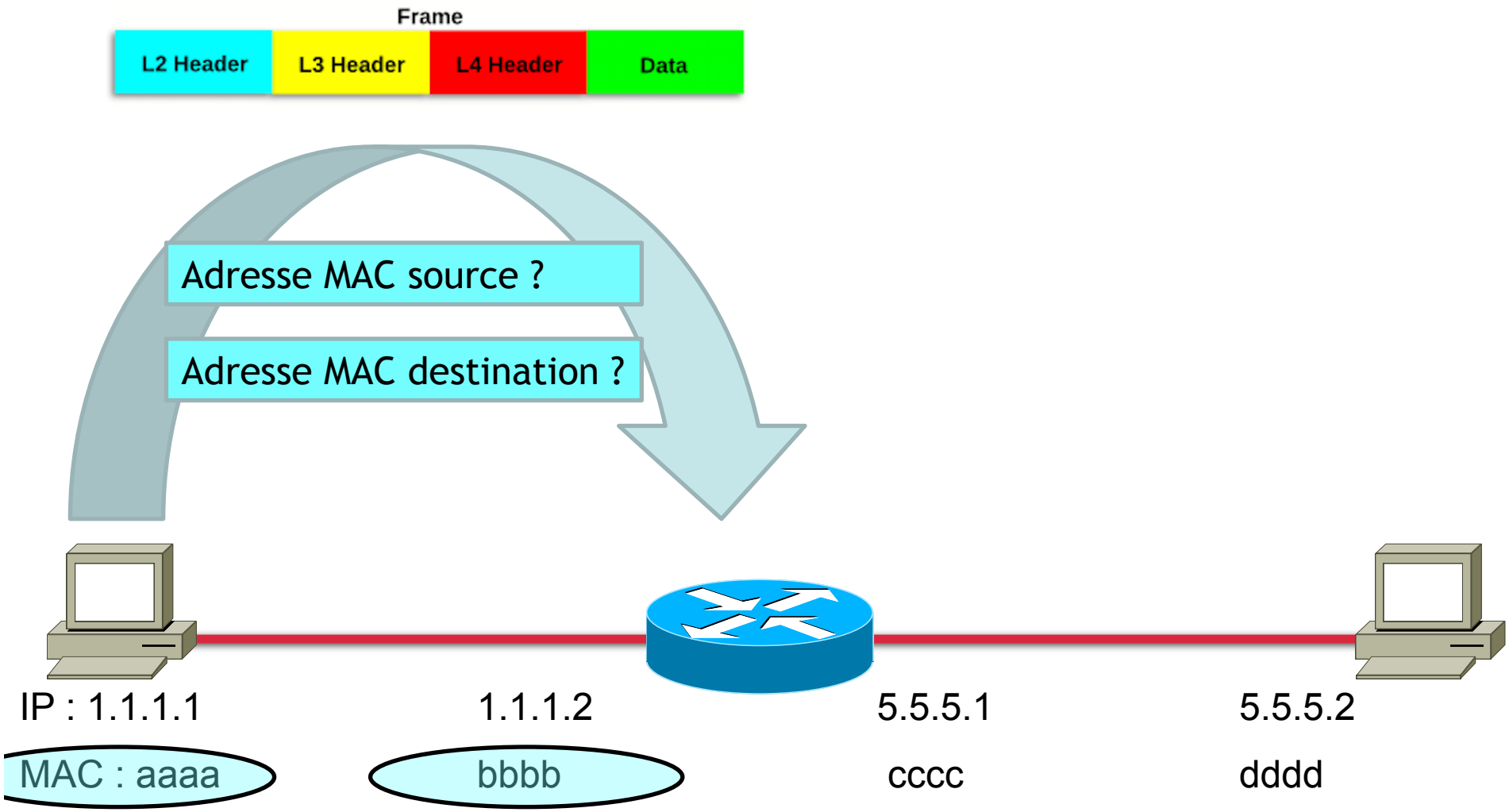
Rappel !


Frame
L2 Header
L3 Header
L4 Header
Data
Packet
L3 Header
L4 Header
Data
Frame
L2 Header
L3 Header
L4 Header
Data
Bits
10101010101011110000101000101

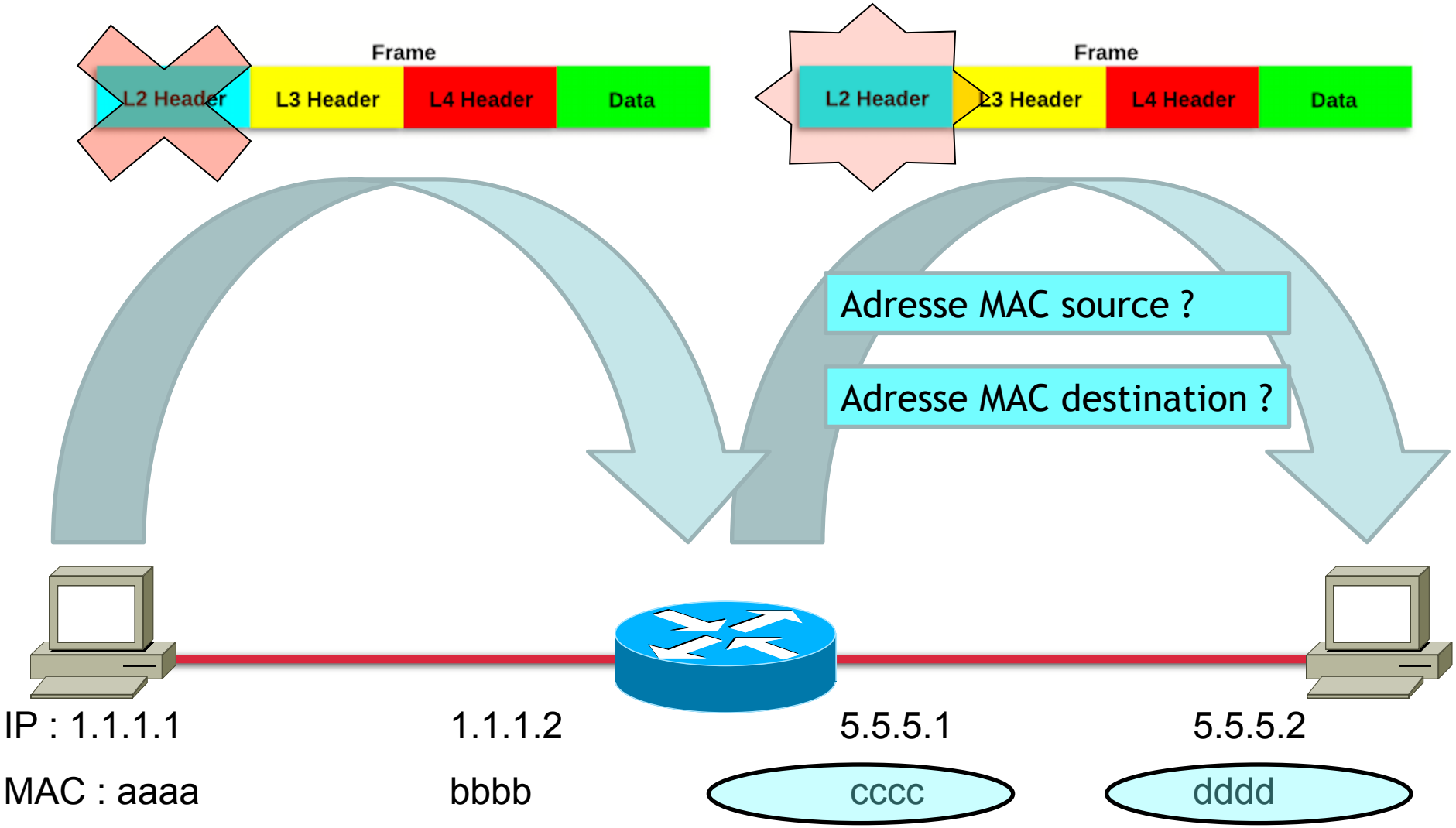
Envoi d'un paquet à travers un routeur



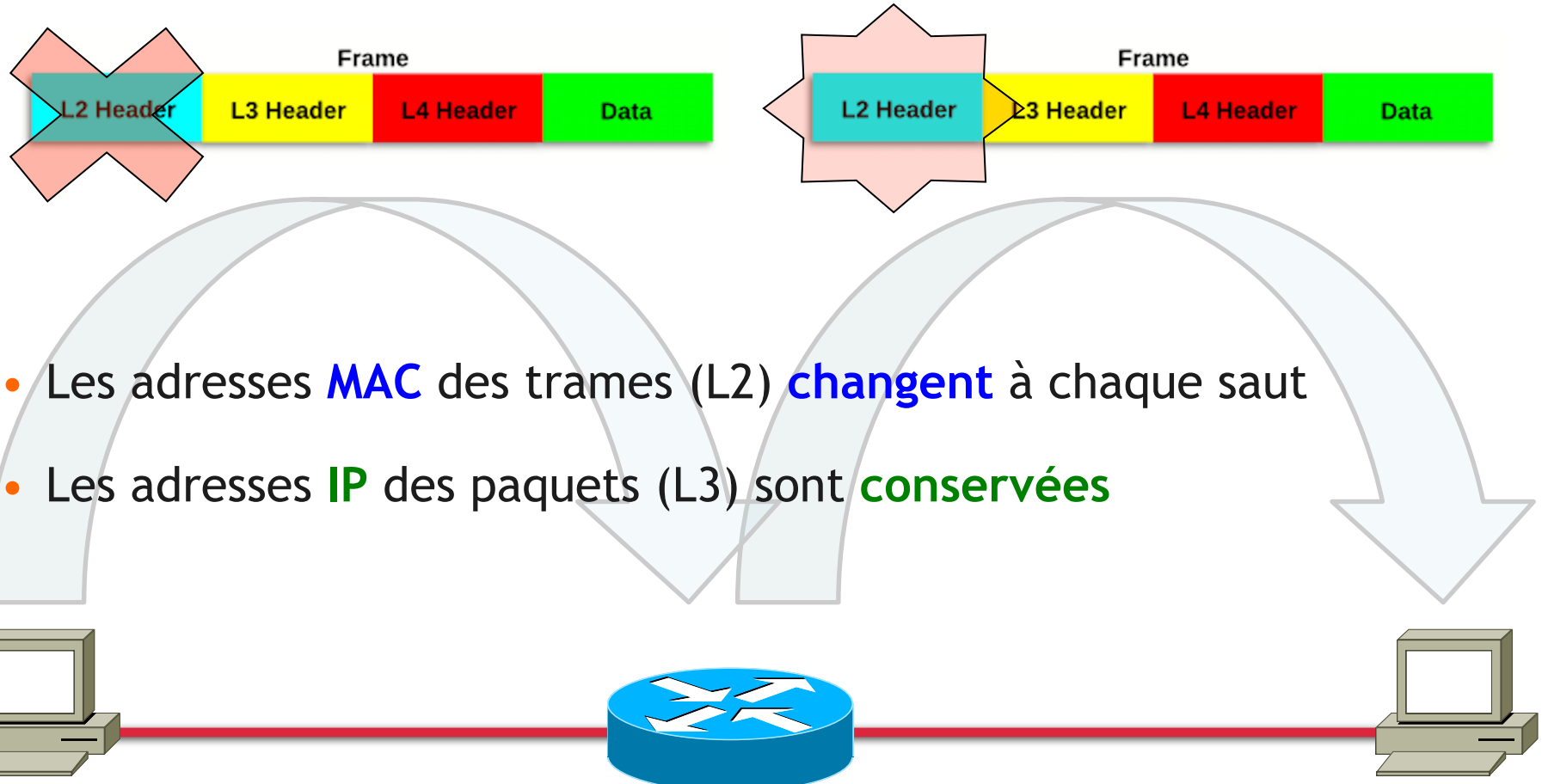
Envoi d'un paquet à travers un routeur



Envoi d'un paquet à travers un routeur



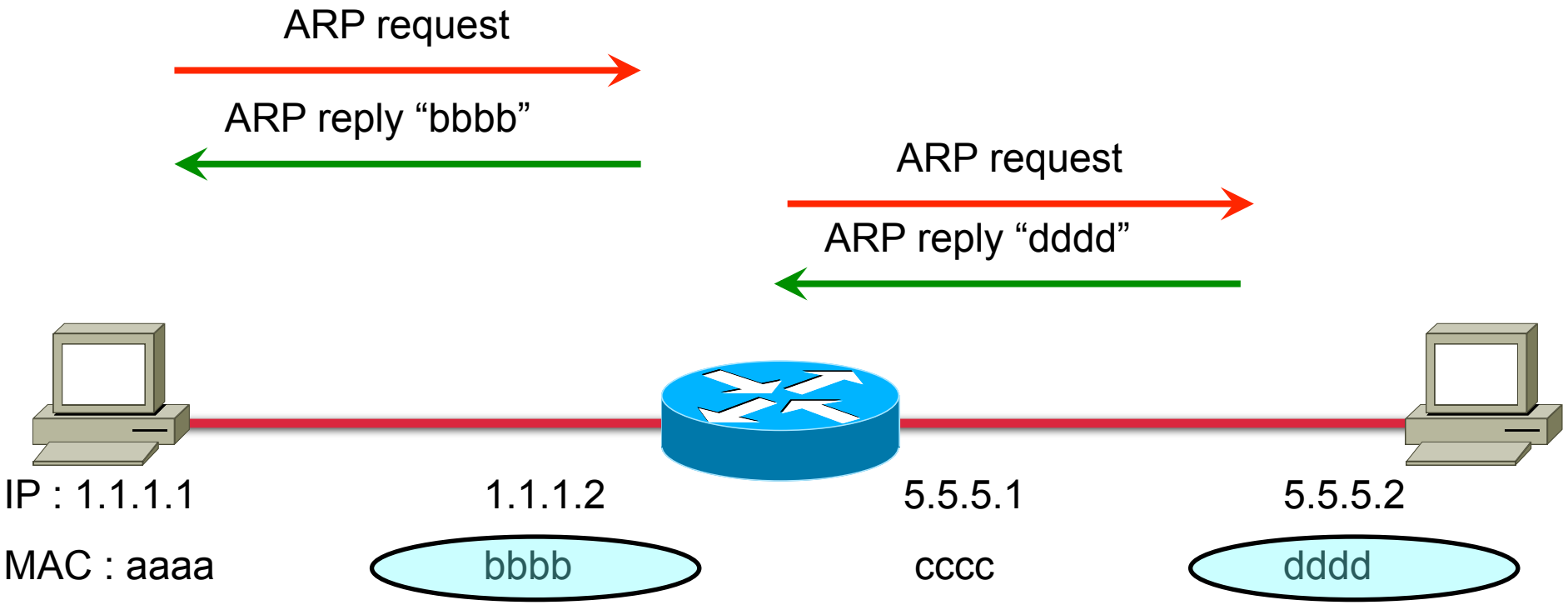
Envoi d'un paquet à travers un routeur



- Les adresses **MAC** des trames (L2) **changent** à chaque saut
- Les adresses **IP** des paquets (L3) sont **conservées**

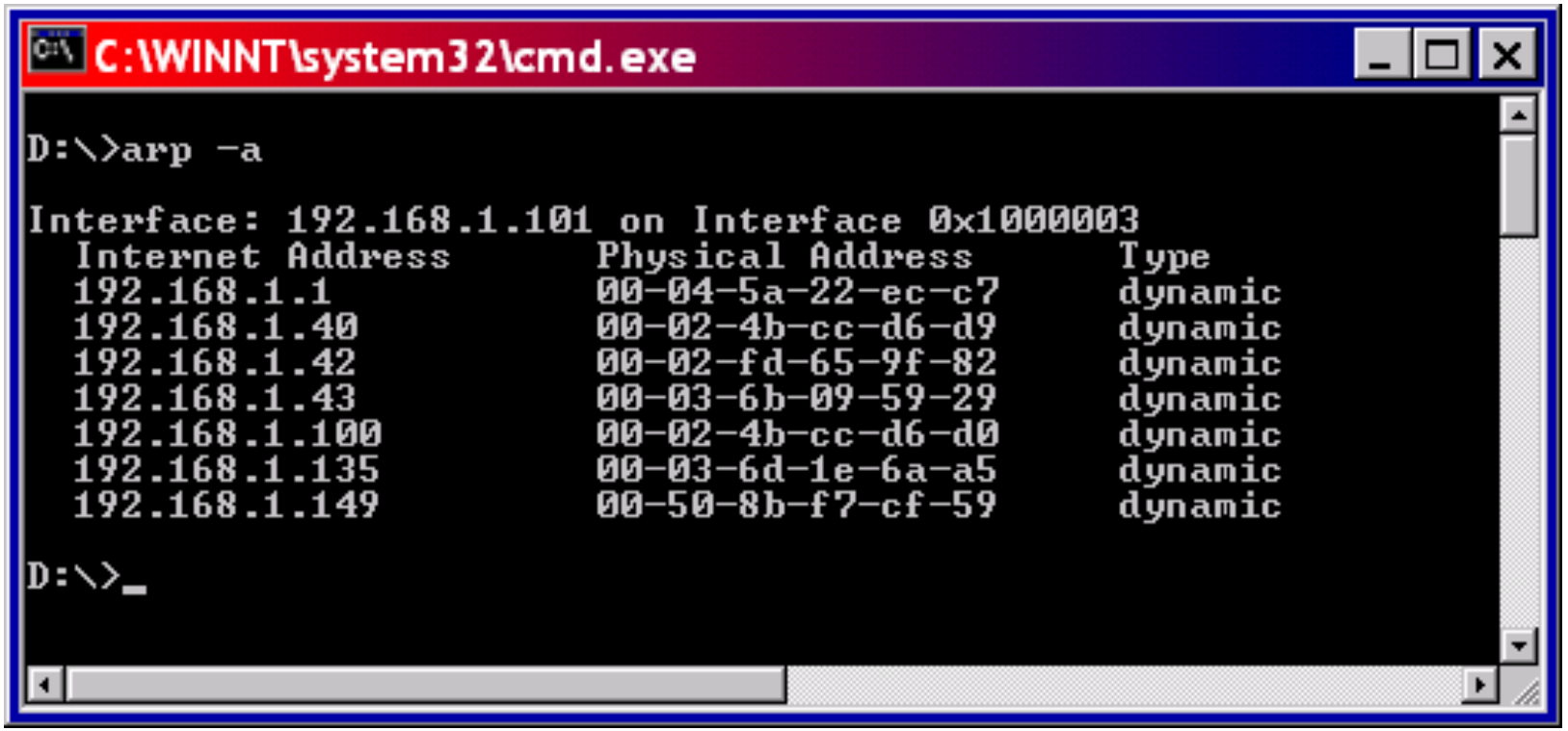
Deux requêtes ARP sont nécessaires

- La première requête ARP obtient l'adresse MAC de la passerelle
- La seconde requête ARP obtient l'adresse MAC du destinataire final.



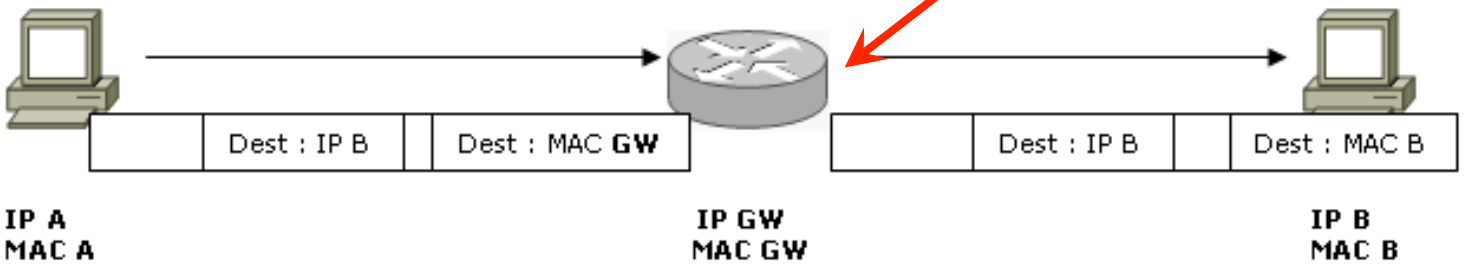
Cache ARP sur un PC

- Un cache ARP permet de se souvenir des correspondances entre IP et MAC



Cache ARP sur un routeur

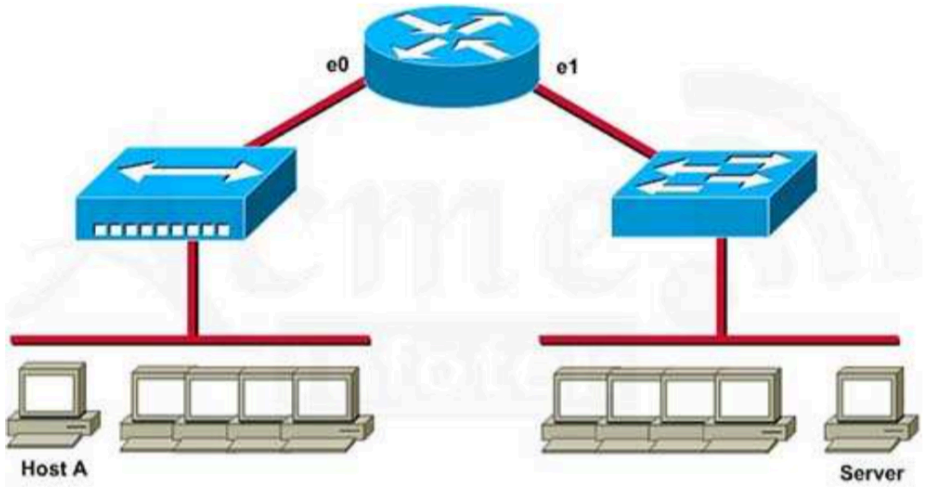
Protocol	Address	Age(min)	Hardware Adddr	Type	Interface
Internet	192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
Internet	192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
Internet	192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
Internet	192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
Internet	192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
Internet	192.168.40.1	-	0000.0c36.696f	ARPA	FastEthernet0/2



Test

- Quelle est l'@ MAC SOURCE des paquets envoyés par le serveur au hôte A lorsqu'il arrive à l'hôte A ?

A. the MAC address of the server network interface
B. the MAC address of host A
C. the MAC address of router interface e1
D. the MAC address of router interface e0



Test

- Que fait le routeur lorsqu' il reçoit cette trame ?

Router1# **show ip arp**

Protocol	Address	Age(min)	Hardware Adddr	Type	Interface
Internet	192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
Internet	192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
Internet	192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
Internet	192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
Internet	192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
Internet	192.168.40.1	-	0000.0c36.6965	ARPA	FastEthernet0/2

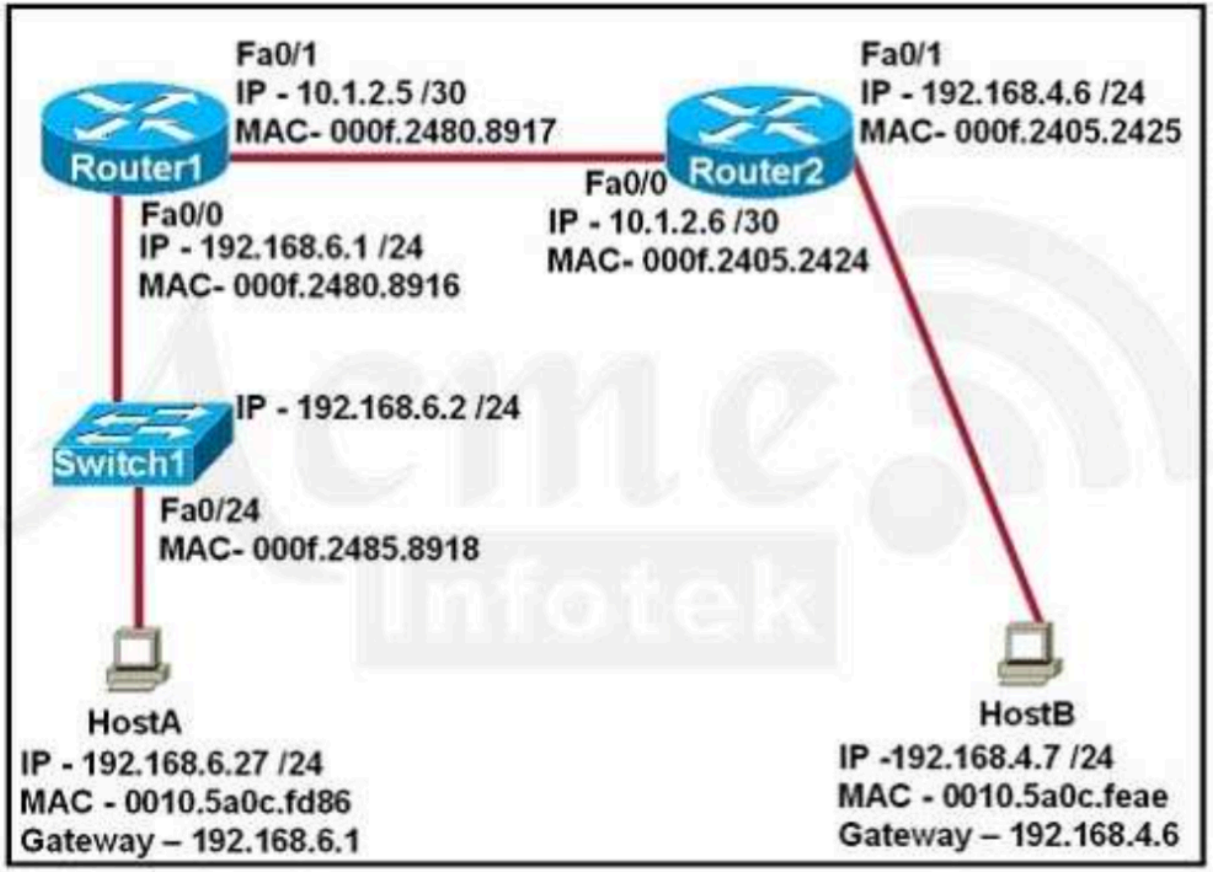
Data Frame:

Source MAC	Source IP	Destination MAC	Destination IP
0000.0c07.f892	192.168.20.5	0000.0c63.ae45	192.168.40.5

- Remplace l' @ MAC source par 0000.0C36.6965
- Remplace l' @ MAC dest par 0000.0c07.4320
- Envoie la trame sur son interface fa0/2

Test

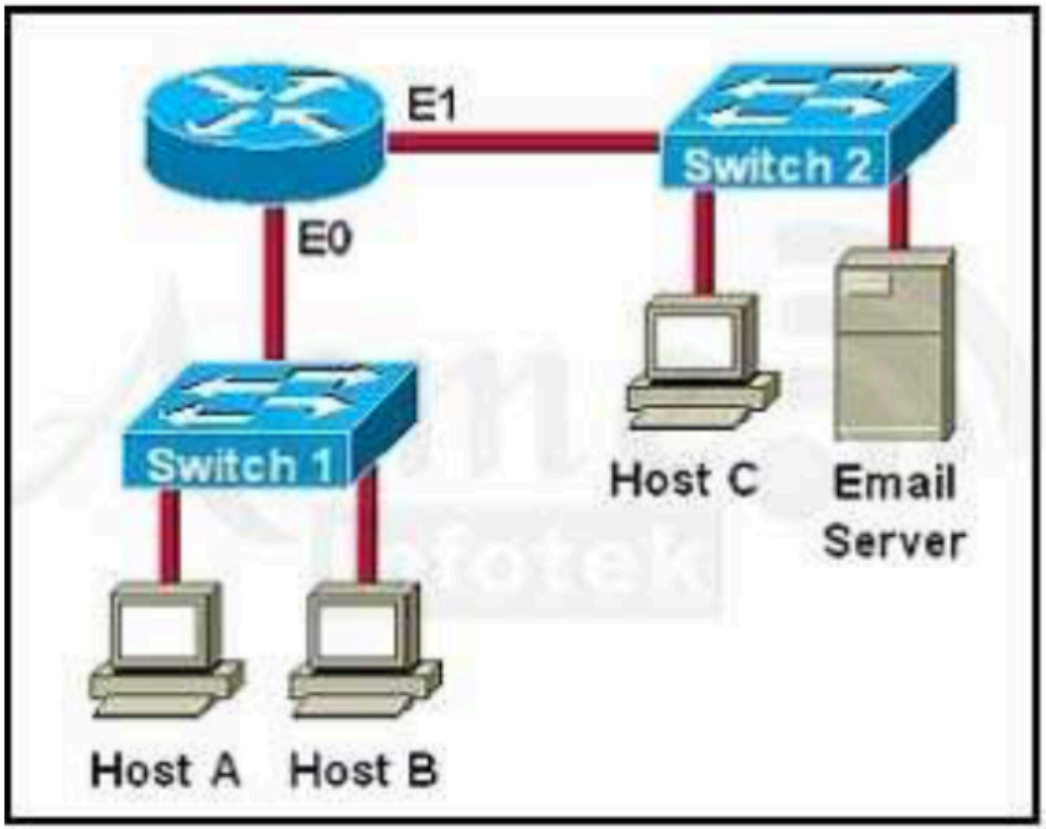
Après que A ait pingé B, quelle entrée est présente dans le cache ARP du host A ?



Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

Test

- Quelles @ destination (IP et MAC) utilisera A pour pinger B ?



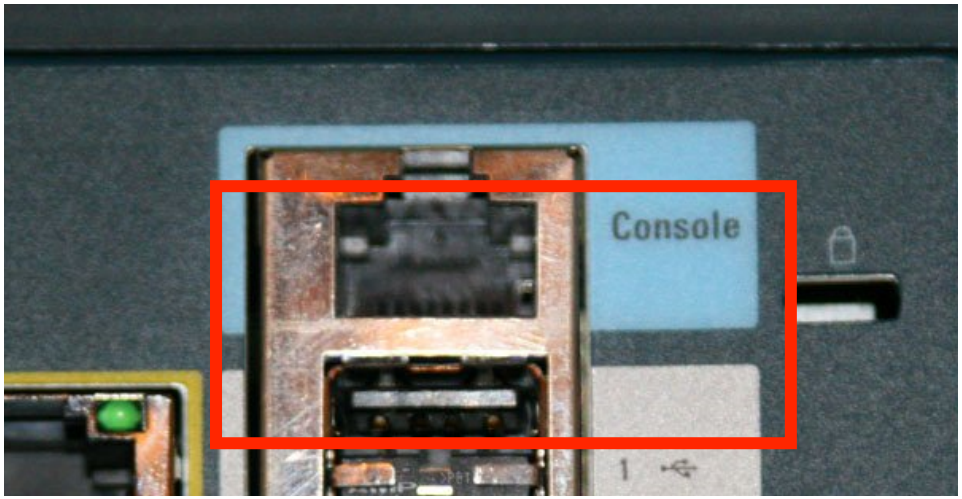
Cisco IOS

Se connecter à l’équipement

Connexion physique du port CONSOLE

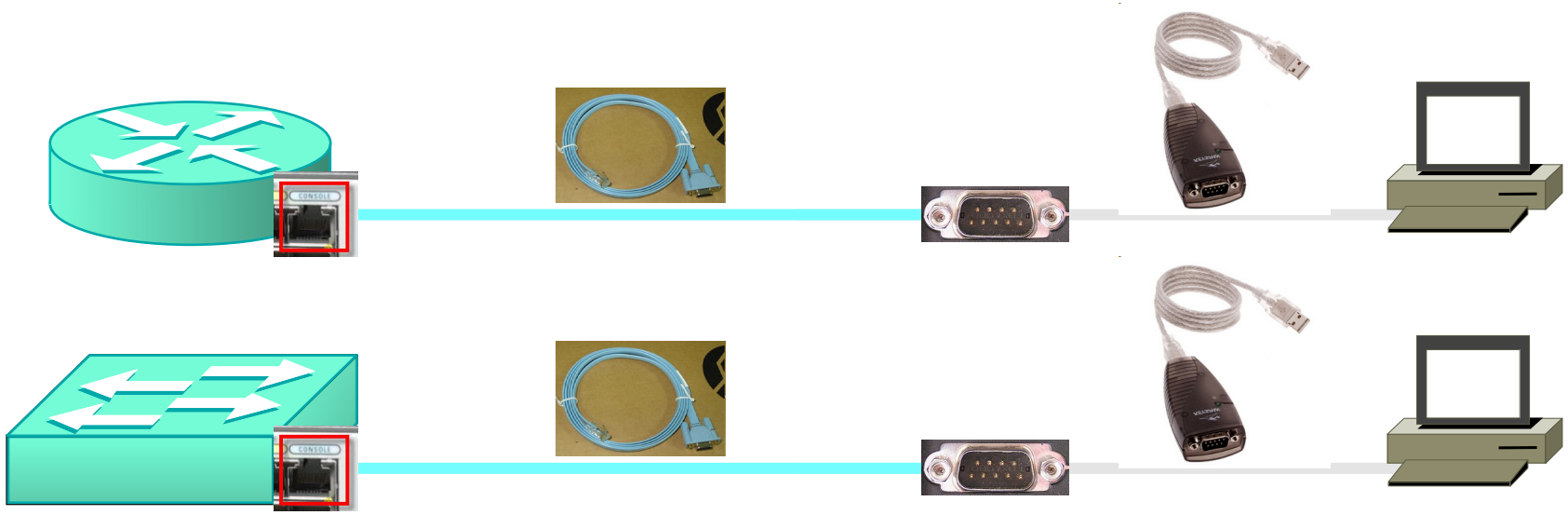
Le port CONSOLE

- C’ est un port RJ45.
- Tous les équipements CISCO ont un port CONSOLE… et toujours un seul port console.



Connexion par port COM ou port USB

- Certains PC n'ont pas de port COM.
  - Utiliser une adaptateur USB :



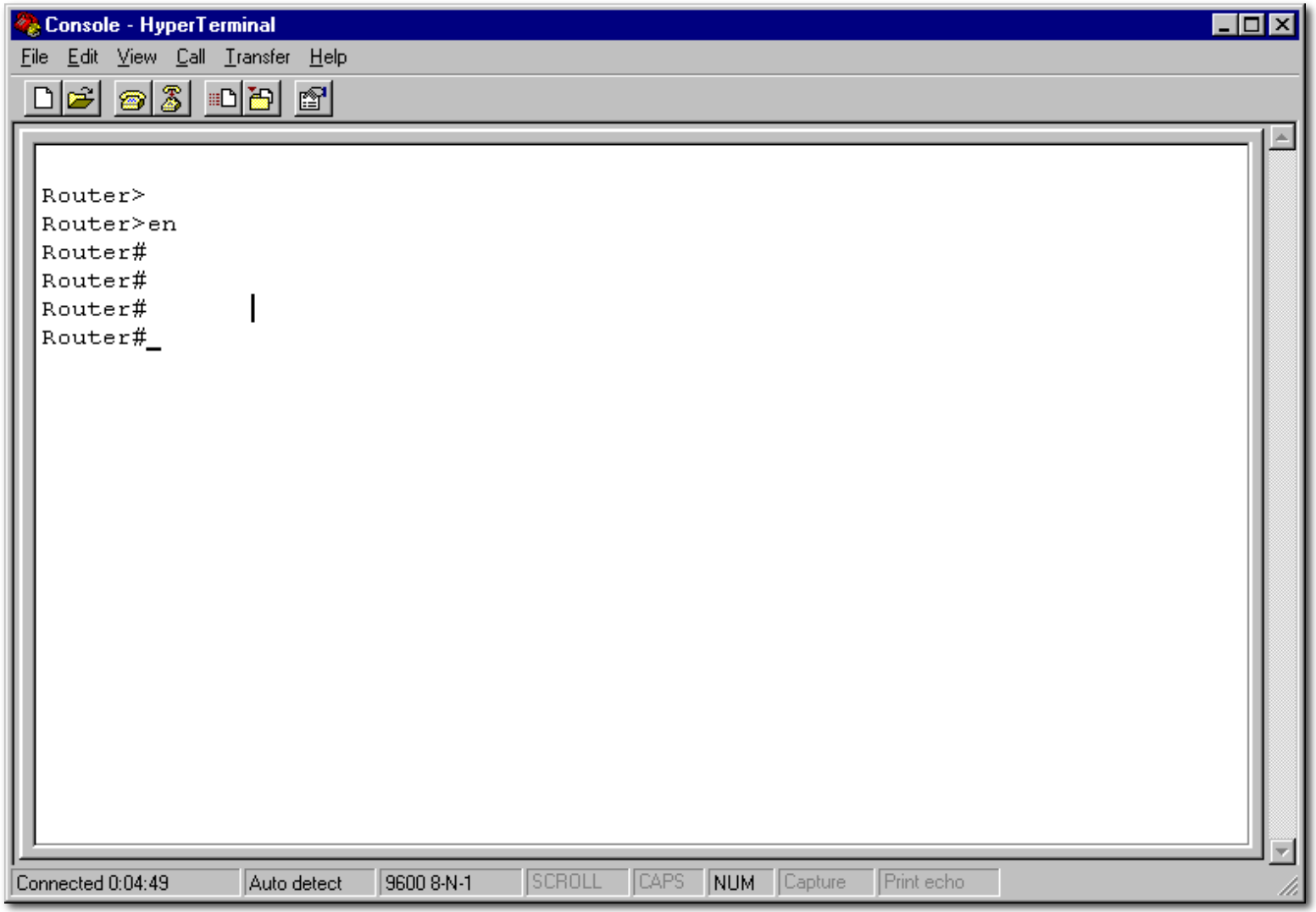
Se connecter à l’équipement

Connexion logicielle

Le Logiciel

- On peut utiliser HyperTerminal
  - à activer sur les OS Windows
- On peut aussi prendre :
  - Putty
  - TeratermPro
  - CRT
  - ...

Interface de connexion



DEUX modes

- Le mode USER :
  - Le ‘prompt’ est « > »
  - Seulement certaines commandes sont disponibles
- Le mode PRIVILEGIE :
  - Le ‘prompt’ est « # »
  - Toutes les commandes sont disponibles

Basculer entre les 2 modes

- Utiliser les commandes `enable` et `disable` :
  - `Router>enable`
  - `Router#`
  - `Router#`
  - `Router#disable`
  - `Router>`
- Par défaut, il n'y a pas de mot de passe pour basculer en mode privilégié.

Passage reservé

- Par défaut en mode console, pas de mot de passe pour passer en mode privilégié :
  - tout individu qui a accès à l'équipement peut modifier sa configuration
- Avec un mot de passe :
  - seuls les personnes ayant ce mot de passe peuvent passer en mode privilégié
  - trois tentatives, proposées en boucle :
    - `TATA>enable`
    - `Password:`
    - `Password:`
    - `Password:`
    - `% Bad secrets`

Le mot de passe PRIVILEGIE

- Deux manières de le configurer :
  - ancienne commande :
    - `TATA#conf t`
    - `TATA(config)#enable password Z3R4`
  - nouvelle commande :
    - `TATA#conf t`
    - `TATA(config)#enable secret R4Z3`
    - est systématiquement crypté
    - cryptage plus robuste
- Si les 2 commandes sont saisies, seule le mot de passe de la nouvelle commande sera demandé.

Activer le cryptage

- Un service permet d'activer le cryptage des mots de passe :

```
TATA#conf t

TATA(config)#service password-encryption
```

- Ce service est rétro actif :
  - les mots de passe déjà configurés seront cryptés, ainsi que tout nouveau mot de passe

Contextes du mode privilégié

- Le mode privilégié contient plusieurs contextes :
  - le contexte de gestion
  - le contexte de configuration globale
  - les contextes de configuration spécifique
    - spécifique à une interface
    - spécifique à une ligne
    - spécifique à un protocole de routage
    - etc..

Contextes

- Le mode privilégié contient plusieurs contextes :
  - le contexte de gestion
  - `Router#`
  - le contexte de configuration globale
  - `Router(config)#`
  - les contextes de configuration spécifique
  - `Router(config-if)#`
  - `Router(config-router)#`

Le contexte de gestion

- Il permet d'interroger le routeur ou le switch pour lui demander d'afficher les paramètres configurés :
  - quelle adresse IP as-tu sur telle interface ?
  - quels sont les équipements voisins que tu as détectés ?
  - etc…
- Il permet d'effectuer les commandes de sauvegarde de la configuration :
  - copier la configuration dans la mémoire
- Il permet de lancer des commandes ICMP, Telnet, Traceroute :
  - pinger un autre équipement du réseau
  - découvrir le chemin emprunté par le traffic entre 2 points

Le contexte de gestion

- Il est identifiable par :
  - **Hostname#**
- Les commandes de consultation par ‘show’ :
  - show ip interface brief (routeur)
  - show interface status (switch)
  - show running-configuration
- Les commandes d’administration de l’équipement et du réseau :
  - copy running-config startup-config
  - ping
  - traceroute

Improve User Experience in CLI (Cont.)

Step 13: Use **begin** and **include** options with **show running-config** command.

```
R1# show running-config | begin interface
```

```
R1# show running-config | include interface
```

Step 14: Use **section** option with **show running-config** command.

```
R1# show running-config | section interface
```

Step 15: Use **exclude** option with **show running-config** command.

```
R1# show running-config | exclude !
```

Contexte de configuration globale

- Il permet de configurer un paramètre global du routeur ou du switch :
  - son hostname
  - le mot de passe du mode privilégié
  - etc..
- Il permet aussi de basculer dans un mode de configuration spécifique

Contexte de configuration globale

- Il est identifié par :
  - `Hostname(config)#`
- Pour rentrer dans le contexte de configuration globale :
  - taper la commande '`configure terminal`'
- Pour quitter le contexte de configuration globale :
  - taper la commande '`exit`'
  - ou la combinaison de touches [C*trl*] + '`Z`' (équivalent de la commande end)

Nécessité des contextes

- Chaque commande ne fonctionne que dans son contexte :
  - Une commande de configuration ne fonctionne pas dans le contexte de gestion.
- Et inversement :
  - Une commande de gestion ne fonctionne pas dans le contexte de configuration.
    - On peut toutefois forcer la commande de consultation avec le prefix ‘do’.

Refus d'une commande de configuration

```
Router>hostname TOTO
        ^
% Invalid input detected at '^' marker.
Router>enable
Router#
Router#hostname TOTO
        ^
% Invalid input detected at '^' marker.
Router#configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
Router(config)#hostname TOTO
TOTO(config)#
```

Refus d'une commande 'show'

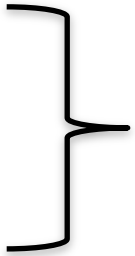
```
TOTO#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down

TOTO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TOTO(config)#show ip interface brief
                   ^
% Invalid input detected at '^' marker.
TOTO(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
```

Les contextes de configuration spécifique

- Il permet de configurer un paramètre spécifique du routeur ou du switch :
  - l'adresse IP d'une interface
  - le mot de passe de la ligne console
  - le mot de passe d'un protocole de routage
- Il sont identifiés par :
  - Hostname(config-X)#
- Pour rentrer dans le contexte de configuration spécifique :
  - il faut d'abord passer en contexte de configuration globale
  - puis taper la commande du contexte spécifique

Les contextes du mode PRIVILEGIE

```
Router#
Router#configure terminal
Router(config)#
Router(config)#interface FastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```



end ou Ctrl-Z

Exemples

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Contexte de gestion

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Contexte de configuration globale

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Contexte de configuration spécifique à une interface

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Contexte de configuration spécifique à une ligne

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-std-nacl)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Contexte de configuration spécifique à un protocole de routage

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Quitter un contexte de configuration spécifique

```
TOTO#
TOTO#configure terminal
TOTO(config)#
TOTO(config)#interface fastEthernet 0/0
TOTO(config-if)#no shutdown
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
TOTO(config-if)#exit
TOTO(config)#
TOTO(config)#line console 0
TOTO(config-line)#password Z3Y6
TOTO(config-line)#exit
TOTO(config)#
TOTO(config)#router ospf 1
TOTO(config-router)#area 0 authentication
TOTO(config-router)#exit
TOTO(config)#
TOTO(config)#exit
TOTO#
```

Quitter à la fois un contexte de configuration spécifique et le contexte de configuration globale

Utiliser la combinaison de touche [*Ctrl*] + 'Z' :

```
TOTO>

TOTO>enable

TOTO#

TOTO#configure terminal

TOTO(config)#

TOTO(config)#interface fastEthernet 0/0

TOTO(config-if)#no shutdown

TOTO(config-if)#^Z

TOTO#
```

Les sauvegardes

DEUX configurations

- Les switch et les routeurs ont deux types de configurations :
  - la running-configuration RAM
  - la startup-configuration NVRAM
- Les switch et les routeurs ont deux types de mémoire :
  - RAM volatile est effacée (*)
  - NVRAM non-volatile est conservée (*)

(*) suite à une coupure de courant

Sauvegarde

- **TOTO#copy running-config startup-config**
- Destination filename **[startup-config]?** taper sur la touche ‘Entrée’
- **TOTO#wr**
- **TOTO#write memory**
- **TOTO#dir nvram:**

```
Directory of nvram:/

  124  -rw-           445      <no date>  startup-config
  125  ----            24      <no date>  private-config
    1  -rw-             0      <no date>  ifIndex-table

129016 bytes total (127471 bytes free)
```

Modification de la running-config

- On ne peut pas modifier la startup-configuration.
  - on ne peut que copier la ‘run’ dans la ‘start’

- A chaque fois qu’on saisit une commande, elle ira modifier la running-config.
  - on modifie donc la config dans la RAM.

Au démarrage

- Le switch ou le routeur ira chercher la startup-config dans la NVRAM :
  - si elle est présente, il charge cette statup-config dans la running-config
  - si elle n'est pas présente (*), il vous propose un dialogue de configuration

(*) cas d'un équipement neuf ou d'un équipement dont le registre de configuration a été modifié

Le dialogue de configuration

Lorsqu'il n'y a pas de fichier de démarrage

```
         --- System Configuration Dialog ---

Would you like to enter the initial
configuration dialog? [yes/no]: no
```

Les aides de la CLI

Utiliser la touche ‘?’

‘?’

- Pour obtenir toutes les commandes qui commencent par certaines lettres.
- Exemples :
  - `TOTO(config)#h?`
  - `help  hostname  http`
    - Dans le contexte de configuration globale, il existe trois commandes qui commencent par ‘h’.
  - `TOTO(config)#ho?`
  - `hostname`
    - Dans le contexte de configuration globale, il n’existe qu’une seule commande qui commence par ‘ho’.

```
--More--
```

- Signifie que l'équipement a plusieurs pages à afficher.

- Trois possibilités :
  - appuyer sur 'Entrée' afficher 1 ligne supplémentaire
  - appuyer sur 'Barre d'espace' afficher 1 page supplémentaire
  - appuyer sur toute autre touche arrêter l'affichage

Les aides de la CLI

Utiliser la touche ‘tabulation’

Auto-complétion

- L'équipement complète automatiquement la fin de chaque mot-clef d'une commande s'il n'existe qu'une seule commande avec les lettres déjà saisies.
- Exemple :
  - `configure terminal`

    Cette commande peut être simplement saisie avec :
  - `conf t`

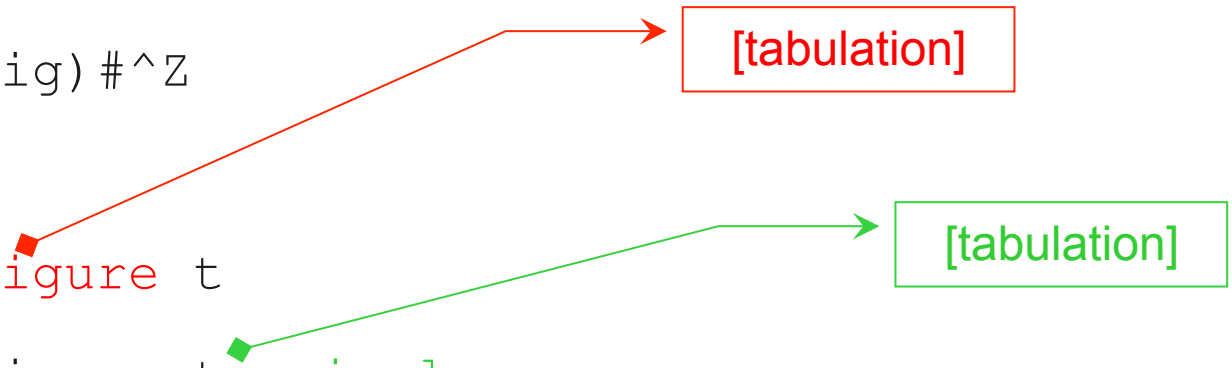
    car il n'existe pas d'autre commande qui commence avec ces mêmes lettres.

Trois possibilités

- Saisir toute la commande :
  - `configure terminal`
- Ne saisir que les lettres minimales :
  - `conf t`
- Saisir les lettres minimales + appuyer sur ‘tabulation’ après chaque mot-clef
  - `conf[tabulation] t[tabulation]`
    - s’ il n’ existe qu’ une seule commande qui commence par les lettres saisies, l’ équipement complète la commande
    - sinon il émet un ‘BIP’

Exemple 1

```
TOTO#configure terminal
TOTO(config)#^Z
TOTO#conf t
TOTO(config)#^Z
TOTO#conf
TOTO#configure t
TOTO#configure terminal
```



Exemple 2

- L'auto-completion permet d'éviter les erreur de frappe. Exemple :

```
TOTO#sh▶

TOTO#show ip in▶

TOTO#show ip interface br▶

TOTO#show ip interface brief
```

Les aides de la CLI

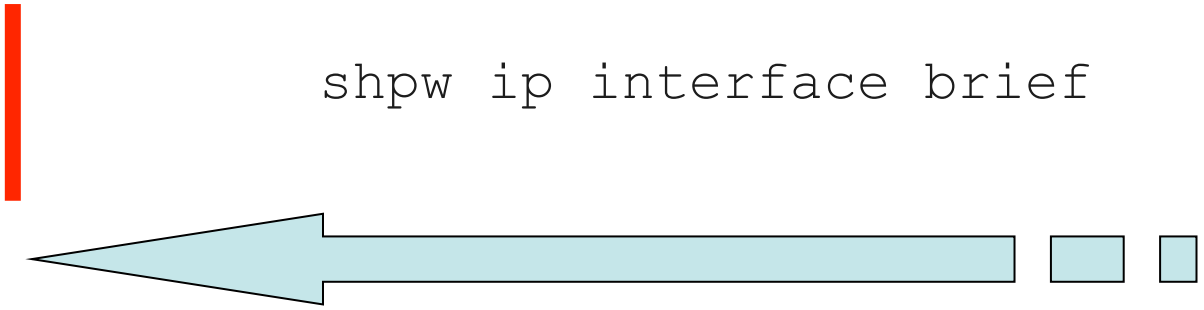
Positionner le curseur

Comment corriger une commande

```
shpw ip interface brief
```

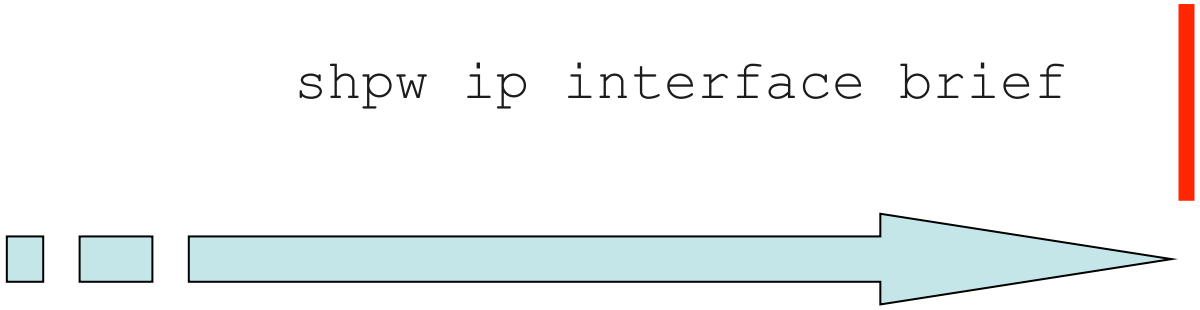
- 1ère méthode :
  - utiliser les flèches de déplacement
- 2ème méthode :
  - utiliser les touches de déplacement rapide

[*Ctrl*] + ‘a’



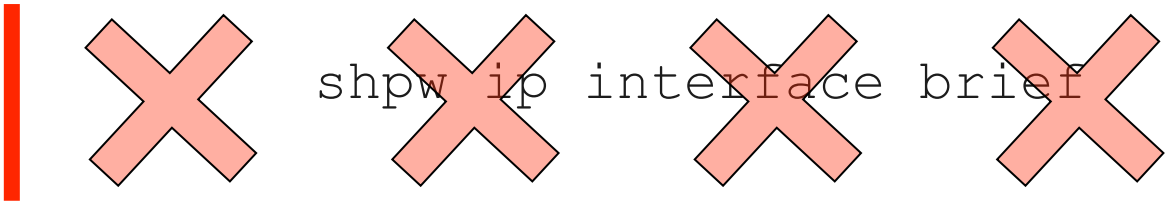
Positionne le curseur en début de ligne

[*Ctrl*] + ‘e’



Positionne le curseur en fin de ligne

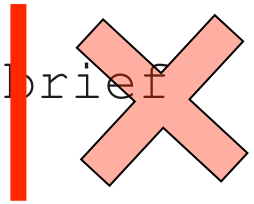
[*Ctrl*] + ‘x’



Efface toutes les lettres
entre le début de la ligne et le curseur.

[*Ctrl*] + ‘w’

```
shpw ip interface brief
```



Efface toutes les lettres
entre le mot courant et le curseur

Les aides de la CLI

Rappeler de commandes

Flèches ‘haut’ et ‘bas’

- Elles permettent de rappeler une commande saisie précédemment.
- Par défaut, l’ équipement mémorise les 10 dernières commandes.
  - `enable`
  - `configure terminal`
  - `history size 30`
    - taille entre 0 et 256
  - `history`
    - activer la mémorisation de commande (par défaut)
  - `no history`
    - désactiver cette mémorisation
  - `exit`
  - `show history`
    - afficher toutes les commandes déjà saisies

Configurations de base

Configurations globales

Hostname

- Par défaut :
  - ‘Router’ sur un routeur
  - ‘Switch’ sur un switch
- Il est modifié dès qu’il est configuré :
  - `TOTO>enable`
  - `TOTO#conf t`
  - `TOTO(config)#hostname TATA`
  - `TATA(config)#`

Les messages syslog

- Ces messages sont affichés à la console.
- Exemple :
  - une interface vient de tomber
  - un protocole de routage vient de découvrir un voisin
- Ces messages sont affichés même si l'administrateur est en train de saisir une commande :
  - « Interférences » entre les messages affichés et les commandes saisies par l'administrateur

Exemple d'interférence

J'active une interface, puis je configure son adresse IP :

```
TATA#conf t

TATA(config)#int fa0/0

TATA(config-if)#no shut

TATA(config-if)#ip add 10.0.0

*Mar  1 03:56:47.891: %LINK-3-UPDOWN: Interface
  FastEthernet0/0, changed state to up

*Mar  1 03:56:48.891: %LINEPROTO-5-UPDOWN: Line
  protocol on Interface FastEthernet0/0, changed state
  to up.1 255.255.255.0
```

Le message syslog a été affiché
au milieu de ma commande !

Eviter les « interférences »

- `TATA#conf t`
- `TATA(config)#line console 0`
- `TATA(config-line)#logging synchronous`

Penser à passer cette commande sur toute nouvelle configuration

sans interférence

Les commandes en cours sont répétées après les syslogs

```
TATA#conf t

TATA(config)#int fa0/0

TATA(config-if)#no shut

TATA(config-if)#ip add 10.0.0

*Mar  1 03:56:47.891: %LINK-3-UPDOWN: Interface
  FastEthernet0/0, changed state to up

*Mar  1 03:56:48.891: %LINEPROTO-5-UPDOWN: Line
  protocol on Interface FastEthernet0/0, changed state
  to up

TATA(config-if)#ip add 10.0.0.1 255.255.255.0

TATA(config-if)#
```

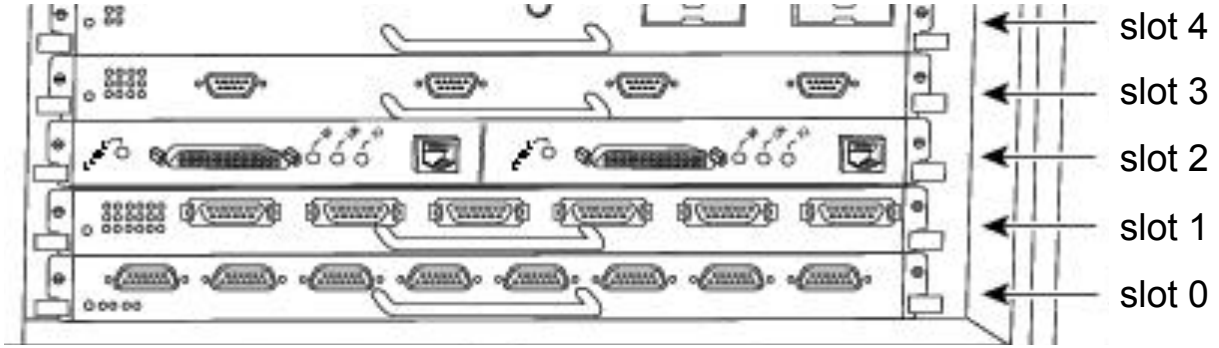
Configurations de base

Configurer une interface

Spécifier une interface

- `Enable`
  `conf t`
  `interface [TYPE] [NUMERO]`
  - Ethernet
  - FastEthernet
  - GigabitEthernet
  - Serial
  - Loopback
  - Tunnel
  - etc …
- Exemples :
  - `interface Ethernet 0`
  - `interface Fasthethernet 1`
  - `interface Serial 0`

Slots



Sélectionner une interface

- `interface Fastethernet 0/3`
  - dans le slot n°0 : interface n°3
- `interface Fastethernet 2/15`
  - dans le slot n°2 : interface n°15

Activer une interface

- Par défaut :
  - sur un switch : toutes les interfaces sont déjà actives
  - sur un routeur : toutes les interfaces sont inactives
- Passer d'abord en mode de configuration d'interface :

```
TOTO#conf t

TOTO(config)#interface fastEthernet 0/0
```

- Activer l'interface :

```
TOTO(config-if)#no shutdown
```

- Des messages sont affichés pour indiquer que l'interface est bien montée :

```
TOTO(config-if)#

*Mar  1 02:53:21.119: %LINK-3-UPDOWN: Interface FastEthernet0/0,
  changed state to up

*Mar  1 02:53:22.119: %LINEPROTO-5-UPDOWN: Line protocol on
  Interface FastEthernet0/0, changed state to up
```

Configurer une adresse IP sur une interface

- Passer d'abord en mode de configuration globale :

```
TOTO#conf t
```

- Passer ensuite en mode de configuration spécifique :

```
TOTO(config)#interface fastEthernet 0/0
```

- Configurer l'adresse IP de l'interface :

```
TOTO(config-if)#ip address 10.0.0.1 255.255.255.0
```

- Chaque nouvelle adresse écrase l'adresse précédente :

```
TOTO(config-if)#ip address 10.0.0.2 255.255.255.0
```

- Supprimer l'adresse IP de l'interface :

```
TOTO(config-if)#no ip address
```

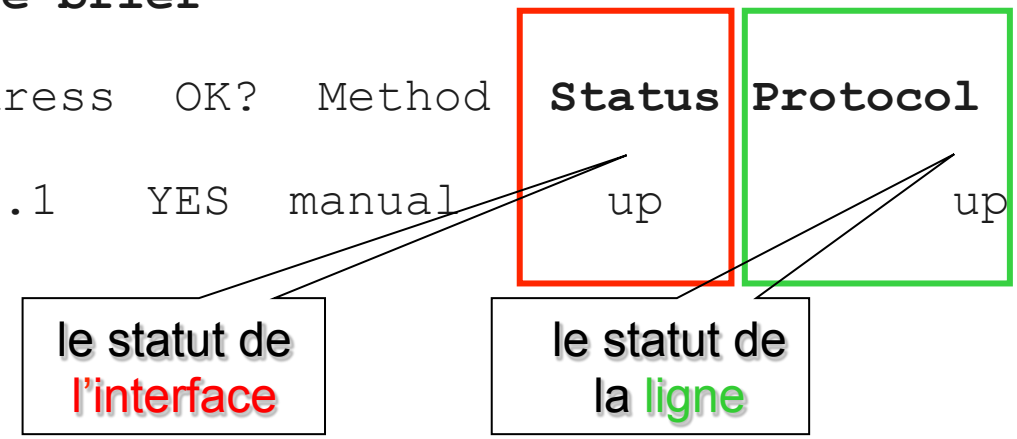
Vérifier le statut de l'interface

- Plusieurs commandes disponibles :
  - `show ip interface brief` [router]
  - `show interfaces status` [switch]
  - `show interfaces`

- Deux informations utiles :
  - le statut de l'interface
  - le statut de la ligne

show ip interface brief sur un routeur

```
ROUTER#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.0.0.1        YES manual up                    up
```



	STATUS	PROTOCOL
Port opérationnel :	Up	Up
Problème couche 2 ISO :	Up	Down
Problème couche 1 (serial) ISO :	Down	Down
Port désactivé :	Administratively Down	Down

show interfaces status sur un switch

```
Switch#show interfaces status
Port     Name               Status       Vlan       Duplex  Speed Type
Fa0/0                       notconnect   1            auto   auto 10/100BaseTX
Fa0/1                       connected    1          a-full  a-100 10/100BaseTX
Fa0/2                       notconnect   1            auto   auto 10/100BaseTX
Fa0/3                       notconnect   1            auto   auto 10/100BaseTX
Fa0/4                       notconnect   1            auto   auto 10/100BaseTX
Fa0/5                       notconnect   1            auto   auto 10/100BaseTX
Fa0/6                       notconnect   1            auto   auto 10/100BaseTX
```

Sécurité

Protéger l'accès CONSOLE

- conf t
- line console 0
  - no login — *ne pas exiger de MDP*
  - login — *exiger le MDP de la ligne*
  - login local — *exiger le MDP de la BDD locale*
  - password TOTO — *configurer le MDP de la ligne*
  - exit
- username JULIE password JU99 — *configurer la BDD locale*

Protéger l'accès TELNET

- conf t
- line vty 0 4
  - no login — *ne pas exiger de MDP*
  - login — *exiger le MDP de la ligne*
  - login local — *exiger le MDP de la BDD locale*
  - password TOTO — *configurer le MDP de la ligne*
- username JULIE password JU99 — *configurer la BDD locale*

SSH

- Telnet — tout passe en clair
- SSH — tout est crypté

- Pour générer une clef asymétrique :
  - hostname
  - nom de domaine
  - image

Configurer SSH

- conf t
- hostname R1
- ip domain-name EL.COM
- crypto key generate rsa general modulus 1024
- username JULIE password JU99
- line vty 0 4
  - login local
  - transport input ssh

Protéger l'accès PRIVILEGIE

- `enable password TOTO`
  - ancienne commande
  - toujours disponible
- `enable secret TOTO`
  - nouvelle commande
  - plus difficile à décrypter
- Si les 2 sont configurés, seul le `enable secret` sera demandé.

Test

Which condition indicates that service password-encryption is enabled?

A. The local username password is in clear text in the configuration.
B. The enable secret is in clear text in the configuration.
C. The local username password is encrypted in the configuration.
D. The enable secret is encrypted in the configuration.

- Réponse : C

CDP

Cisco Discovery Protocol

CDP

- Protocole propriétaire Cisco
- Objectifs :
  - découvrir des informations sur mes voisins
  - envoyer des informations à mes voisins
- L'équipement Cisco envoie ces informations :
  - toutes les 60 secondes
  - Trames en multicast
    - à l'adresse 0100.0ccc.cccc
  - quelque soit le type d'encapsulation configuré sur l'interface

Contenu des messages CDP

- Hostname
- Adresse IP
- Capacité de l'équipement
  - switching, routing, multicast
- Numéro de l'interface
- Nom de l'image IOS
- Pour un port de switch:
  - Nom de domaine VTP
  - N° du VLAN natif
  - Type d'encapsulation (access, 802.1Q, ISL)
  - Mode full ou half-duplex

si CDP version 2

Validité des messages CDP

- Sur réception d'un message CDP, l'équipement le considère valide pendant une durée limitée :
  - HOLD timer par défaut 180 sec

- L'équipement envoie des messages CDP sur toutes les interfaces où CDP est activée, à fréquence fixe :
  - HELLO timer par défaut 60 sec

Activer CDP

```
R1#configure terminal
R1(config)#no cdp run
R1(config)#cdp run
```

désactiver CDP globalement

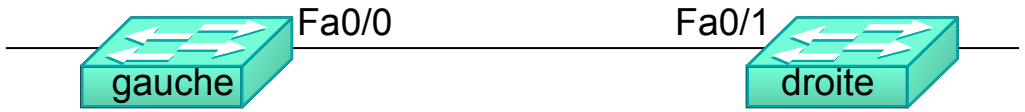
activer CDP globalement

```
R1(config)#int s0/0
R1(config-if)#cdp enable
R1(config-if)#no cdp enable
```

activer CDP sur l'interface

désactiver CDP sur l'interface

Exercice

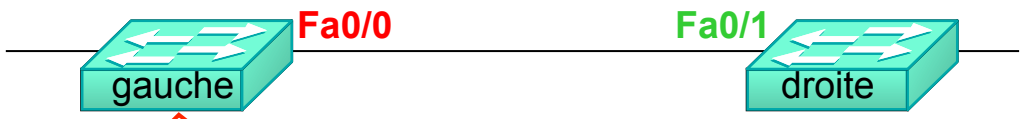


gauche#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
?	?	174	R S I	3550	?

Solution




```
gauche#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
droite           Fa0/0             174        R S I       3550      Fa0/1
```

LLDP = 802.1AB

Présentation

- Similaire à CDP :
  - CDP : propriétaire Cisco
    - actif par défaut sur tout équipement Cisco
  - LLDP : standard IEEE
    - actif ou non selon les modèles
- Avantage :
  - Hautement configurable
  - Utilise les TLV (Type Length Value)
- Désavantage :
  - Charge

Configuration

- Activer sur un équipement :
  - `Conf t`
    - `lldp run`
- Désactiver sur une interface:
  - `Interface X`
    - `No lldp enable`
- Vérifier :

```
Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 second
    LLDP hold time advertised is 120 seconds
```

Configuring LLDP (Cont.)

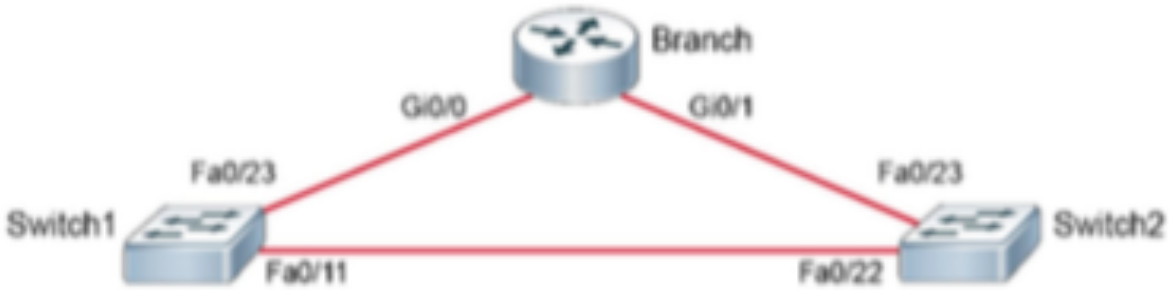
Enable or disable LLDP globally.

```
[no] lldp run
```

Enable or disable LLDP on an interface.

```
[no] lldp transmit
[no] lldp receive
```

Exemple




```
Switch1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability         Port ID
Switch2               Fa0/11           120        B               Fa0/22
Branch                Fa0/23           120        R               Gi 0/0
Total entries displayed: 2
```

show lldp neighbor detail

```
Chassis id: 001e.145e.4984
Port id: LINK TO SWITCH1
Port Description: FastEthernet0/22
System Name: Switch2.cisco.com

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(44)SE6, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-12 18:10 by gereddy

Time remaining: 94 seconds
System Capabilities: B,R
Enabled Capabilities: B
Management Addresses:
    IP: 10.1.1.12
Auto Negotiation - supported, enabled
Physical media capabilities:
    10base-T(HD)
    10base-T(FD)
    100base-TX(HD)
    100base-TX(FD)
Media Attachment Unit type: 16
-------------------------------------------
```

Test

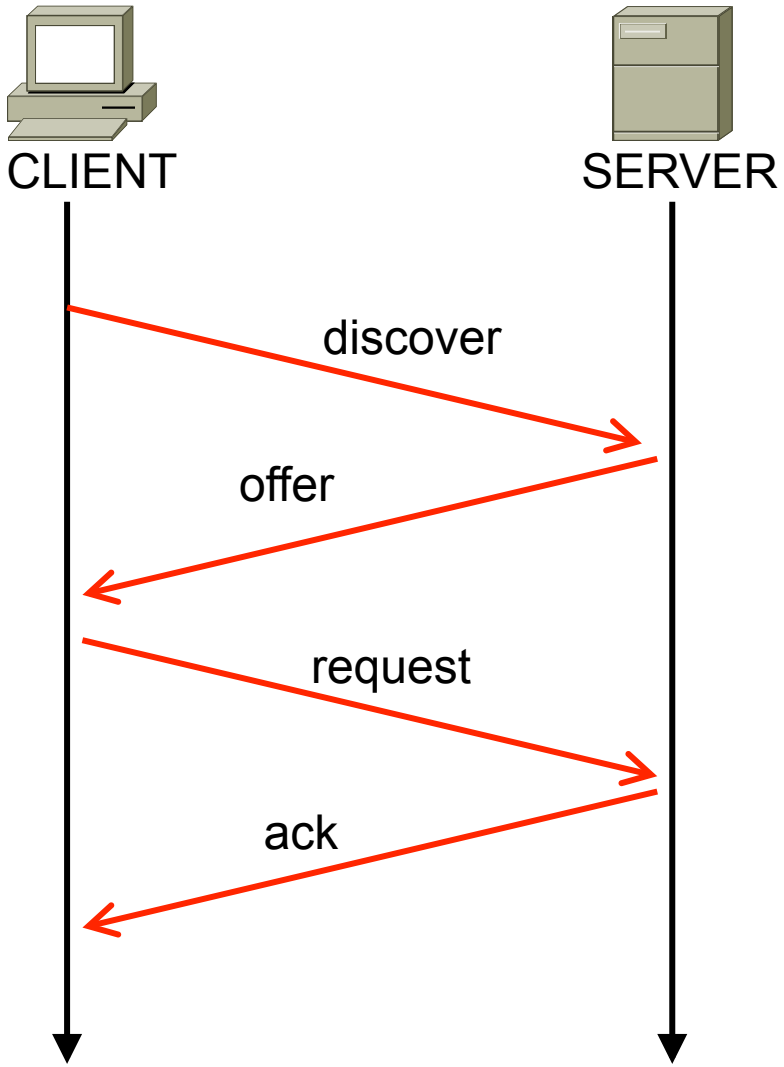
Which statement about LLDP is true?

A. It is a Cisco proprietary protocol.
B. It is configured in global configuration mode.
C. The LLDP update frequency is a fixed value.
D. It runs over the transport layer.

- Réponse : B

DHCP

Mécanisme DHCP



- 1. DISCOVER
  - IP src 0.0.0.0
  - IP dest 255.255.255.255
- 2. OFFER (unicast)
  - une adresse IP
  - masque
  - l'@ IP de passerelle
  - l'@ IP des serveurs DNS
  - le lease time
  - etc…
- 3. REQUEST (broadcast)
  - intention d'accepter l'offre
- 4. ACK
  - confirmation fin du processus

@ destination

	@ MAC destination	@ IP destination
Discover	FFFF.FFFF.FFFF	255.255.255.255
Offer	@ MAC du client	0.0.0.0
Request	FFFF.FFFF.FFFF	
Ack	@ MAC du client	

- Le bail est attribué pour une période.
  - Le client contacte périodiquement le serveur DHCP pour renouveler son bail et conserver la même adresse IP.
- Avant d'offrir une adresse à un client, le serveur peut vérifie que cette adresse n'est pas déjà attribuée en faisant des ping ou des ARP gratuits.
  - En cas de conflit, l'adresse est inutilisée : show ip dhcp conflict
  - Nécessite l'intervention de l'administrateur

Router = server DHCP

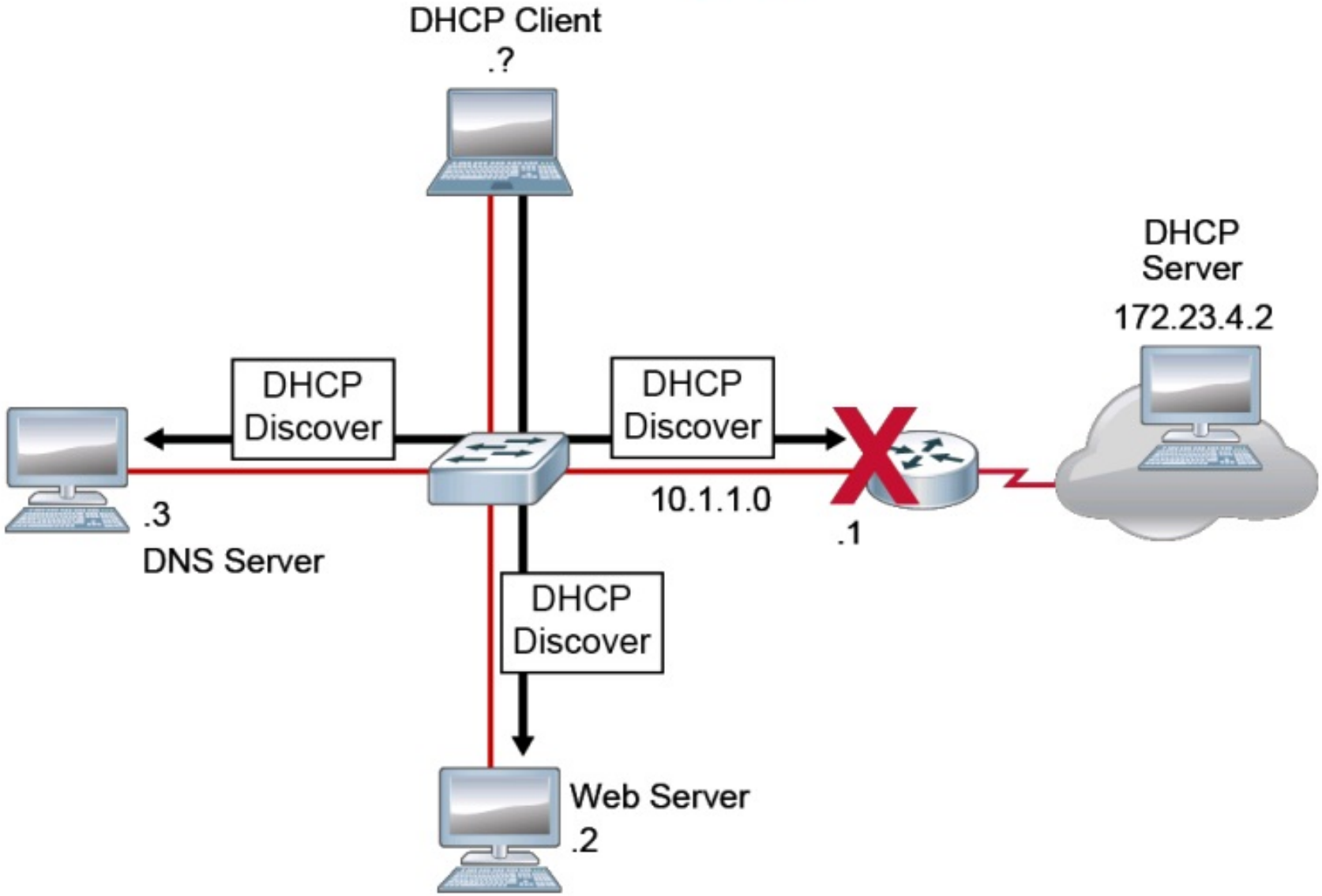
- conf t
- ip dhcp excluded-address 192.168.10.250 192.168.10.254
- ip dhcp pool TOTO
  - domain-name X
  - network 192.168.10.0 255.255.255.0

  Ou : network 192.168.10.0 /24
  - default-router 192.168.10.254
  - dns-server 192.160.1.1

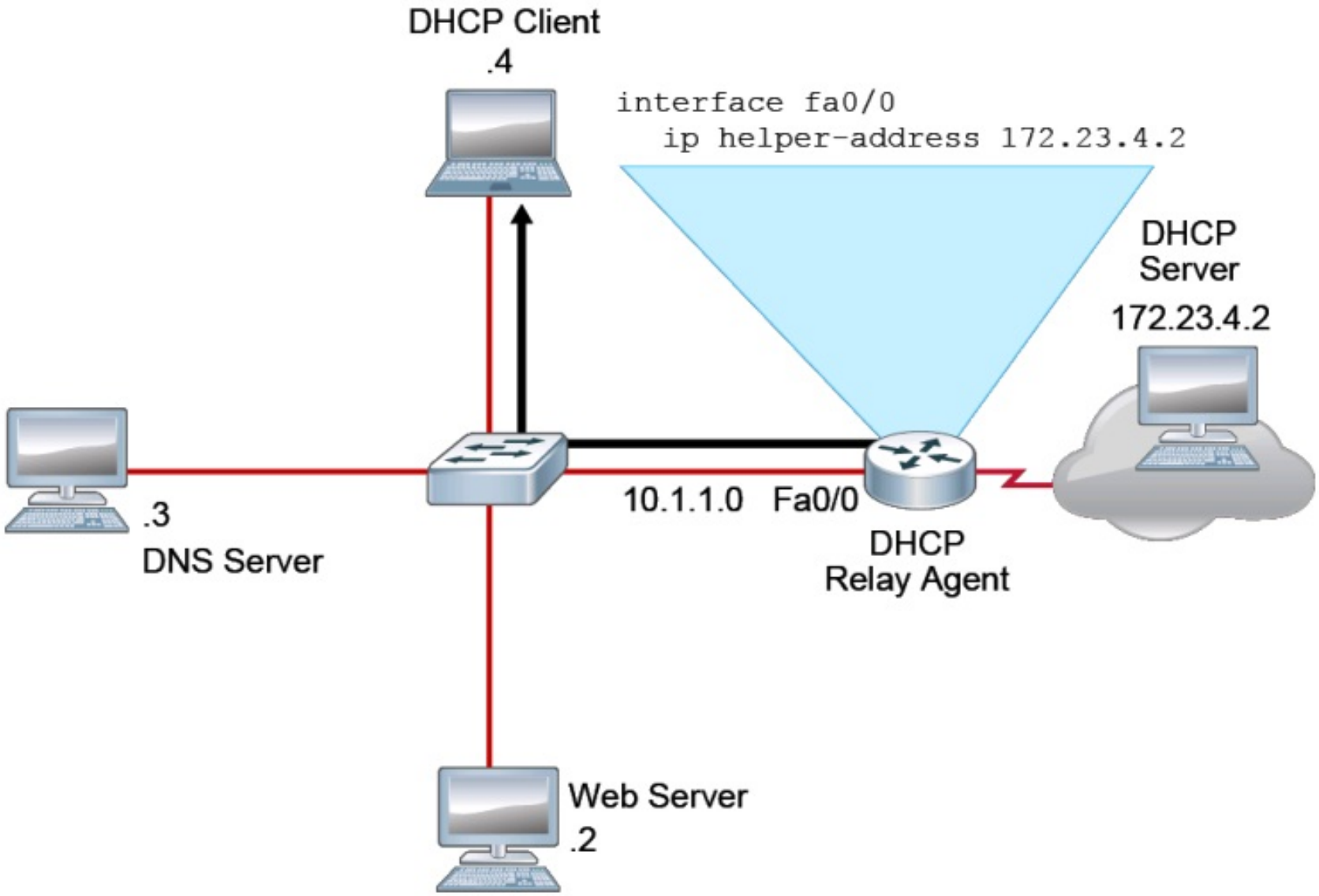
Activer la fonction DHCP

- La fonction DHCP est automatiquement activée dès qu'une adresse IP est attribuée à une interface du routeur, dans la plage de pool
- conf t
- int fa0/0
- ip address 192.168.10.254 255.255.255.0

Cisco Device as DHCP a Relay Agent



Cisco Device as a DHCP Relay Agent (Cont.)



Network Time Protocol

Correct time within networks is important for the following reasons:

- Correct time allows the tracking of events in the network in the correct order.
- Clock synchronization is critical for the correct interpretation of events within syslog data.
- Clock synchronization is critical for digital certificates.

Network Time Protocol (Cont.)

NTP provides time synchronization between network devices.

- NTP can get the correct time from an internal or external time source:
  - Local master clock
  - Master clock on the Internet
  - GPS—global positioning system or atomic clock
- A router can act as an NTP server and client. Other devices (NTP clients) synchronize time with the router (NTP server).

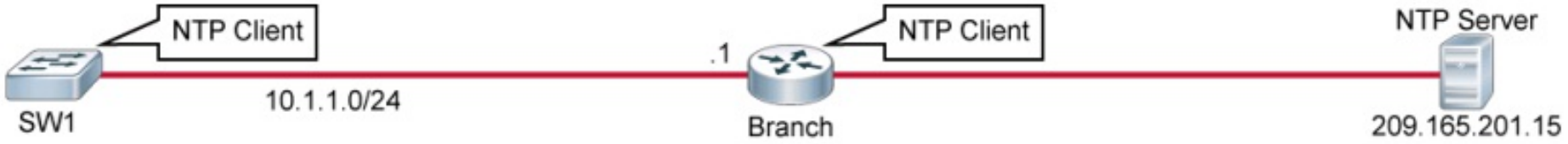
Configuring NTP

Configure the Branch router as an NTP client, which will synchronize its time with the NTP server.

```
Branch(config)# ntp server 209.165.201.15
```

Configure the SW1 switch as an NTP client, which will synchronize its time with the Branch router.

```
SW1(config)# ntp server 10.1.1.1
```



Configure and Verify NTP

Step 1: Review the clocks on SW1, SW2 and R1.

Step 2: Configure R1 as an NTP server.

```
R1(config)# ntp master
```

Step 3: Configure SW2 to use R1 as its NTP server.

```
SW2(config)# ntp server 10.10.1.1
```

Step 4: On SW2, display the current NTP associations and NTP status.

```
SW2# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.10.1.1       127.127.1.1      8     49     64     1  0.000   0.000 189.47
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

SW2# show ntp status | include Clock is
Clock is synchronized, stratum 9, reference is 10.10.1.1
```

Configure and Verify NTP (Cont.)

Step 5: The clocks on the SW2 and R1 should be synchronized.

Step 6: On R1, configure the CET time zone.

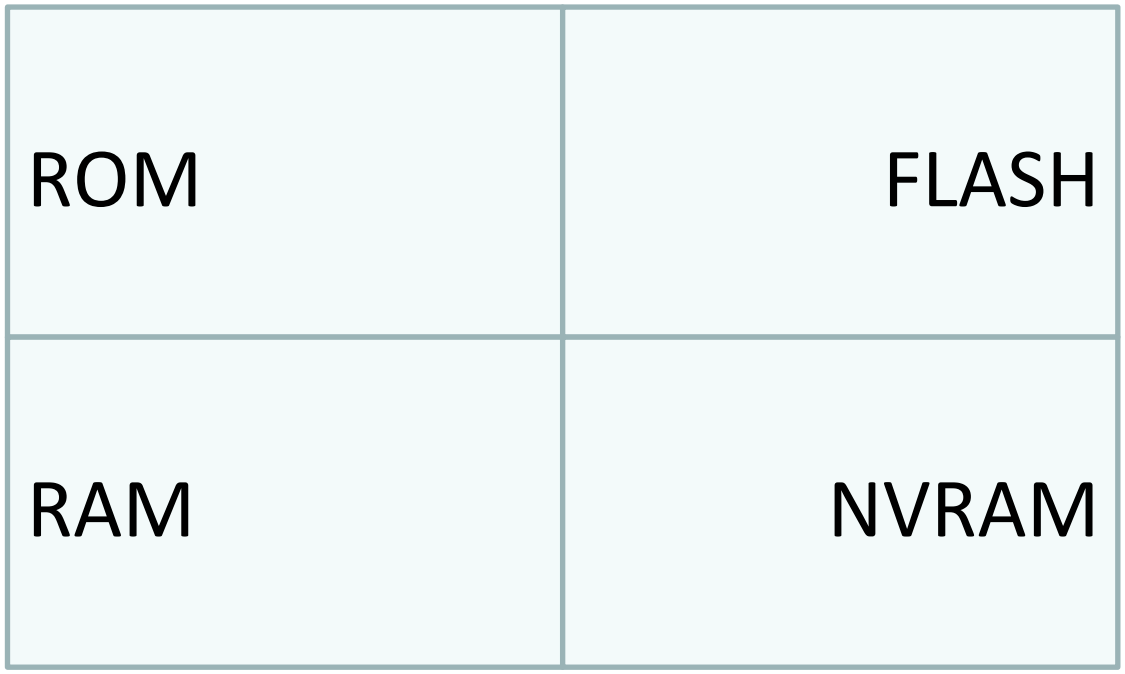
```
R1(config)# clock timezone CET 2
```

Step 7: On R1, display the current time and observe that the time zone has changed.

```
R1# show clock
10:53:05.222 CET Tue Nov 24 2015
```

Architecture interne

Architecture interne



ROM


• Instructions du **POST**, Power On Self Test
• **Rxboot** ou **bootstrap** Programme d'amorçage
FLASH
RAM
NVRAM

FLASH

ROM	Image = IOS
RAM	NVRAM

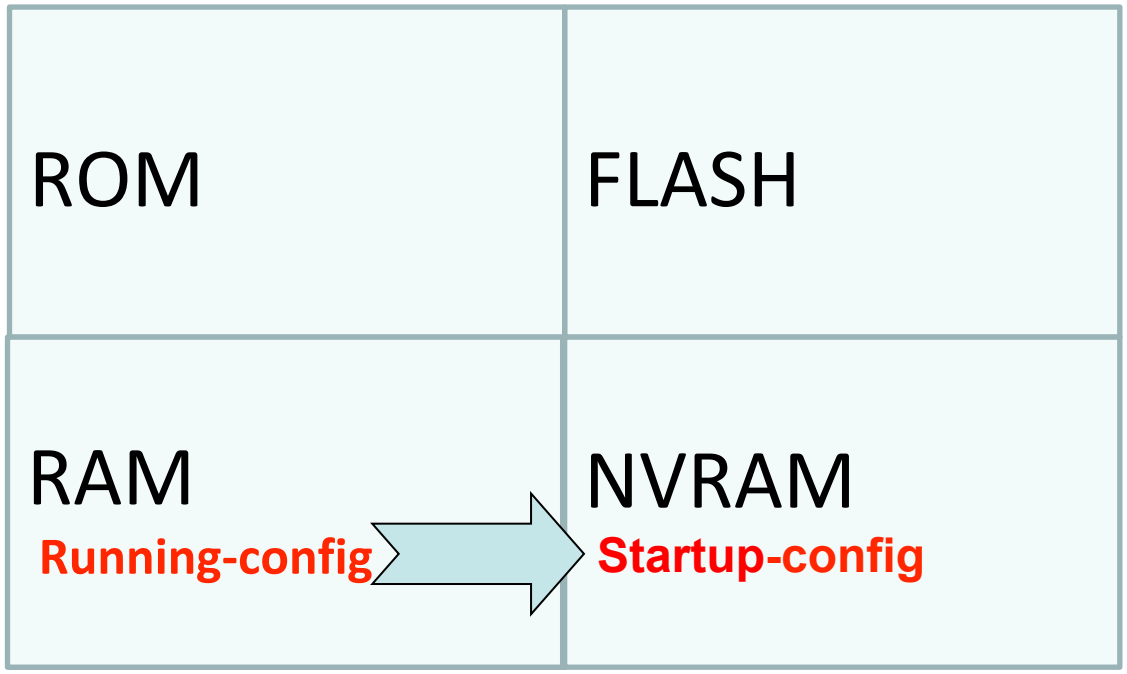
NVRAM

ROM	FLASH
RAM	**Startup- configuration**

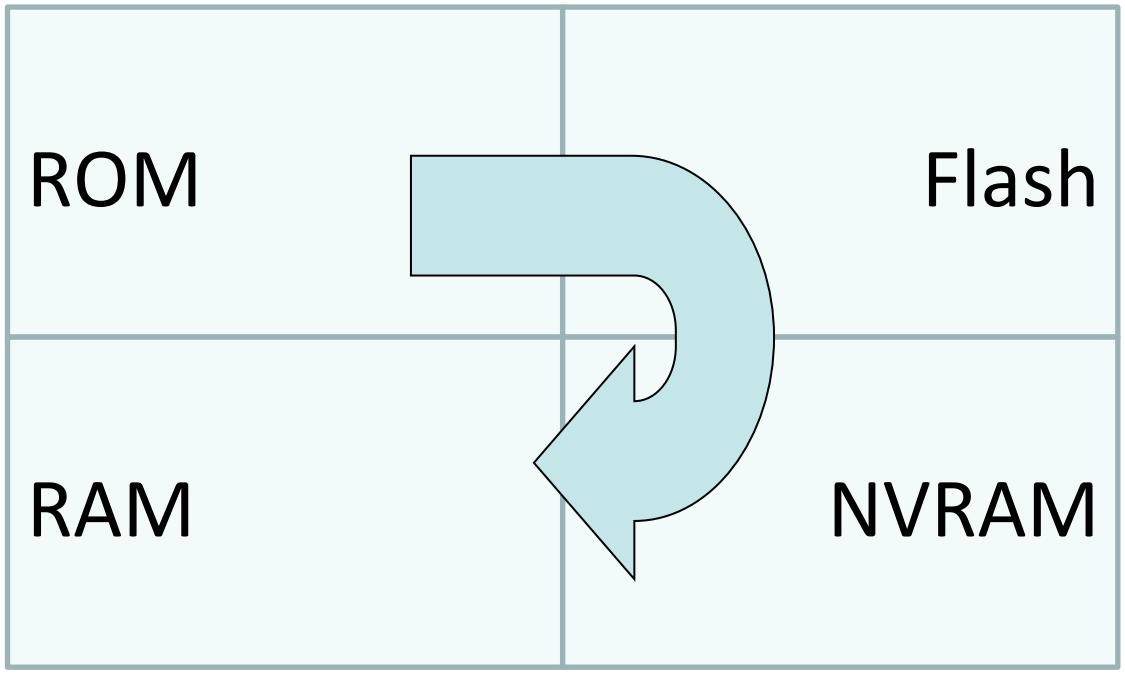
RAM

ROM	FLASH
• Running-config • Table d'@MAC • Table de routage • Paquets etc….	NVRAM

write



Au démarrage…



Choisir une autre image

- Si plusieurs images IOS dans la flash
  - Laquelle prendre ?
- Le choix sera fait selon le dernier chiffre du registre de configuration
  - 0x2100 ne prendre aucune image
  - 0x2101 prendre la 1ère image de la Flash
  - 0x2102 se référer aux commandes **boot system**

Commandes boot system

- **conf t**
- **boot system flash:IOS2.bin**
- **boot system tftp://10.0.0.1/IOS.bin**

- Pour vérifier la valeur du registre de configuration :
  - **Show version**
- Pour vérifier l'espace disque sur la flash :
  - **Show flash**

Quel fichier de conf charger ?

- Le choix sera fait selon l'avant-dernier chiffre du registre de configuration
  - 0x2102 prendre la startup de la NVRAM
  - 0x2142 ne pas charger de startup

- Quelle utilité de modifier ce registre ?

Perte de mot de passe

1. Séquence « break »
2. Rommon 1>confreg 0x2142
3. Rommon 2>reset (ou i, ou redémarrer)
4. Enable
5. Copy start run
6. Conf t
7. Enable secret TOTO
8. Config-register 0x2102
9. Réactiver les interfaces (no shut)
10. End
11. write

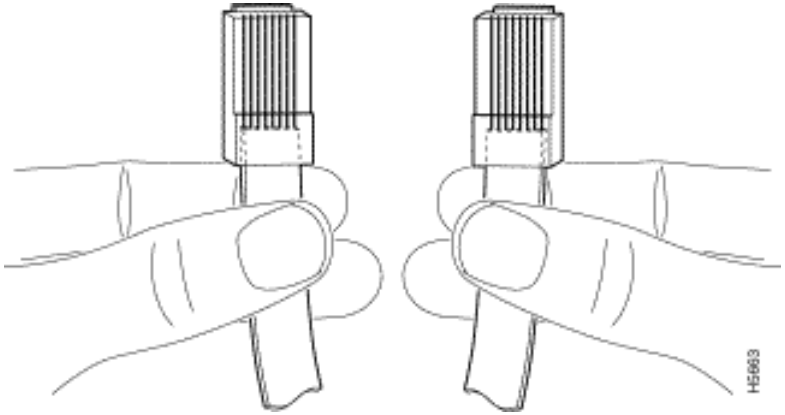
show version

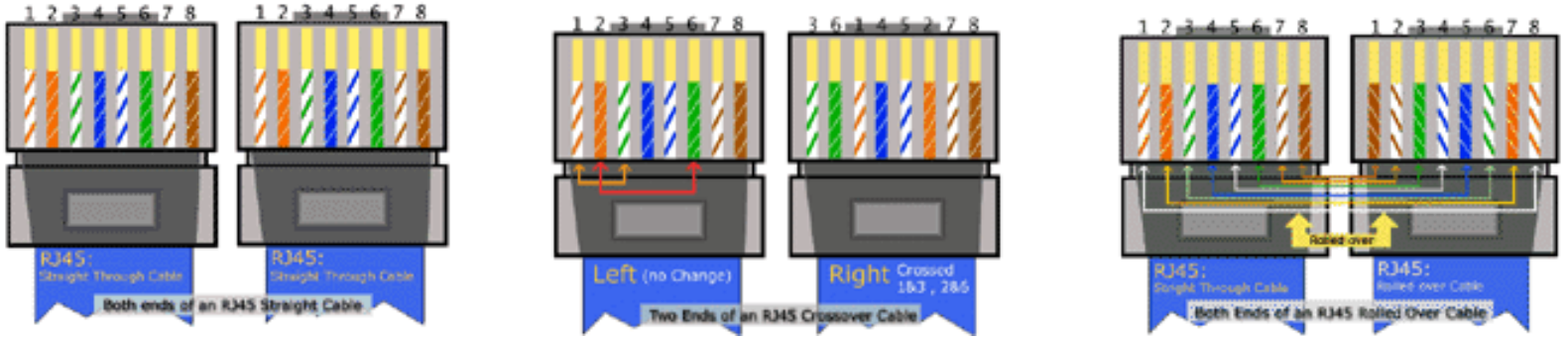
```
Router1#show version

Cisco IOS Software(C2600-ADVIPSERVICESK9-M), Version
12.3(4)T4,  ROM: System Bootstrap, Version 12.2(8r) [cmong
8r], RELEASE SOFTWARE (fc1)
Router1 uptime is 20 minutes
System returned to ROM by power-on
System image file is "flash:c2600-advipservicesk9-mz.
123-4.T4.bin
Cisco 2621XM (MPC860P) processor (revision 0x300) with
125952K/5120K bytes of memory.
Processor board ID JAE081160XR (3618058385)
M860 processor: part number 5, mask 2
2 FastEthernet interfaces
32K bytes of NVRAM.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Switching

Differents types de cables :
Droits, Croisés, Rollover

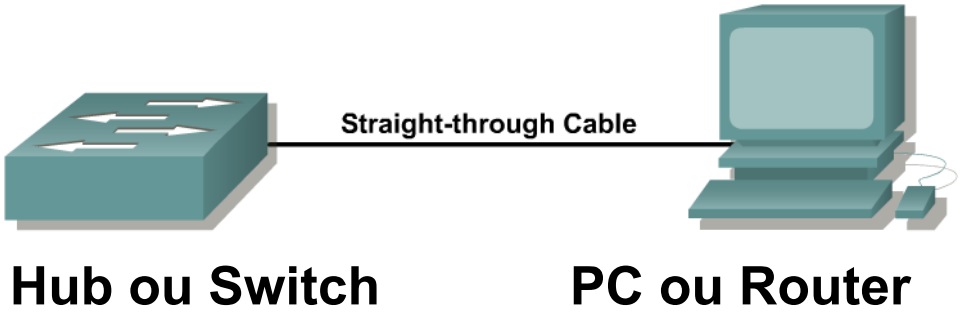
3 types de cables





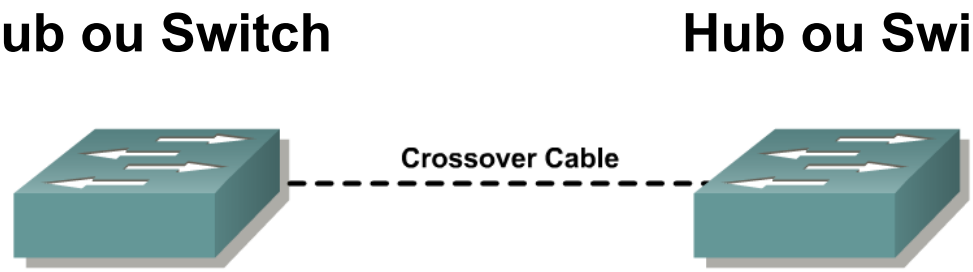
droit **Croisé** **Rollover**

Le cable droit



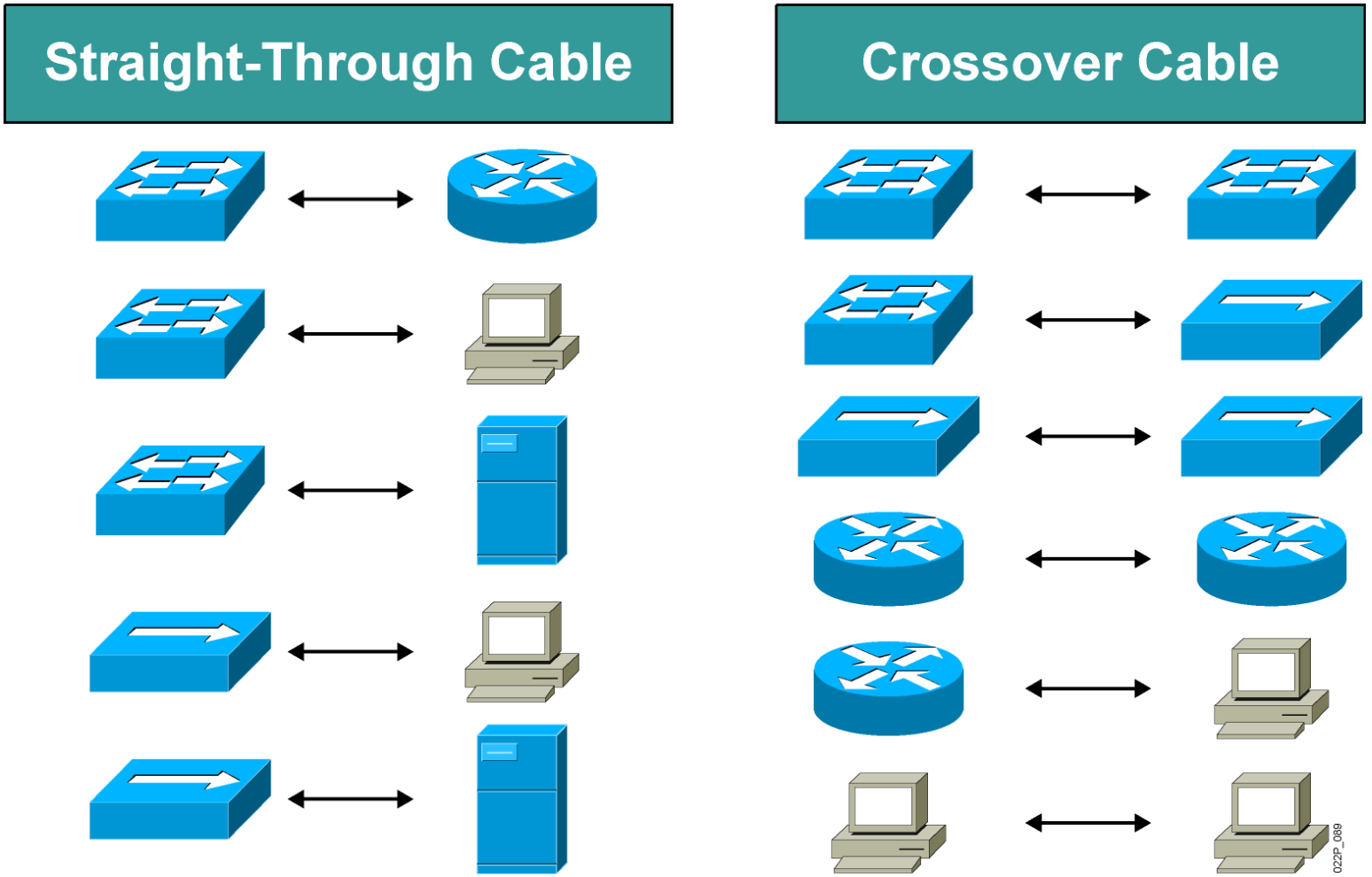
- Le cable droit connecte des équipements de nature différentes.

Cable croisé

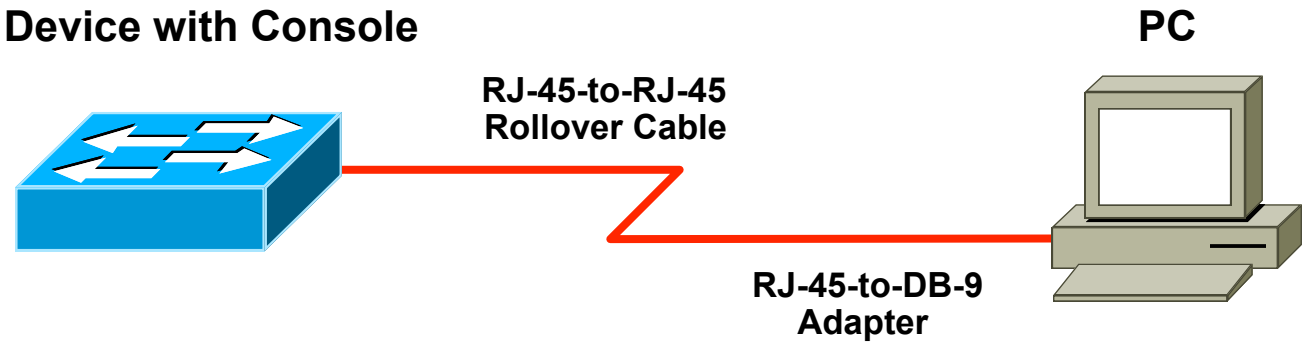


- Pour interconnecter les switchs
- Connecte les port de même nature

Droit, versus croisé



Le cable Rollover



- Permet de se connecter à la console
- La console est un accès “hors bande” par opposition aux accès via Telnet ou SSH

LED : statut du port Ethernet

LED	Signification
Eteint	Pas de liaison présente
Orange	Port désactivé (administrativement, ou suite à une violation de sécurité)
Vert	Liaison opérationnelle, sans trafic
Vert clignotant	Liaison opérationnelle, avec trafic
Alternatif Vert & Orange	Erreurs (collision, CRC)

Description Ethernet

Le principe d'encapsulation

- Pour envoyer une donnée 'XYZ', l'expéditeur encapsule cette donnée 'XYZ' dans une trame :
- Donnée à envoyer : XYZ
- Cette donnée est encapsulée dans une trame :

la trame Ethernet

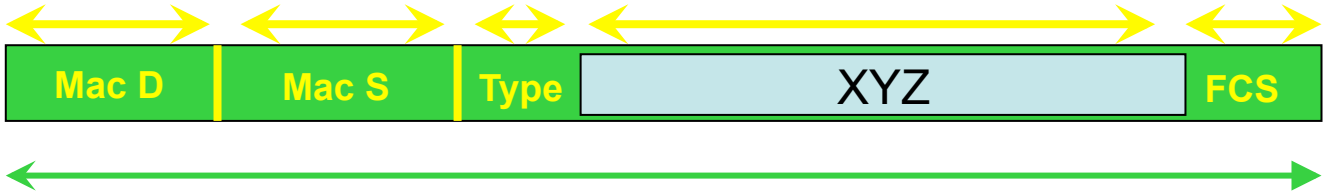
Ethernet Frame Structure

Field Length (Bytes)	8	6	6	2	46-1500	4
Typical Ethernet Frame	Preamble	Destination Address	Source Address	Type	Data	FCS

Définition d'une trame

- L'entête de la trame Ethernet contient :
  - l'adresse MAC destination — 6 octets
  - l'adresse MAC source — 6 octets
  - le type — 2 octets

  } 14
- La partie utile — entre 46 et 1500 octets
- Le pied de la trame Ethernet contient :
  - FCS, Frame Check Sequence — 4 octets



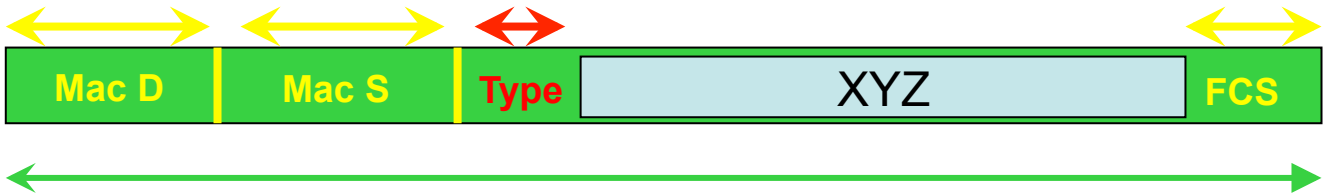
Taille de la trame

- Taille maximale de la trame :
  - = 14 + 1500 + 4 = 1518 octets

- Taille minimale de la trame :
  - = 14 + 46 + 4 = 64 octets
  - si la partie utile fait moins de 46 octets, des octets de bourrages sont rajoutés

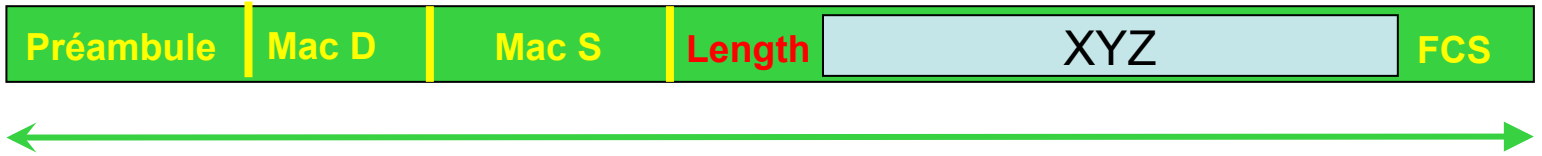
Le ‘type’ de la trame

- Il identifie le protocole de la donnée encapsulée :
  - Exemples :
    - si ‘XYZ’ est en IP, alors ‘type’ = 0x800
    - si ‘XYZ’ est en ARP, alors ‘type’ = 0x806



La trame 802.3

- La trame Ethernet n'est pas conforme au modèle OSI qui exige l'indépendance entre les couches :
  - la trame Ethernet n'indique pas la longueur de la partie utile.
- La trame 802.3 est conforme au modèle OSI :
  - le champ 'Type' est remplacé par un champ 'Longueur'
  - un champ supplémentaire est rajouté : le 'préambule'



la trame 802.3

Adresse MAC

- Chaque carte réseau est identifiée par une adresse unique au monde (*) : l'adresse MAC.
  - BIA = Burned In Address
  - Inscrite sur la NIC = Network Interface Card
  - 12 caractères héxadécimaux
  - Exemples :
    - 0007.1234.abcd = 00:07:12:34:ab:cd
    - a123.b587.ef7f = a1:23:b5:87:ef:7f

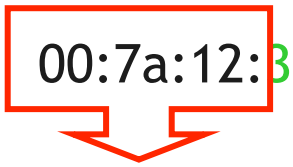
(*) l'unicité est garantie lorsque le 7ème bit est égal à 0.
Si le 7ème bit vaut 1, alors il s'agit d'une adresse MAC administrée localement.

Unicité de l'adresse MAC

- L'adresse MAC est composée de 2 parties :
  - partie 'O.U.I.' :
    - Organizational Unique Identifier
    - 3 octets
    - attribués par IANA
  - partie 'constructeur'
    - 3 octets
    - attribués par le Constructeur

- Exemples :
  - 007a.1234.abcd

00:7a:12:34:ab:cd



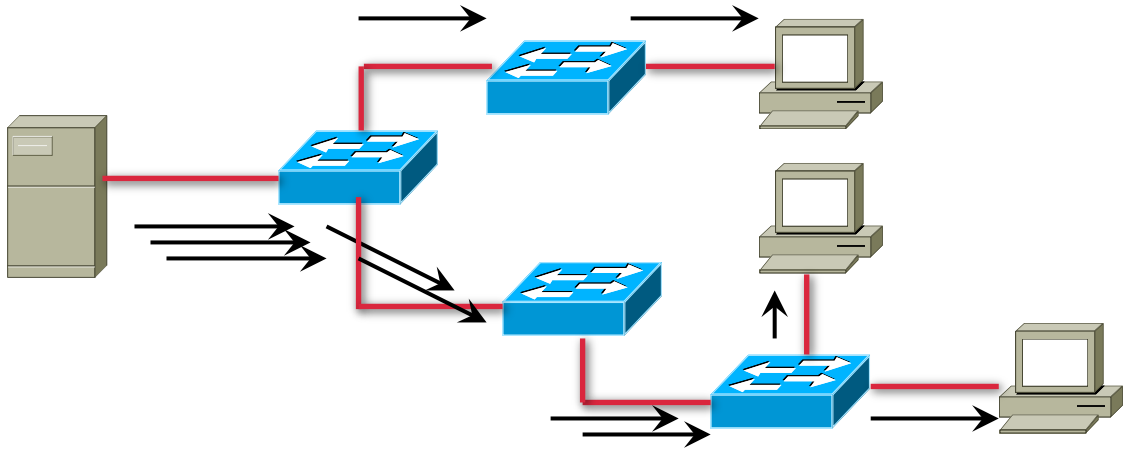
Ethernet

Les trois types de trames

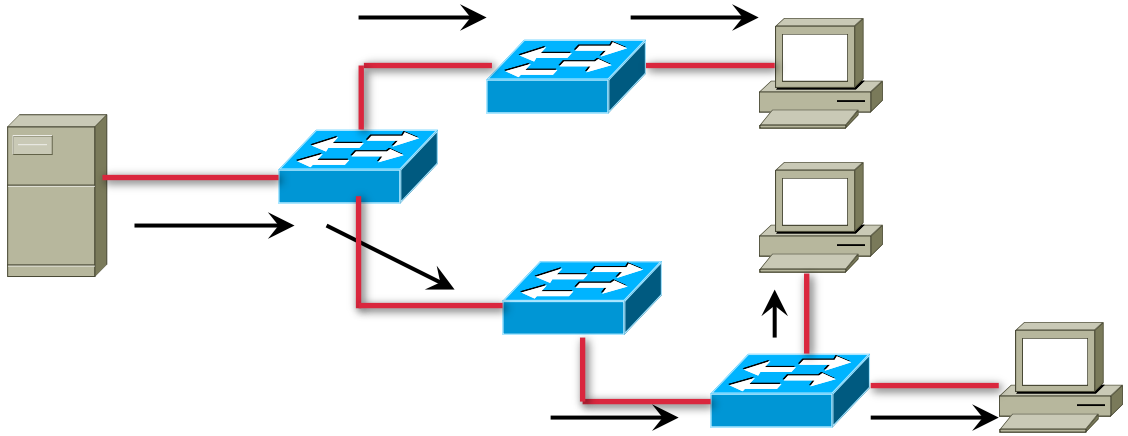
Types de trames

- Unicast
  - un équipement veut parler avec un autre équipement
- Broadcast :
  - un équipement veut parler avec tous les autres équipements de son réseau.
- Multicast :
  - un équipement veut parler avec plusieurs autres équipements mais pas tous

Intérêts d'un broadcast



Unicast



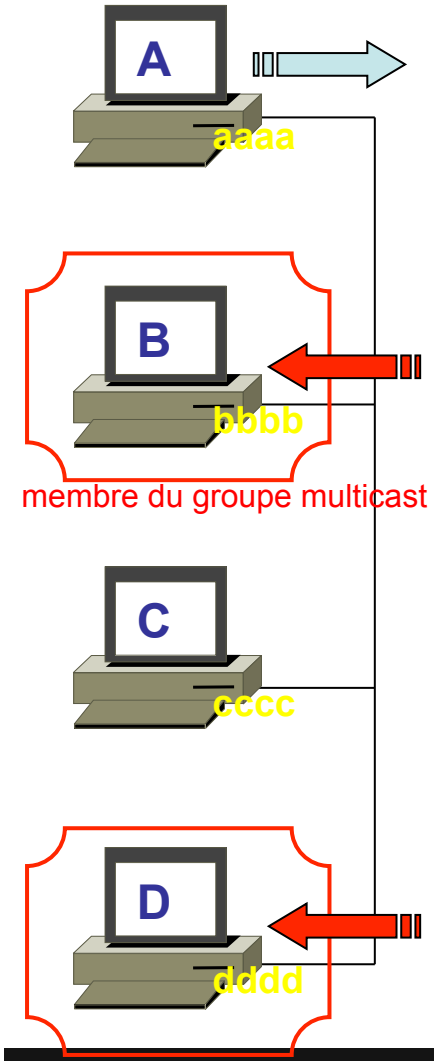
Broadcast

Intérêts d'un broadcast

- Réduire la charge sur le réseau.
- L'expéditeur n'a besoin de créer qu'une seule trame.

- Par contre :
  - tous les équipements du réseau doivent écouter cette trame, la désencapsuler et étudier sa partie utile… même s'ils ne sont pas concernés !

Multicast



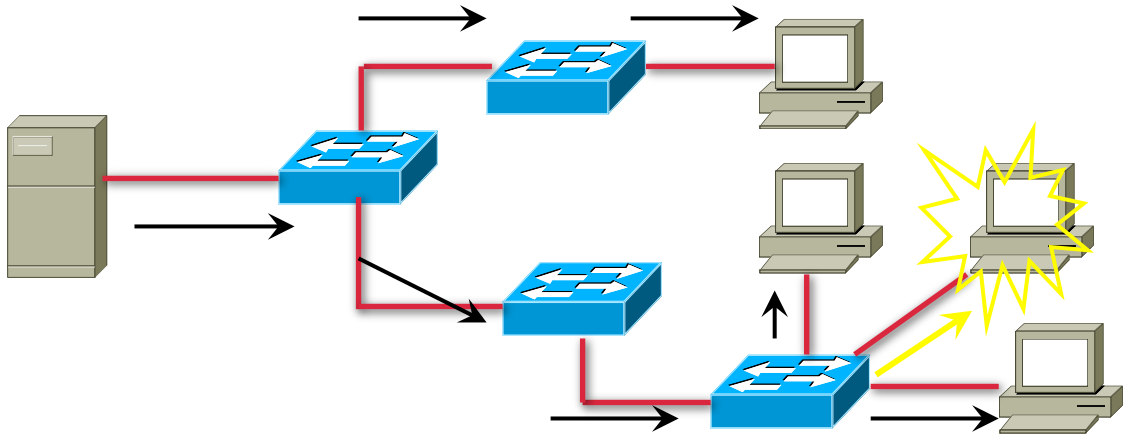
- Utiliser l'adresse MAC destinataire qui identifie les membres du groupe multicast :
  - le 8ème bit est égal à 1
  - exemple : 0100.5E01.1111

- Exemple : multicast de A pour 0100.5E01.1111

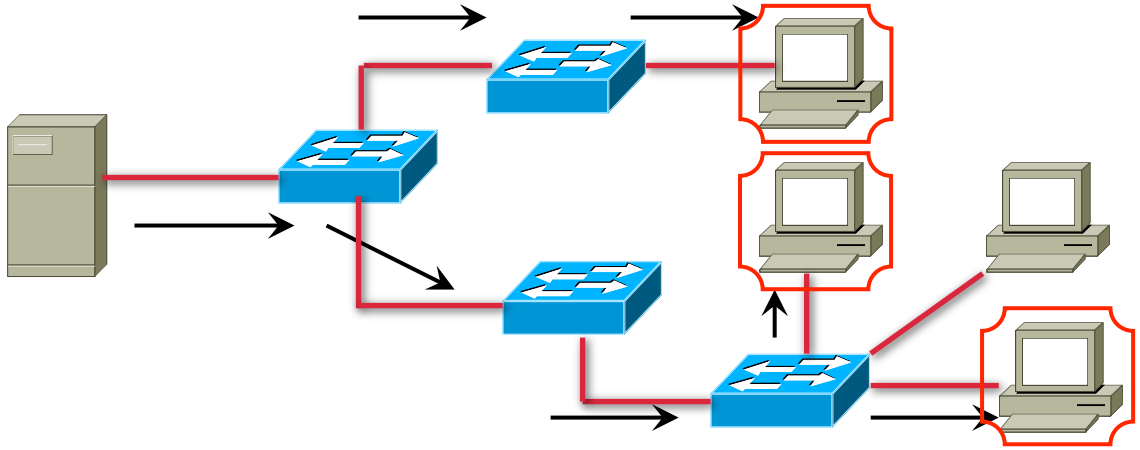
Intérêts d'un multicast

- Réduire la charge sur le réseau.
- L'expéditeur n'a besoin de créer qu'une seule trame.
- Seuls les équipements intéressés écoutent ces trames, la désencapsulent et étudient sa partie utile.
  - les équipements qui ne sont pas membres du groupe multicast ne sont pas dérangés par ces trames
  - la charge de leur CPU est réduite.

Intérêts d'un multicast



Broadcast



Multicast

Ethernet

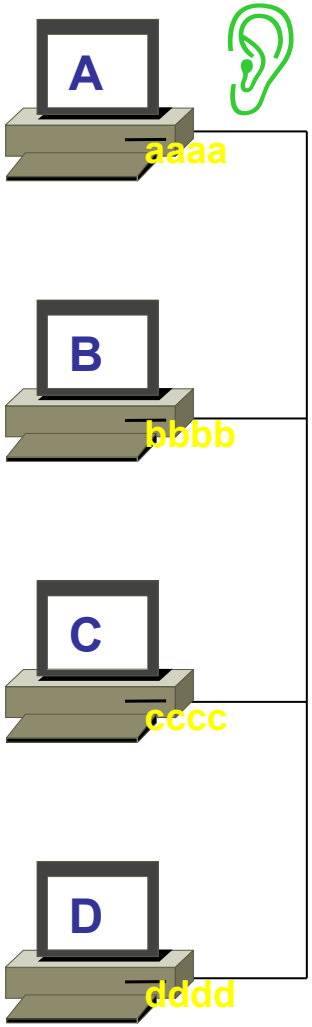
Les collisions

CSMA / CD : toutes les étapes

Un équipement veut envoyer une trame sur le réseau :

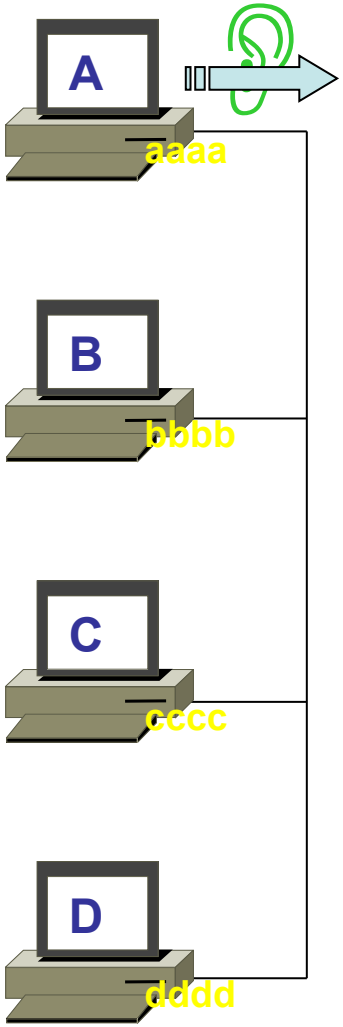
1. Il écoute le réseau pour voir s' il est libre.
2. Si le réseau est libre, il commence à déposer sa trame
3. Il continue à écouter le réseau pour vérifier qu' il est le seul à l' utiliser
    1. il compare ce qu' il dépose sur le réseau avec ce qu' il entend sur le réseau
4. S' il y a divergence, cela signifie qu' une collision a eu lieu :
    1. il arrête d' émettre et attend un temps aléatoire.
5. Il essaie à nouveau d' émettre après l' écoulement du temps aléatoire.

1. Ecouter le réseau



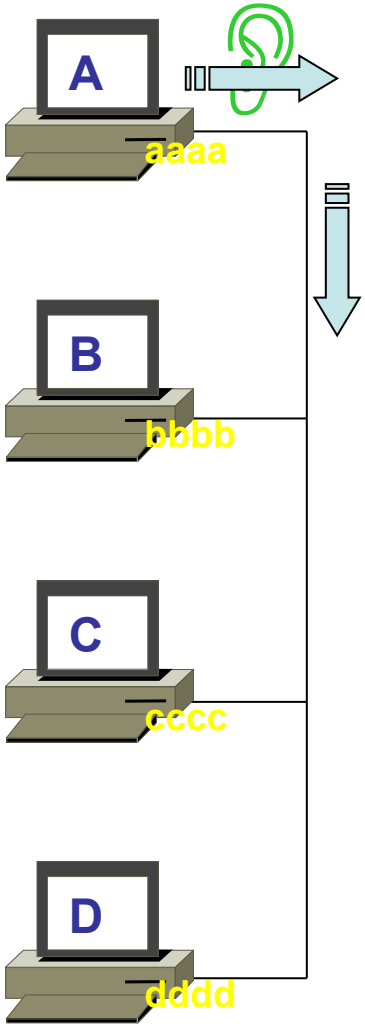
- Y a-t-il déjà du trafic sur le réseau ?

2. A dépose sa trame



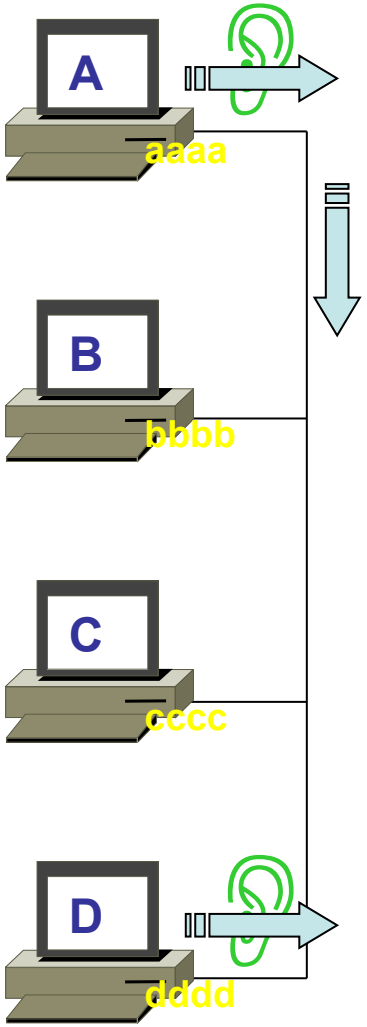
- Pas de trafic.
- La voie est libre.
- A dépose sa trame et continue à écouter
- A vérifie que ses données ne sont pas perturbées par l'émission d'un aute équipement

3. Propagation de la trame



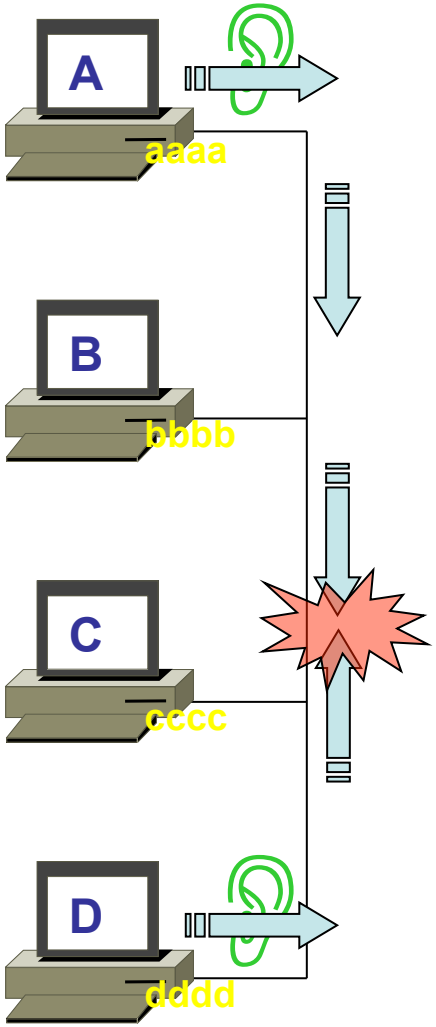
- La trame déposée par A se propage dans le réseau.
- Elle n'a pas encore atteint D
- D veut également envoyer une trame.

4. D dépose sa trame



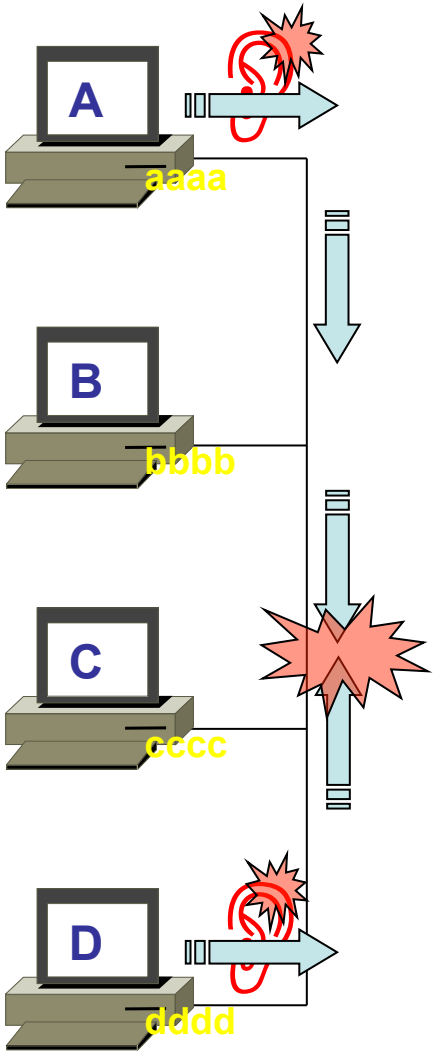
- La trame de A n'a pas atteint D.
- D écoute le réseau : il croit que le réseau est libre.
- D dépose sa trame

4. Collision



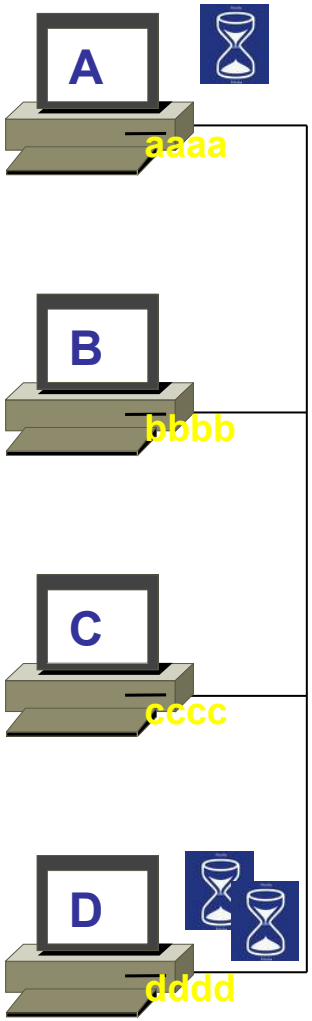
- Les 2 trames se rencontrent.
- Les trames n'ont pas pu être entièrement déposées sur le réseau :
  - on parle alors de fragments

5. Détection de la collision



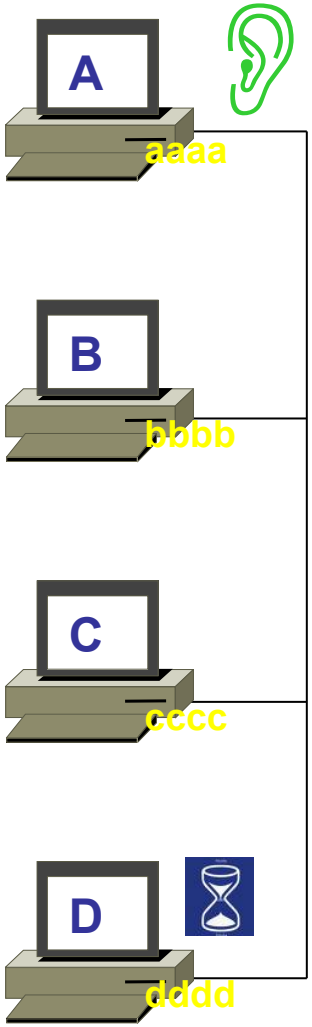
- A et D constatent qu' il y a divergence entre ce qu' ils envoient et ce qu' ils entendent.

6. Arrêt de l'émission



- A et D arrêtent d'émettre leur trame.
- Ils emmettent un signal de bourrage pour avertir tout le segment de la collision
- Chacun attent un certain temps calculé de manière aléatoire.

6. Nouvel essai



- D attend plus longtemps que A.
- Donc A essaie à nouveau d'émettre : il commence par écouter le réseau.

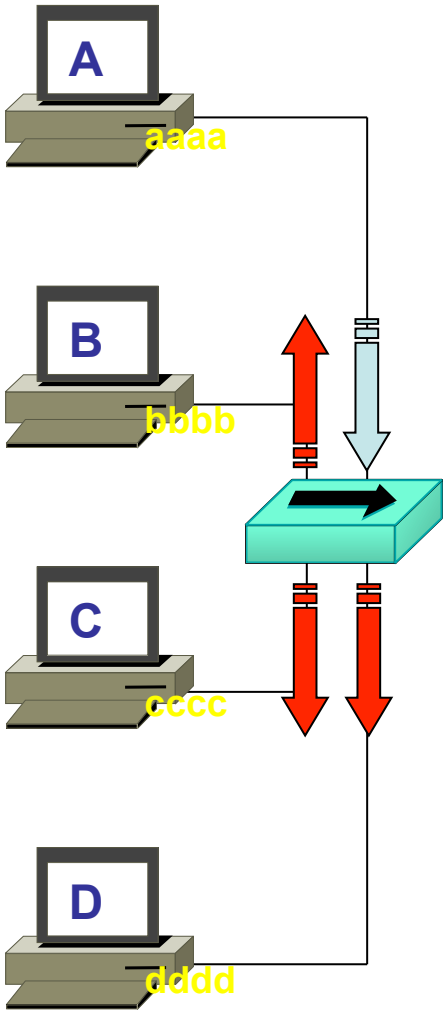
CSMA / CD

- CS
  - Carrier Sense :
    - l' équipement écoute le réseau
- MA
  - Multiple Access :
    - attention : plusieurs équipements peuvent vouloir accéder au réseau en même temps (= collision)
- CD
  - Collision Detection :
    - il faut donc un mécanisme pour détecter ces collisions

Ethernet

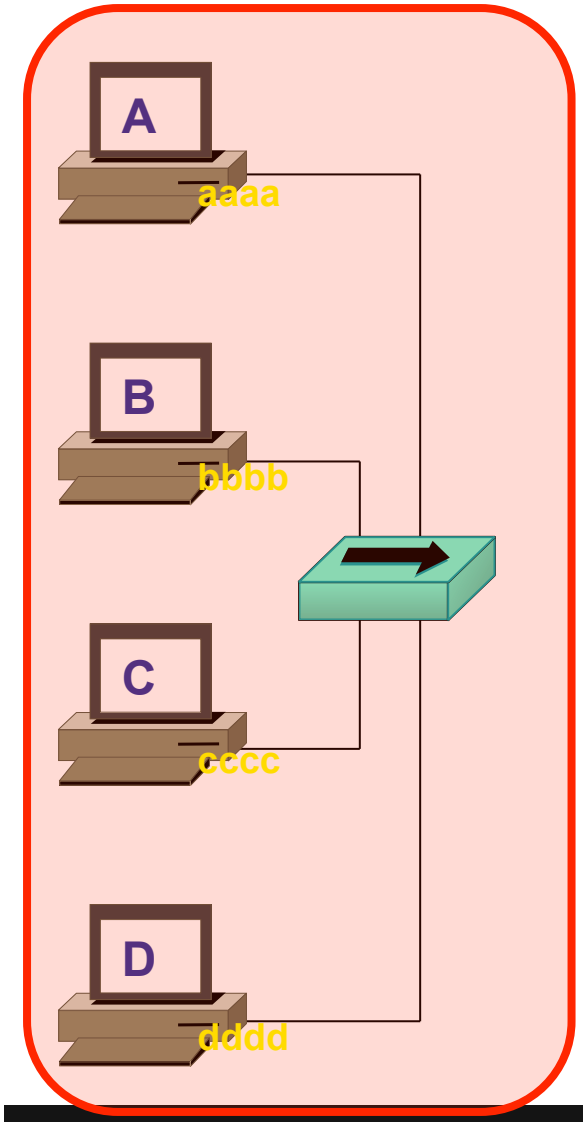
Le HUB

Fonctionnement du HUB



- Il reçoit une trame sur une interface.
- Il la duplique sur toutes les autres interfaces, quel que soit le type de trame : unicast, broadcast, multicast

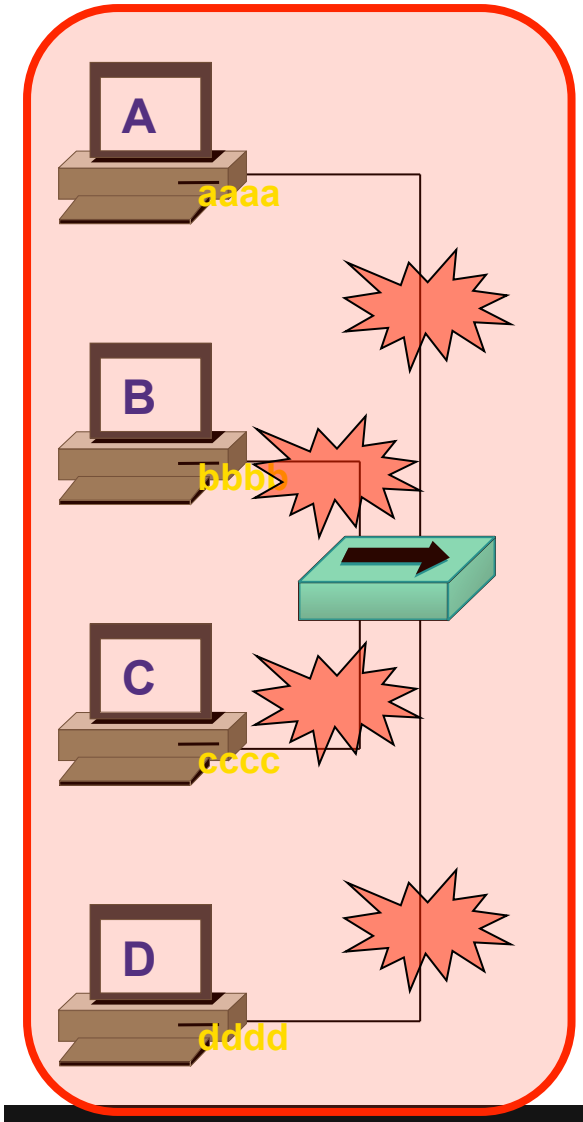
Domaine de collision



- Tous les équipements placés autour d'un même HUB peuvent avoir des collisions entre eux :

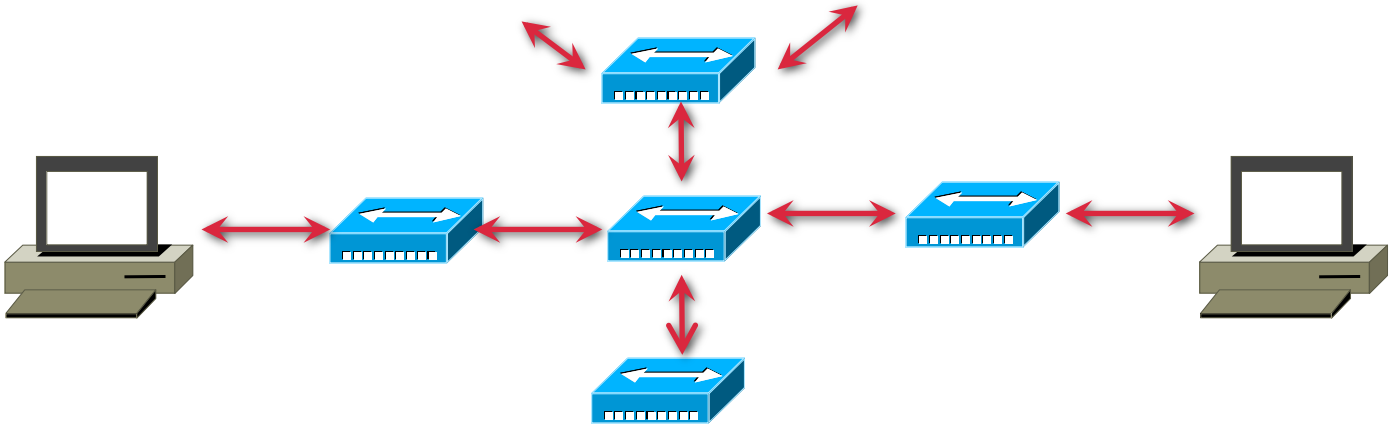
- Ils sont dans le même domaine de collision.

Domaine de collision

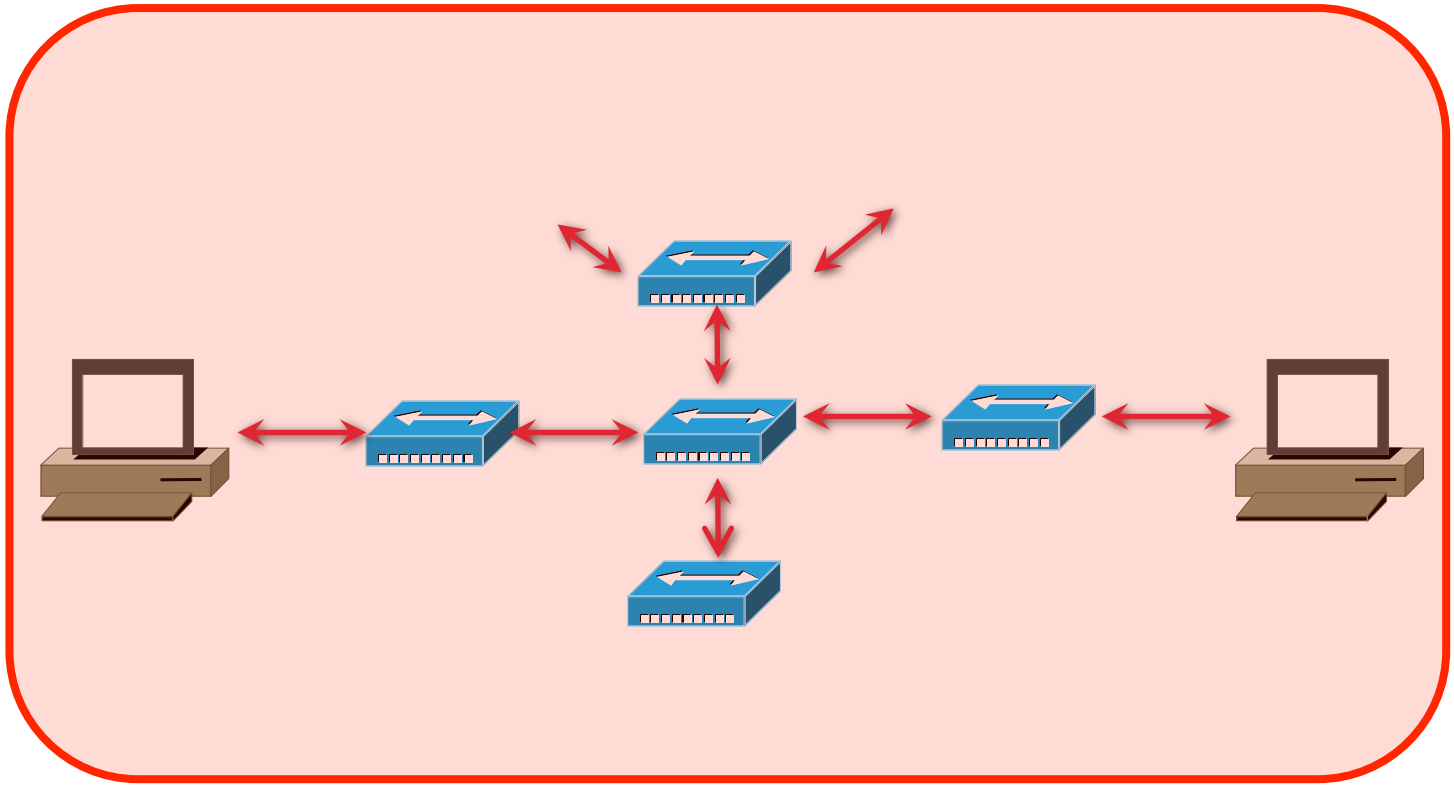


- Si une collision se produit sur un segment :
  - il se répand sur tous les segments autour du HUB
  - tout le réseau est impacté
  - aucun équipement ne peut utiliser la bande passante

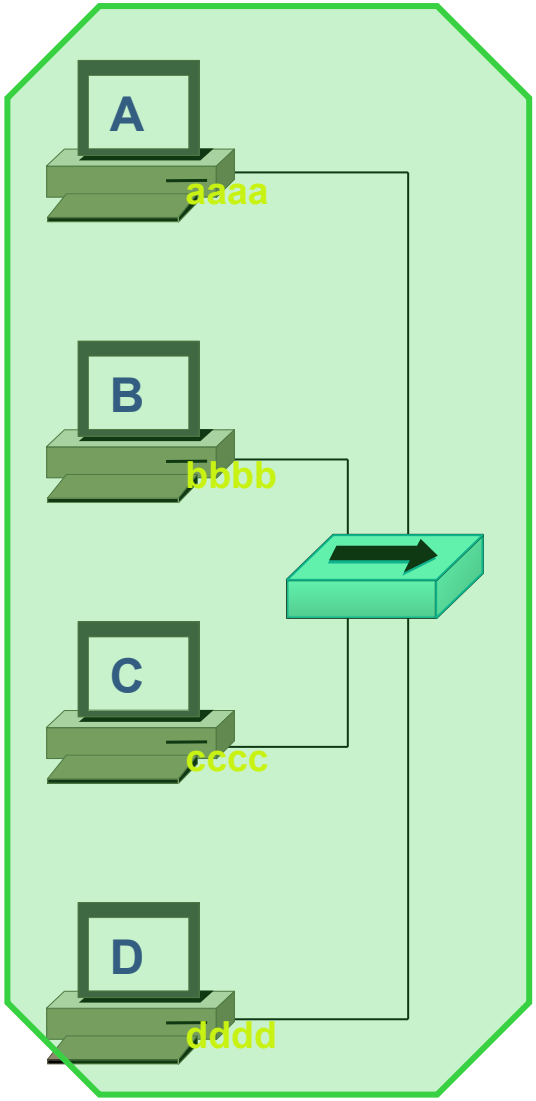
Combien de domaines de collision?



Un seul



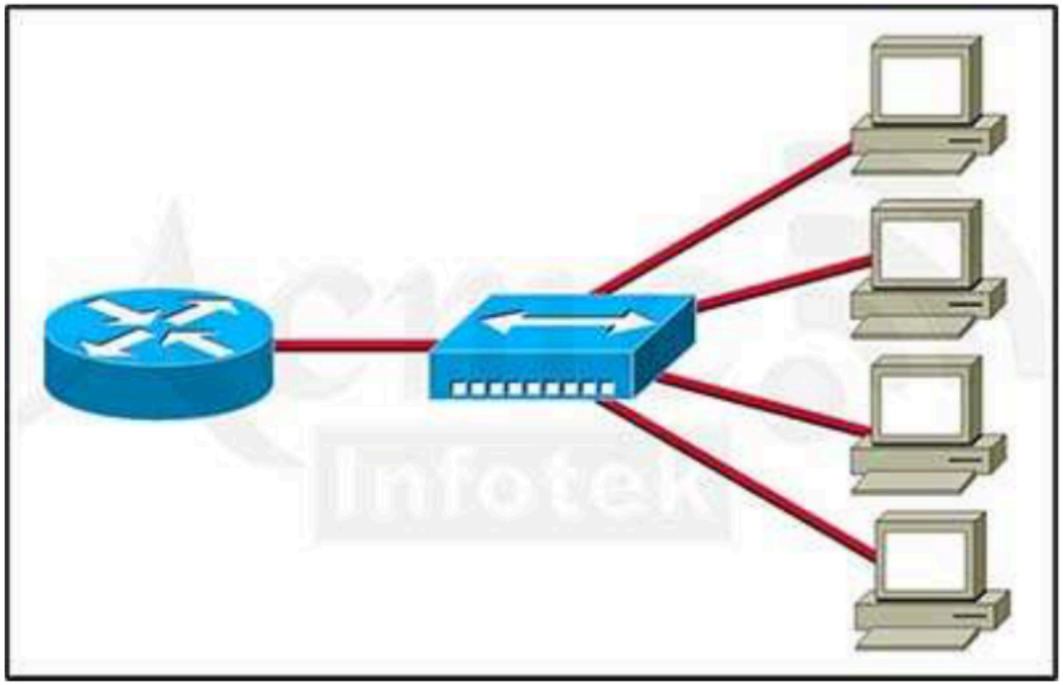
Domaine de broadcast



- Un équipement placs autour d'un HUB reçoit les broadcasts de tous les équipements placés autour de ce HUB :

- Ils sont dans le même domaine de broadcast.

Test



- Combien de domaines de collision ?
- Combien de domaines de broadcast ?

- 1
- 1

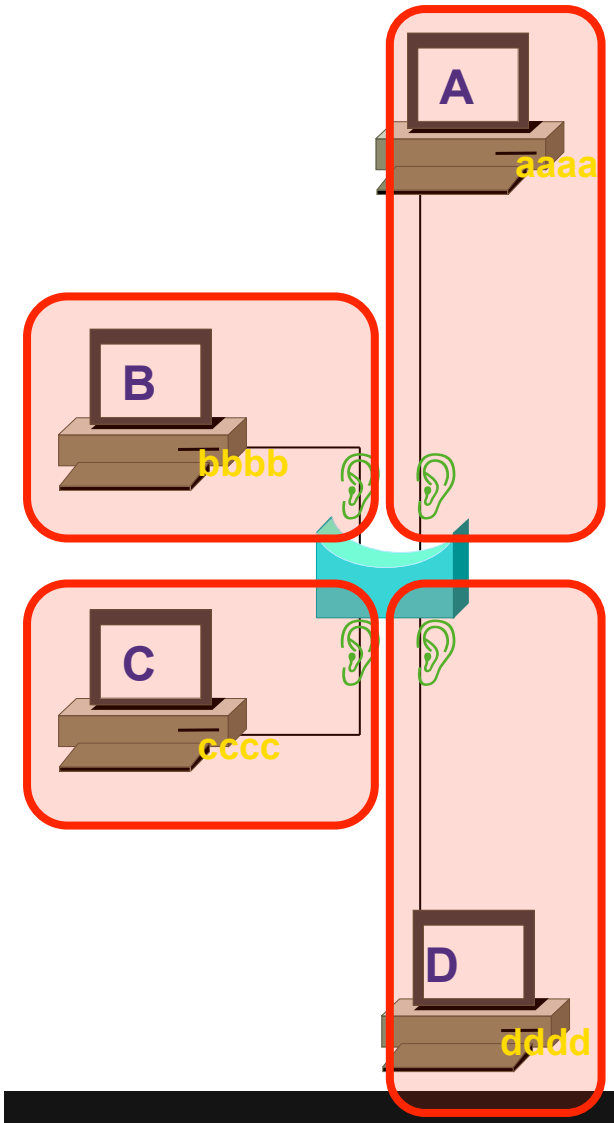
Ethernet

Le PONT

Fonctionnement du PONT

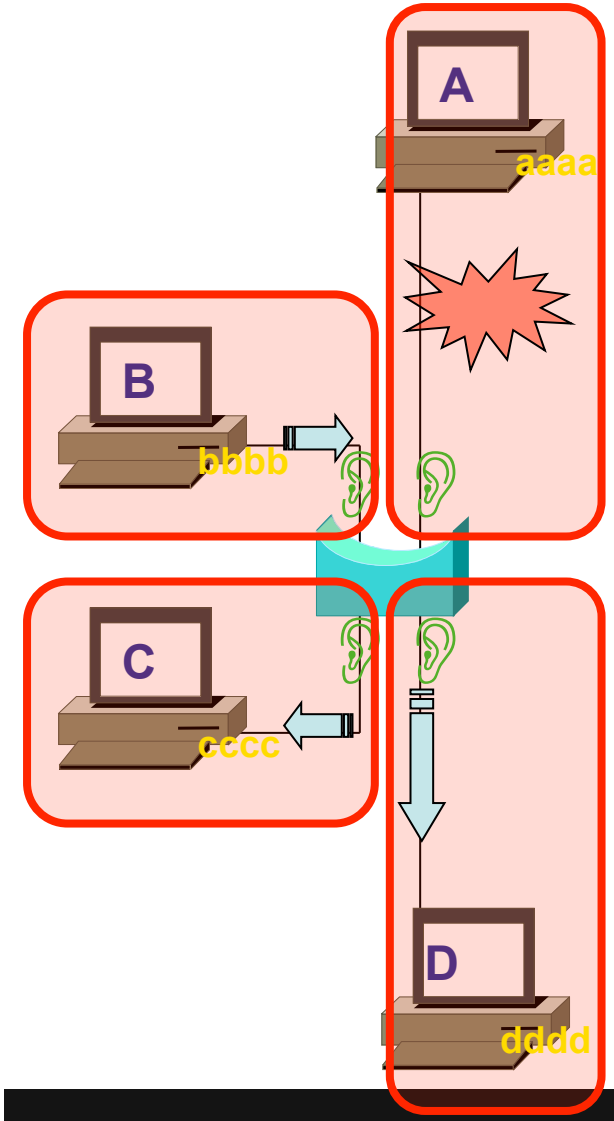
- Le PONT a une mémoire sur chaque interface.
  - Il est donc capable de conserver des trames dans cette mémoire, le temps que la voie devienne libre.
  - Il écoute sur chaque interface, avant de faire suivre une trame.
  - Les fragments restent confinés dans leur domaine de collisions.

Domaine de collision



- Il ne peut y avoir de collisions qu'entre les équipements placés sur un même port du PONT
- Chaque port possède son propre domaine de collision.

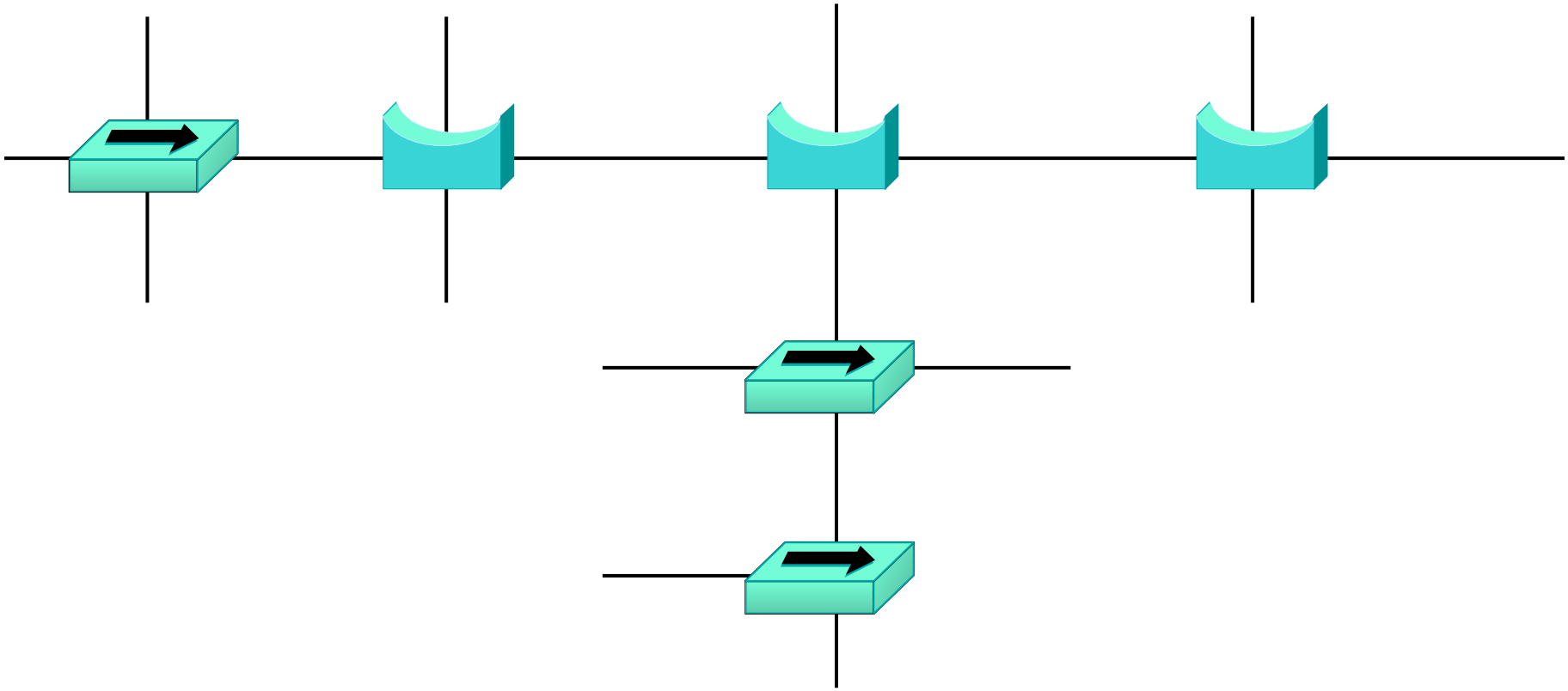
Domaine de collision



- Une collision sur un segment n'affecte pas les autres segments.
- Le pont a découpé le domaine de collision en plusieurs domaines de collision plus petits.

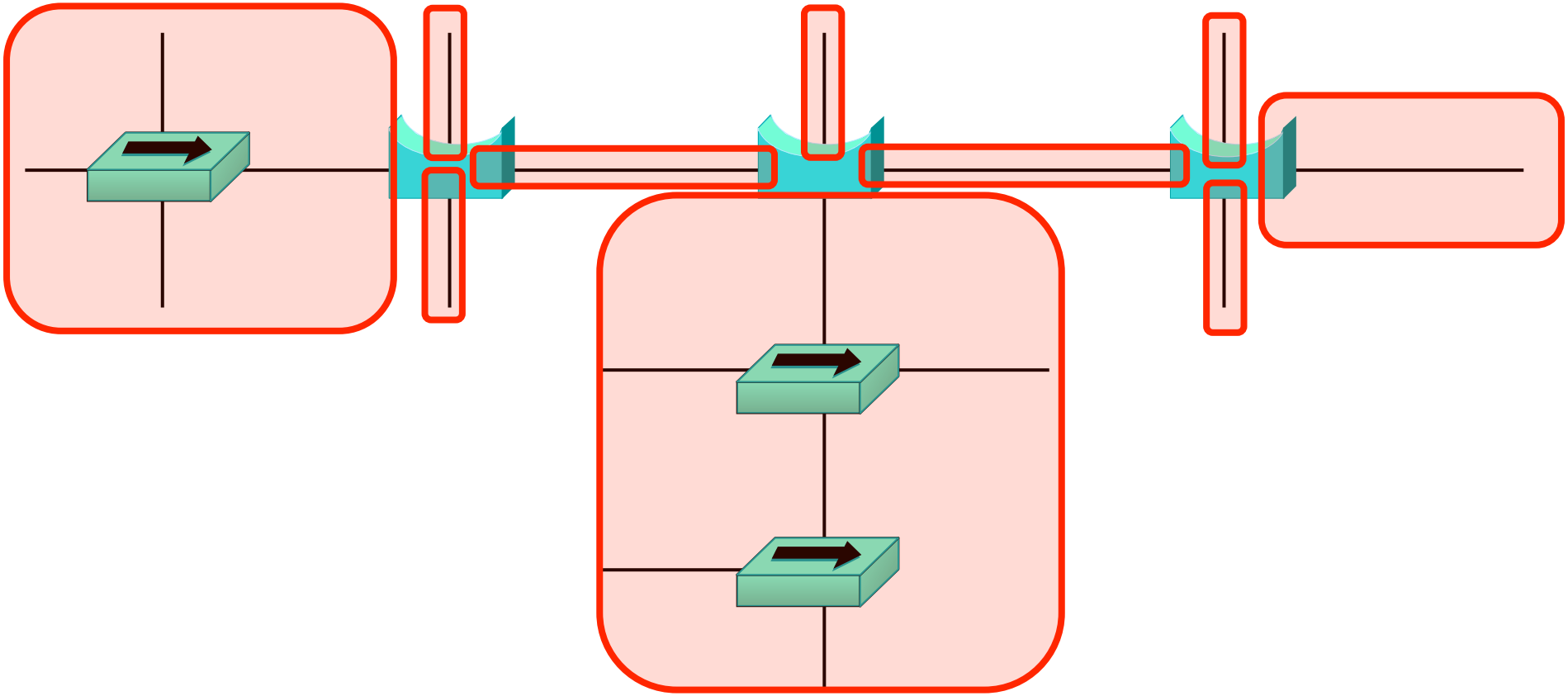
Exercice

Combien y a-t-il de domaines de collision ?



Solution

10 domaines de collision.



Fonctionnement du pont

Lorsqu'il reçoit une trame :

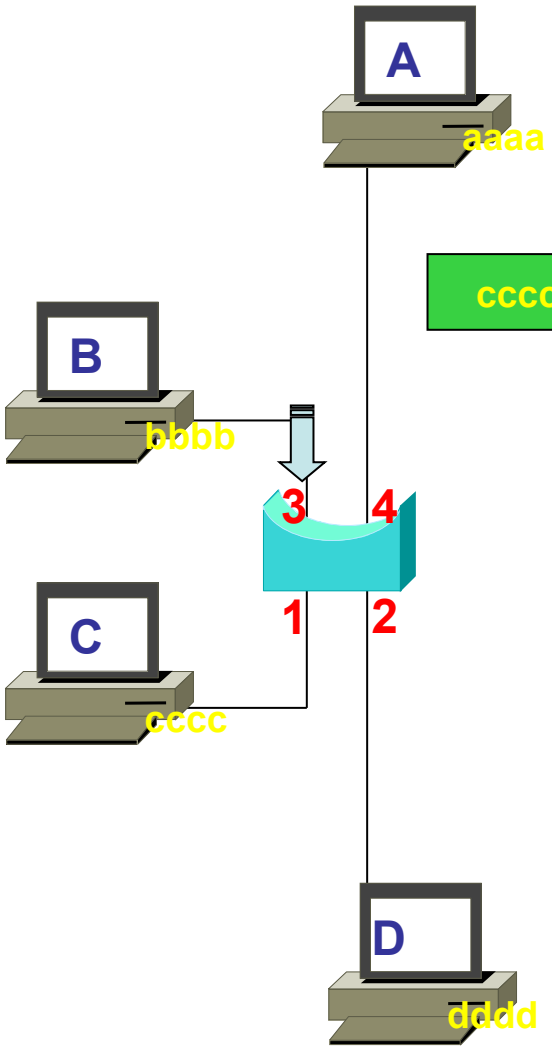
1. il regarde l'adresse MAC source de la trame et met à jour sa table

2. il cherche l'adresse MAC destination de la trame pour savoir sur quelle interface faire suivre la trame.

Fonctionnement du pont

- S'il ne trouve pas l'adresse Mac destination dans sa table :
  - il s'agit d'un 'unknown unicast'
  - il duplique la trame sur toutes ses interfaces, sauf celle où il l'a reçue.
  - C'est un unicast flooding
- Si l'adresse Mac de destination est broadcast (FFFF.FFFF.FFFF) ou multicast :
  - il duplique la trame sur toutes ses interfaces, sauf celle où il l'a reçue.

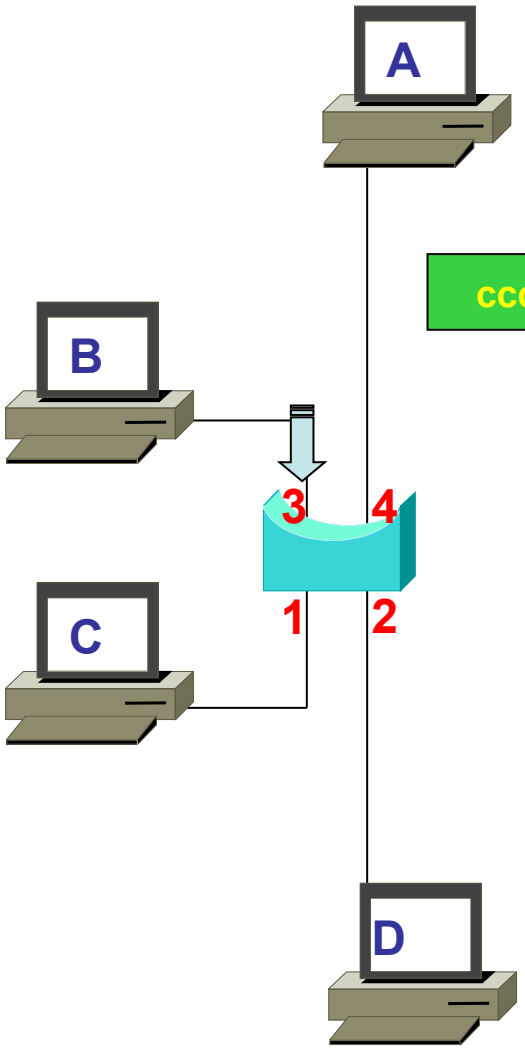
Exercice 1



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface

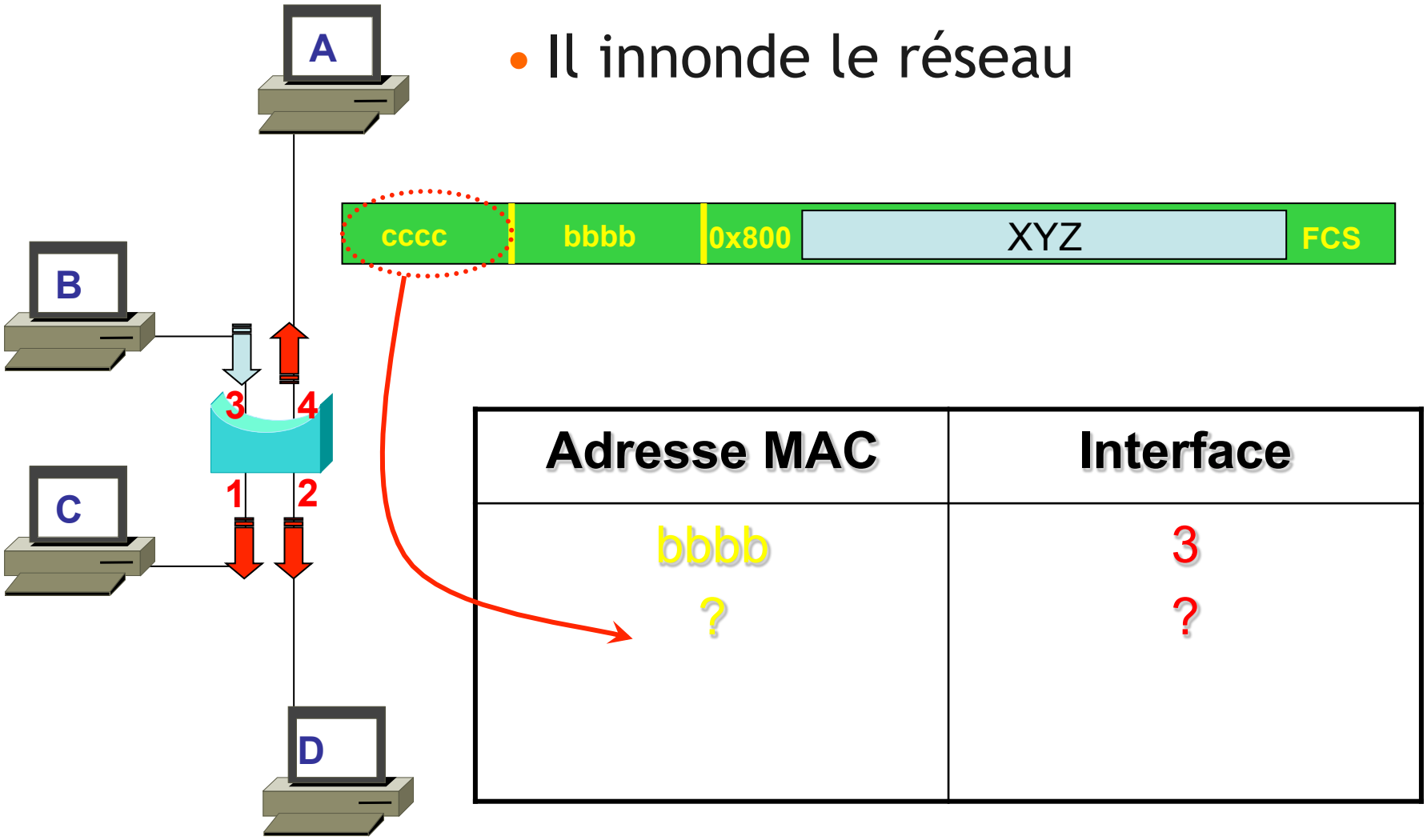
Solution 1



- Il met à jour sa table avec l' adresse Mac SOURCE

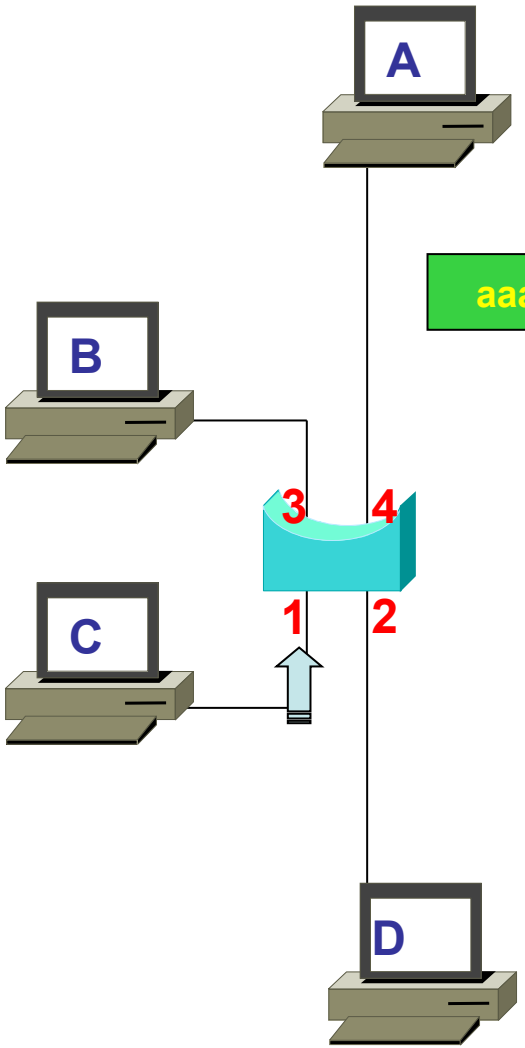
Adresse MAC	Interface
bbbb	3

Solution 1, suite



- Il innonde le réseau

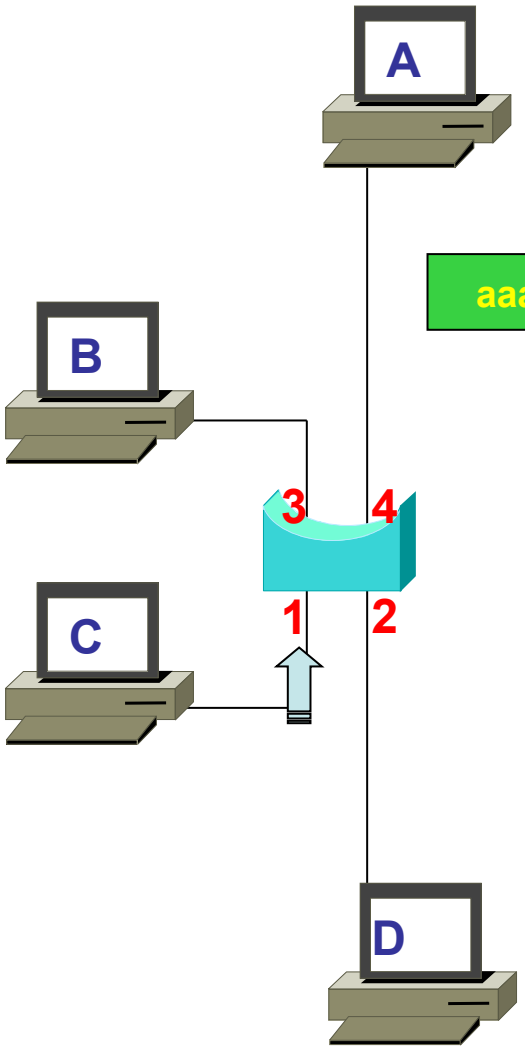
Exercice 2



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
bbbb	3

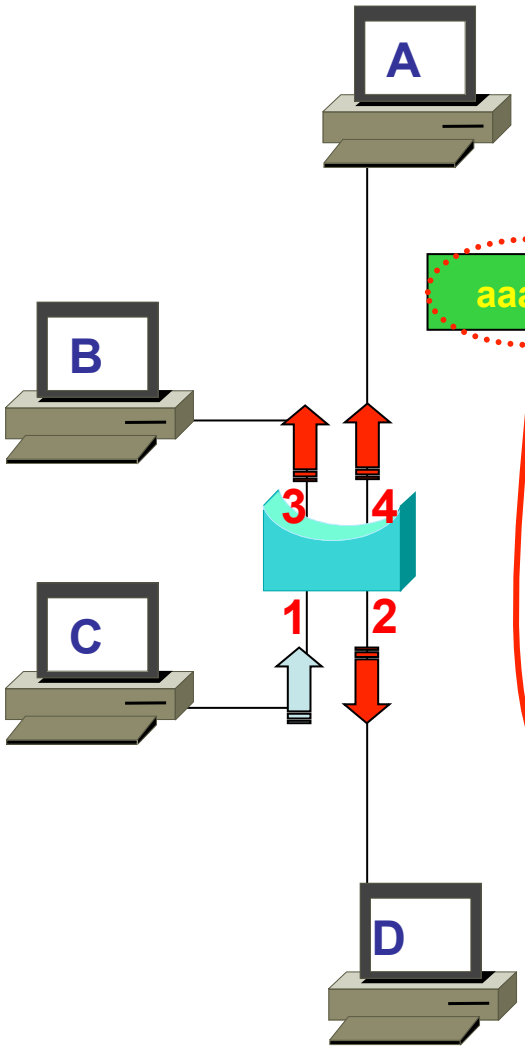
Solution 2



- Il met à jour sa table avec l' adresse Mac SOURCE

Adresse MAC	Interface
bbbb	3
cccc	1

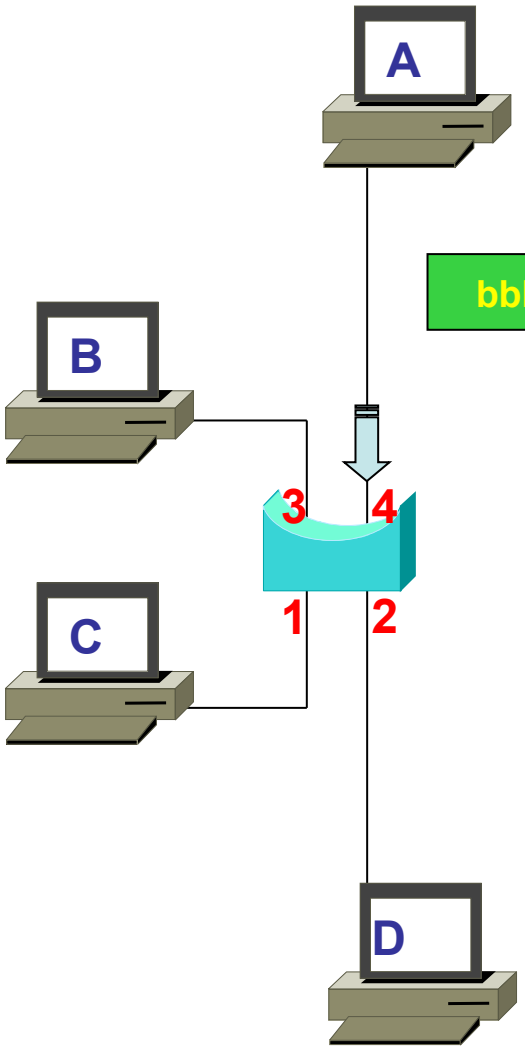
Solution 2, suite



- Il innonde le réseau

Adresse MAC	Interface
bbbb	3
cccc	1
?	?

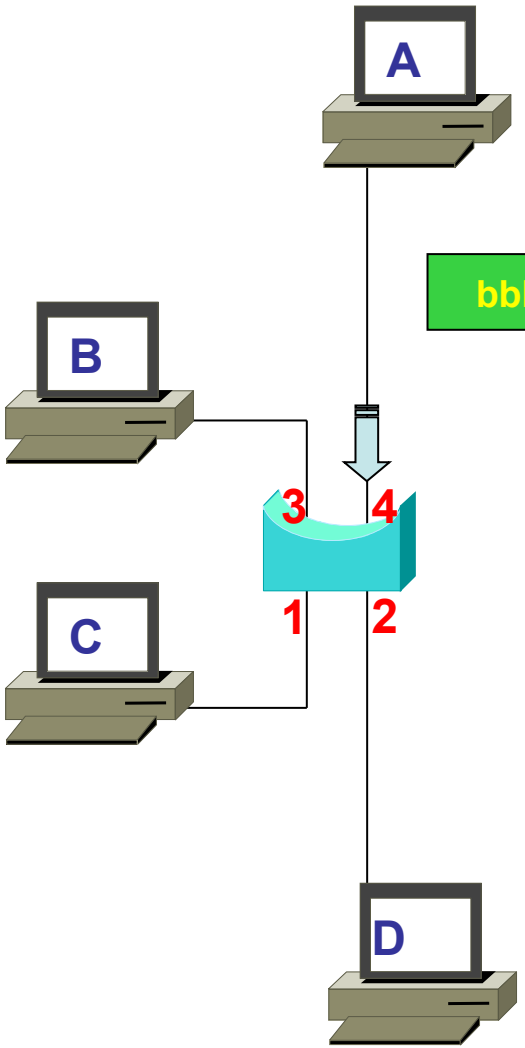
Exercice 3



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
bbbb	3
cccc	1

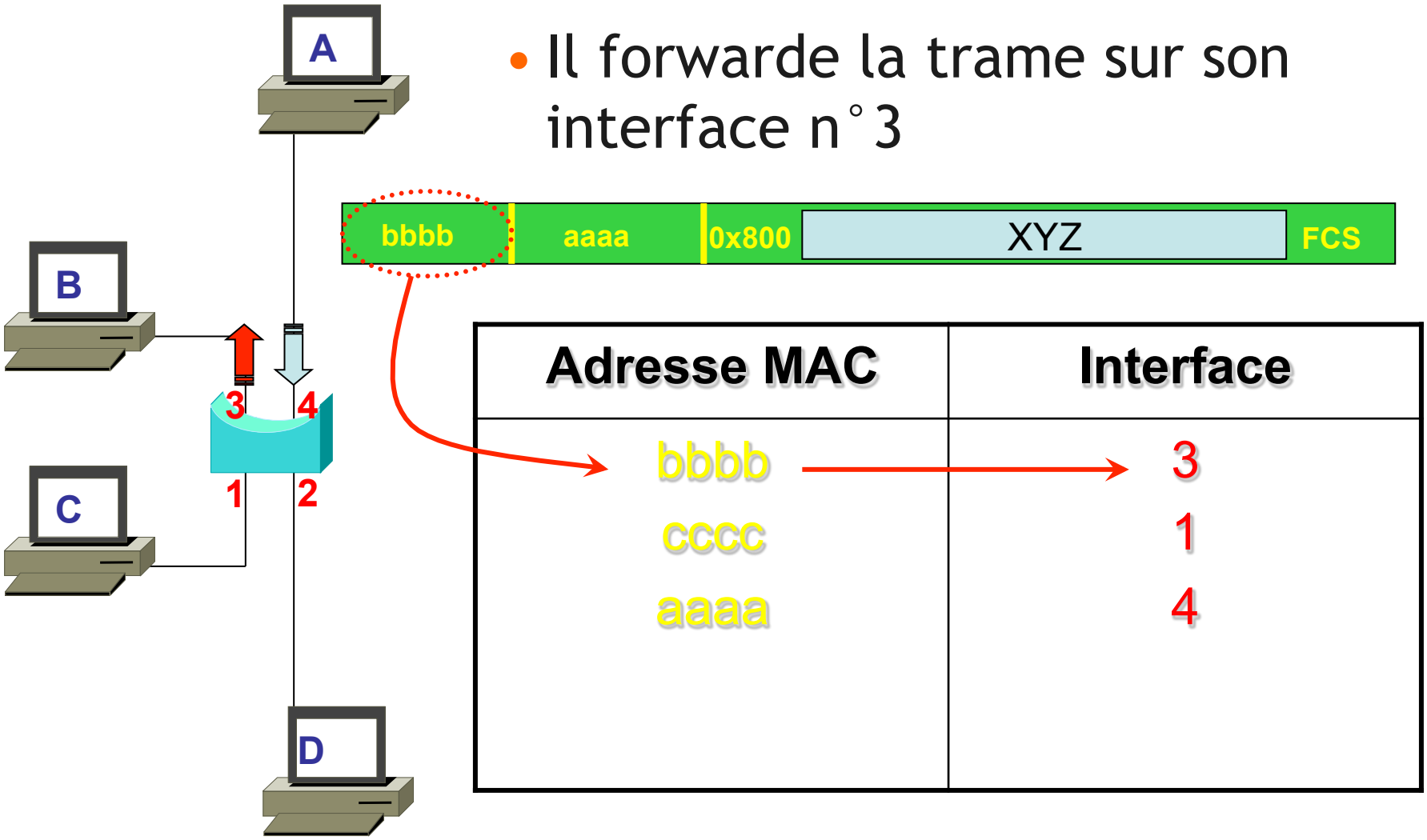
Solution 3



- Il met à jour sa table avec l'adresse Mac SOURCE

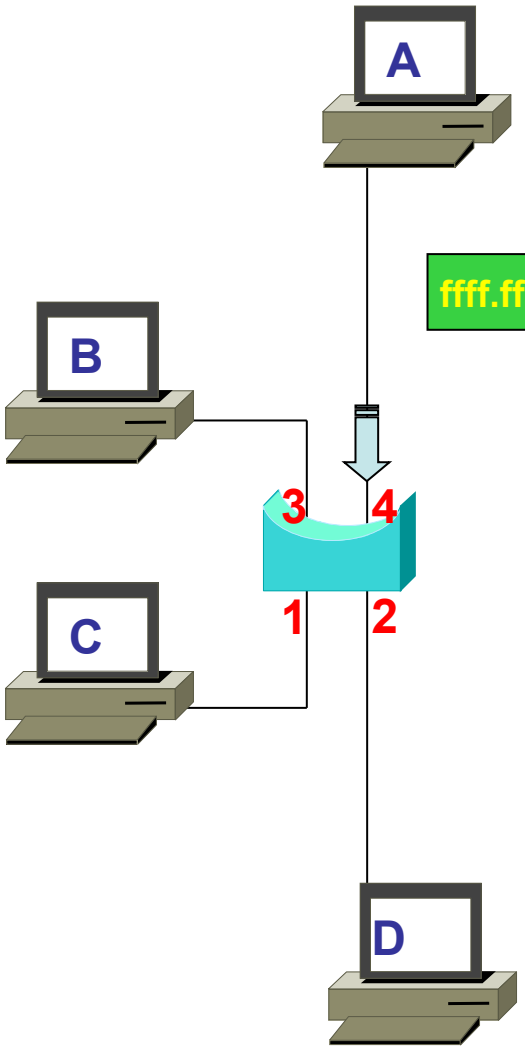
Adresse MAC	Interface
bbbb	3
cccc	1
aaaa	4

Solution 3, suite



- Il forwarde la trame sur son interface n°3

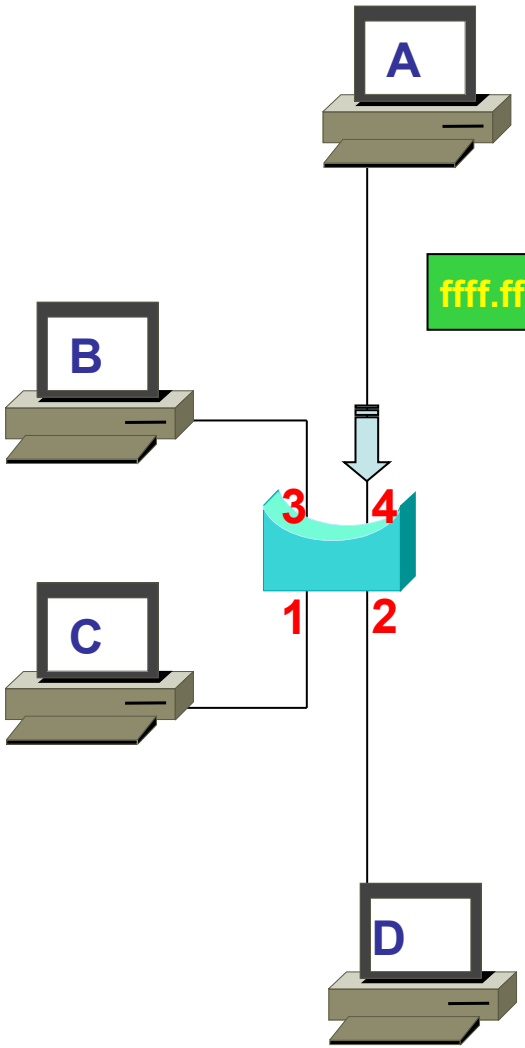
Exercice 4



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
bbbb	3
cccc	1
aaaa	4

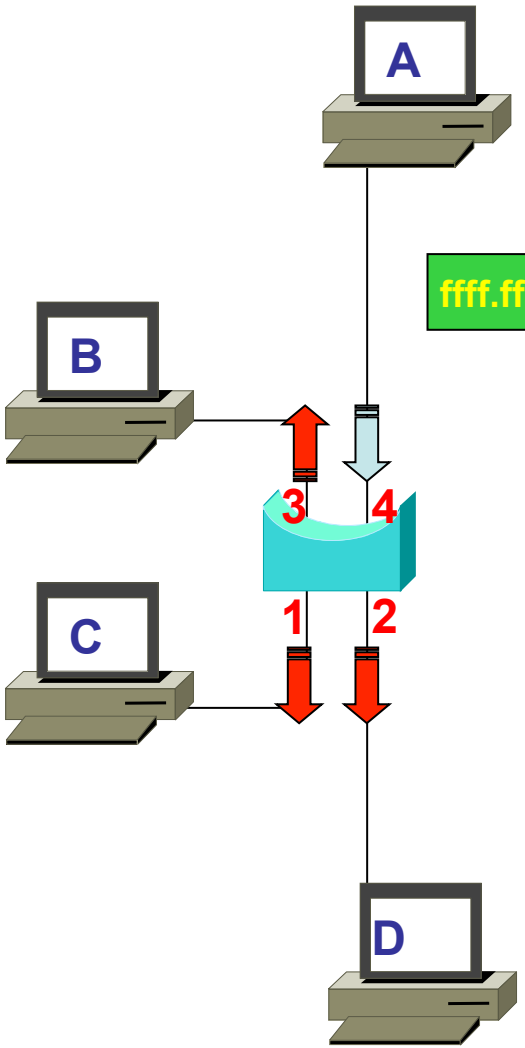
Solution 4



- Il met à jour le timer de sa table pour l'adrersse aaaa.

Adresse MAC	Interface	Timer
bbbb	3	250
cccc	1	244
aaaa	4	300

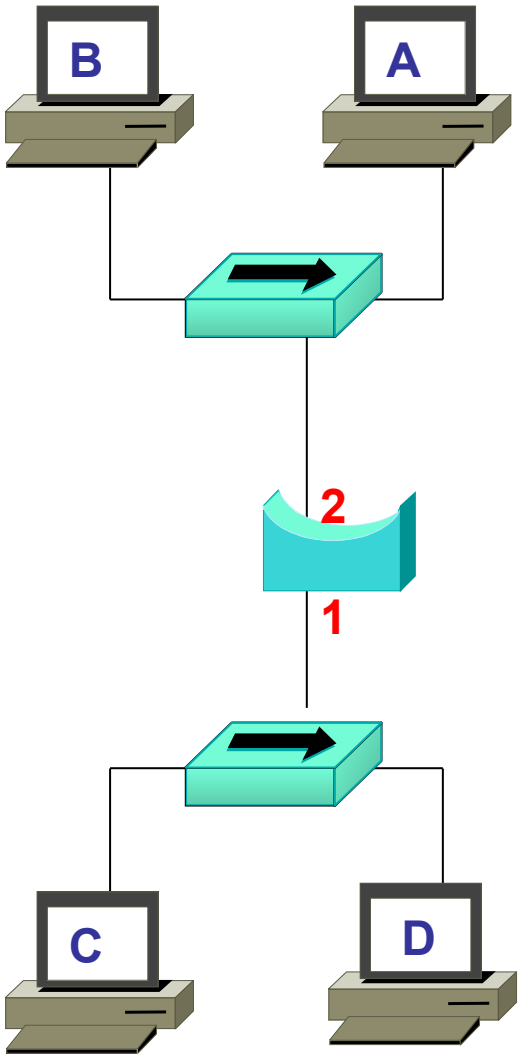
Solution 4, suite



- Il innonde le réseau.

Adresse MAC	Interface	Timer
bbbb	3	250
cccc	1	244
aaaa	4	300

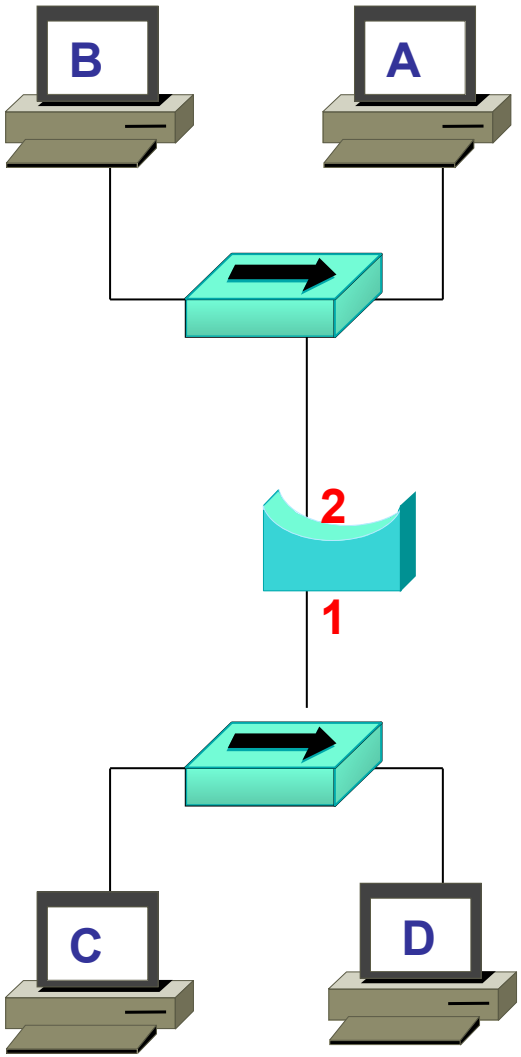
Exercice 5



- Que contient la table d'adresses Mac quand tout le monde a parlé ?

Adresse MAC	Interface

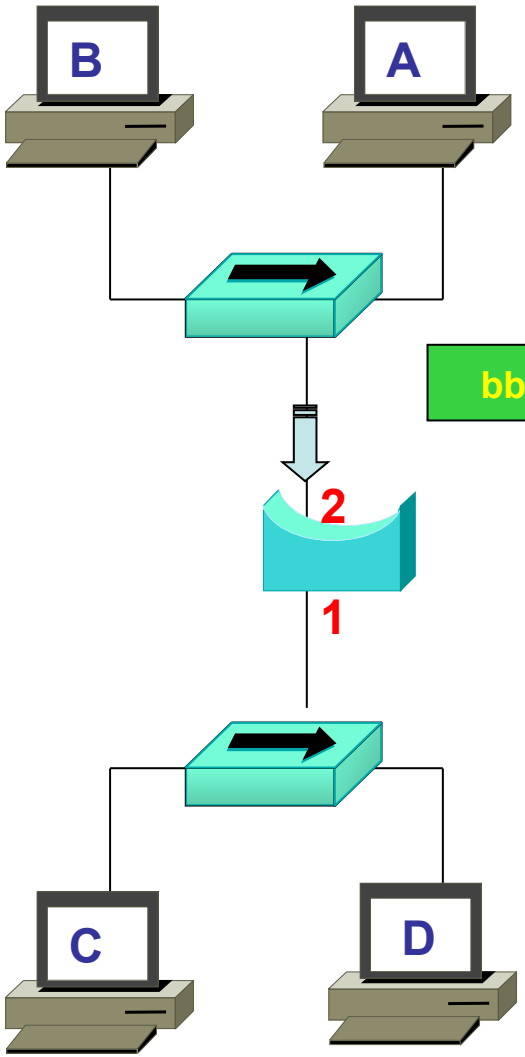
Solution 5



- Que contient la table d'adresses Mac quand tout le monde a parlé ?

Adresse MAC	Interface
aaaa	2
bbbb	2
cccc	1
dddd	1

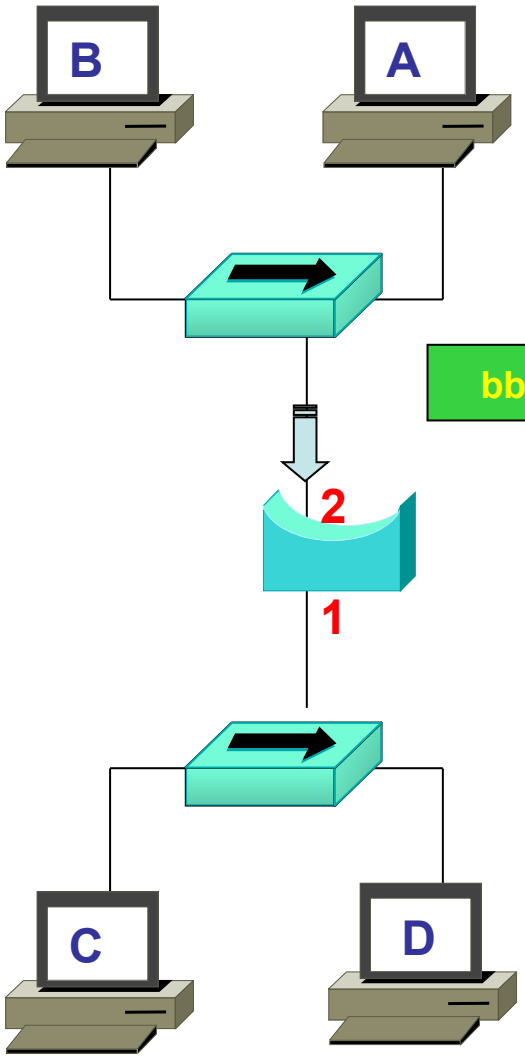
Exercice 6



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
aaaa	2
bbbb	2
cccc	1
dddd	1

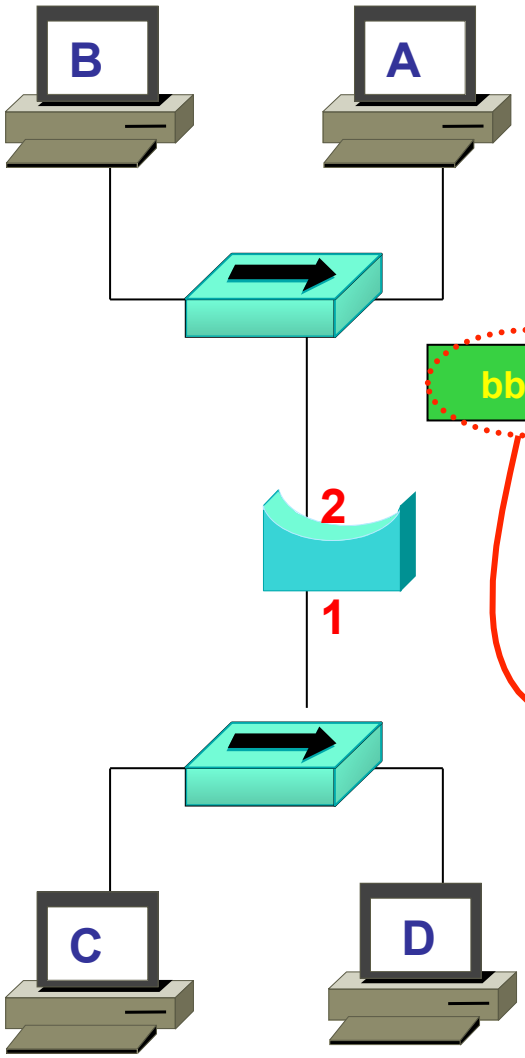
Solution 6



- Il met à jour le timer de sa table pour l'adresse aaaa.

Adresse MAC	Interface	Timer
aaaa	2	300
bbbb	2	250
cccc	1	111
dddd	1	222

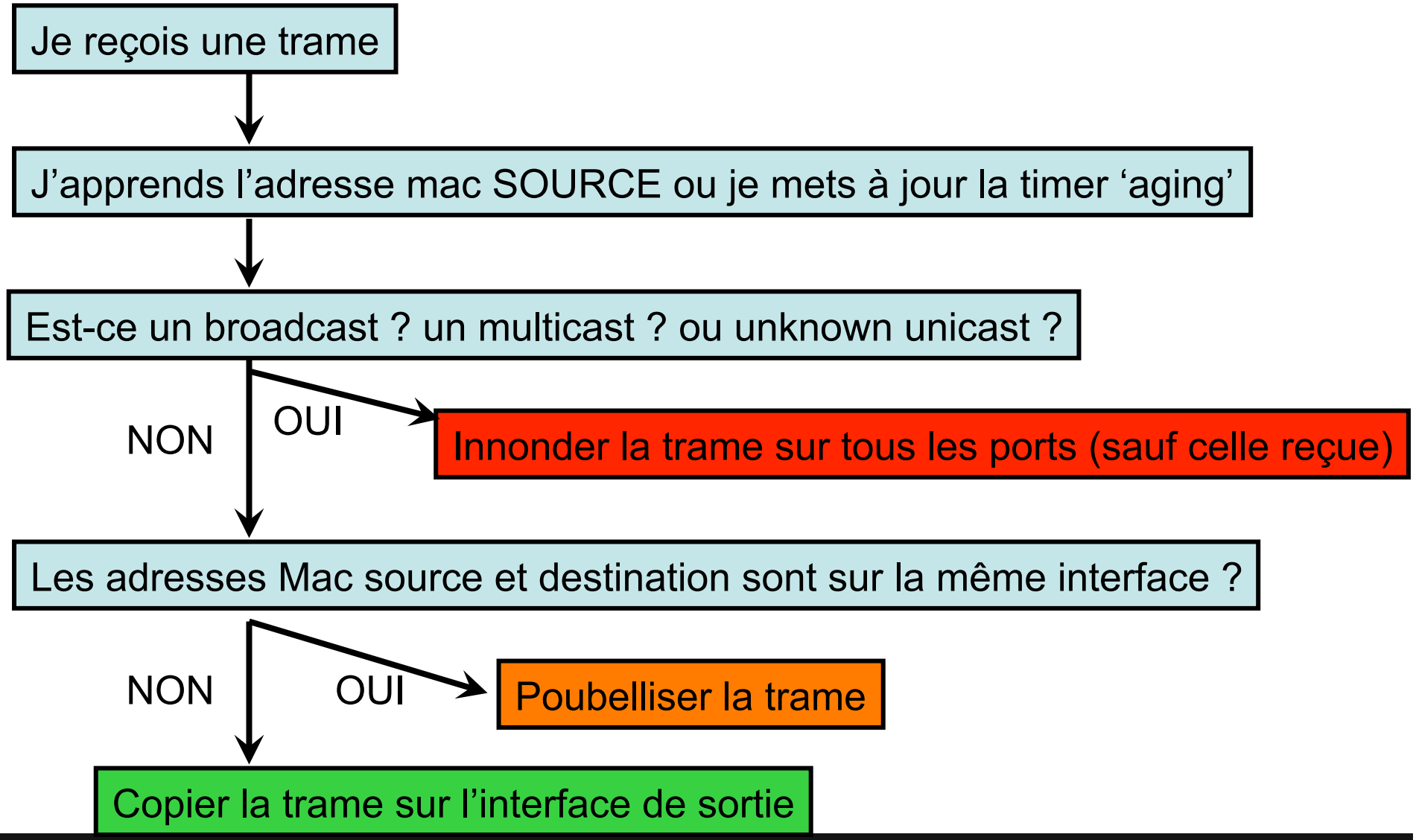
Solution 6, suite



- Il poubellise la trame, car B l'a déjà reçue !

Adresse MAC	Interface	Timer
aaaa	2	300
bbbb	2	250
cccc	1	111
dddd	1	222

Bilan : l'algorithme 802.3



Test

- Que fera le switch s'il reçoit une trame avec @ destination 00b0.d056.efa4 ?

```
Switch-1# show mac address-table
Dynamic Addresses Count:                   3
Secure Addresses (User-defined) Count:     0
Static Addresses (User-defined) Count:     0
System Self Addresses Count:               41
Total Mac addresses:                       50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic       1     FastEthernet0/1
0010.7b00.1540       Dynamic       2     FastEthernet0/3
0010.7b00.1545       Dynamic       2     FastEthernet0/2
```

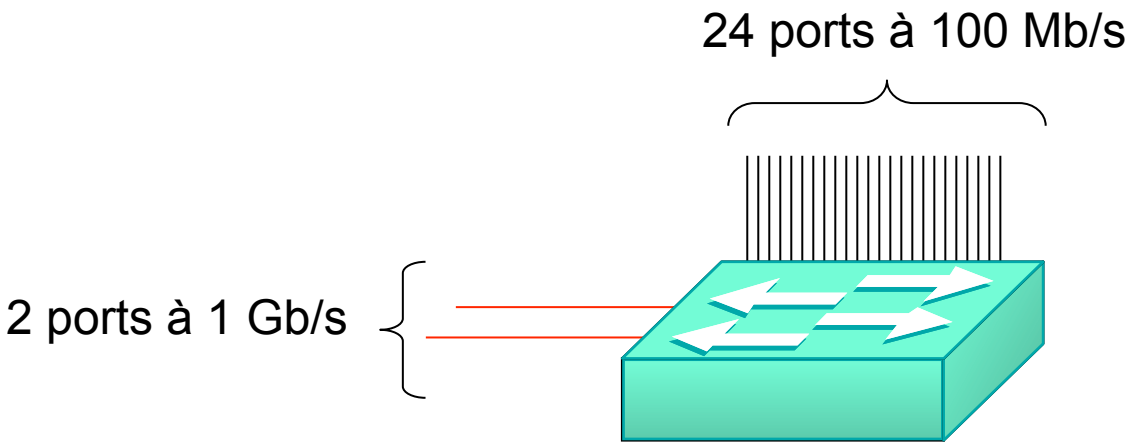
Ethernet

Le switch ou commutateur

Avantages du switch

- Collisions :
  - fonctionne comme le pont
- Table de Mac addresses :
  - fonctionne comme le pont
- Nombre de ports :
  - peut avoir de nombreux ports !
    - plusieurs cartes de 48 ports chacuns
  - tous les ports n'ont pas obligatoirement la même vitesse
    - sur la même carte, des ports à 100 Mb/s, 1 Gb/s, 10 Gb/s
- Rapidité :
  - beaucoup plus rapide que le pont
    - utilise des ASICs :Application Specific Integrated Circuits.

La diversité du ‘speed’



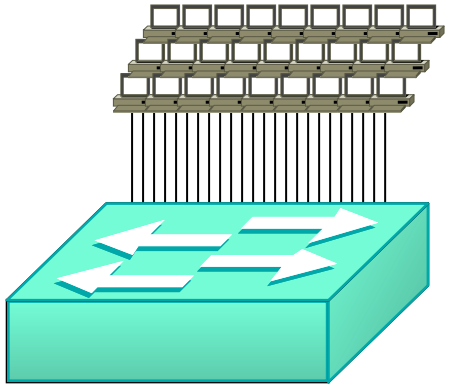
Les ports à 1 Gb/s sont appelés ‘uplink’.

Ils sont reliés à d’autres switch et permettent d’aggréger le trafic reçu sur pluseurs ports à 100 Mb/s

La densité de ports

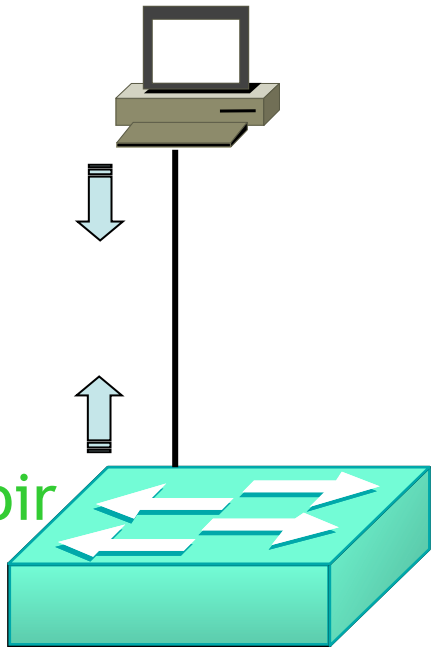
- Le switch a beaucoup de ports.
- Il devient possible de ne mettre qu'un seul équipement (PC, imprimante, serveur) sur chaque port du switch.

Micro-segmentation :



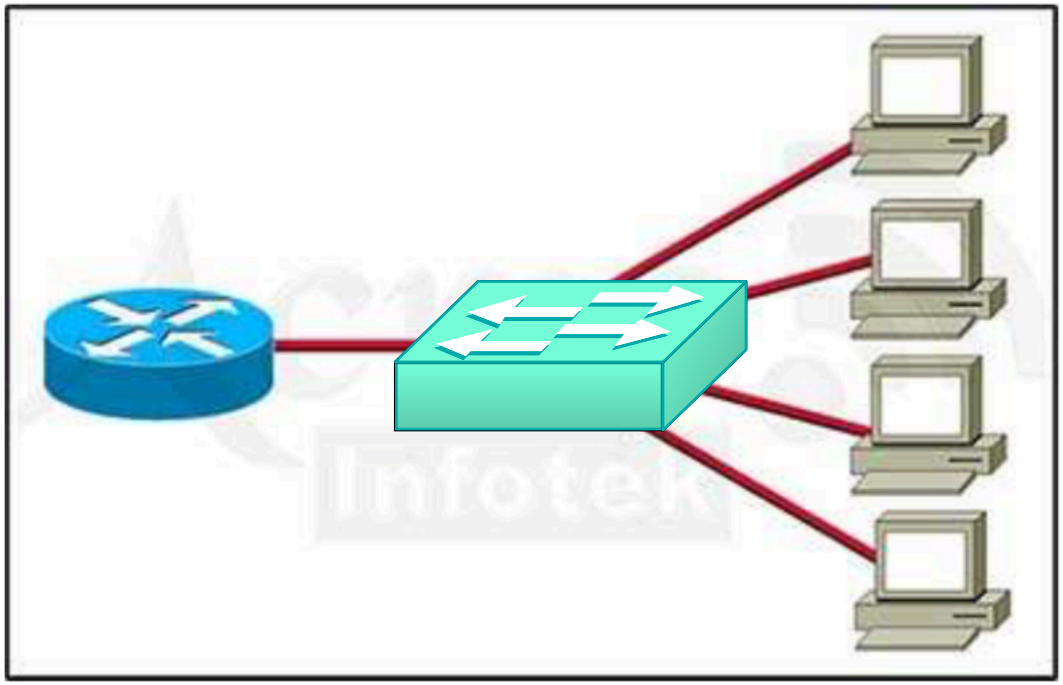
Full-duplex

- S'il n'y a que 2 équipements sur un même segment (*), alors il n'y a pas de collision :
  - pas de CSMA / CD
  - chaque équipement peut émettre et recevoir en même temps



(*) et si les 2 cartes réseau savent fonctionner en full-duplex

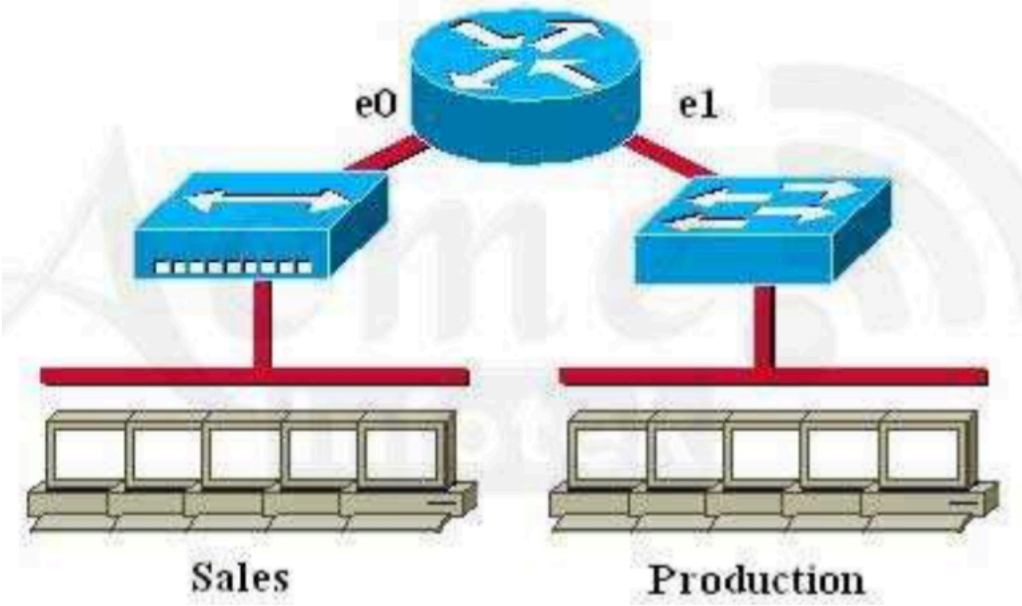
Test



- Combien de domaines de collision ?
- Combien de domaines de broadcast ?

- 5
- 1

Test

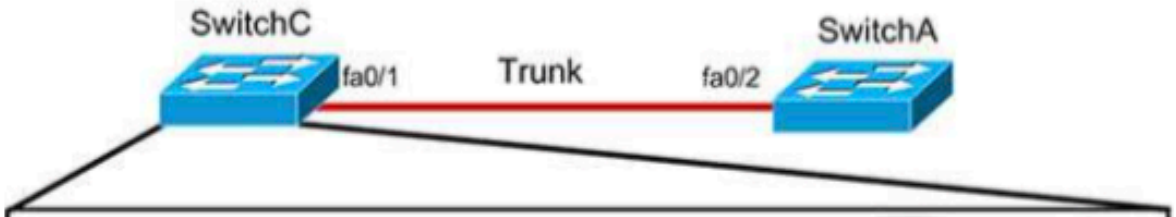


- Combien de domaines de collision ?
- Combien de domaines de broadcast ?

- 7
- 2

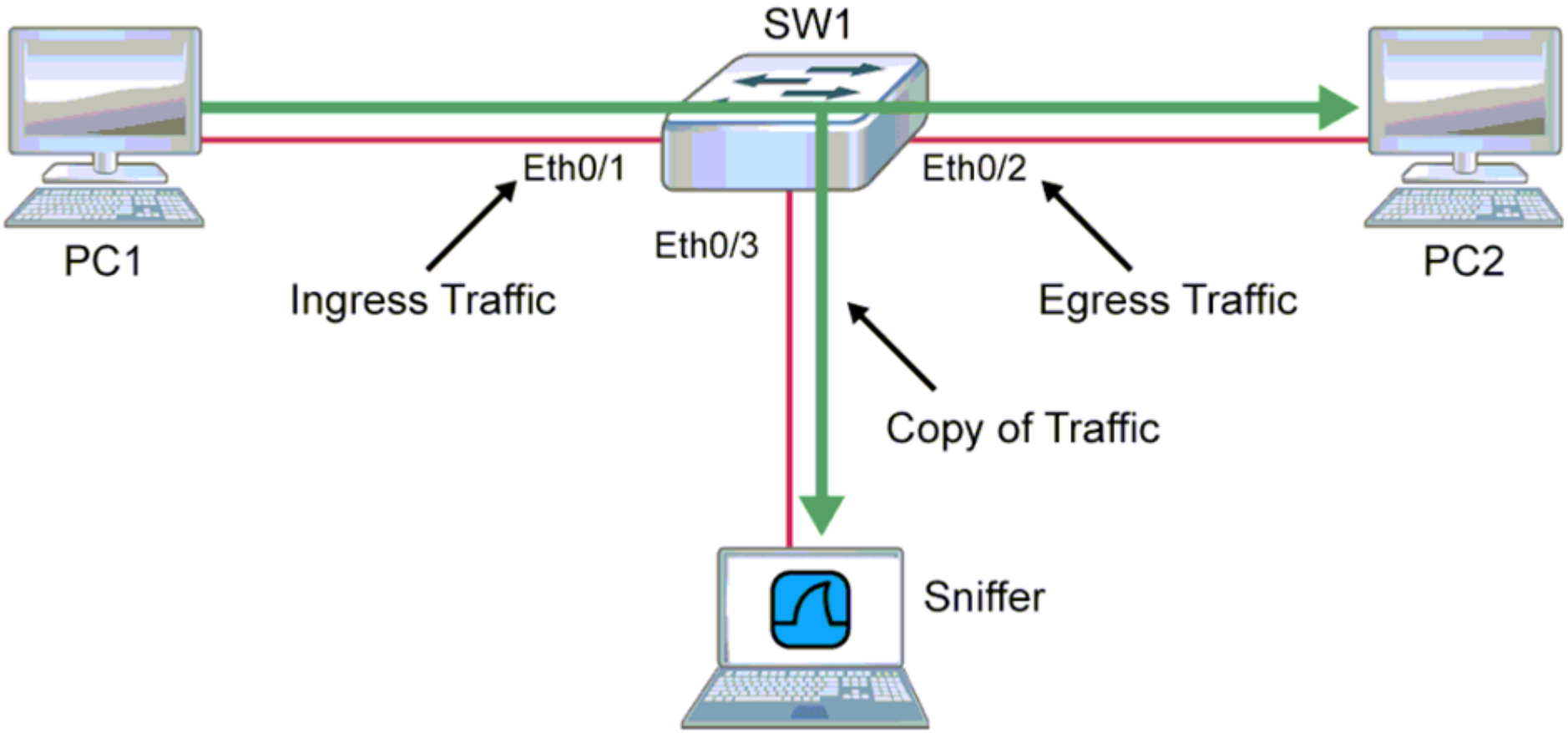
Duplex mismatch

- Un côté en Full-duplex (C) – CRC
- L'autre côté en Half-duplex (A) – Late collision

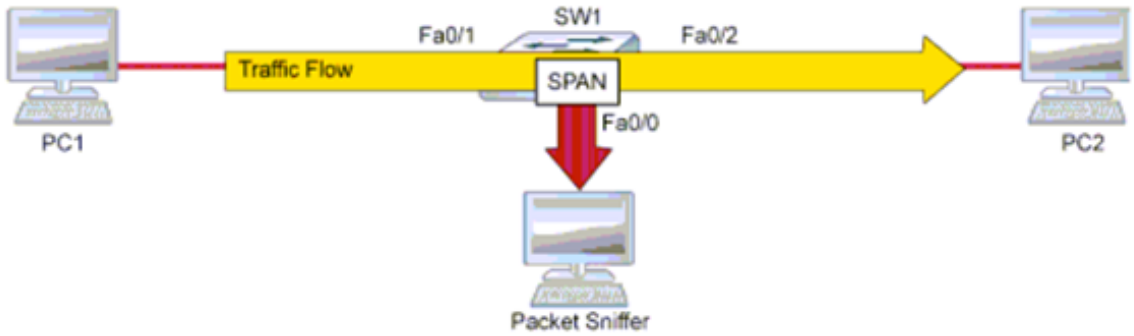



```
SwitchC# show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0013.8030.5e83
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 14/255, rxload 14/255
  Encapsulation ARPA, Loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
• Text omitted
  5 minute input rate 364000 bits/sec, 344 packets/sec
  5 minute output rate 367000 bits/sec, 338 packets/sec
     16973 packets input, 2400313 bytes, 0 no buffer
     Received 1244 broadcasts (0 multicast)
     0 runts, 3 giants, 0 throttles
     741 input errors, 738 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 1243 multicast, 0 pause input
    0 input packets with dribble condition detected
    16420 packets output, 2375034 bytes, 0 underruns
• Text omitted
```

Redirection de ports (Source Port Analyser)



Redirection de ports SPAN



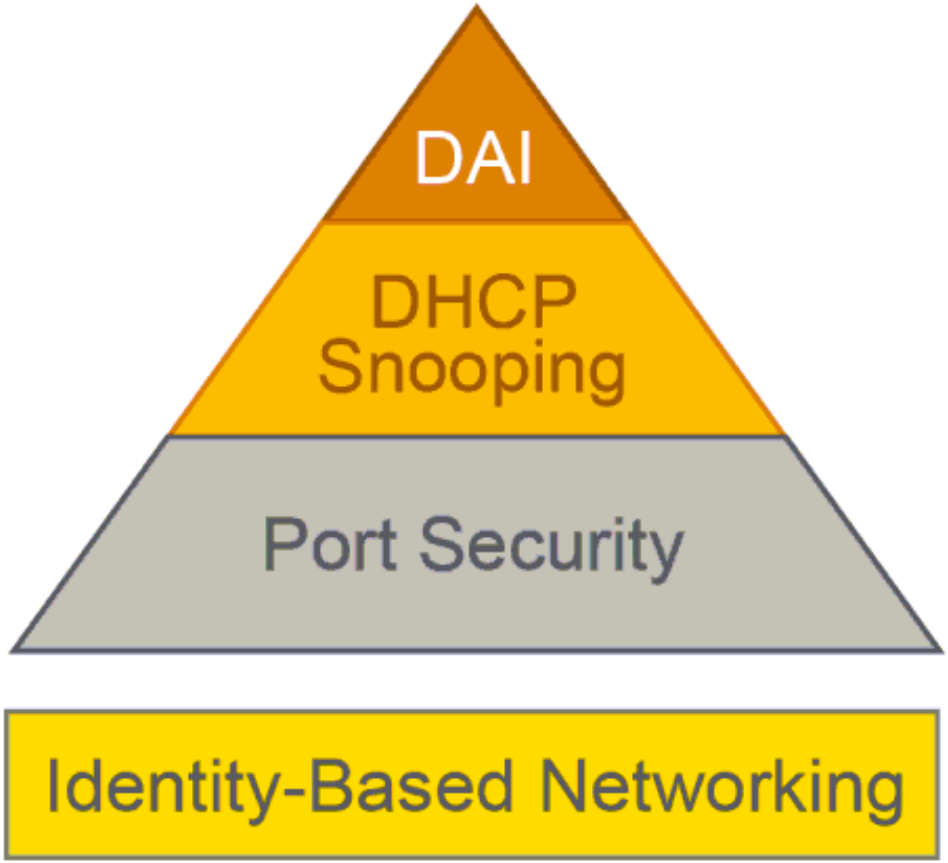

```
SW1(config)# monitor session 1 source interface FastEthernet0/2 both
SW1(config)# monitor session 1 destination interface FastEthernet0/0
```

Sécurité des accès

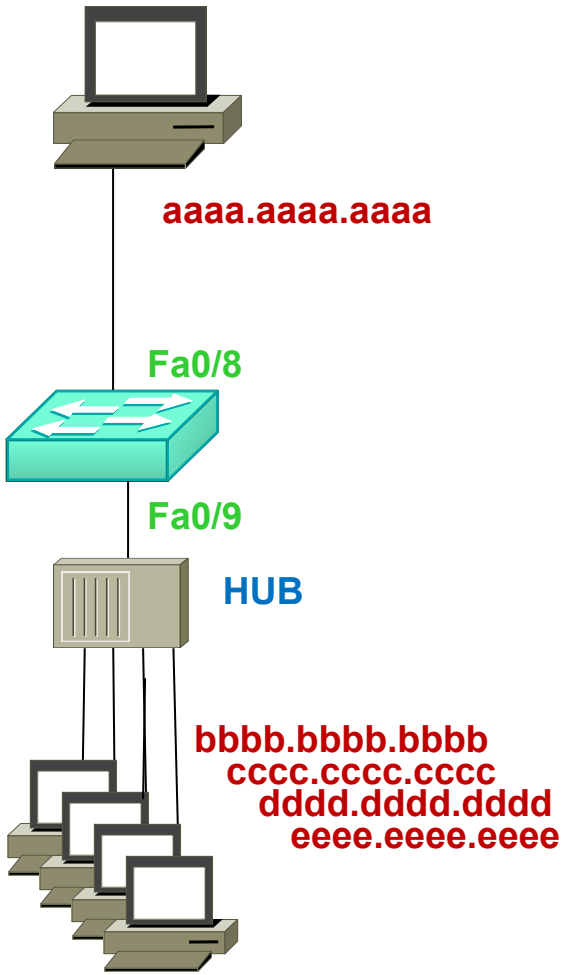
Mitigating Threats at Access Layer

You can mitigate most access layer threats with these features:

- **Port security:** Restricting a port to a specific set of MAC addresses
- **DHCP snooping:** Preventing rogue DHCP servers
- **Dynamic ARP Inspection (DAI):** Preventing ARP attacks
- Also, implement **identity-based networking** to protect network resources and provide user mobility.

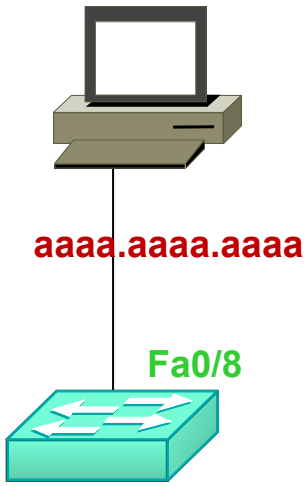


Port Security : Objectif



- Seul l'équipement dont l'adresse MAC est aaaa.aaaa.aaaa est autorisé à se connecter au port Fa0/8
- Possible de configurer plusieurs MAC en présence d'un HUB
- Impossible à configurer sur les ports :
  - Trunk Dynamic
  - EtherChannel (aggrégation de liens)
  - Voice VLAN (sur les port de téléphones IP)

Méthode n°1




```
configure terminal

interface fa0/8

switchport port-security mac-address aaaa.aaaa.aaaa
```

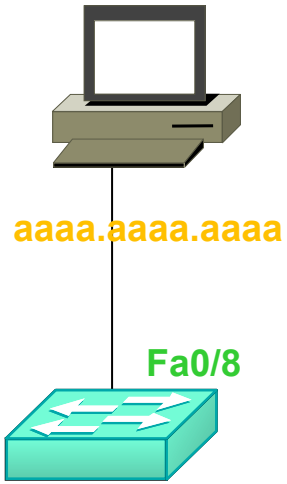
➔ n' autoriser que cette adresse Mac.

`switchport port-security`

➔ activer la fonctionalité 'port-security'.

méthode fastidieuse :
il faut saisir chaque adresse Mac !

Méthode n°2




```
configure terminal
interface fa0/8
switchport port-security maximum 1
```

➔ n'autoriser qu'une seule adresse Mac

`switchport port-security`

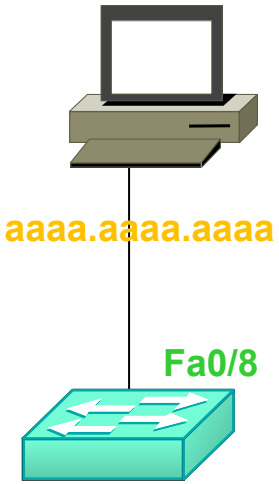
➔ activer la fonctionalité 'port-security'

Si aucune adresse Mac n'est configurée statiquement :

➔ la première trame reçue fixera l'adresse Mac autorisée.

méthode dangeureuse :
il suffit de couper le courant et le switch acceptera l'adresse Mac de tout nouvel équipement connecté au port Fa0/8 !

Méthode n°3




```
configure terminal
interface fa0/8
switchport port-security maximum 1
```

➔ n'autoriser qu'une seule adresse Mac

```
switchport port-security mac-address sticky
```

➔ autoriser l'adresse Mac de la 1ère trame reçue

➔ et enregistrer cette adresse dans la mémoire ('running-config')

```
switchport port-security
```

➔ activer la fonctionalité 'port-security'

penser à sauvegarder la configuration :
`write` ou `write memory` ou `copy run start`

Trois modes de violation

- Si le switch reçoit une trame dont l'adresse Mac source n'est pas autorisée :
  - il peut couper l'interface
    - l'interface se trouve en état 'error-disabled'
    - personne ne pourra alors utiliser cette interface, même les adresses Mac autorisées
    - l'administrateur devra saisir shutdown puis no shutdown pour réactiver l'interface
    - on peut aussi configurer le switch pour réactiver l'interface demanière automatique au bout d'un certain temps
  - il peut détruire la trame et informer l'administrateur :
    - via un message à la console
    - via un message à une serveur SNMP
  - il peut détruire la trame sans informer l'administrateur

Configurer les modes de violation

```
configure terminal
interface fa0/8
switchport port-security violation shutdown
```

➔ couper l'interface

➔ mode par défaut

```
switchport port-security violation restrict
```

➔ détruire les trames interdites et informer

```
switchport port-security violation protect
```

➔ détruire les trames interdites sans informer

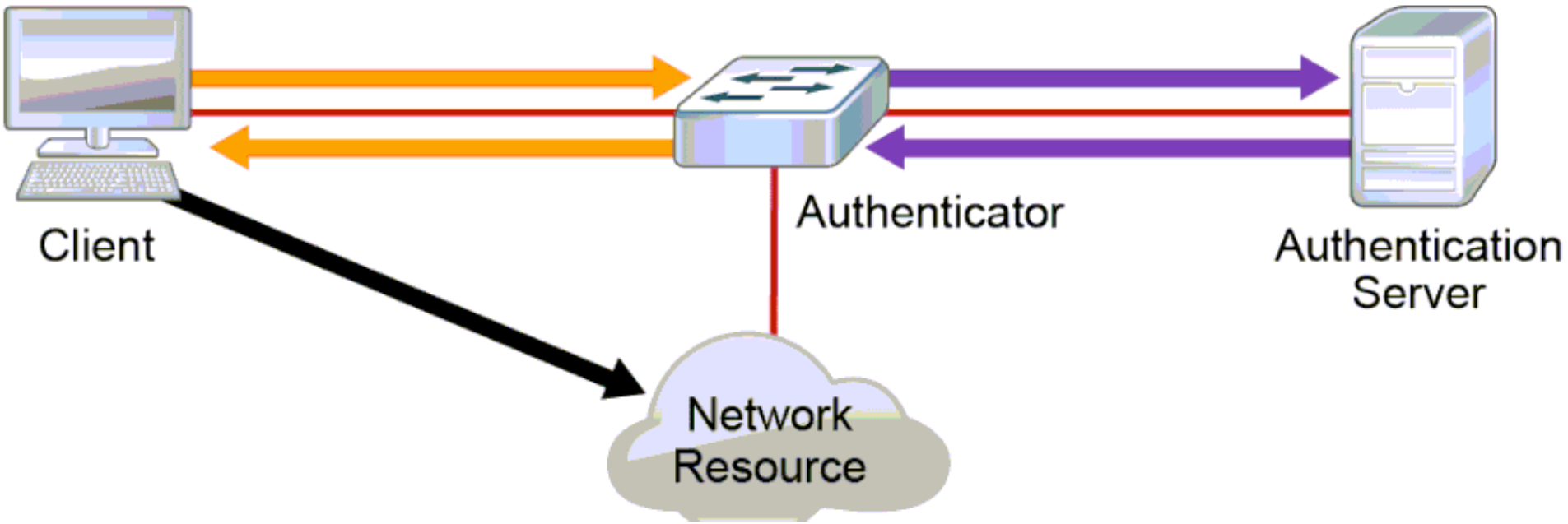
Suite à une violation

```
Switch# show interfaces f0/13

FastEthernet0/13 is down, line protocol is down (err-
disabled)

  Hardware is Fast Ethernet, address is 0099.1234.1234
(bia 0099.1234.1234)

  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

     reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation ARPA, loopback not set

...
```

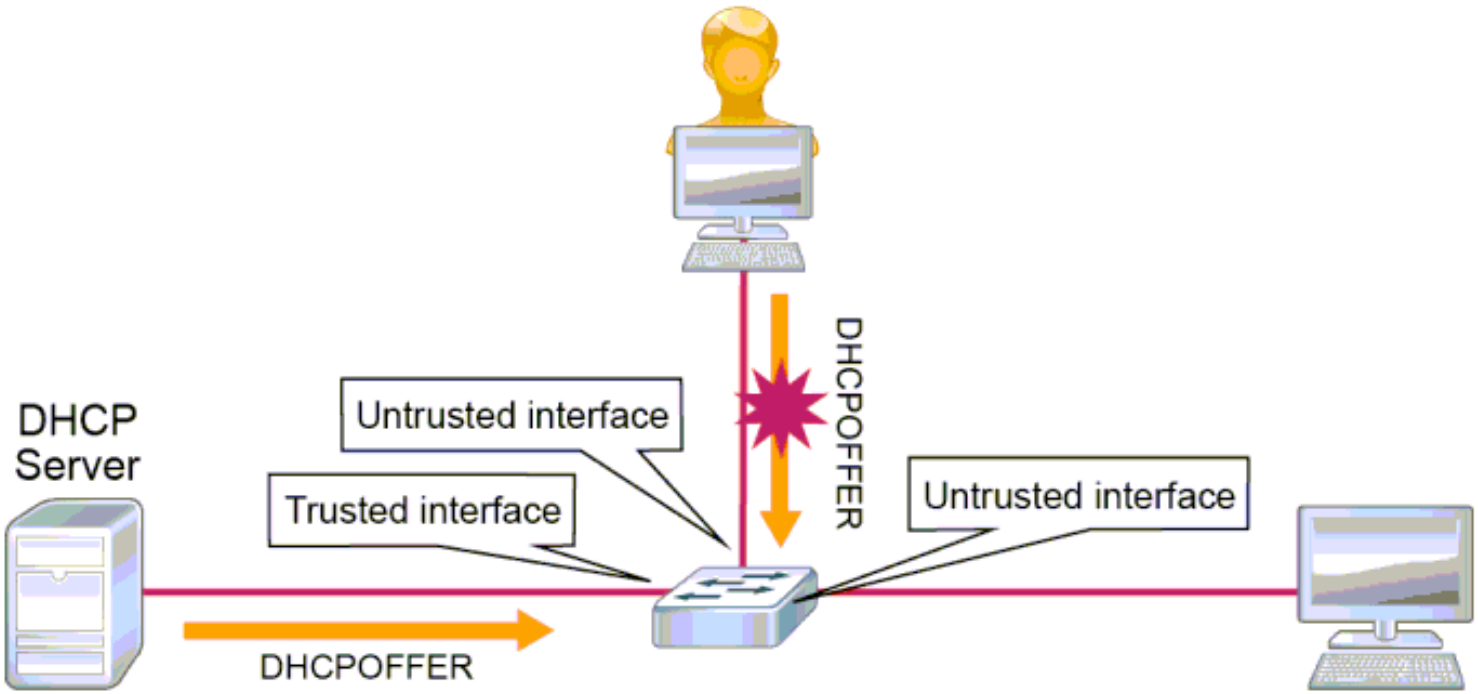
Identity-Based Networking

Identity-based network verifies the users when they connect regardless of their physical location.

- IEEE 802.1x standard defines the identity-based networking.



DHCP Snooping and DAI

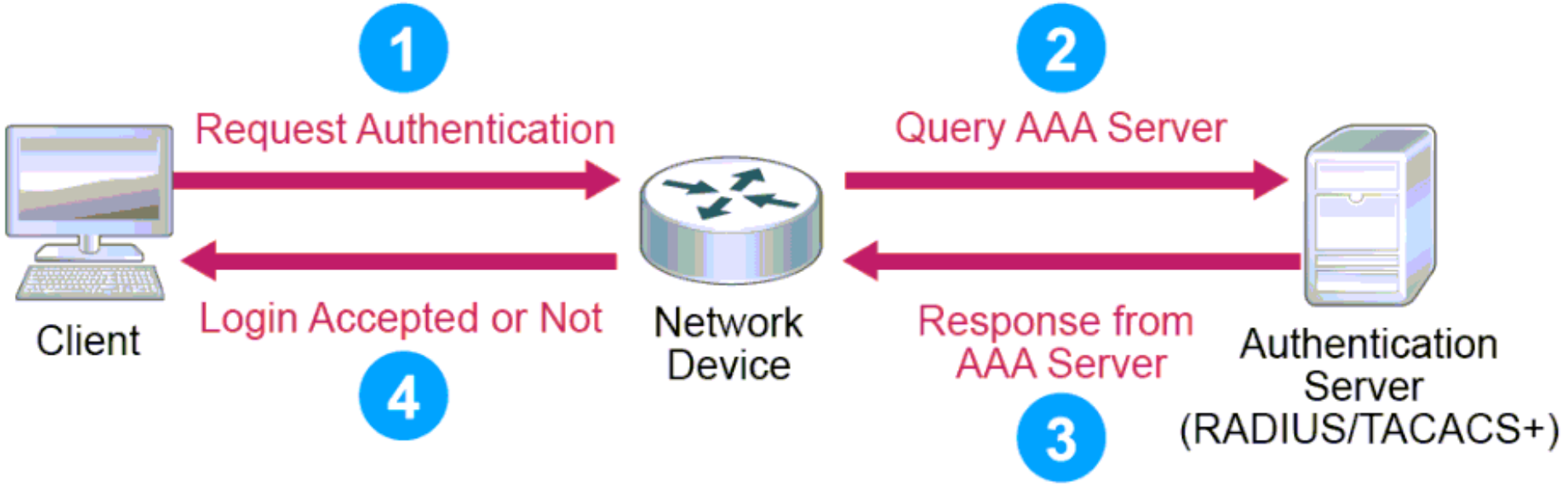


DHCP snooping is a Layer 2 security feature that validates the DHCP messages.

DAI tracks IP-to-MAC bindings from DHCP transactions to protect against ARP poisoning. DHCP snooping is required, to build MAC-to-IP bidings for DAI validation.

External Authentication Options

Using the local database for AAA implementation on network devices does not scale well.



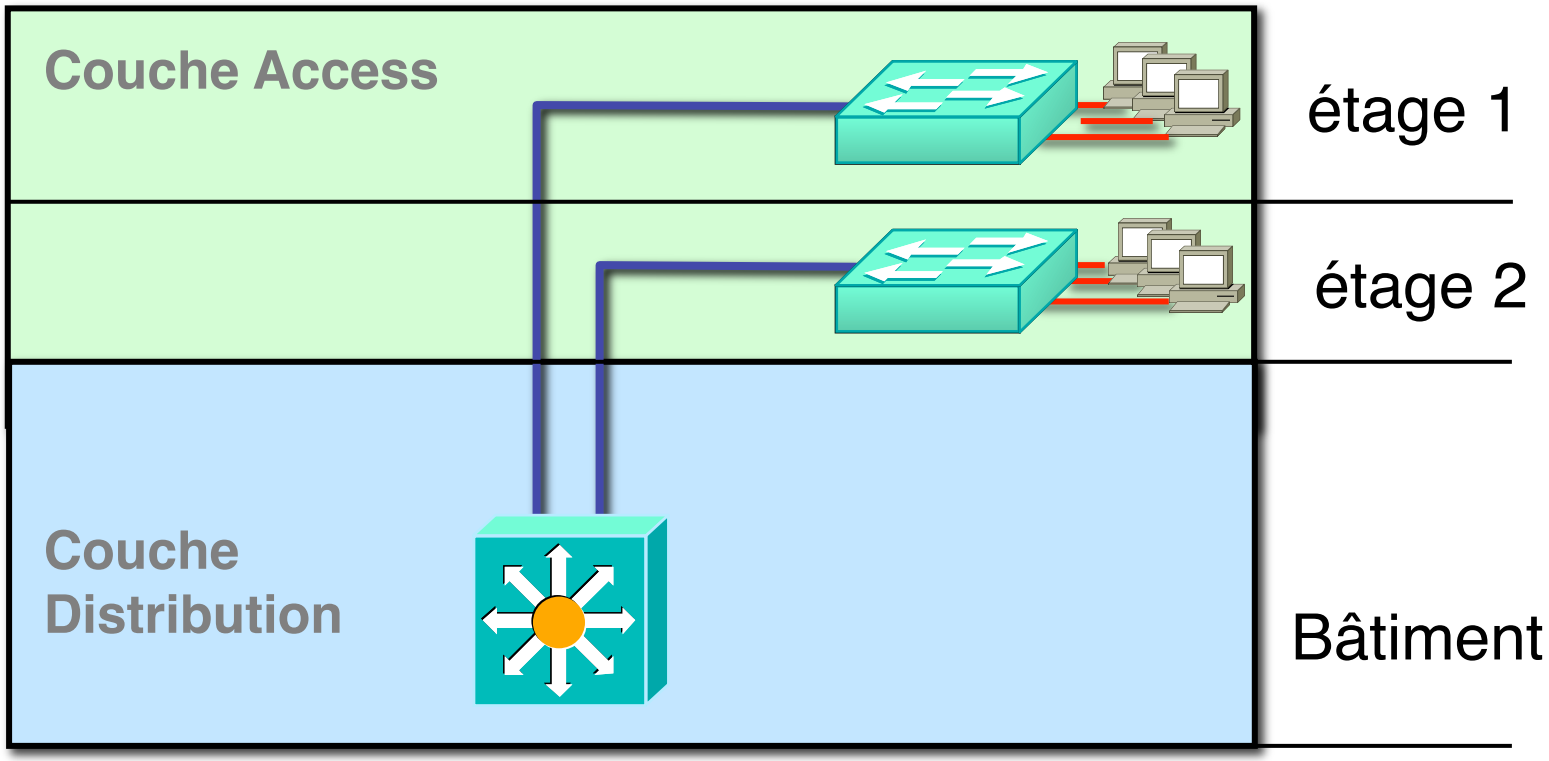
Ethernet

Le modèle hiérarchique

Conception d'un LAN

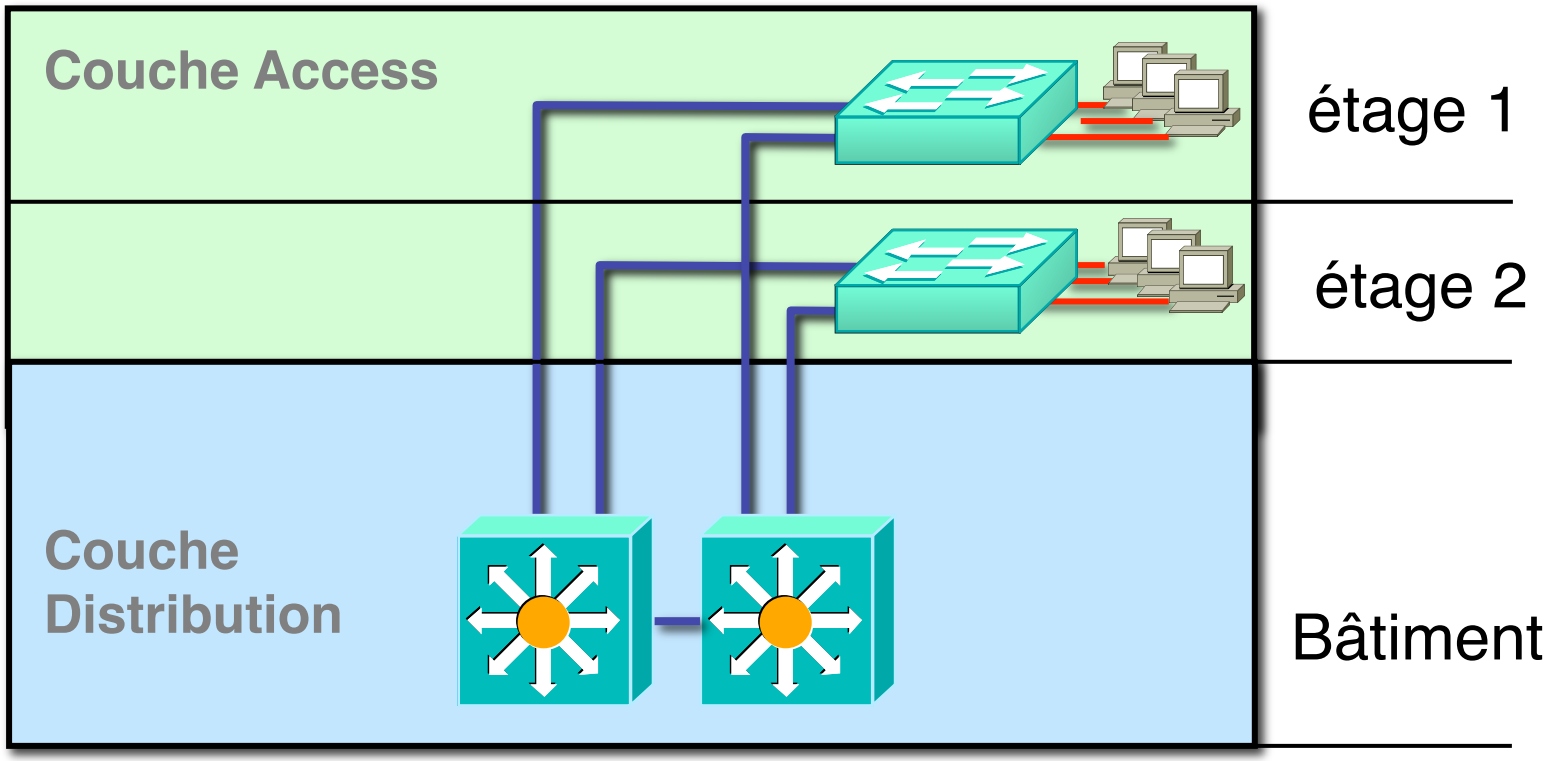
- On utilisera classiquement :
  - des switchs à chaque étage
    - nommés « switch d'accès »
    - directement connectés aux PCs
  - des switchs pour relier les étages entre eux
    - nommés « switch de distribution »
    - connectés aux switch d'accès

Exemple



le switch de distribution est alors un point de défaillance du réseau

Redondance



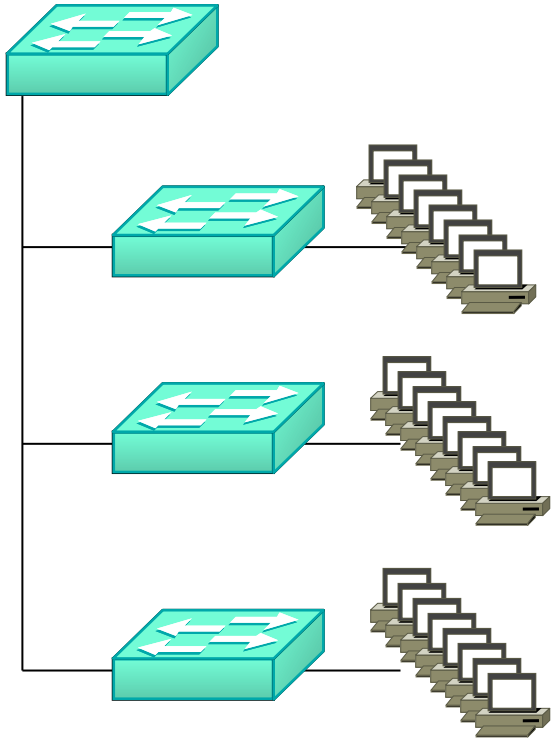
On utilisera DEUX switchs de distribution.

Cette redondance apportera des difficultés supplémentaires, qui seront résolues par le protocole STP.

VLAN

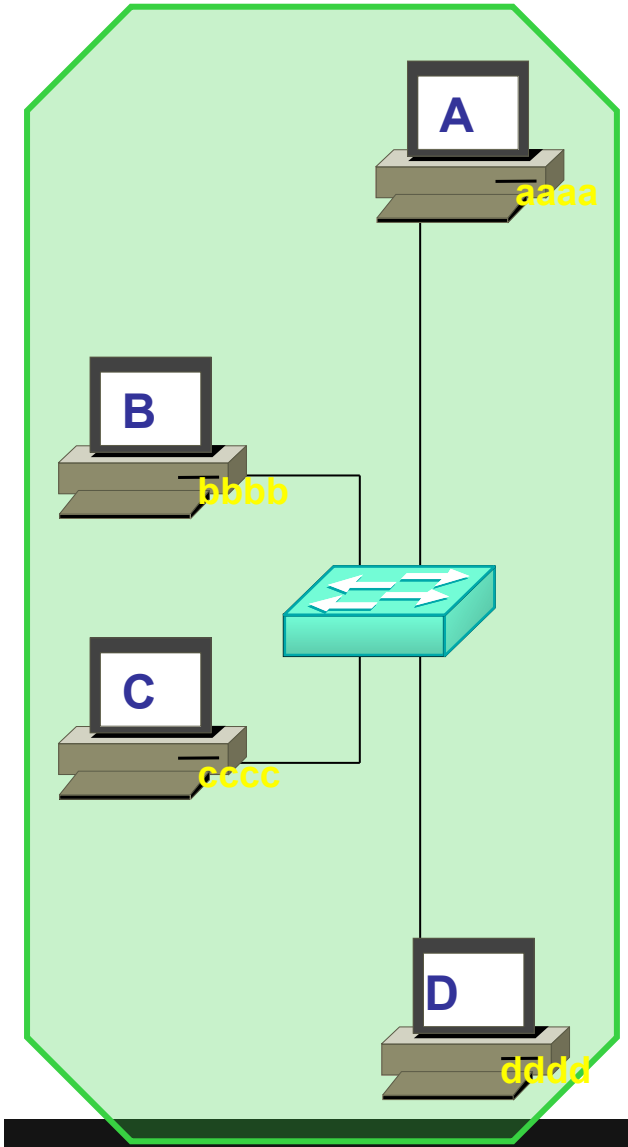
Virtual Local Area Network

Problèmes du LAN à plat



- Chaque broadcast innonde le réseau
  - consomme la bande passante du réseau
  - consomme du CPU sur les hôtes
- Chaque multicast innonde le réseau.
  - consomme la bande passante du réseau
- Chaque 'unknown unicast' est envoyé sur tous les ports du switch
  - consomme la bande passante du réseau
  - présente des risques de sécurité

Domaine de broadcast

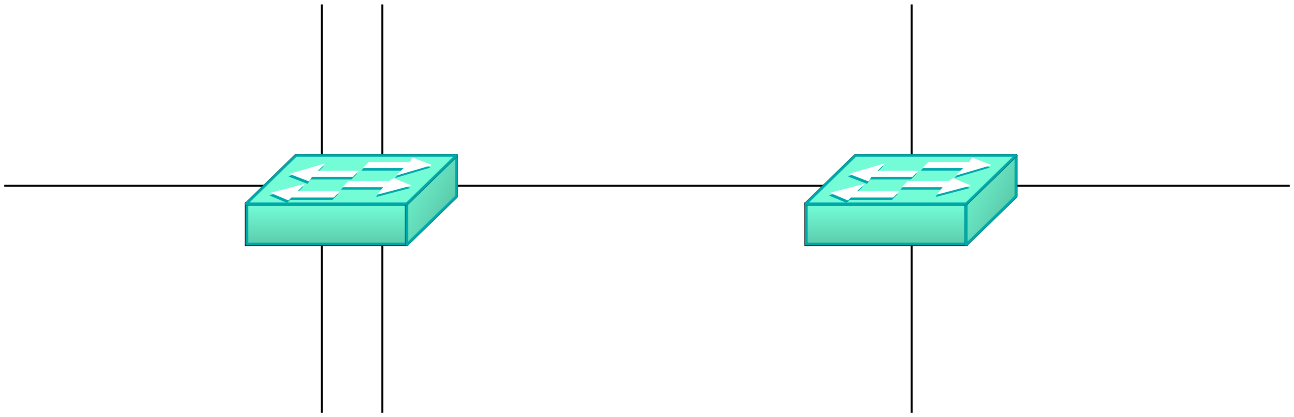


- Un équipement placé autour d'un SWITCH reçoit les broadcasts de tous les équipements placés autour de ce SWITCH :

- Ils sont dans le même domaine de broadcast.

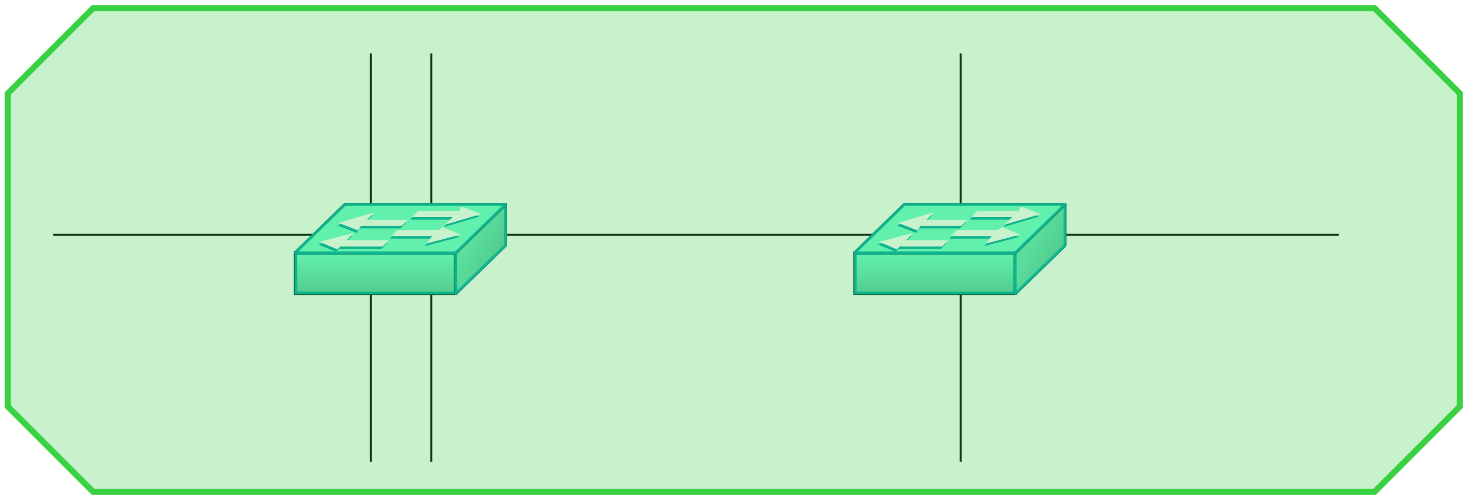
Exercice 1

Combien y a-t-il de domaine de broadcast ?



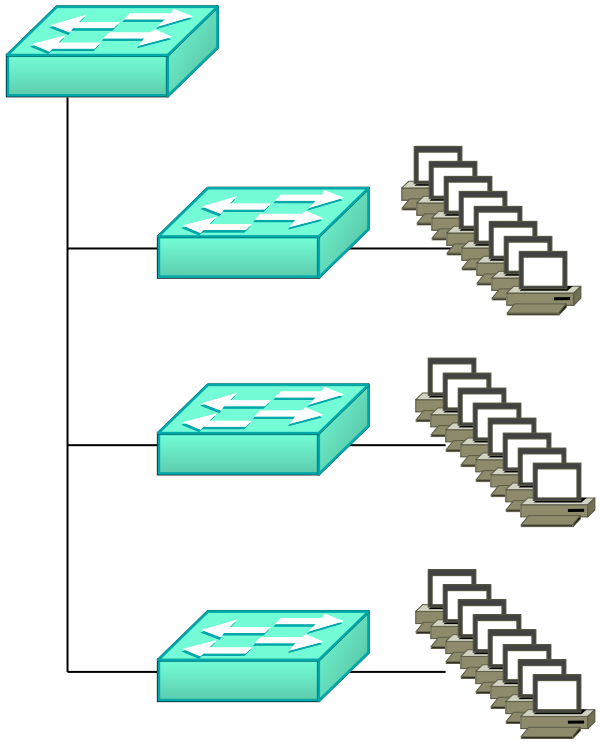
Solution 2

Un seul domaine de broadcast !



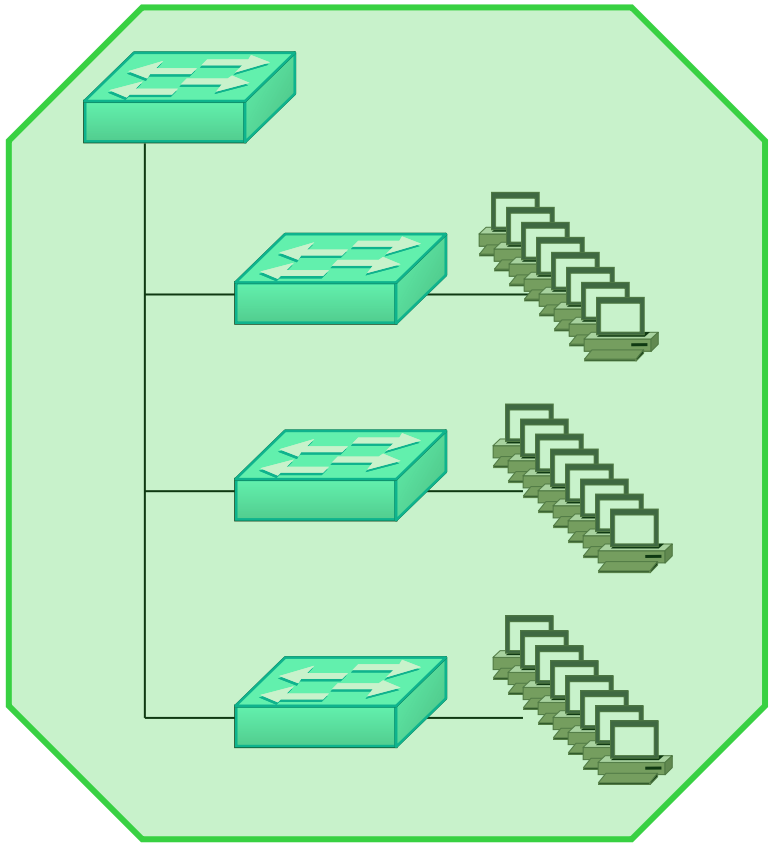
Exercice 2

Combien y a-t-il de domaine de broadcast ?



Solution 2

Un seul domaine de broadcast !



Comment limiter la diffusion des broadcast ?
des multicast ?
des unknown unicast ?

Diviser le domaine de broadcast en plusieurs domaines de broadcast

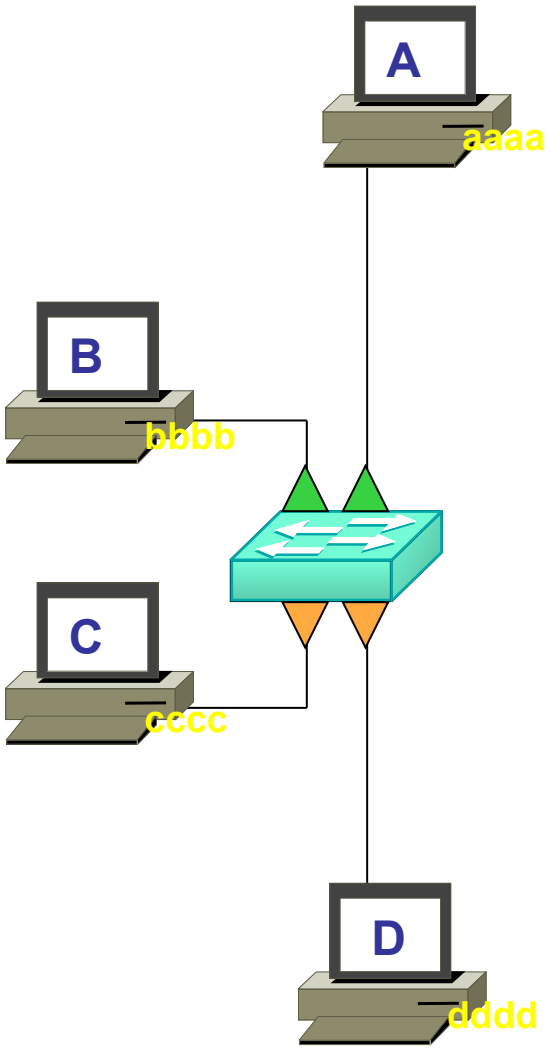
Les VLANs

- Créer plusieurs VLANs sur le switch

- Chaque VLAN représente un domaine de broadcast :
  - le switch ne permettra aucune communication entre 2 VLANs

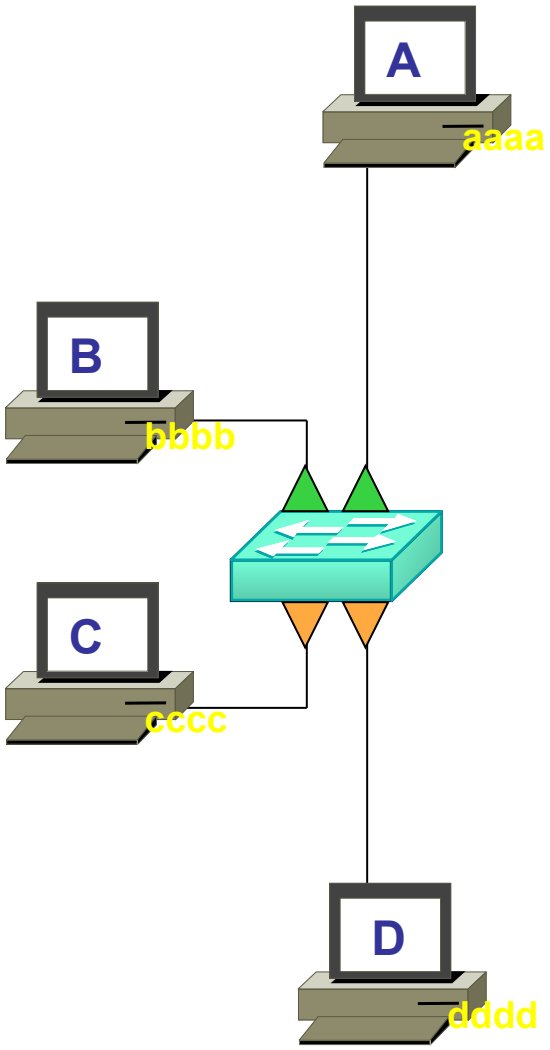
- Chaque VLAN est identifié par un numéro entre 1 et 4096

Exemple : 2 VLANs



- Créer 2 VLANs sur un switch :
  - le VLAN n°100
  - le VLAN n°200
- Attribuer :
  - certains ports au VLAN 100
  - certains ports au VLAN 200

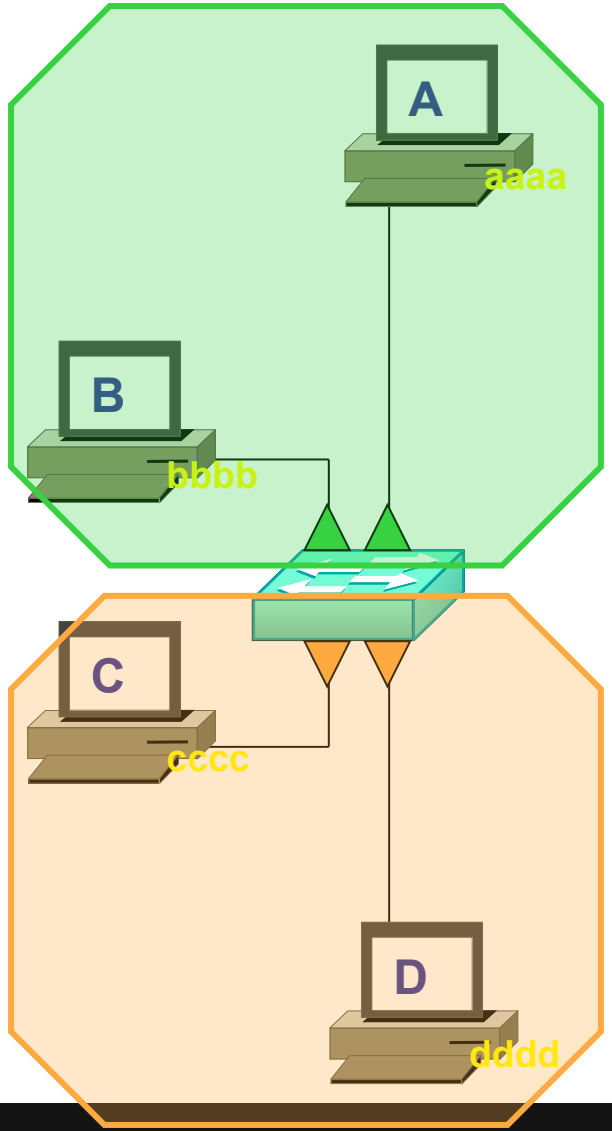
Exemple : 2 VLANs



- Quel que soit le type de trame (unicast, broadcast, multicast) , seules les communications suivantes seront possibles :
  - A et B
  - C et D

Aucune autre communication ne sera autorisée par le switch !

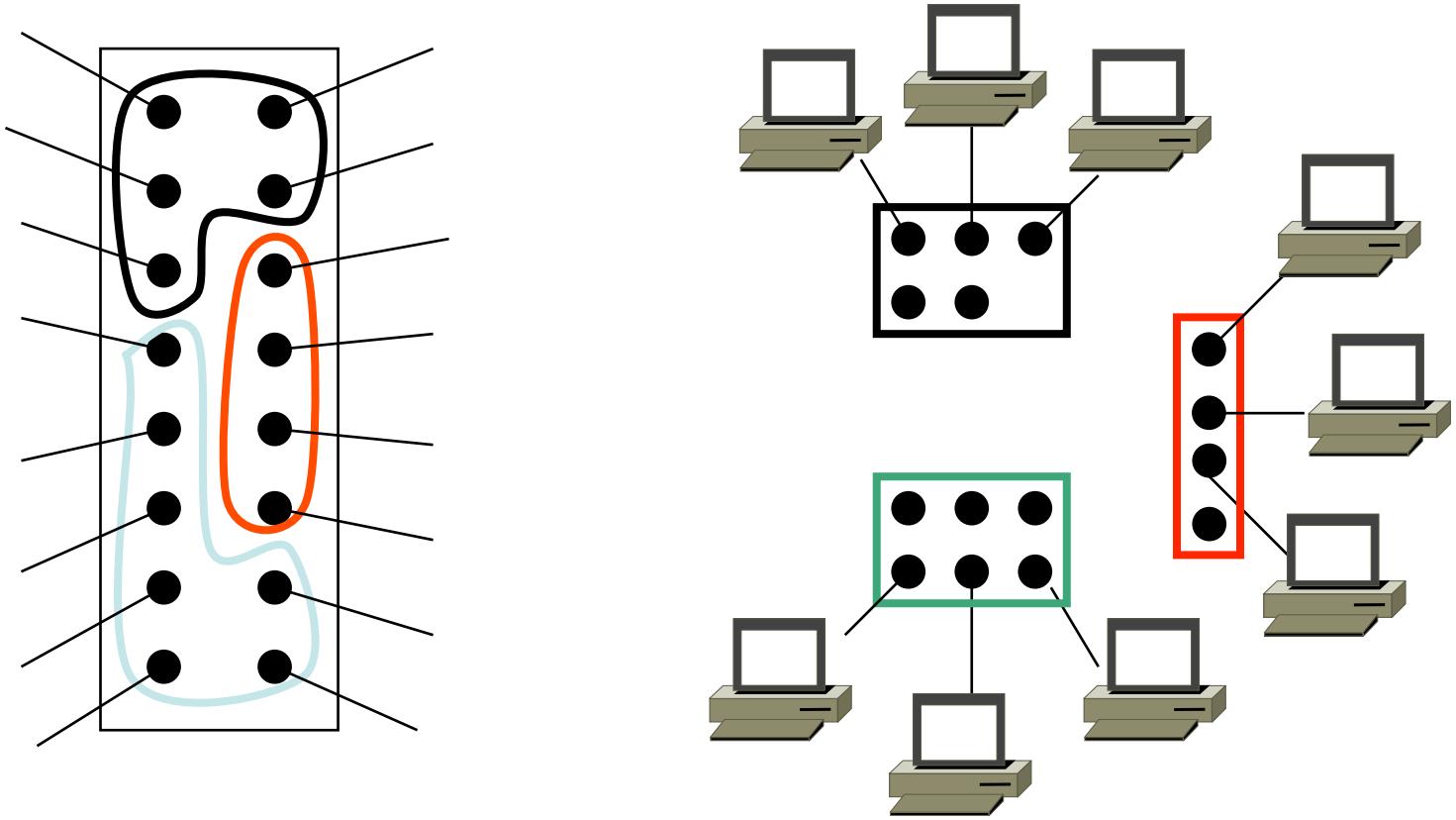
Exemple : 2 VLANs



- Deux domaines de broadcast.
  - les domaines de broadcast sont plus petits.
  - la bande passante est utilisée de manière plus efficace.
  - la CPU des équipements est moins sollicitée.
  - le switch maintient 2 tables d'adresses MAC.

Vue logique des VLANs

- Tout se passe comme s' il y avait plusieurs switchs :



VLAN

Configuration

Le VLAN par défaut

- Il existe toujours un VLAN sur les switch CISCO : le VLAN n°1.

- Tous les ports appartiennent à ce VLAN.

- Impossible de supprimer le VLAN n°1, ni de changer son nom : ‘default’.

Deux étapes

CRÉER les VLANs :

AFFECTER les interfaces aux VLANs :

Deux étapes

CRÉER les VLANs :

ANCIENNE METHODE :

```
vlan database
vlan 100 name TOTO
vlan 200 name TATA
exit
```

NOUVELLE METHODE :

```
configure terminal
vlan 100
name TOTO
vlan 200
name TATA
```

AFFECTER les interfaces aux VLANs :

Deux étapes

CRÉER les VLANs :

ANCIENNE METHODE :

```
vlan database
vlan 100 name TOTO
vlan 200 name TATA
exit
```

NOUVELLE METHODE :

```
configure terminal
vlan 100
name TOTO
vlan 200
name TATA
```

AFFECTER les interfaces aux VLANs :

```
configure terminal
interface Fa0/0
switchport mode access
switchport access vlan 100
```

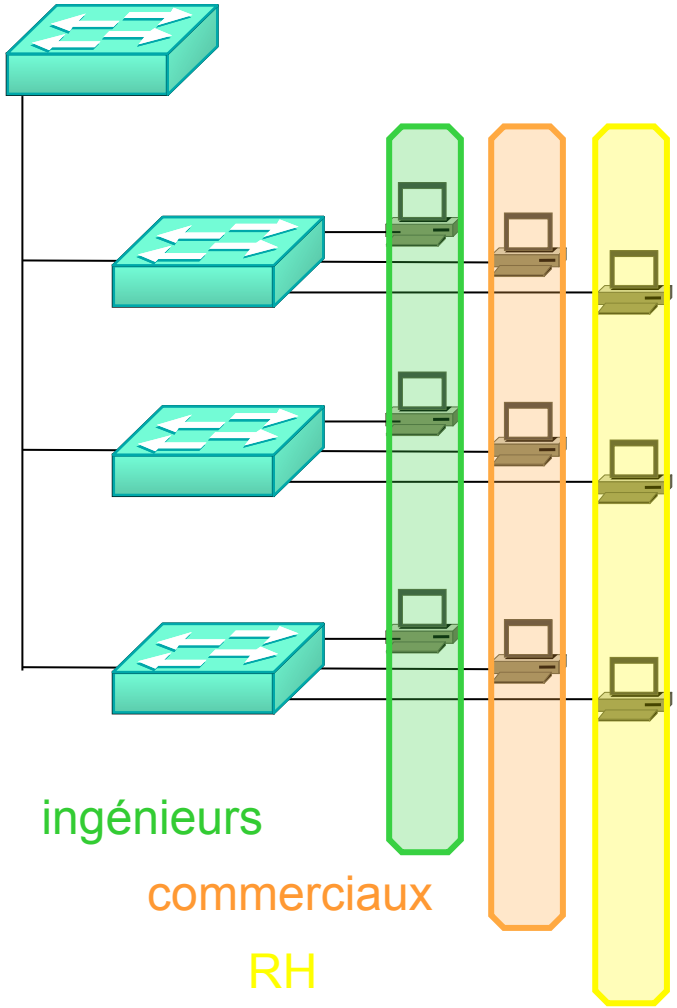
Vérifier les VLAN

- Show vlan-switch (dans les TPs)
- Show vlan brief
- Show vlan Id (suivi du numéro de VLAN)

VLAN

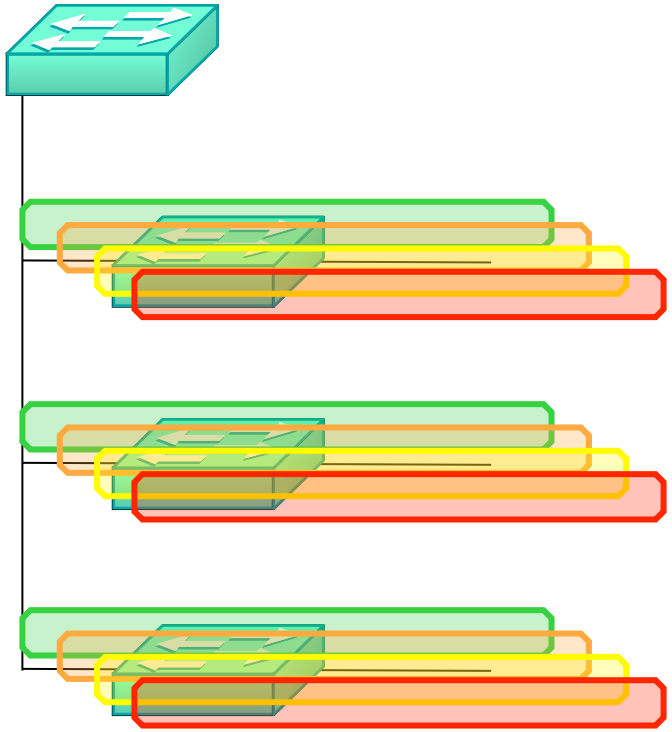
Implémentation

Implémentation n°1



- Objectifs recherchés :
  - segmentation
  - flexibilité
  - sécurité

Implémentation n°2

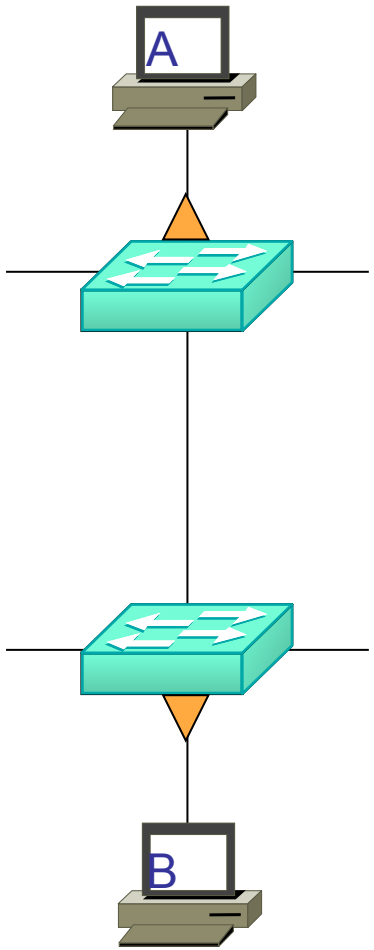


- Objectifs recherchés :
  - chaque VLAN regroupe un certain type de trafic :
    - Data
    - Management réseau
    - Voix
    - accès invités
    - Wi-Fi
    - Imprimantes

VLAN

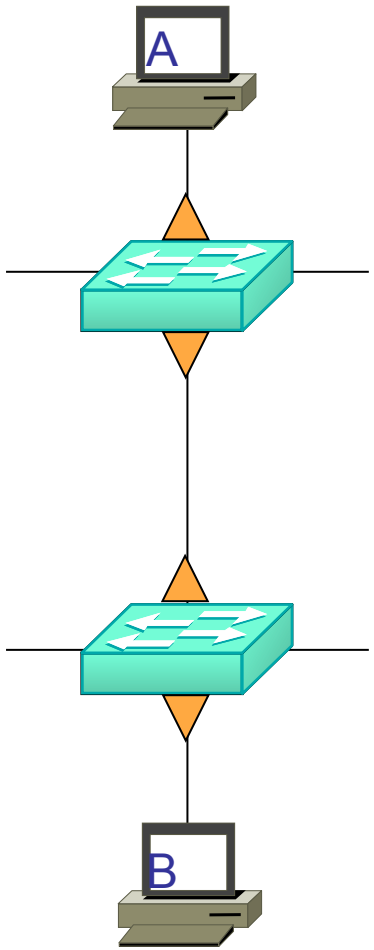
Liaisons « Trunk »

Un VLAN sur plusieurs switchs



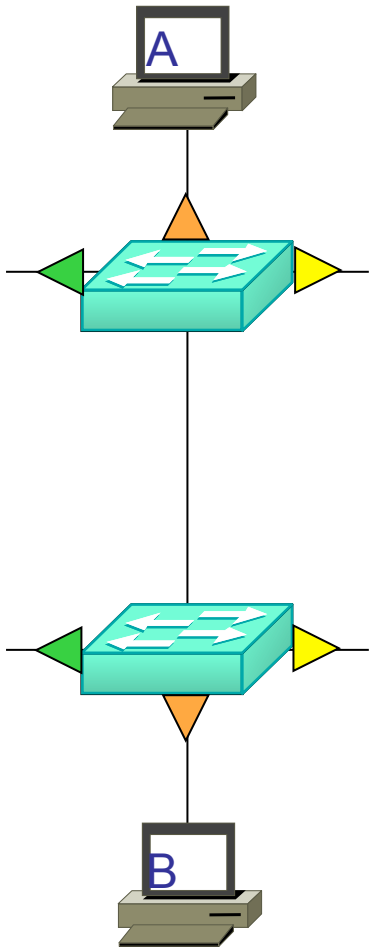
- Le VLAN 100 est utilisé sur les 2 switch.
- Comment permettre aux équipements A et B de communiquer ensemble ?

Un VLAN sur plusieurs switchs



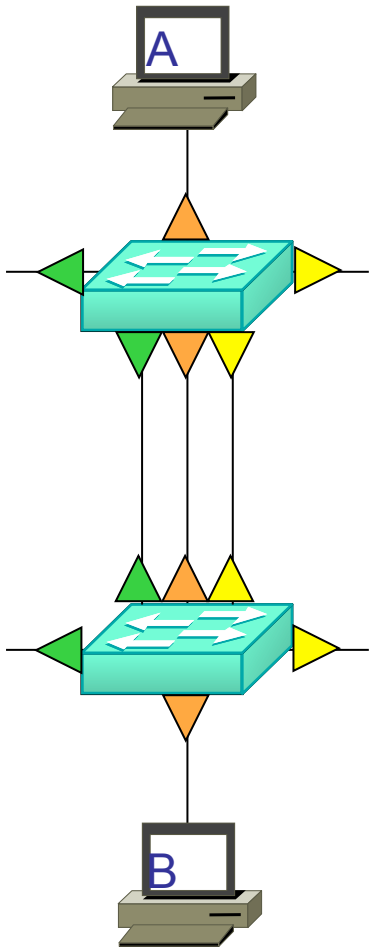
- Le VLAN 100 est utilisé sur les 2 switch.
- Affecter l' inter-switch au VLAN 100

Trois VLAN sur plusieurs switchs



- Les VLAN 100, 200 et 300 sont utilisés sur les 2 switch.
- Comment permettre aux équipements d'un même VLAN de communiquer ensemble ?

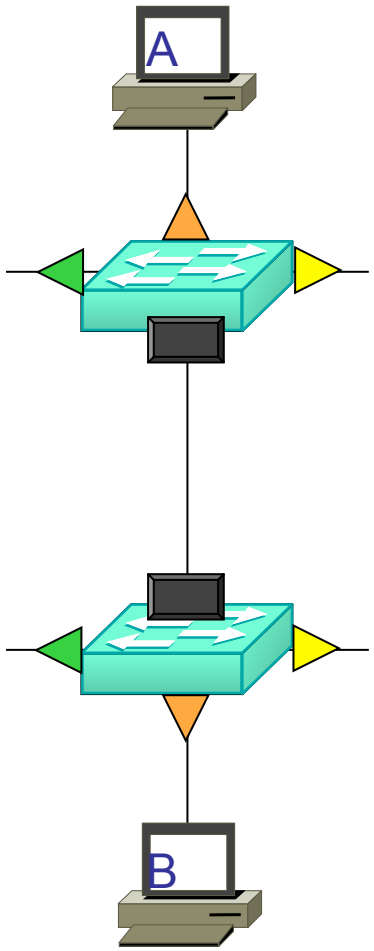
Trois VLAN sur plusieurs switchs



- Les VLAN 100, 200 et 300 sont utilisés sur les 2 switch.
- Consommer 3 ports pour interconnecter les 2 switches ?!

peu efficace !

Trois VLAN sur plusieurs switchs

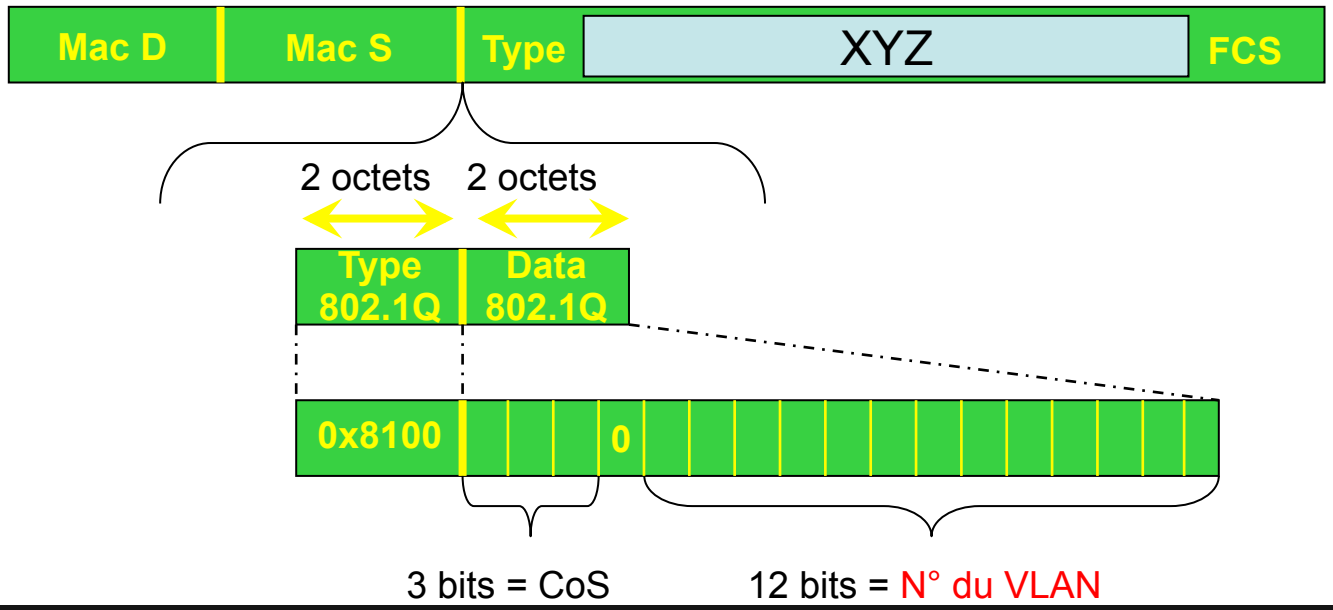


- Les VLAN 100, 200 et 300 sont utilisés sur les 2 switch.
- Configurer l'interco entre les 2 switchs en mode TRUNK :
  - Tous les VLANs seront autorisés sur l'interface trunk
  - Sur l'interface trunk, les trames seront taggées avec le n° du VLAN

Le TAG 802.1Q

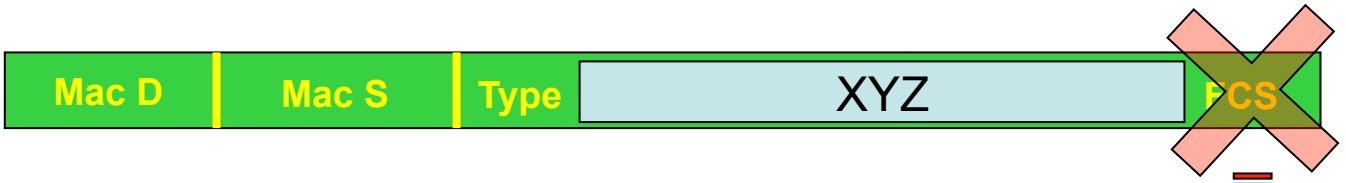
- Trame originale, non taggée :

- Trame modifiée, taggée :

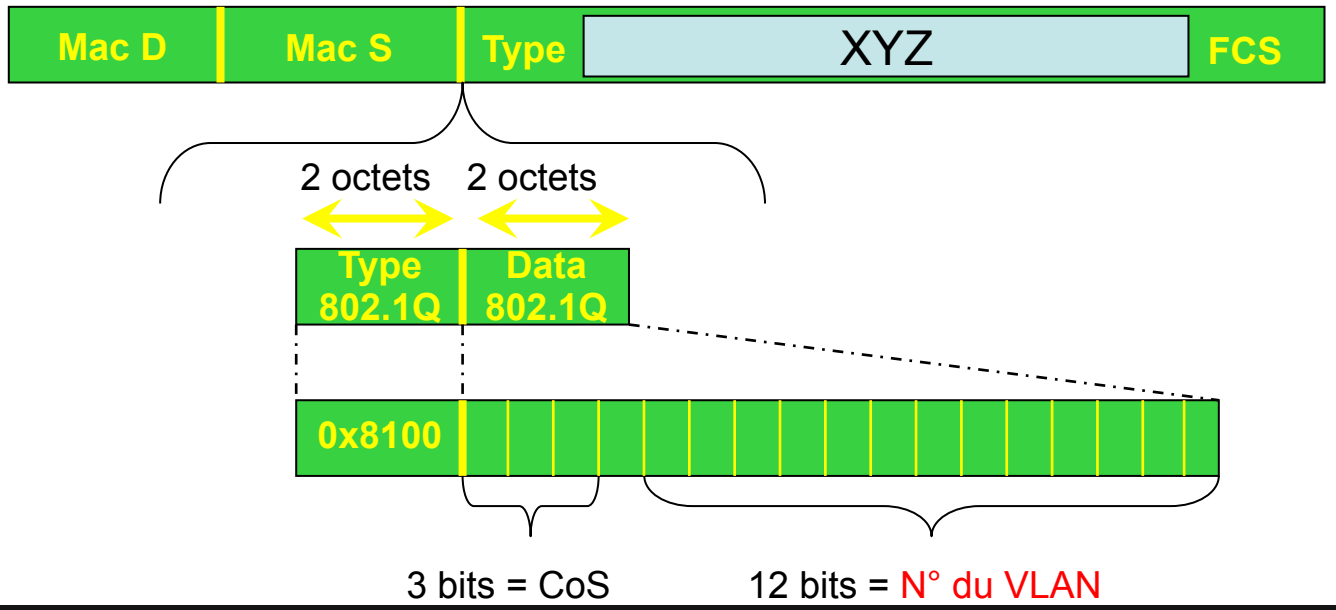


FCS recalculée !

- Trame originale, non taggée :



- Trame modifiée, taggée :

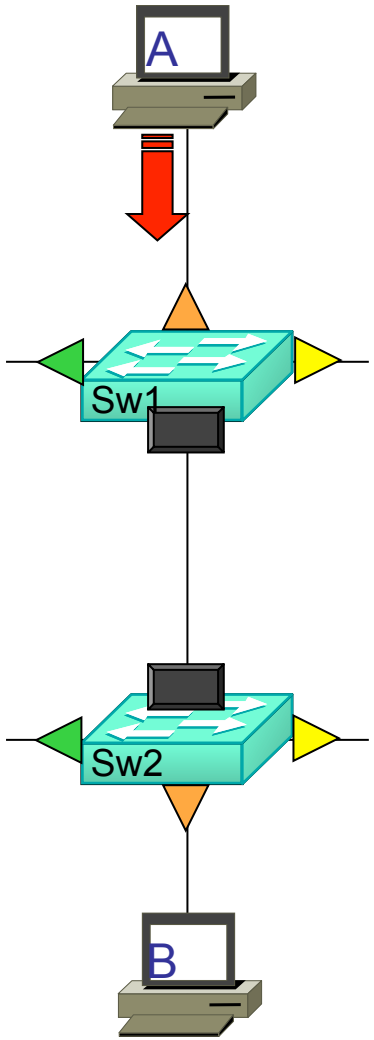


A quoi sert le TAG ?

- Il permet d'indiquer au switch distant à quel VLAN appartient la trame envoyée.

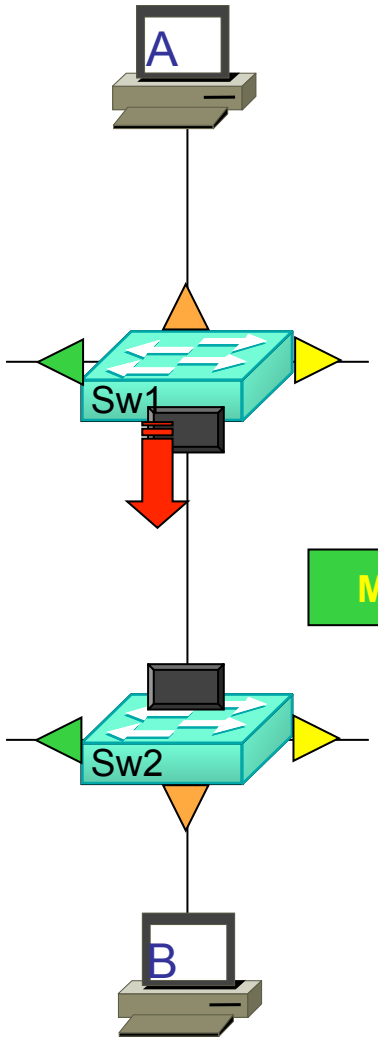
- Le switch distant saura alors quelle table d'adresse Mac utiliser pour forwarder cette trame.
  - Rappel : chaque VLAN possède sa propre table d'adresse Mac.

Exemple 1/3

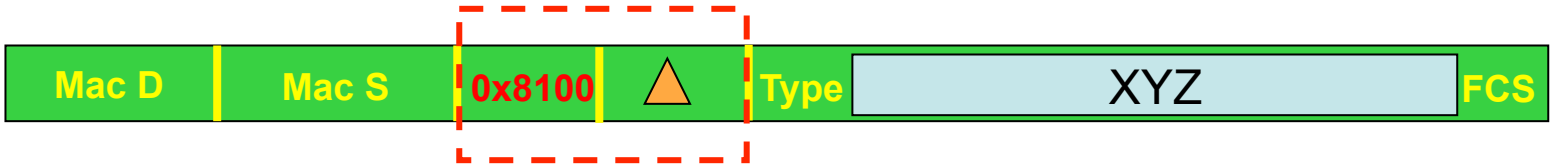


- A envoie une trame à B.
- A génère cette trame.
- Elle n'est pas taggée :

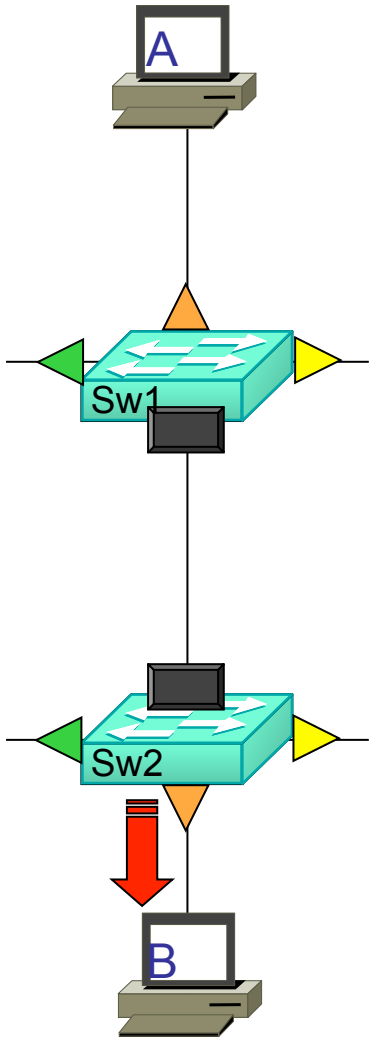
Exemple 2/3



- Sw1 veut envoyer cette trame sur l'interface Trunk.
- Sw1 rajoute le TAG et recalcule la FCS :



Exemple 3/3



- Sw2 reçoit une trame taggée.
- Sw2 retire le TAG, recalcule la FCS et envoie la trame à B :

VLAN

Configurer le « Trunk »

Passer une interface en mode trunk

- `configure terminal`
- `interface fa0/0`
- `switchport mode trunk`

les DEUX switchs doivent passer
en mode trunk !

Quitter le mode trunk

- `configure terminal`
- `interface fa0/0`
- `switchport mode access`
- `switchport access vlan 100`

pour repositionner l'interface
dans le VLAN 100

Vérifier le trunk

```
Sw1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/0       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/0       1-1005

Port        Vlans allowed and active in management domain
Fa0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/0       1
```

Les modes dynamiques

- On peut laisser les switchs communiquer entre eux et décider dynamiquement s'ils doivent passer en trunk :

```
configure terminal
 interface fa0/0
 switchport mode dynamic auto
```

  - je passerai en trunk si mon voisin me le demande.

```
switchport mode dynamic desirable
```

  - je demande à mon voisin s'il accepte de passer en trunk.

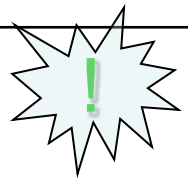
Définitions

- Mode administratif :
  - c'est le mode configuré sur l'interface :
    - access
    - trunk
    - dynamic auto
    - dynamic desirable
- Mode opérationnel :
  - c'est le mode dans lequel fonctionne l'interface :
    - access
    - trunk

Vérifier les modes :

```
Sw1#show interface fa0/0 switchport
Name: Fa0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
```

Table de correspondances

	access	trunk	dynamic desirable	dynamic auto
access	access			
trunk		trunk		
dynamic desirable	access	trunk	trunk	
dynamic auto	access	trunk	trunk	access

VLANs autorisés

- On peut limiter la liste des VLANs autorisés à emprunter une interface :

```
configure terminal
  interface fa0/0
```

- `switchport trunk allowed vlan 1,100-200`
  - liste exhaustive des VLANs autorisés
- `switchport trunk allowed vlan add 300`
  - ajouter le vlan 300 à la liste actuelle
- `switchport trunk allowed vlan remove 100`
  - retirer le vlan 100 à la liste actuelle
- `switchport trunk allowed vlan except 400`
  - autoriser tous les VLANs sauf le vlan 400
- `switchport trunk allowed vlan all`
  - autoriser tous les VLANs

Vérifier les VLANs autorisés 1/2

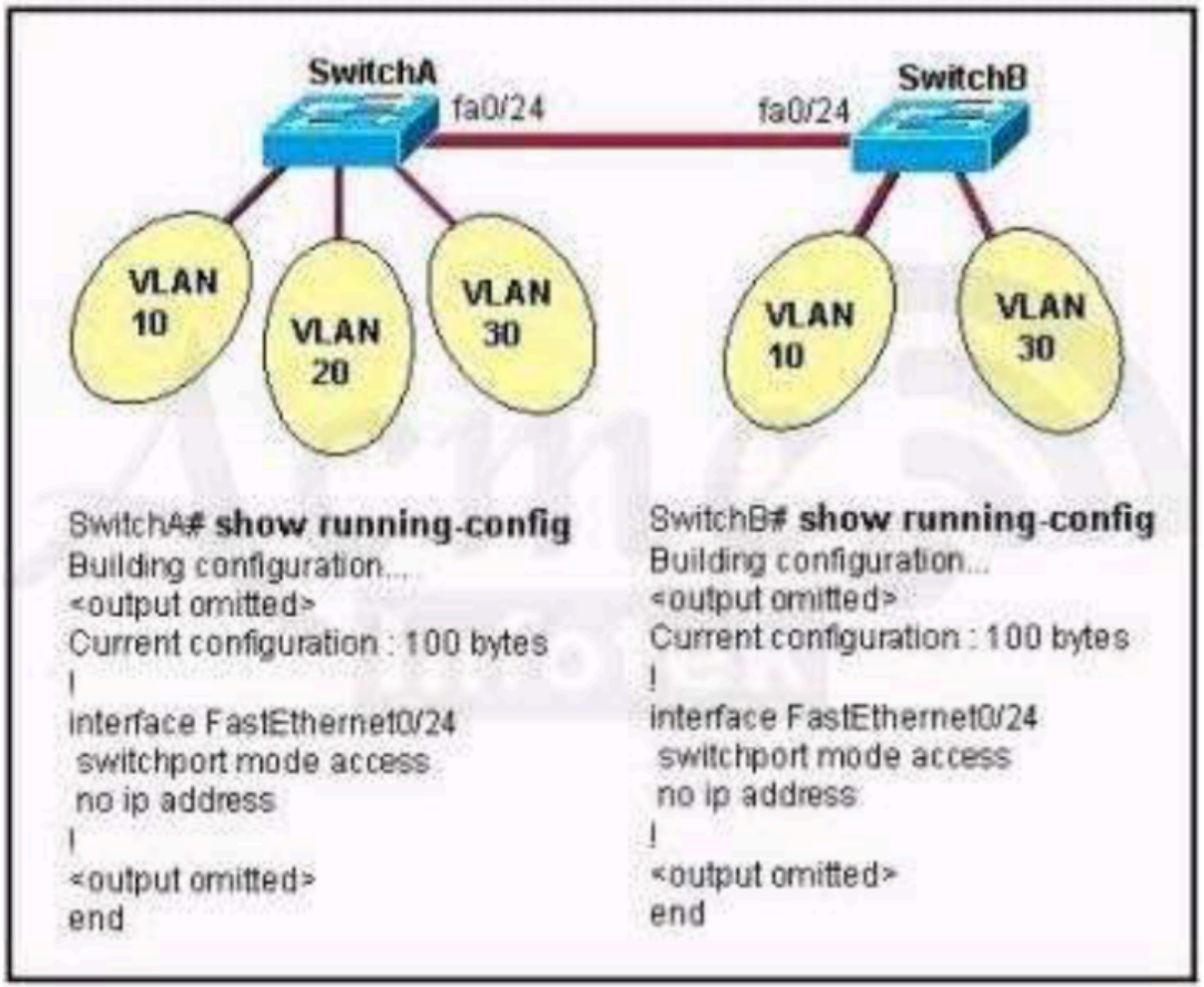
```
Sw2#show interfaces fastEthernet 0/0 switchport

Name: Fa0/0
  Switchport: Enabled
  Administrative Mode: trunk
  Operational Mode: trunk
  Administrative Trunking Encapsulation: dot1q
  Operational Trunking Encapsulation: dot1q
  Negotiation of Trunking: Disabled
  Access Mode VLAN: 0 ((Inactive))
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-199,1001-1005
  Trunking VLANs Active: 1,100
  trust: none
  …
```

Vérifier les VLANs autorisés 2/2

```
Sw2#show interfaces trunk
Port        Mode         Encapsulation  Status       Native vlan
Fa0/0       on           802.1q         trunking     1

Port        Vlans allowed on trunk
Fa0/0       1-199,1001-1005

Port        Vlans allowed and active in management domain
Fa0/0       1,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/0       1,100
```

Test

Pourquoi les équipements situés dans le même VLAN et sur 2 switch différents n'arrivent pas à communiquer ensemble ?



VLAN

Le Vlan Natif

Définition

- Le trunk rajoute un TAG sur les trames.

- Exception : si une trame appartient au VLAN dit « natif », elle ne sera pas taggée.

- Par défaut, le vlan « natif » est le VLAN 1

Exemple d'utilisation du VLAN natif

Configurer le Vlan Natif

- `configure terminal`
- `interface fa0/0`
- `switchport mode trunk`
- `switchport trunk native vlan 10`

les DEUX switchs doivent utiliser
le même Vlan Natif sur le lien qui les interconnecte !

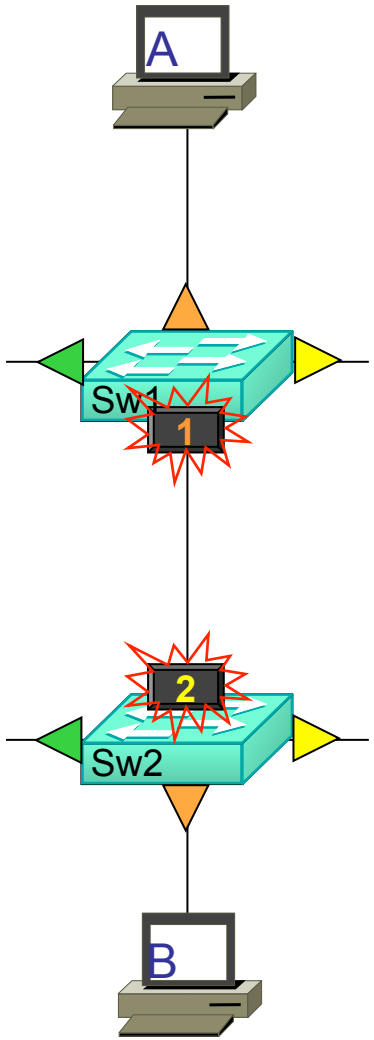
Vérifier le vlan Natif 1/2

```
Sw2#show interfaces fastEthernet 0/0 switchport
  Name: Fa0/0
  Switchport: Enabled
  Administrative Mode: trunk
  Operational Mode: trunk
  Administrative Trunking Encapsulation: dot1q
  Operational Trunking Encapsulation: dot1q
  Negotiation of Trunking: Disabled
  Access Mode VLAN: 0 ((Inactive))
  Trunking Native Mode VLAN: 100 (TOTO)
  Trunking VLANs Enabled: 1-199,1001-1005
  Trunking VLANs Active: 1,100
  Priority for untagged frames: 0
  …
```

Vérifier le vlan Natif 2/2

```
Sw2#show interfaces trunk
Port        Mode         Encapsulation  Status       Native vlan
Fa0/0       on           802.1q         trunking     100

Port        Vlans allowed on trunk
Fa0/0       1-199,1001-1005

Port        Vlans allowed and active in management domain
Fa0/0       1,100

Port    Vlans in spanning tree forwarding state and not pruned
Fa0/0       1,100
```

Native Vlan Mismatch



- Que se passe-t-il si le Vlan Natif n'est pas le même des deux côtés du trunk ?
  - aucune communication ?
  - mauvaise communication ?

Bilan des commandes trunk

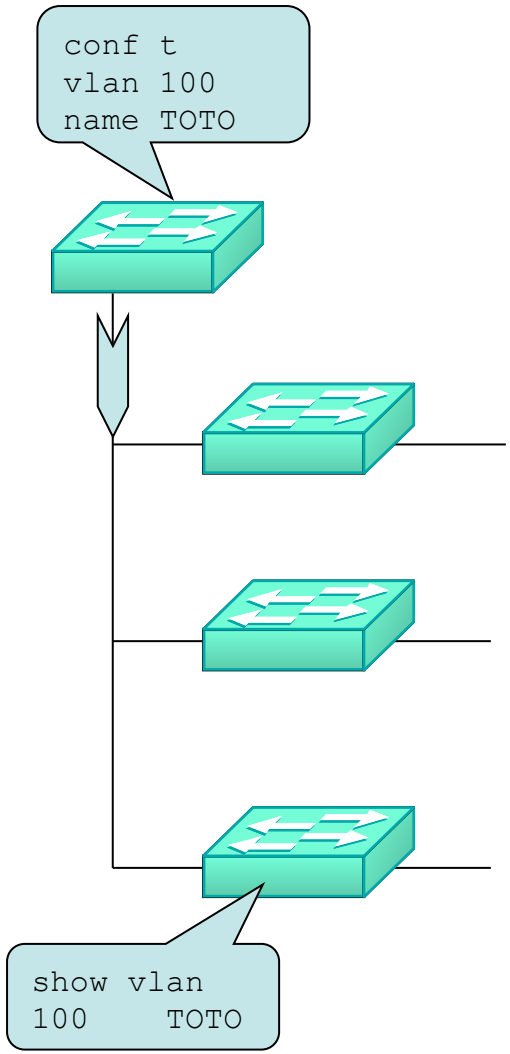
- `configure terminal`
- `interface fa0/0`
- `switchport trunk allowed vlan 1-3`
- `switchport trunk native vlan 100`
- `switchport mode trunk`

sur les DEUX côtés du trunk !

VTP

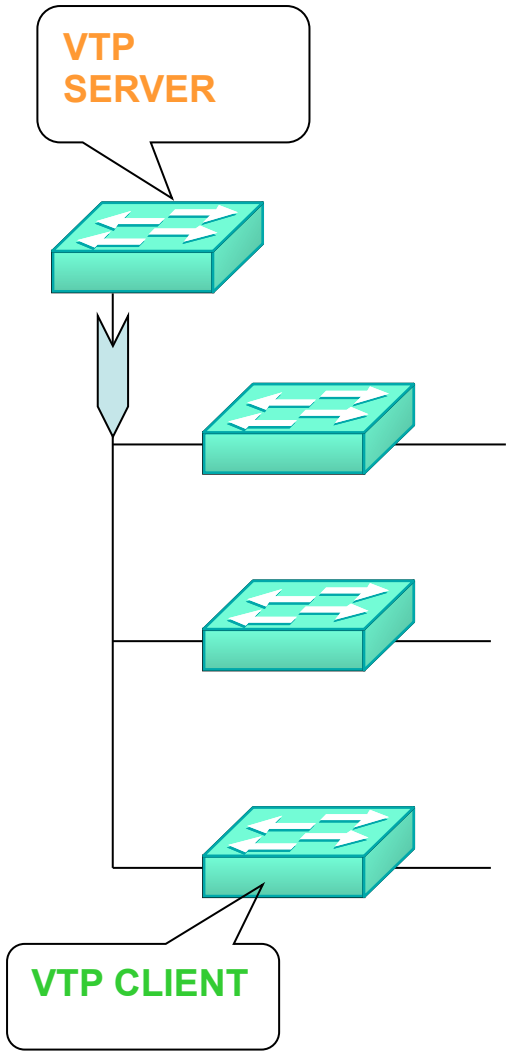
Vlan Trunking Protocol

VTP



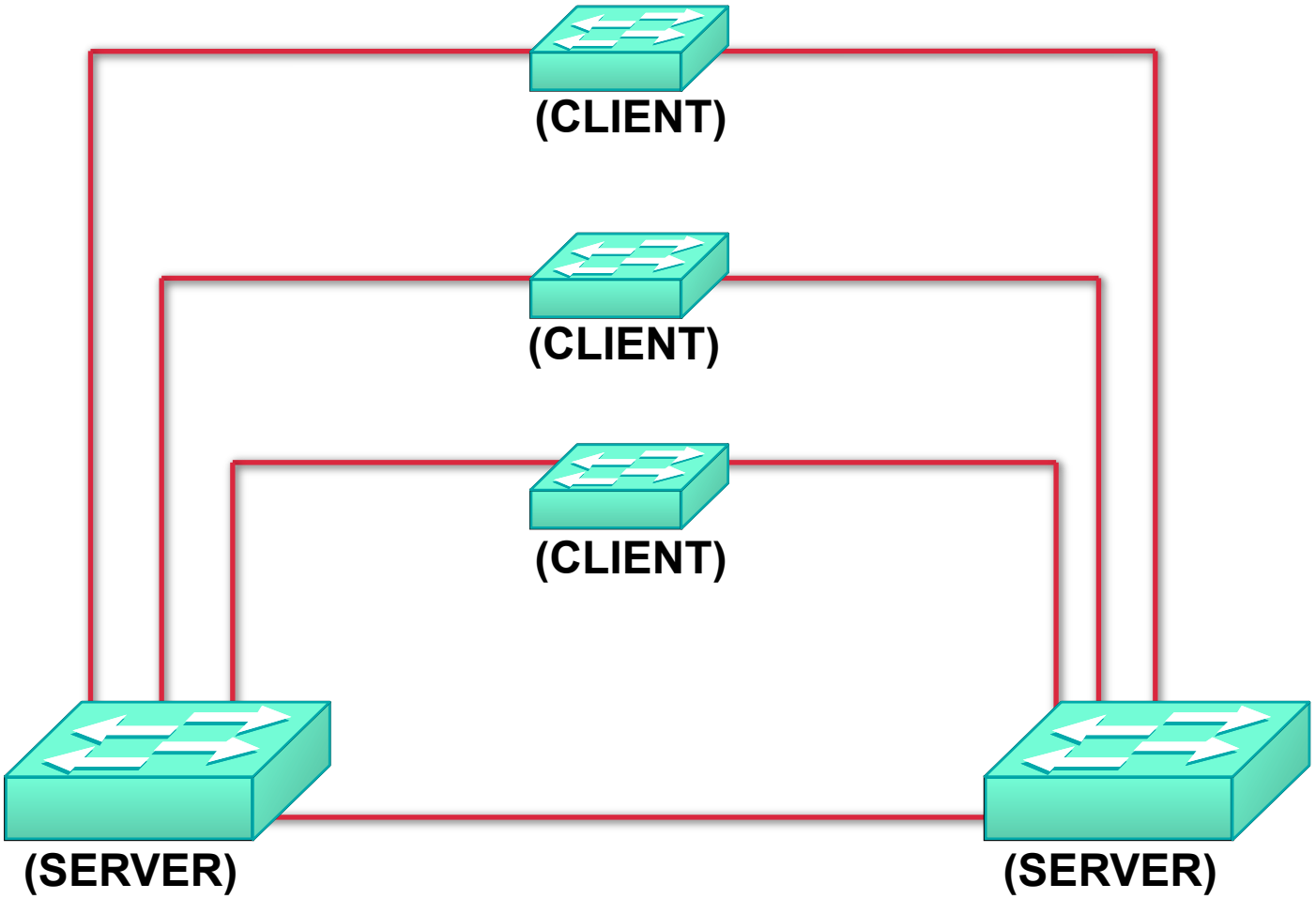
- Protocole propriétaire CISCO
- Objectif : diffuser sur l'ensemble du réseau les créations / modifications / suppressions de VLANs.
- Méthode : envoyer des messages VTP
  - toutes les 5 minutes
  - après chaque modification
  - sur toutes les interfaces trunk
  - en multicast
  - dans le VLAN 1
  - avec la liste des VLANs à jour

Server et Client

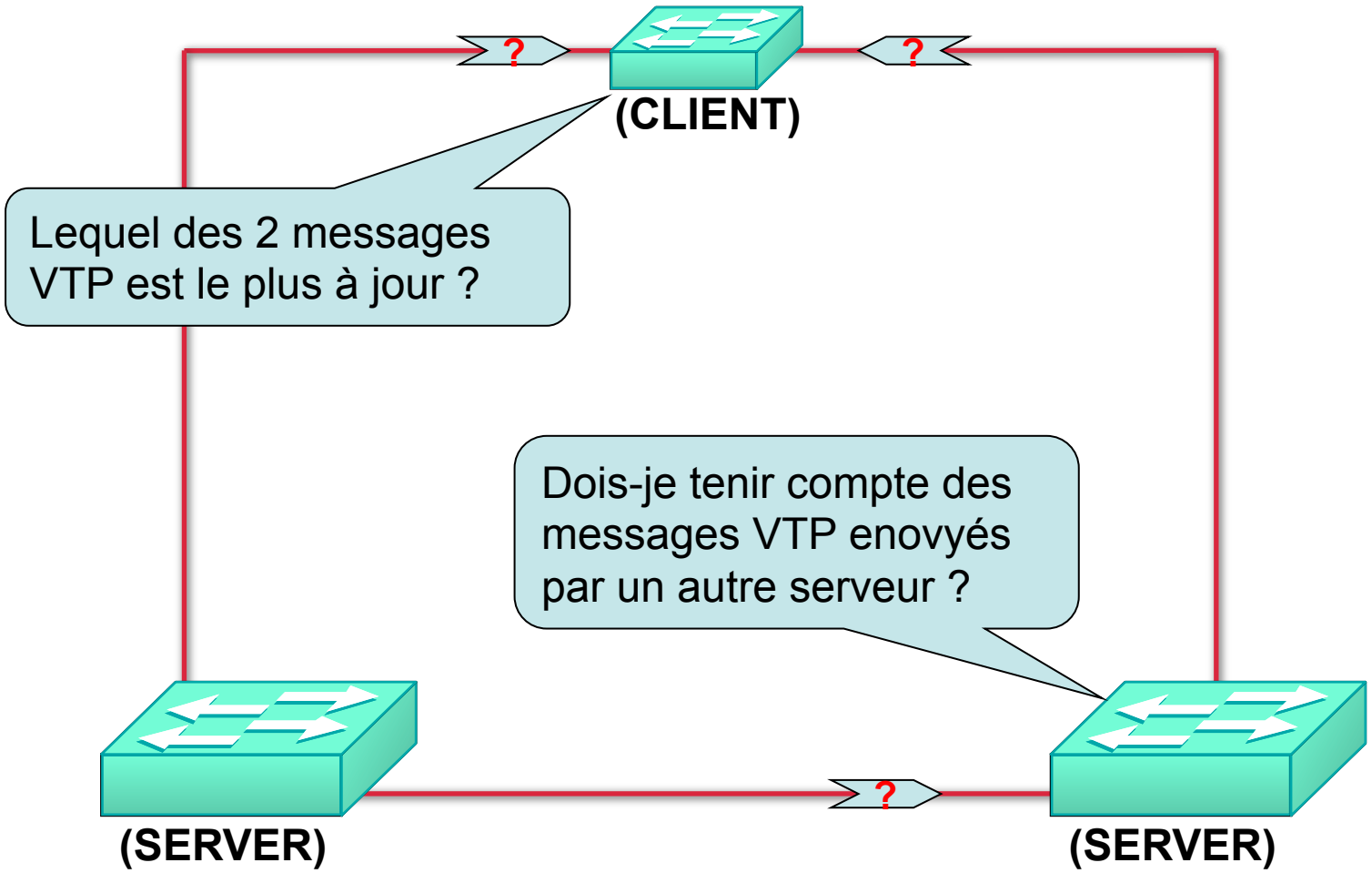


- Le switch VTP server :
  - celui sur lequel l'administrateur configure les Vlans
- Les switchs VTP client :
  - ceux qui synchronisent leurs bases de données avec les messages VTP reçus
- Et si le switch VTP server tombe en panne ?

Plusieurs VTP server.



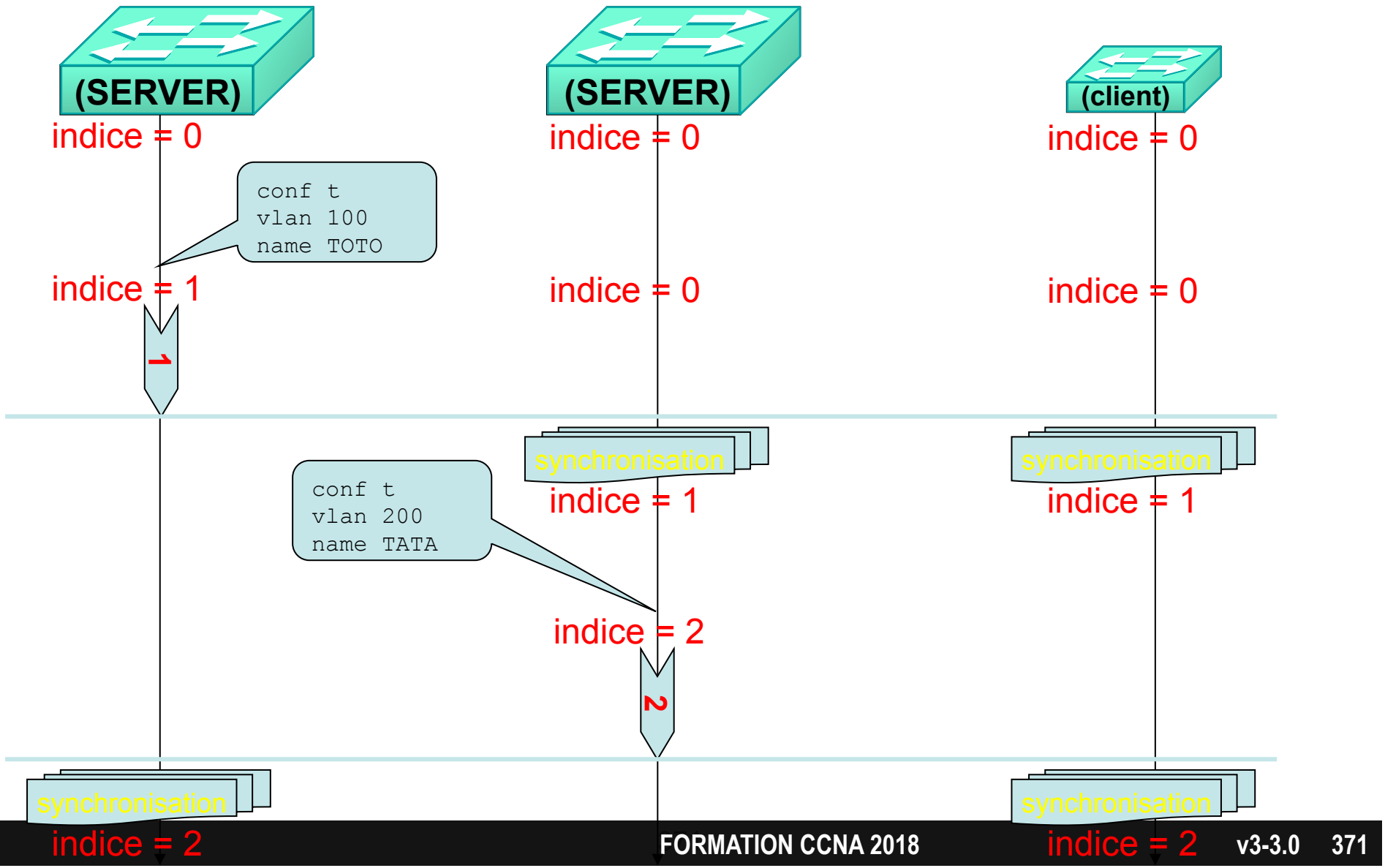
Plusieurs messages VTP !



L'indice de révision

- Au démarrage, l'indice est égal à 0.
- L'indice est incrémenté de 1 à chaque fois qu'une modification de VLAN est configurée par l'administrateur.
- Le client et le serveur ne tiennent compte que des messages VTP dont l'indice de configuration est supérieur à l'indice local.
  - dans ce cas, le switch synchronise sa base de données locale et ajuste l'indice local à l'indice reçu.

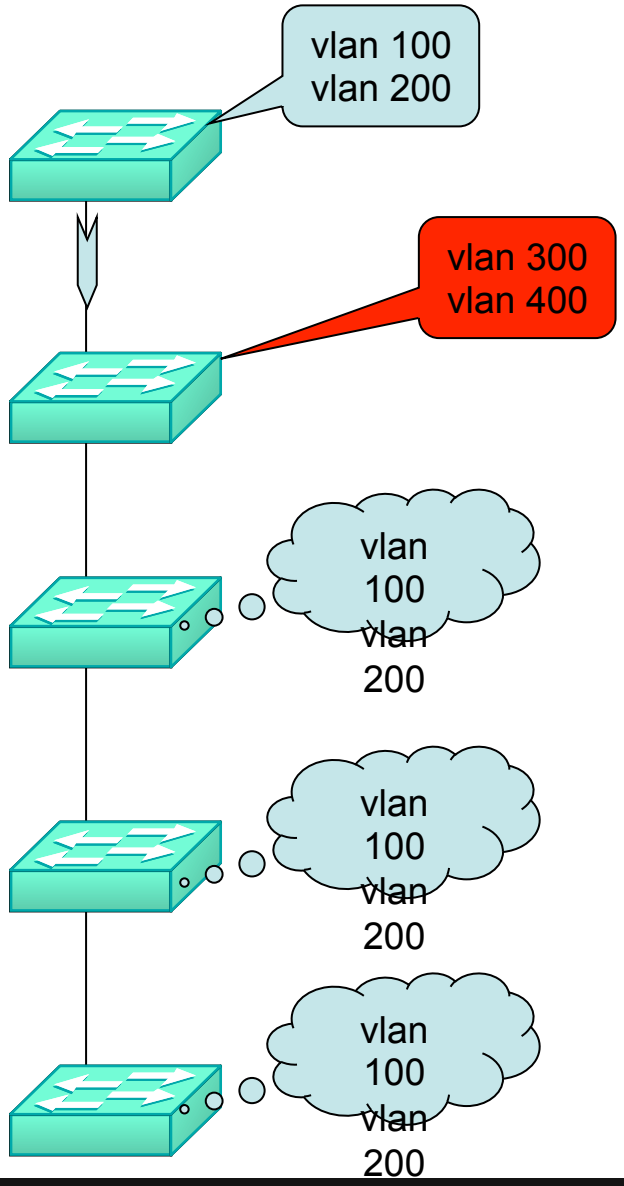
Exemple


(SERVER)
(SERVER)
(client)
indice = 0
indice = 0
indice = 0
conf t
vlan 100
name TOTO
indice = 1
indice = 0
indice = 0
1
synchronisation
synchronisation
conf t
vlan 200
name TATA
indice = 1
indice = 1
indice = 2
2
synchronisation
synchronisation
indice = 2
indice = 2

Sauvegarde

- Le switch server sauvegarde la configuration des VLANs
  - dans un fichier ‘vlan.dat’ (dans la mémoire flash)
  - dans la ‘startup-config’ (dans la NVRAM)
  - ➔ le switch server est indépendant
  - ➔ suite à une coupure de courant, il sait retrouver sa configuration de VLANs
- Le switch client ne sauvegarde pas la configuration des VLANs
  - ➔ suite à une coupure de courant, il a besoin de recevoir un message VTP pour créer les VLANs
  - ➔ aucun trafic dans les VLANs (autre que le vlan 1)

Problème….



- Tous les switchs doivent avoir la même configuration, sauf un.
- Ce switch différent ne doit pas empêcher la propagation des messages VTP !
- Le mode transparent :
  - il ne tient pas compte des messages VTP reçus, mais il les fait suivre sur toutes ses interfaces trunk.
  - il est indépendant : il sauvegarde sa configuration

Bilan VTP

MODE VTP :	Serveur	Client	Transparent
L'administrateur peut y ajouter / modifier / supprimer des VLANS ?	OUI	NON	OUI
Quand l'administrateur y a modifié des VLANs, l'indice de révision incrémente de 1 ?	OUI	non applicable	NON
Le switch tient compte des messages VTP reçus ?	OUI	OUI	NON
Le switch fait suivre les messages VTP reçus ?	OUI	OUI	OUI
Le switch sauvegarde la configuration de VLANs dans une mémoire non volatile ?	OUI	NON	OUI

Versions

- VTP existe en 2 versions.
- La version 2 a des fonctionnalités supplémentaires :
  - support pour le Token-ring
  - le switch transparent peut faire suivre les messages VTP d'un autre domaine VTP.
  - l'analyse de cohérence n'est effectuée que lorsqu'un VLAN est modifié via CLI ou SNMP, pas sur réception d'un message VTP
    - exemple : 2 VLANs ne doivent pas avoir le même nom
- Tous les switchs d'un même domaine VTP doivent fonctionner dans la même version VTP.

Mot de passe

- Il est possible de garantir la validité d'un message VTP en y ajoutant une signature MD5.

- Objectif : éviter qu'un switch malveillant supprime les VLANs du réseau en injectant des messages VTP dont l'indice de configuration est supérieur à l'indice courant dans le réseau.

VTP

Configuration

Activer VTP

- Par défaut, VTP n'est pas activé.
  - car le nom de domaine VTP est vide :

```
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 256
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDF 0x7D 0xFE 0x3A
  0xF7 0xD7 0xA2 0x44
Configuration last modified by 0.0.0.0 at 3-1-02 00:06:01
Local updater ID is 0.0.0.0
```

Activer VTP

Ancienne commande :	Nouvelle commande :
vlan database vtp domain eLearnCisco exit	configure terminal vtp domain eLearnCisco

```
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 256
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : eLearnCisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

Activer VTP

- Un switch ne peut appartenir qu'à un seul domaine VTP à la fois.
- Deux switchs doivent appartenir au même domaine VTP pour qu'ils tiennent compte des messages VTP échangés.
- Rappel : les messages VTP ne sont envoyés que sur les interfaces trunk.

Définir le mode VTP

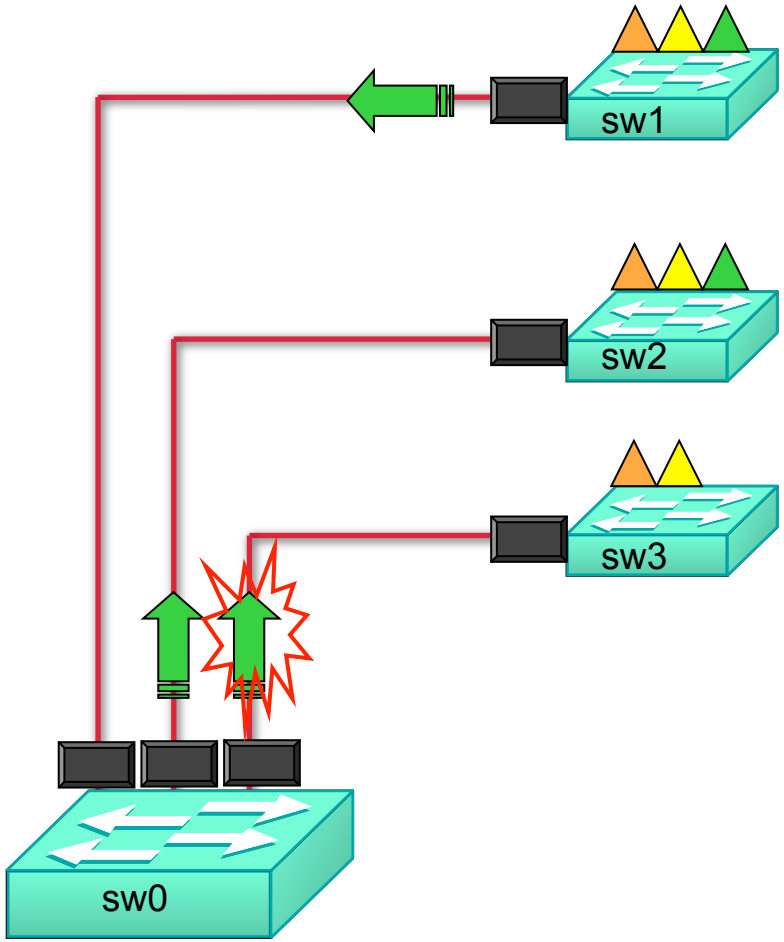
Ancienne commande :	Nouvelle commande :
vlan database vtp {server | client | transparent} exit	configure terminal vtp mode {server | client | transparent}

```
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 256
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : eLearnCisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
```

VTP

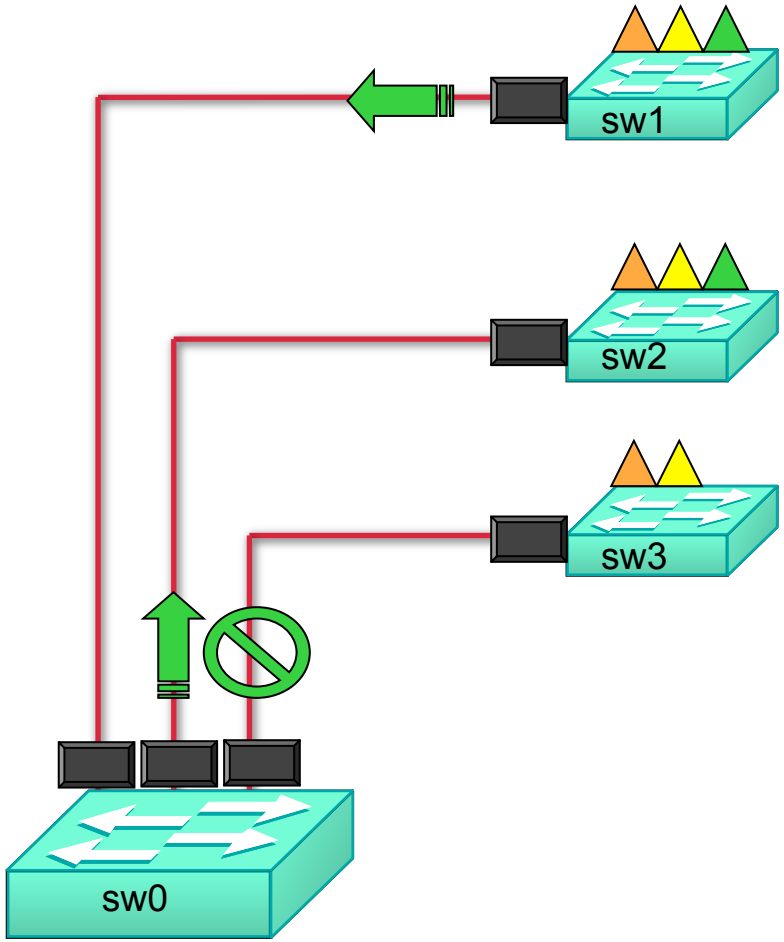
Pruning

Sans VTP pruning



- Sw1 reçoit un broadcast pour le Vlan VERT.
- Le broadcast est envoyé sur tous les trunks !
- Mais Sw3 n'a aucun port dans le Vlan VERT
- Le broadcast entre Sw0 et Sw3 aurait pu être évité.

Avec VTP pruning



- Certaines trames ne sont envoyés sur un trunk, que s' il existe en aval un switch intéressé, i.e. avec un port dans le VLAN de la trame :
  - les broadcast
  - les multicast
  - les unicast flooding

Activer VTP pruning

- Par défaut, VTP pruning n'est pas activé.

```
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 256
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : eLearnCisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDF 0x7D 0xFE 0x3A
  0xF7 0xD7 0xA2 0x44
Configuration last modified by 0.0.0.0 at 3-1-02 00:06:01
Local updater ID is 0.0.0.0
Sw2#
```

Activer VTP pruning

Ancienne commande :	Nouvelle commande :
vlan database vtp pruning exit	configure terminal vtp pruning

```
Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 256
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : eLearnCisco
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
```

Bilan des commandes VTP

Ancienne commande :	Nouvelle commande :
`vlan database`	`configure terminal`
`vtp domain eLearnCisco`	`vtp domain eLearnCisco`
`vtp server`	`vtp mode server`
`vtp client`	`vtp mode client`
`vtp transparent`	`vtp mode transparent`
`vtp password TOTO`	`vtp password TOTO`
`vtp v2-mode`	`vtp v2-mode`
`vtp pruning`	`vtp pruning`
`exit`	`exit`

How to enable vlans automatically across multiple switches?

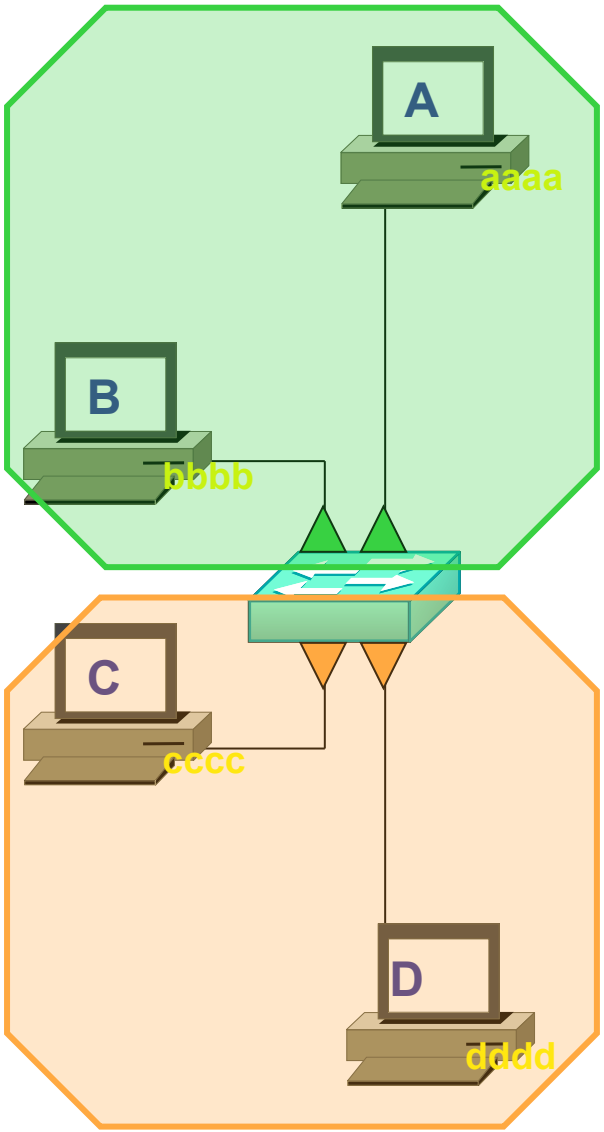
A. Configure VLAN
B. Confiture NTP
C. Configure each VLAN
D. Configure VTP

Correct Answer: D

Router on the stick

Routage inter-VLAN

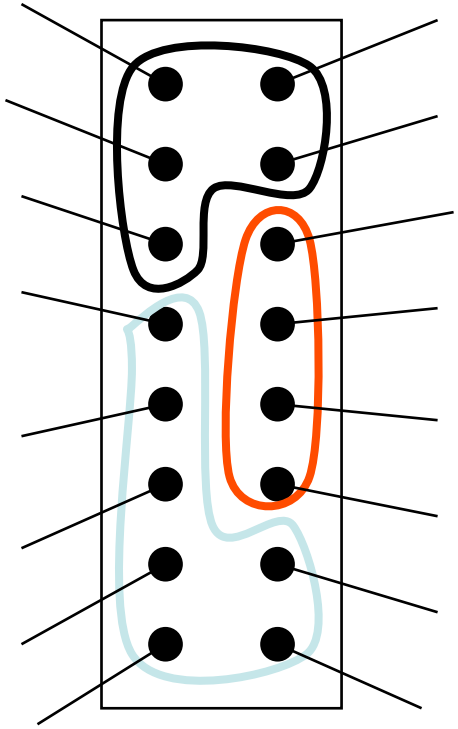
Rappel : 2 VLANs

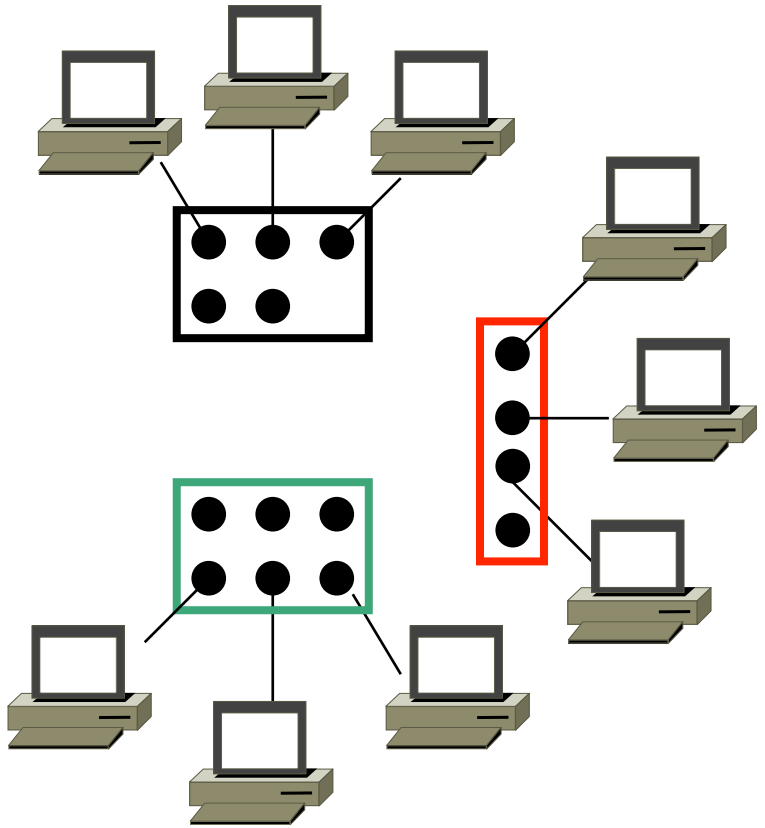


- Deux domaines de broadcast.
  - le switch ne permet aucune communication entre les 2 VLANs.
- Chaque VLAN doit avoir sa propre adresse réseau.

Vue logique des VLANs

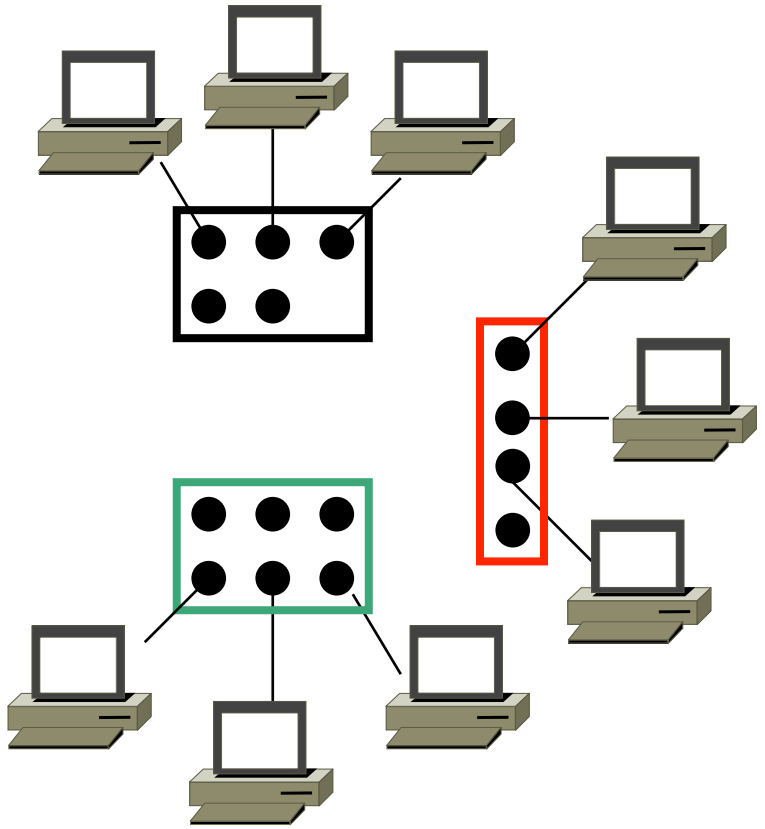
- Tout se passe comme s' il y avait plusieurs switchs :





Plan d'adressage des VLANs

- Chaque VLAN a sa propre adresse réseau.
- Exemple :
  - 10.0.0.0 /8
  - 11.0.0.0 /8
  - 12.0.0.0 /8

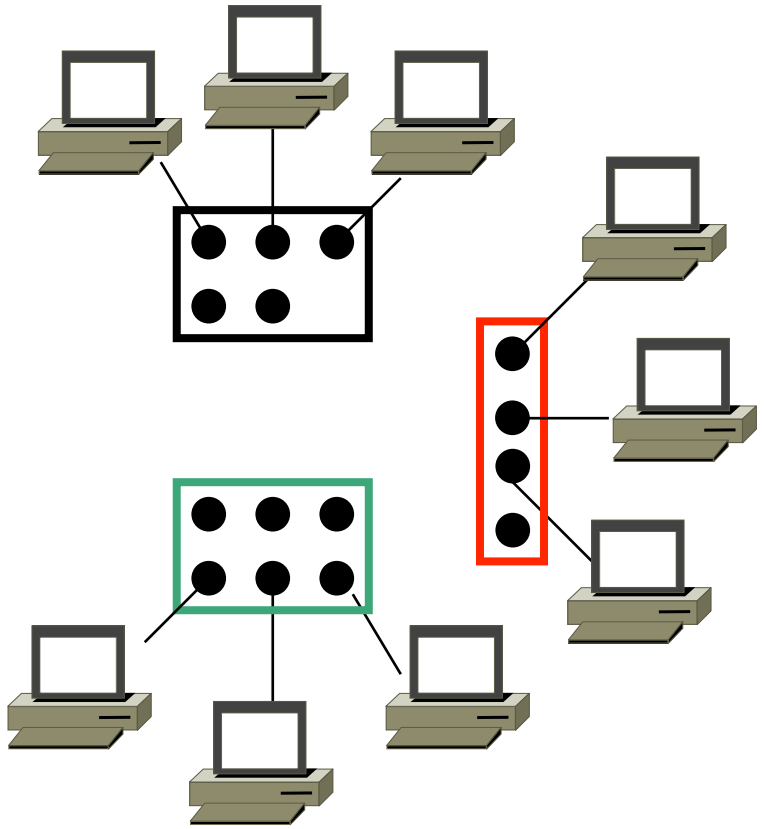


Vue logique des VLANs

- Tout se passe comme s'il y avait plusieurs switchs :

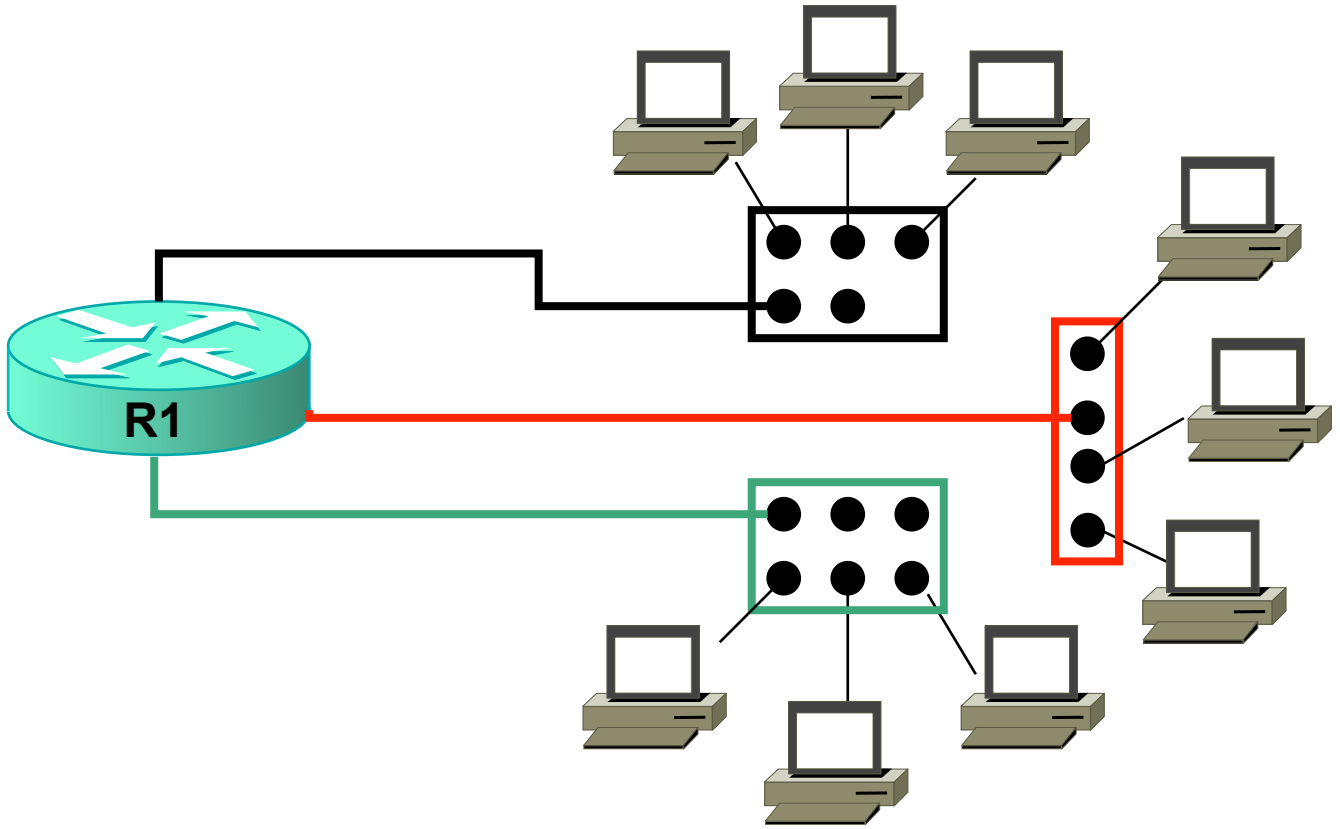
PROBLEME :
les équipements placés dans différents VLANs ne peuvent plus communiquer ensemble !

SOLUTION :
utiliser un ROUTEUR.



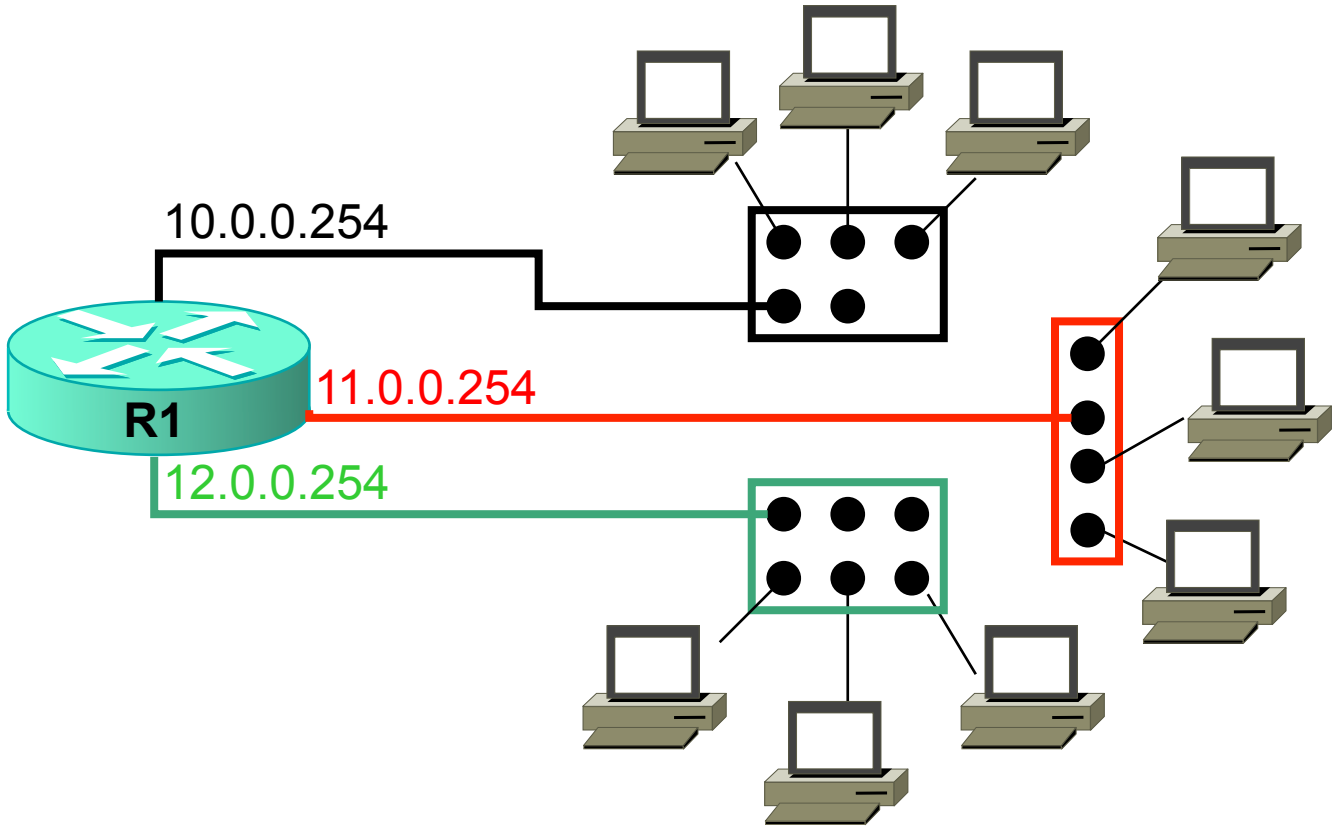
Utiliser un routeur

- Le routeur devra avoir une interface dans chaque VLAN :



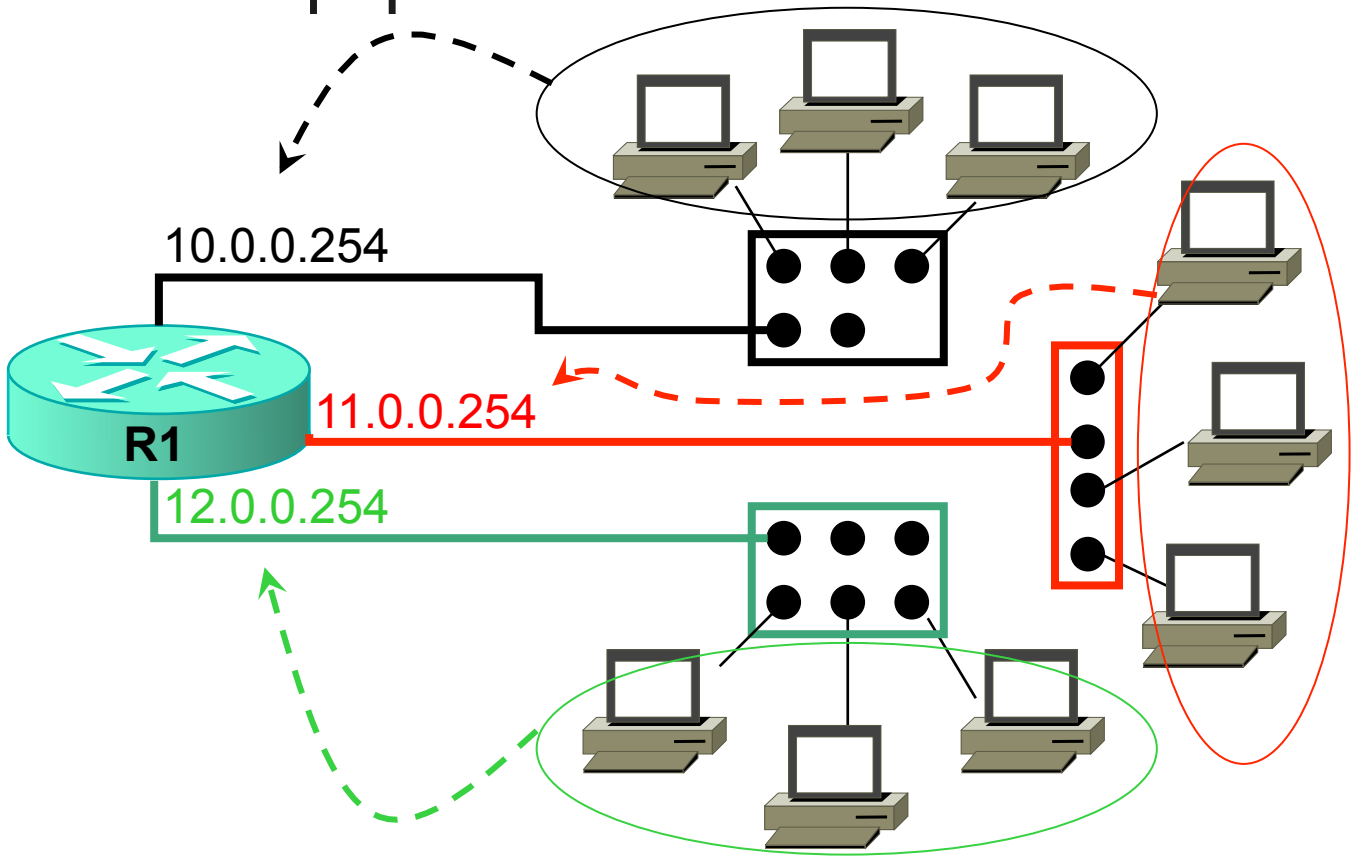
Utiliser un routeur

- L'adresse IP de chaque interface devra correspondre au plan d'adressage des VLANs :



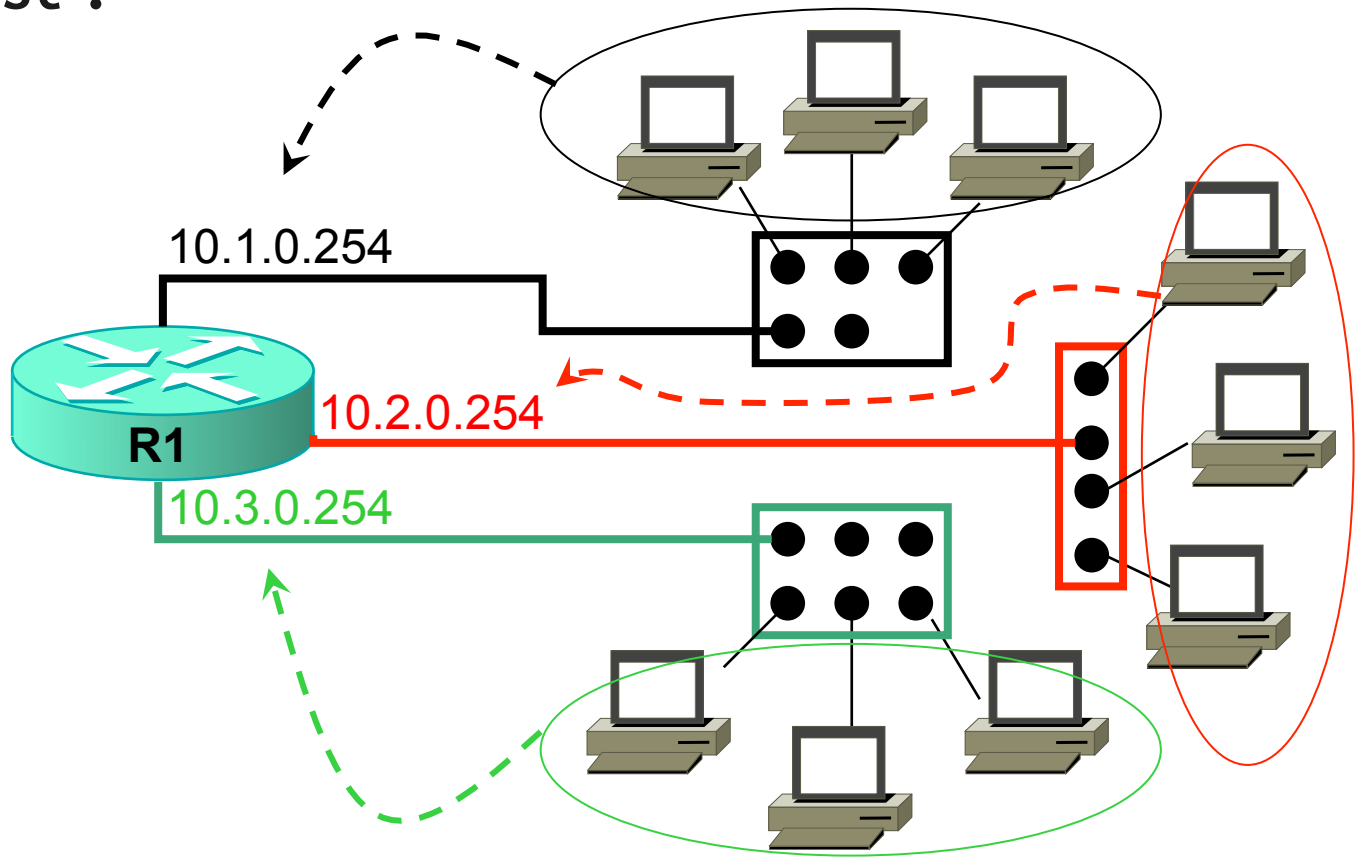
Utiliser un routeur

- L'adresse IP du routeur doit être la passerelle par défaut des équipements du VLAN :



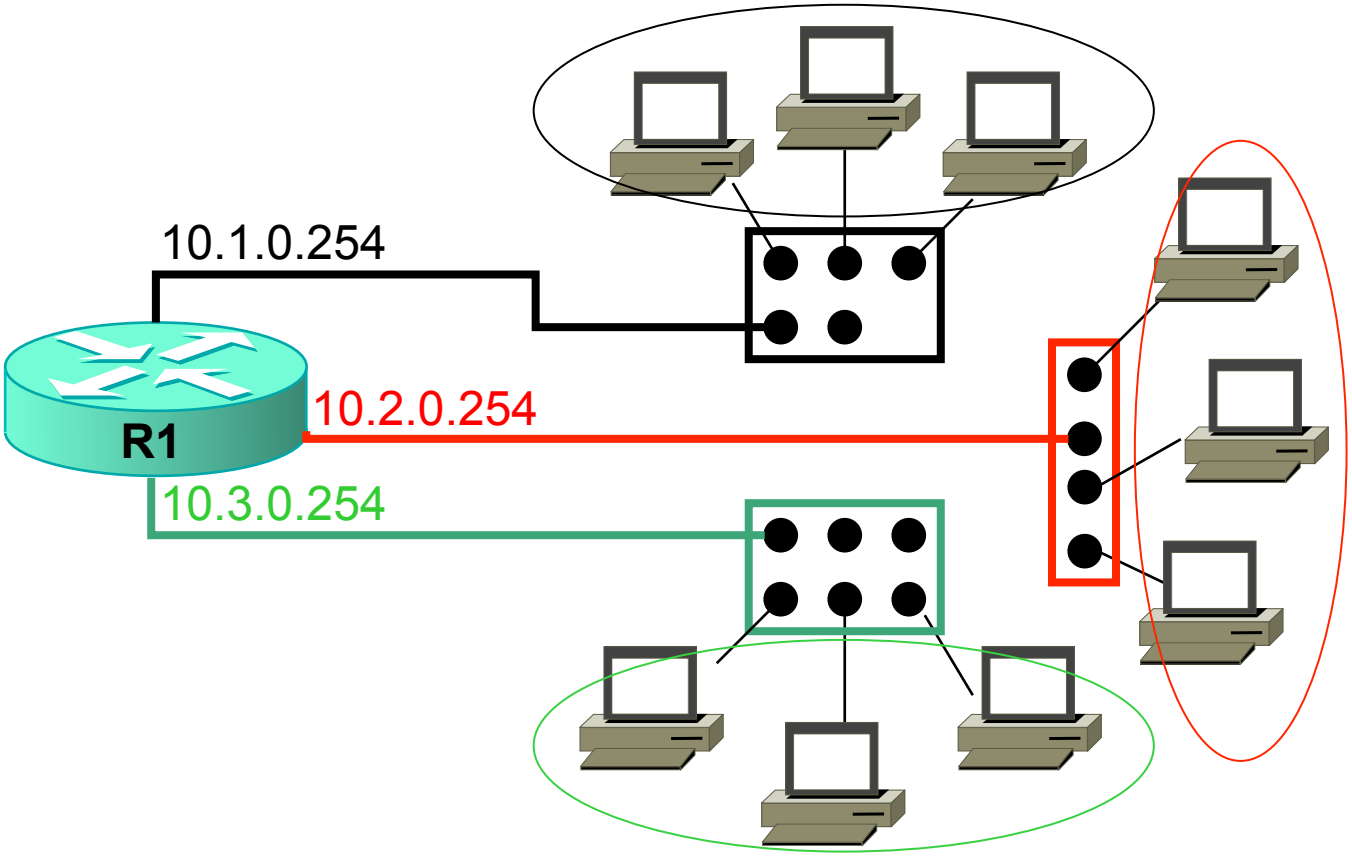
Domaine de broadcast

- Combien y a-t-il maintenant de domaines de broadcast ?



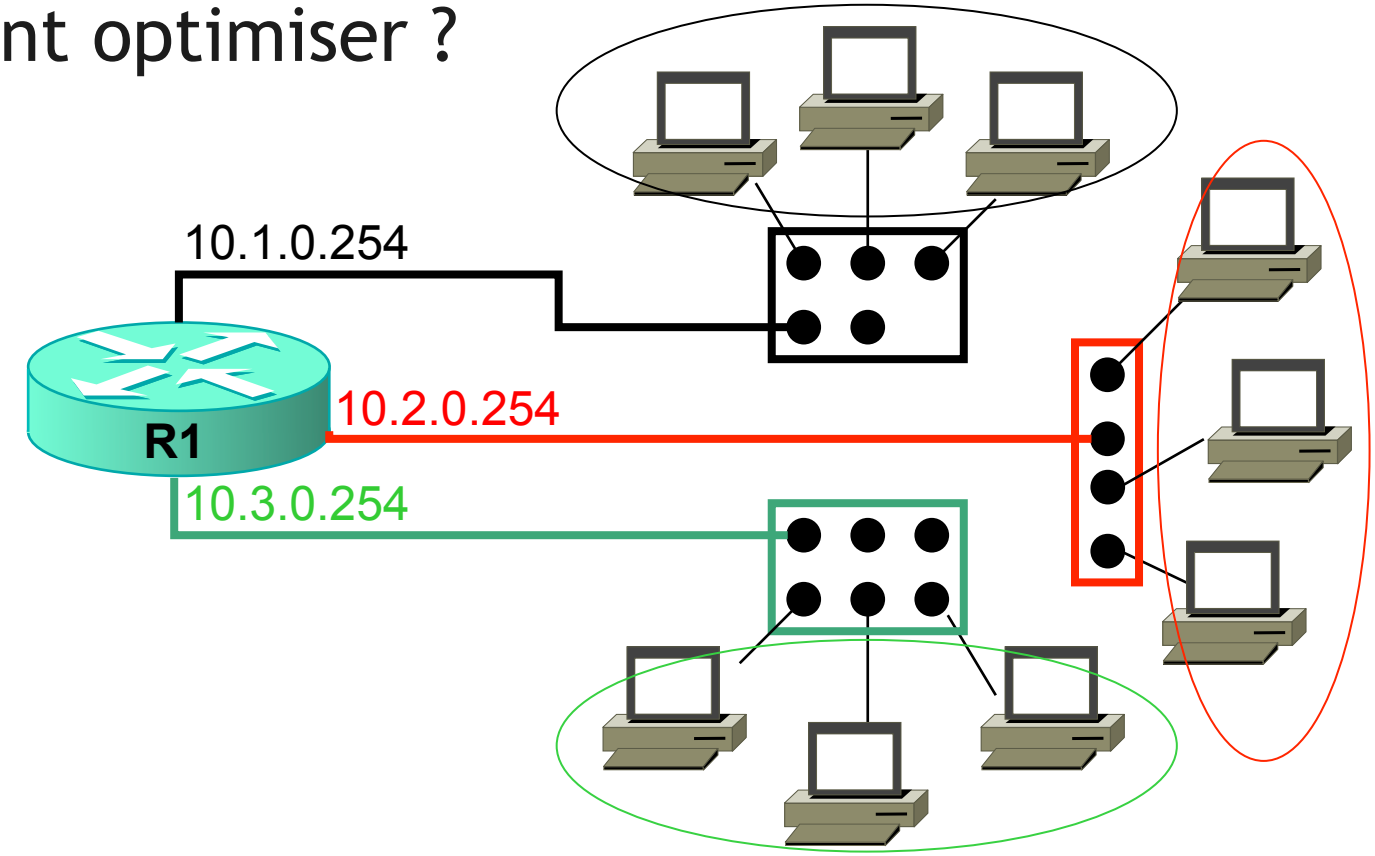
Domaine de broadcast

- Toujours TROIS !



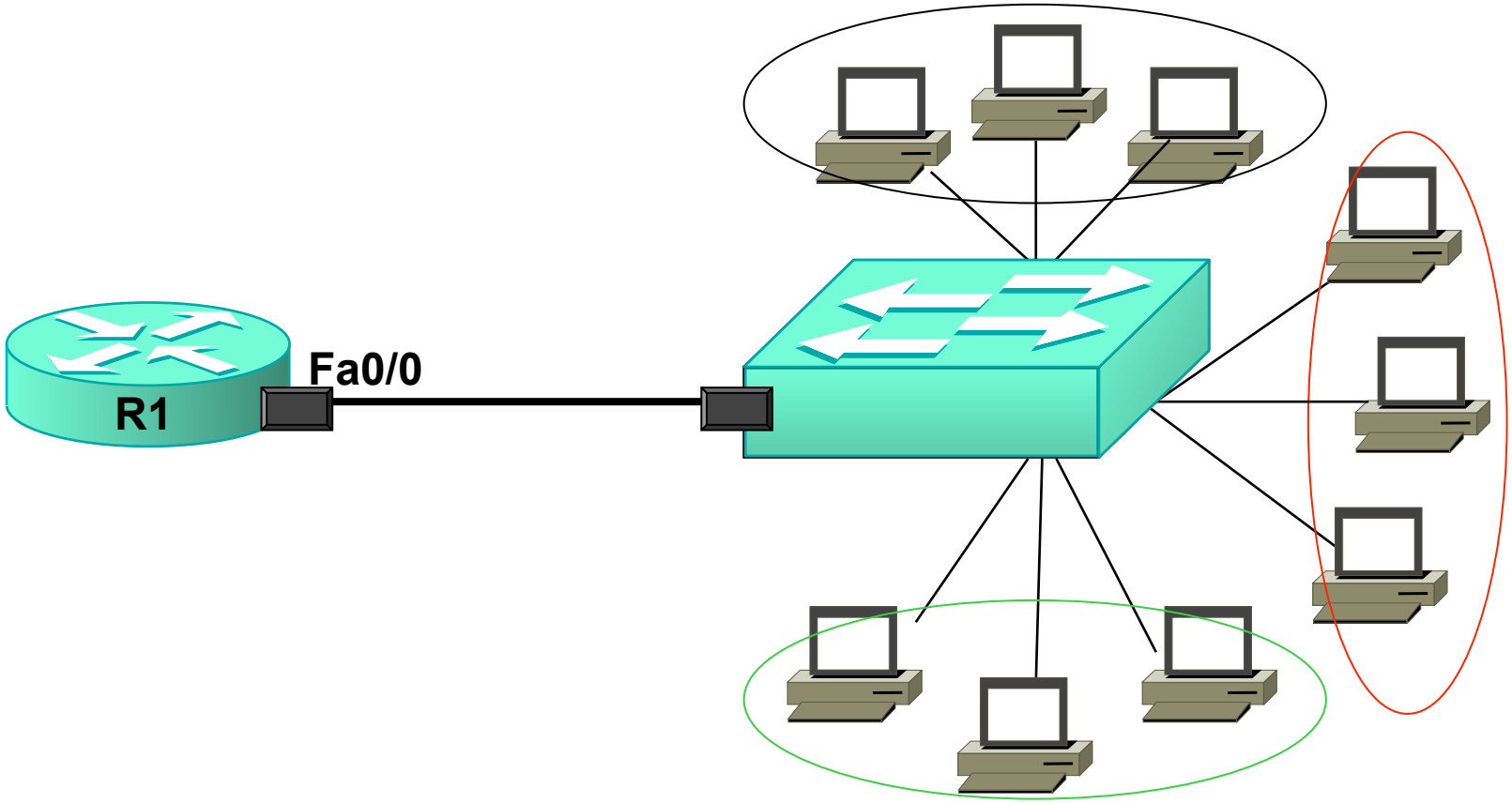
Optimiser

- 3 VLANs = je consomme 3 interfaces !
- Comment optimiser ?



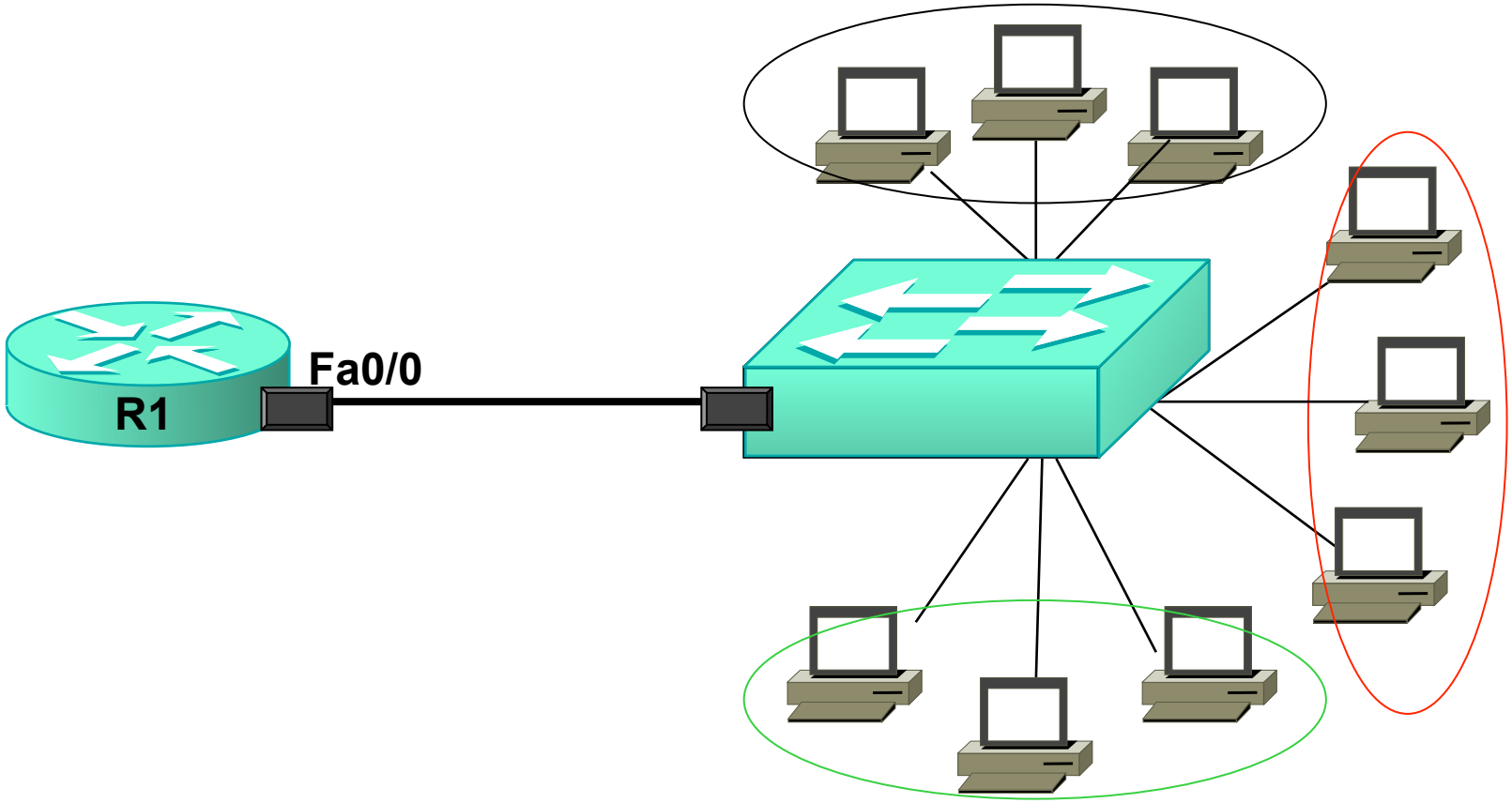
Trunk

- Utiliser une seule interface, en trunk !



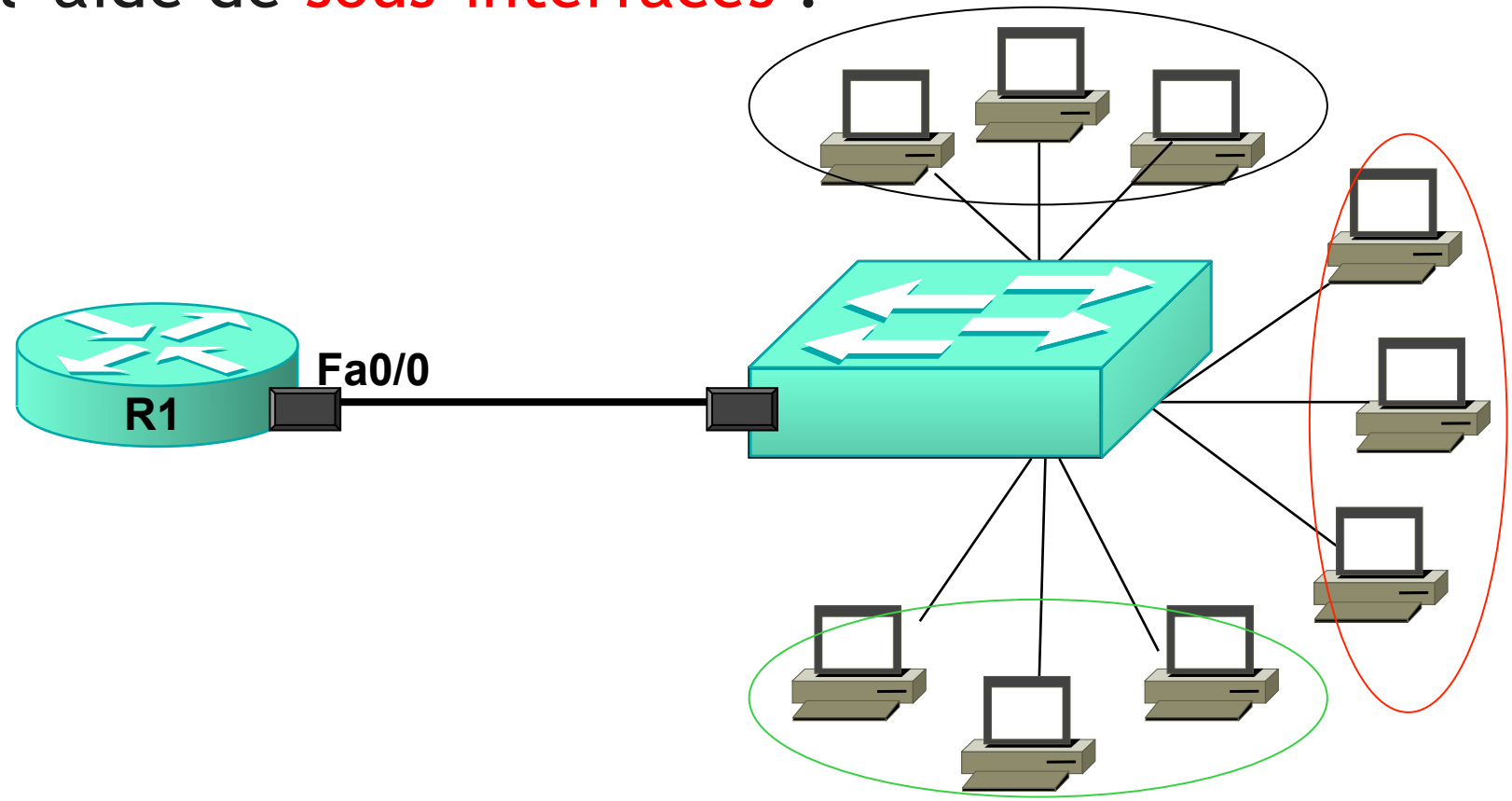
Trunk

- Quelle adresse IP mettre sur le routeur ?



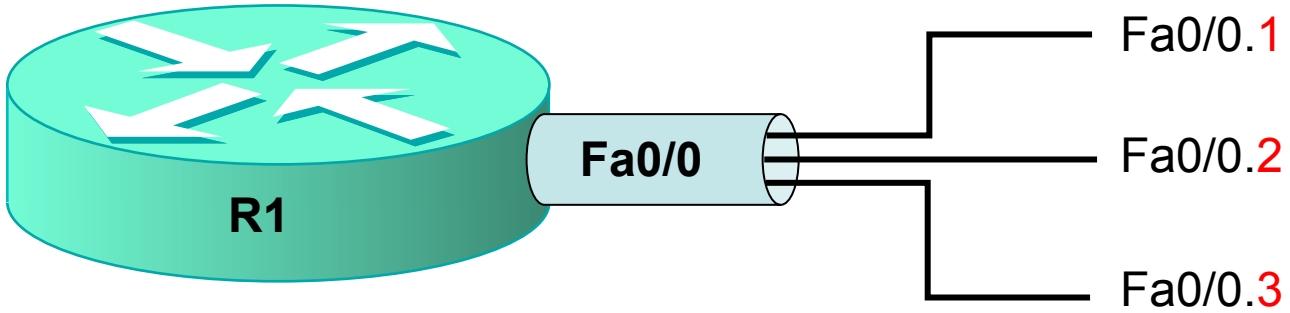
Trunk

- Configurer les 3 adresses IP sur le routeur à l'aide de sous-interfaces :



Sous-interfaces

- Chaque sous-interface est définie par un numéro choisi arbitrairement : l'interface physique est divisée en plusieurs interfaces logiques.

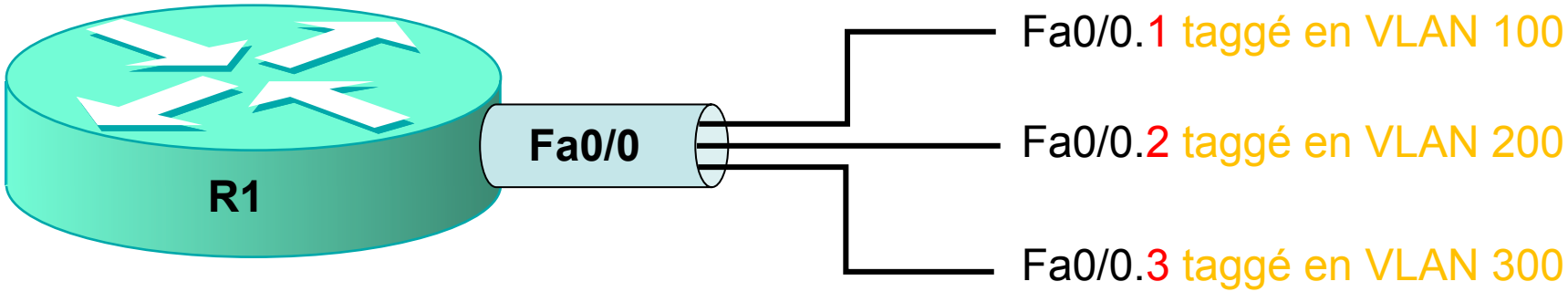


POUR CRÉER les SOUS-INTERFACES :

```
configure terminal
interface Fa0/0.1
interface Fa0/0.2
interface Fa0/0.3
```

Sous-interfaces

- Chaque sous-interface est associée à un numéro de VLAN

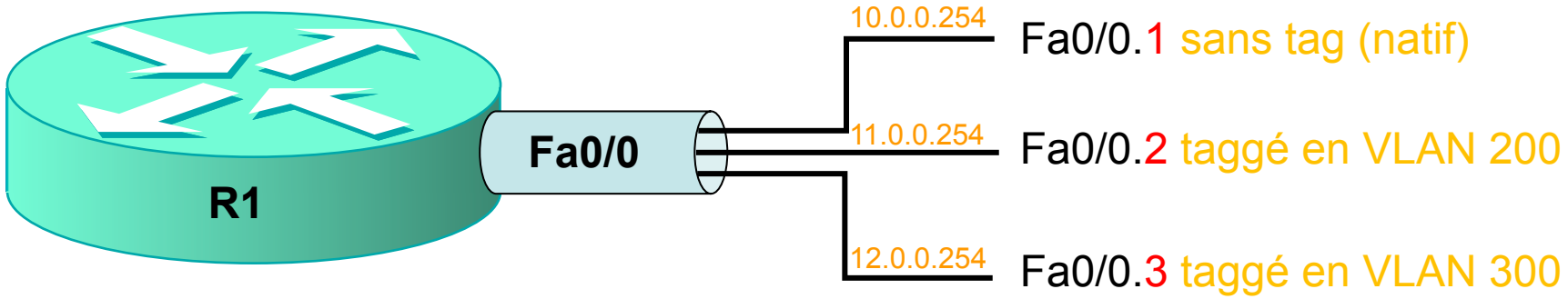


POUR ASSOCIER les SOUS-INTERFACES à un numéro de VLAN :

```
configure terminal
interface Fa0/0.1
        encapsulation dot1q 100
interface Fa0/0.2
        encapsulation dot1q 200
interface Fa0/0.3
        encapsulation dot1q 300
```

Sous-interfaces

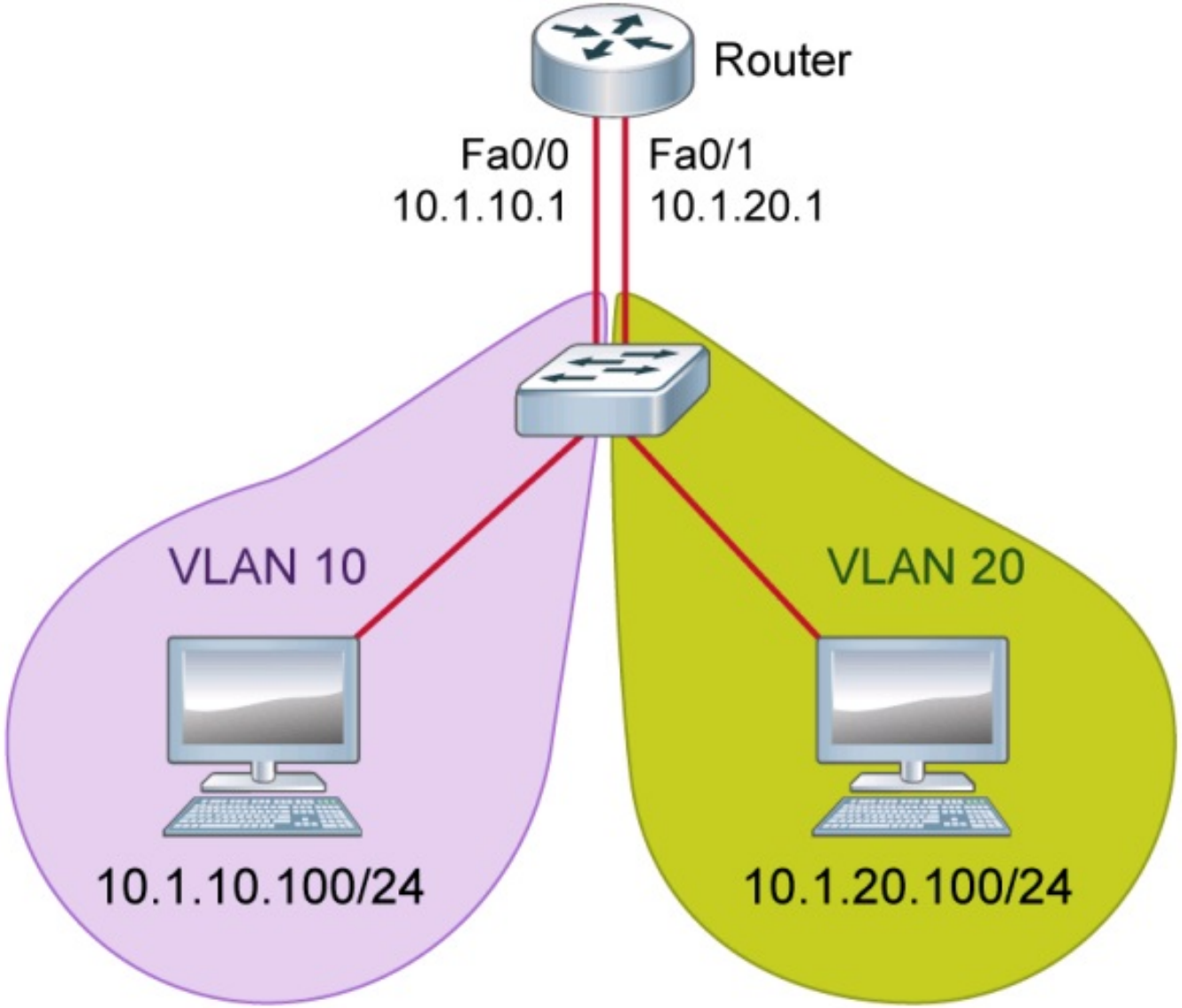
- Chaque sous-interface doit avoir une adresse IP : la passerelle du VLAN.



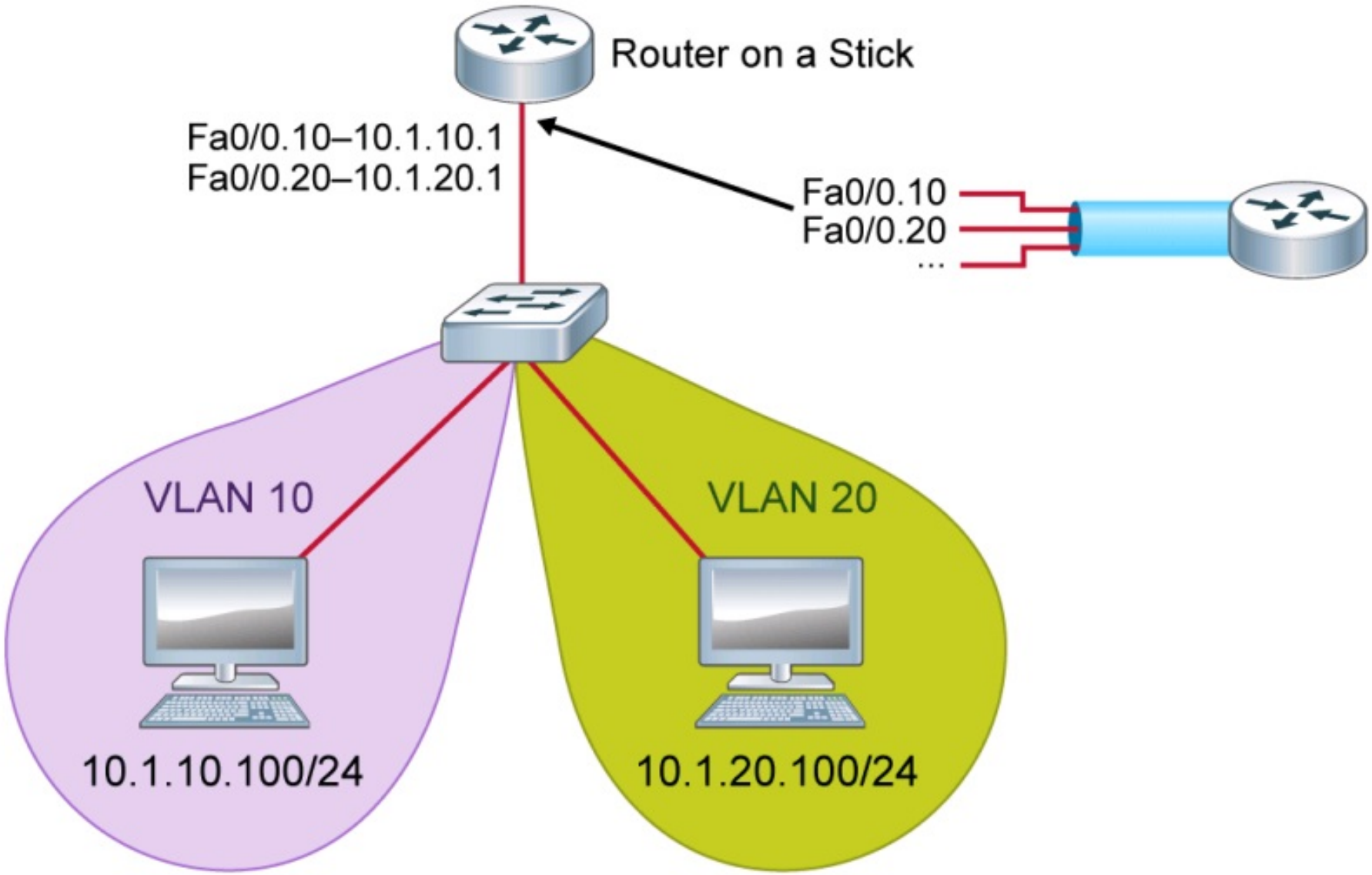
POUR CONFIGURER une adresse IP dans chaque SOUS-INTERFACE :

```
configure terminal
interface Fa0/0.1
   encapsulation dot1q 100
   ip address 10.0.0.254 255.0.0.0 native
interface Fa0/0.2
   encapsulation dot1q 200
   ip address 11.0.0.254 255.0.0.0
interface Fa0/0.3
   encapsulation dot1q 300
   ip address 12.0.0.254 255.0.0.0
```

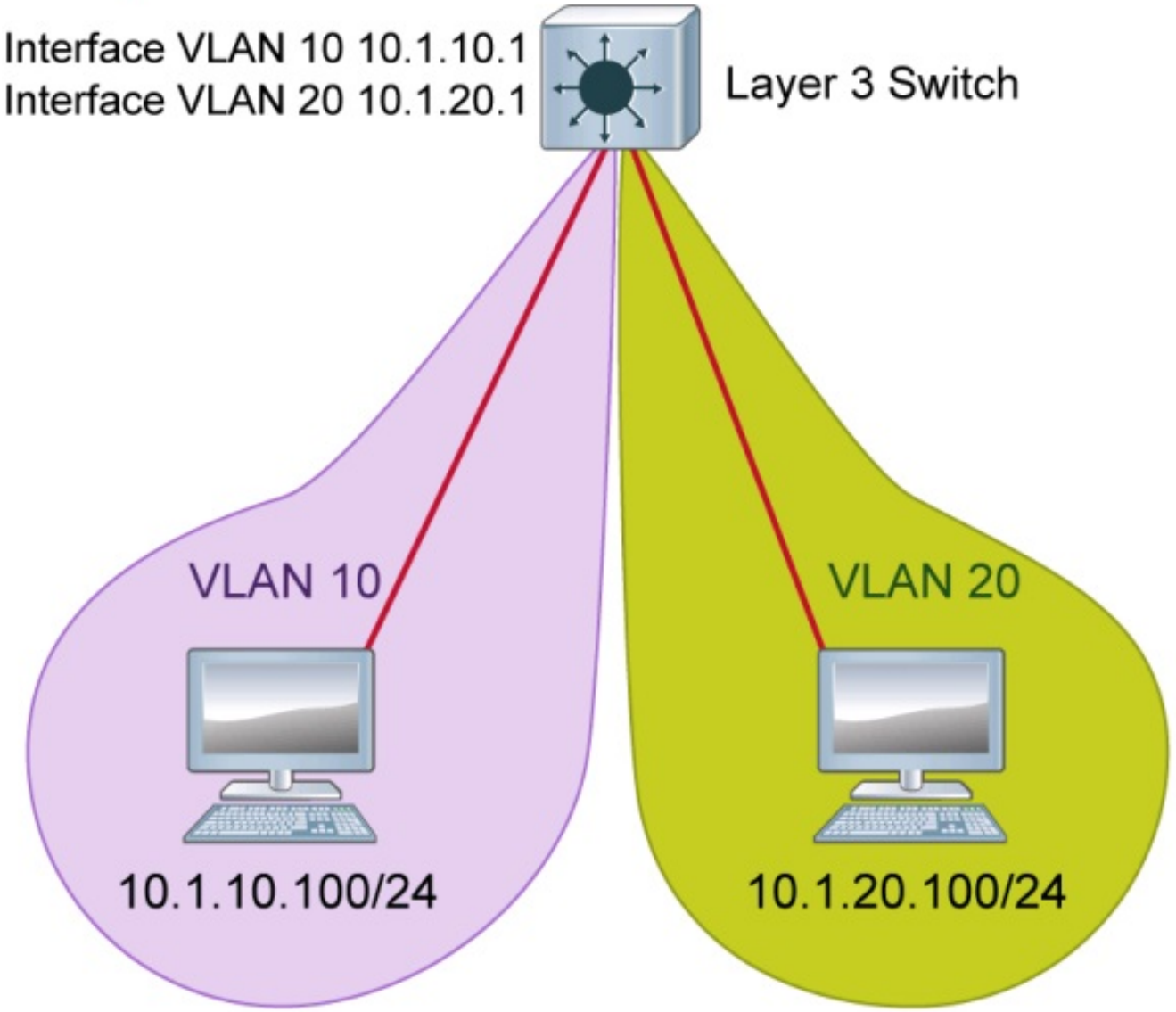
Option 1: Router with a Separate Interface in Each VLAN



Option 3: Router on a Stick



Option 2: Layer 3 Switch

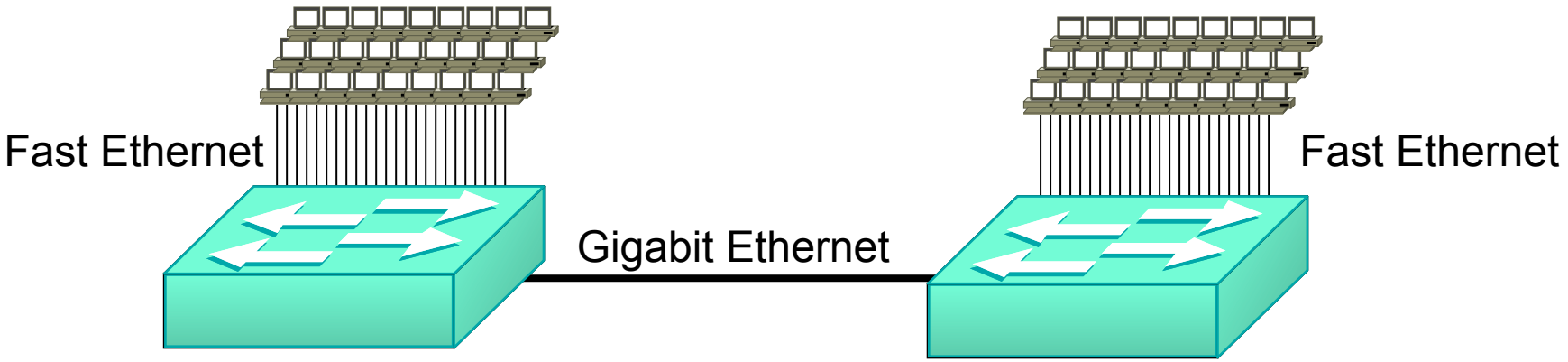


Le management du switch

Introduction

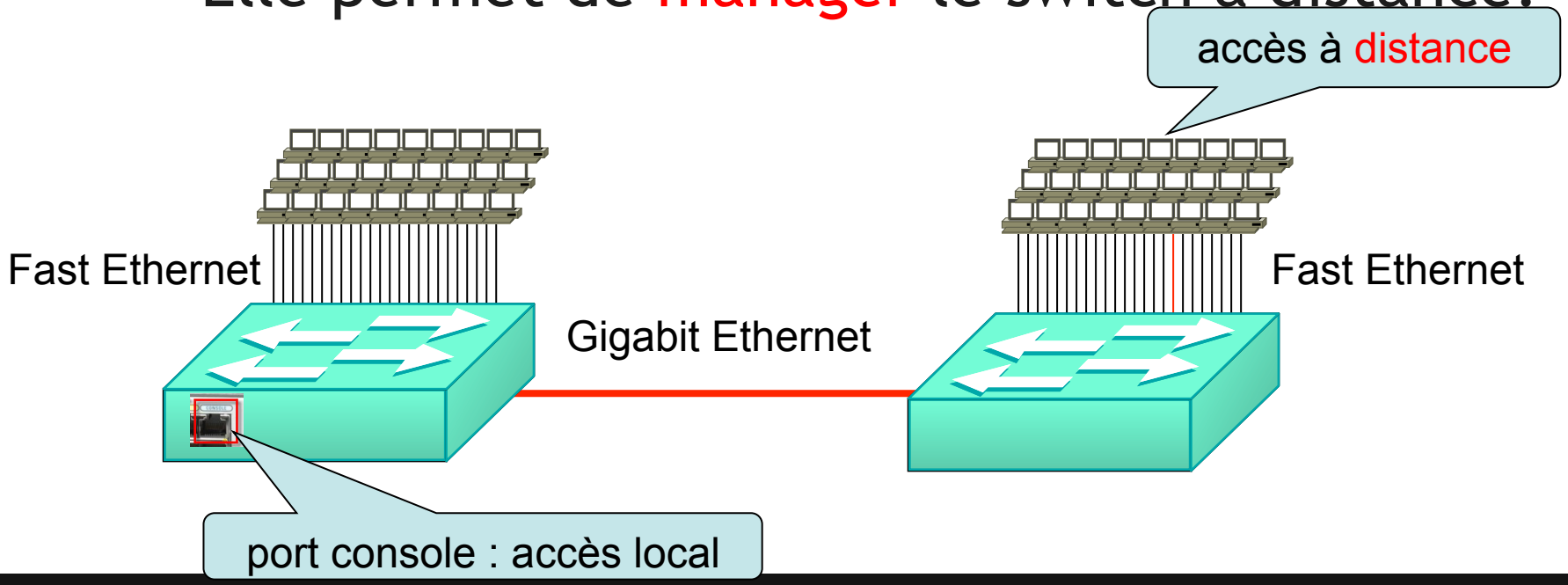
L'adresse IP d'un switch.

- Est-il obligatoire de mettre une adresse IP sur un switch ?
- Sur quelle interface configurer l'adresse IP ?
- A quoi cette adresse peut-elle servir ?



L'adresse IP d'un switch.

- Elle n'est pas obligatoire.
- Elle sera configurée sur l'interface VLAN 1.
- Elle permet de manager le switch à distance.

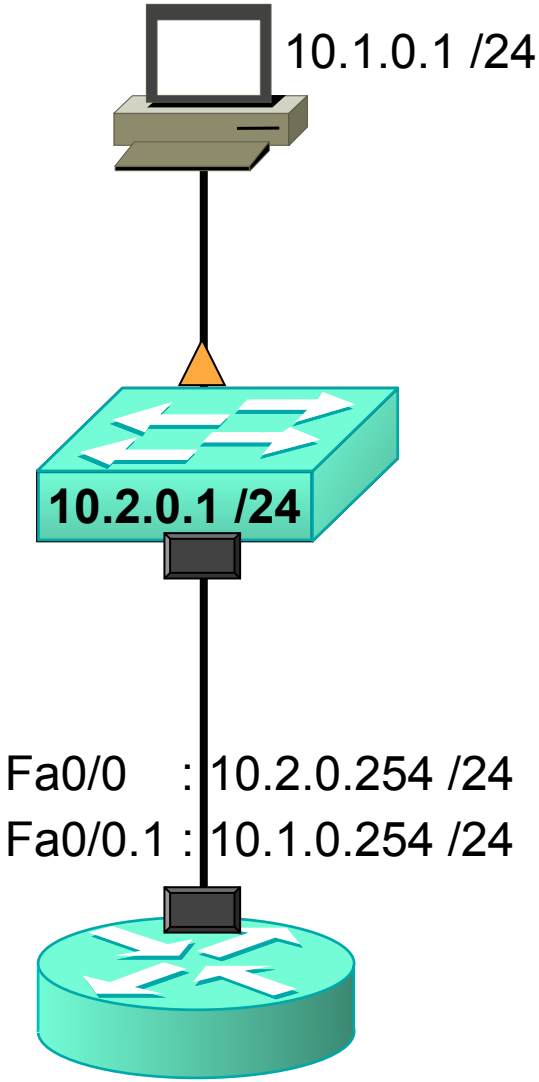


Configuration

Exemple de configuration :

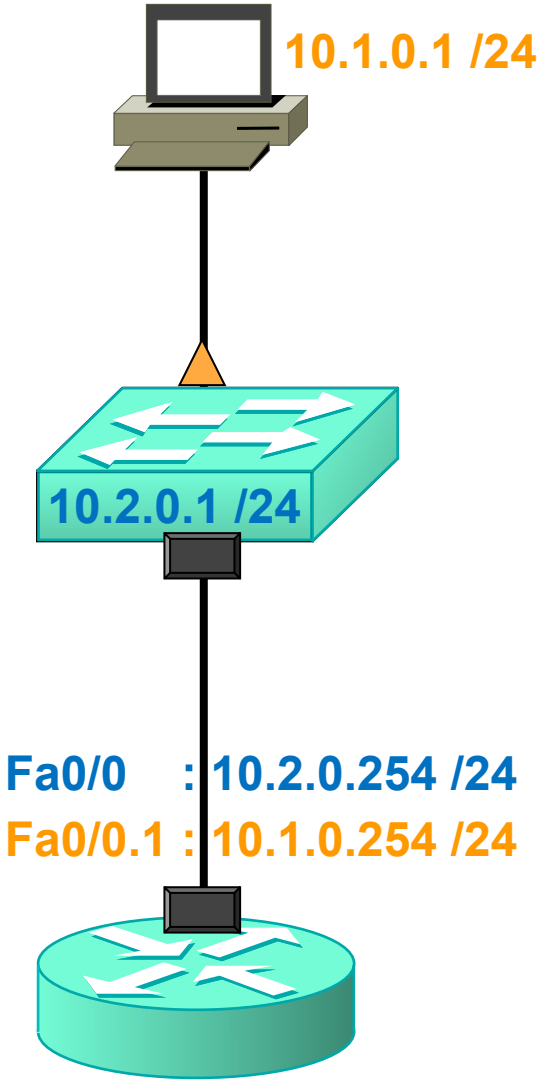
```
configure terminal
interface vlan 1
ip address 10.0.0.1 255.255.255.0
exit

default-gateway 10.0.0.254
```

Exercice



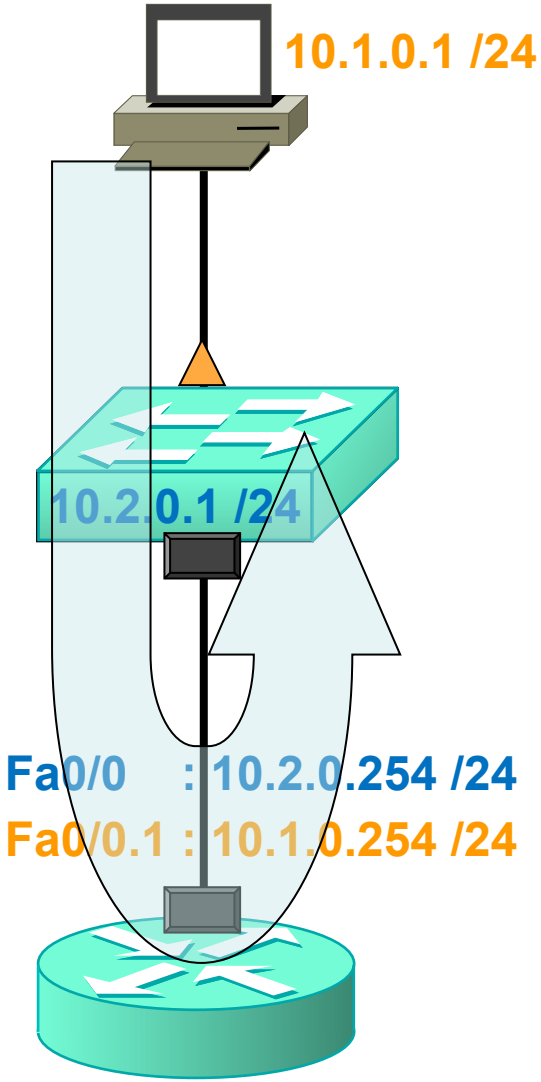
- Quelle est la passerelle par défaut du PC ?
- Quelle est la passerelle par défaut du switch ?
- Quel chemin empruntera le traffic entre le PC et le switch ?

Solution



- La passerelle par défaut du PC est 10.1.0.254
- La passerelle par défaut du switch est 10.2.0.254.

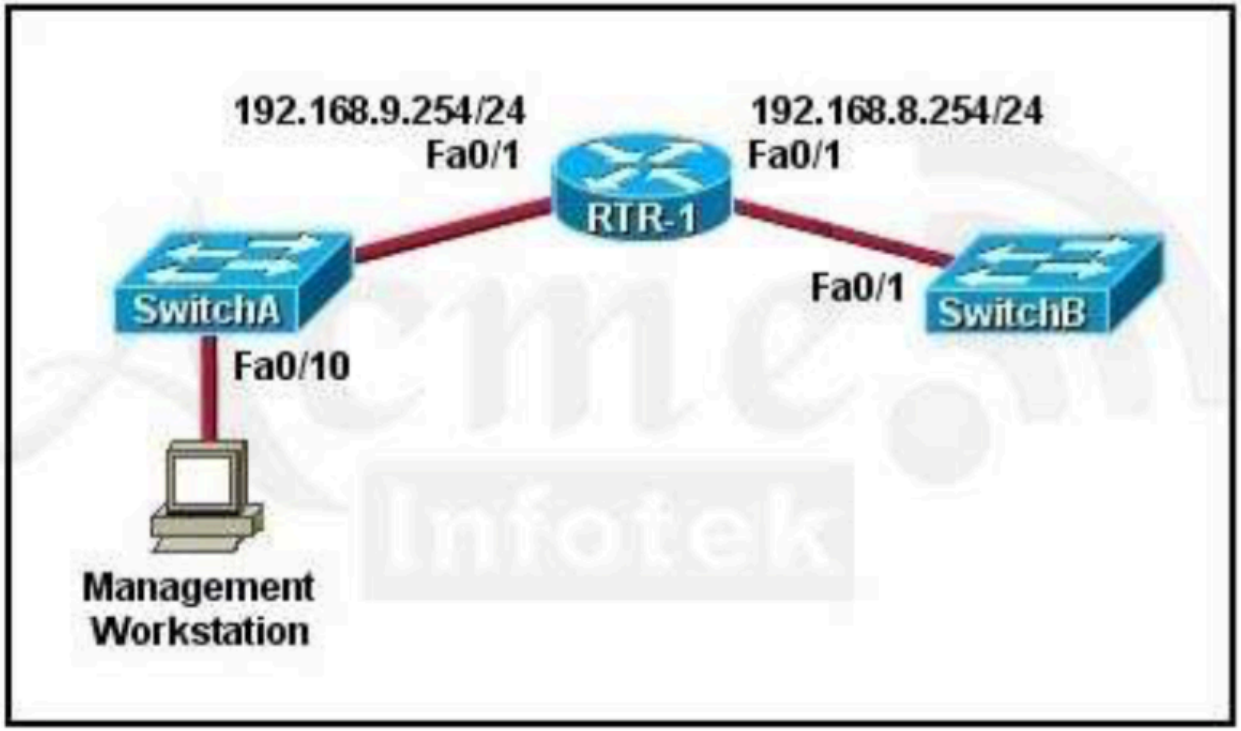
Solution



- Chemin emprunté par le traffic de management entre le PC et le switch.

Test

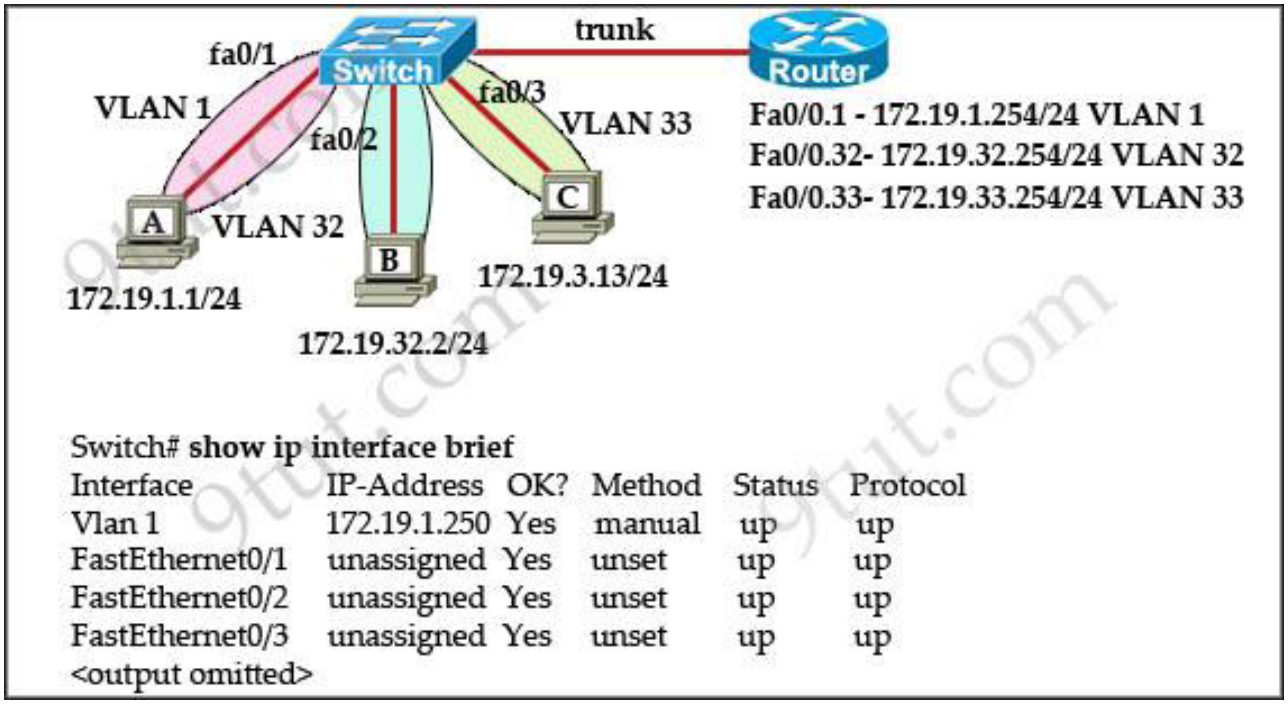
Quelle configuration permettra de manager le switch B à distance ?




```
SwitchB(config)# ip default-gateway 192.168.8.254
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
```

Test

The network administrator normally establishes a Telnet session with the switch from host A. However, host A is unavailable. The administrator's attempt to telnet to the switch from host B fails, but pings to the other two hosts are successful. What is the issue?



Switch# **show ip interface brief**

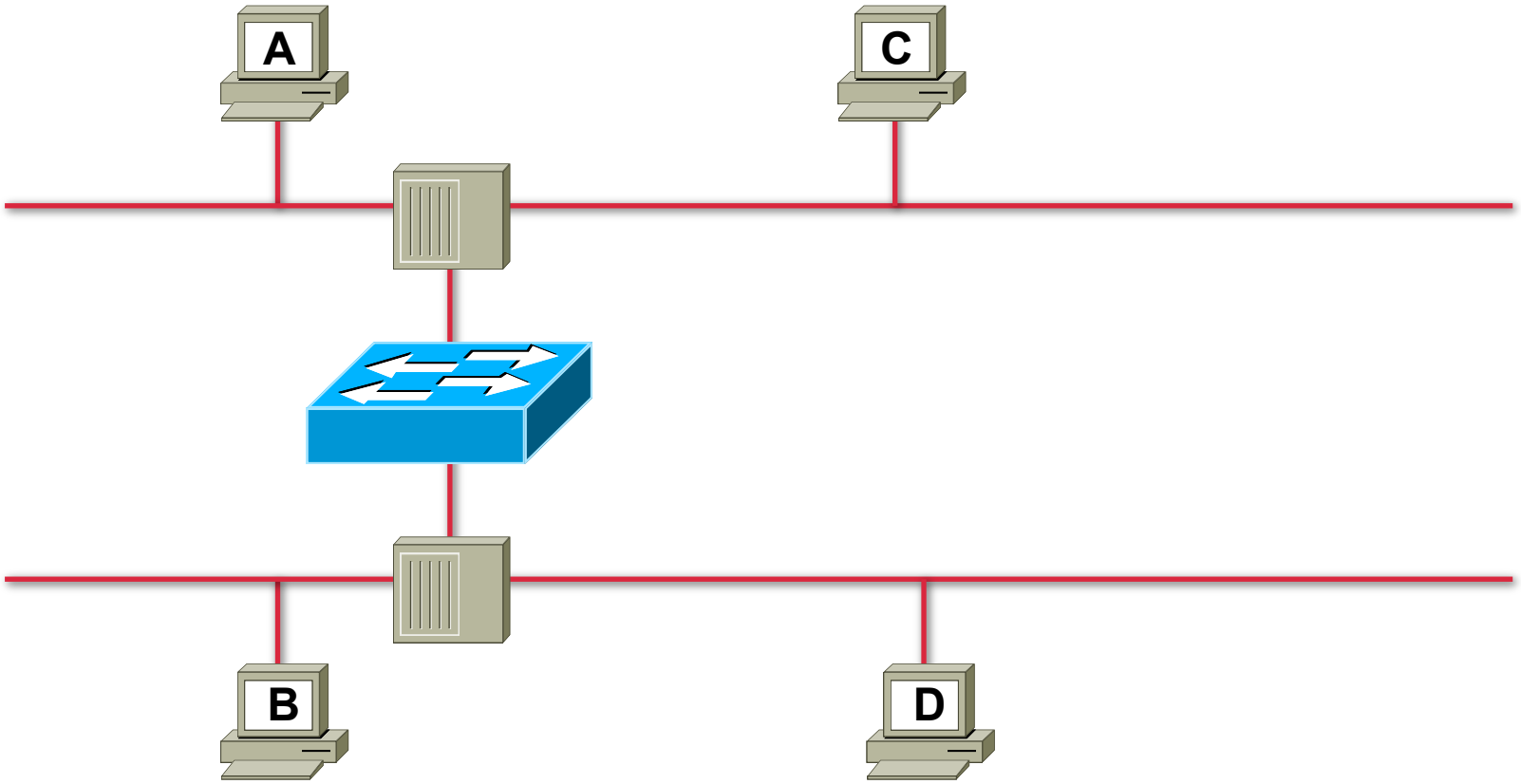
Interface	IP-Address	OK?	Method	Status	Protocol
Vlan 1	172.19.1.250	Yes	manual	up	up
FastEthernet0/1	unassigned	Yes	unset	up	up
FastEthernet0/2	unassigned	Yes	unset	up	up
FastEthernet0/3	unassigned	Yes	unset	up	up

<output omitted>

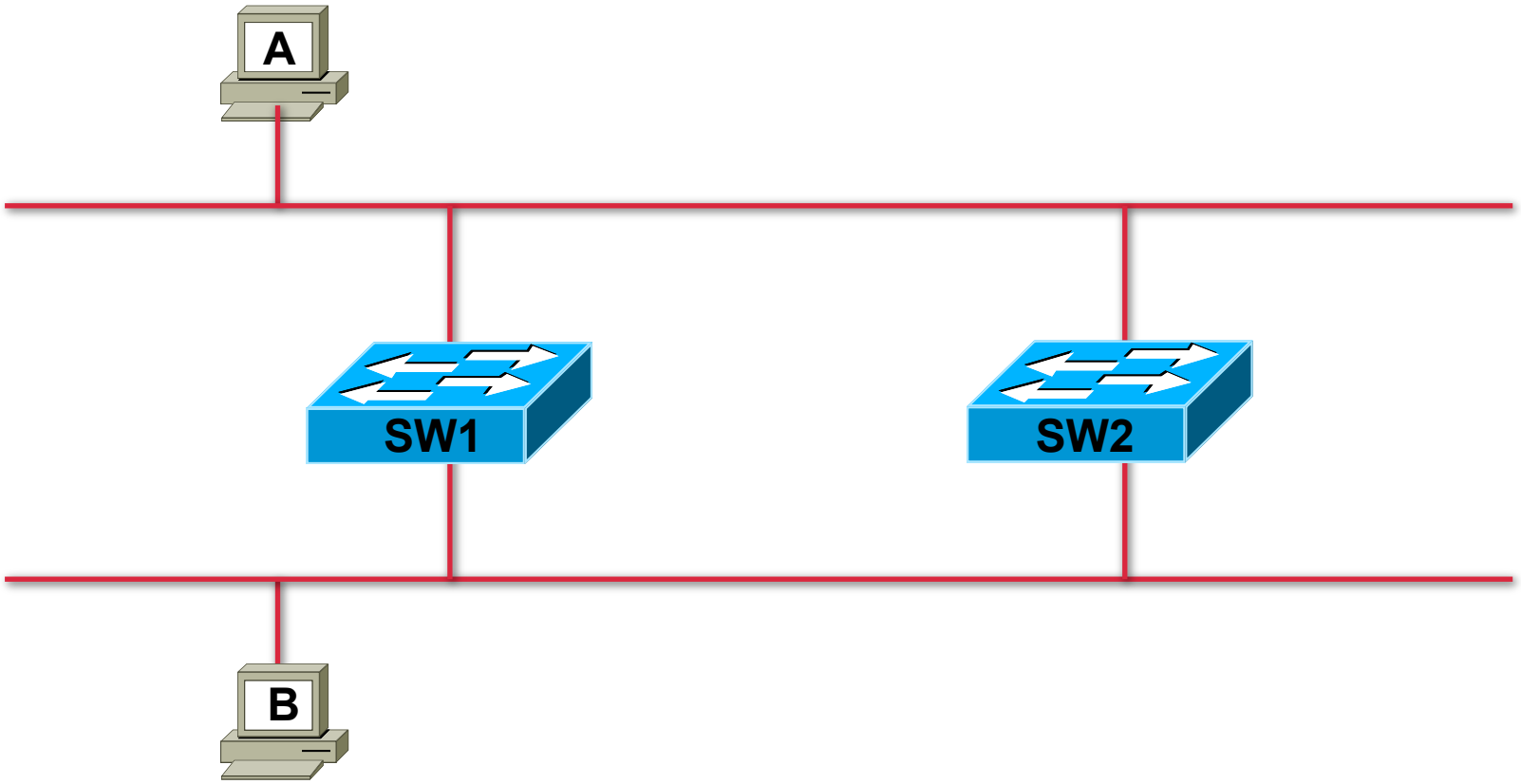
STP

Spanning-Tree Protocol

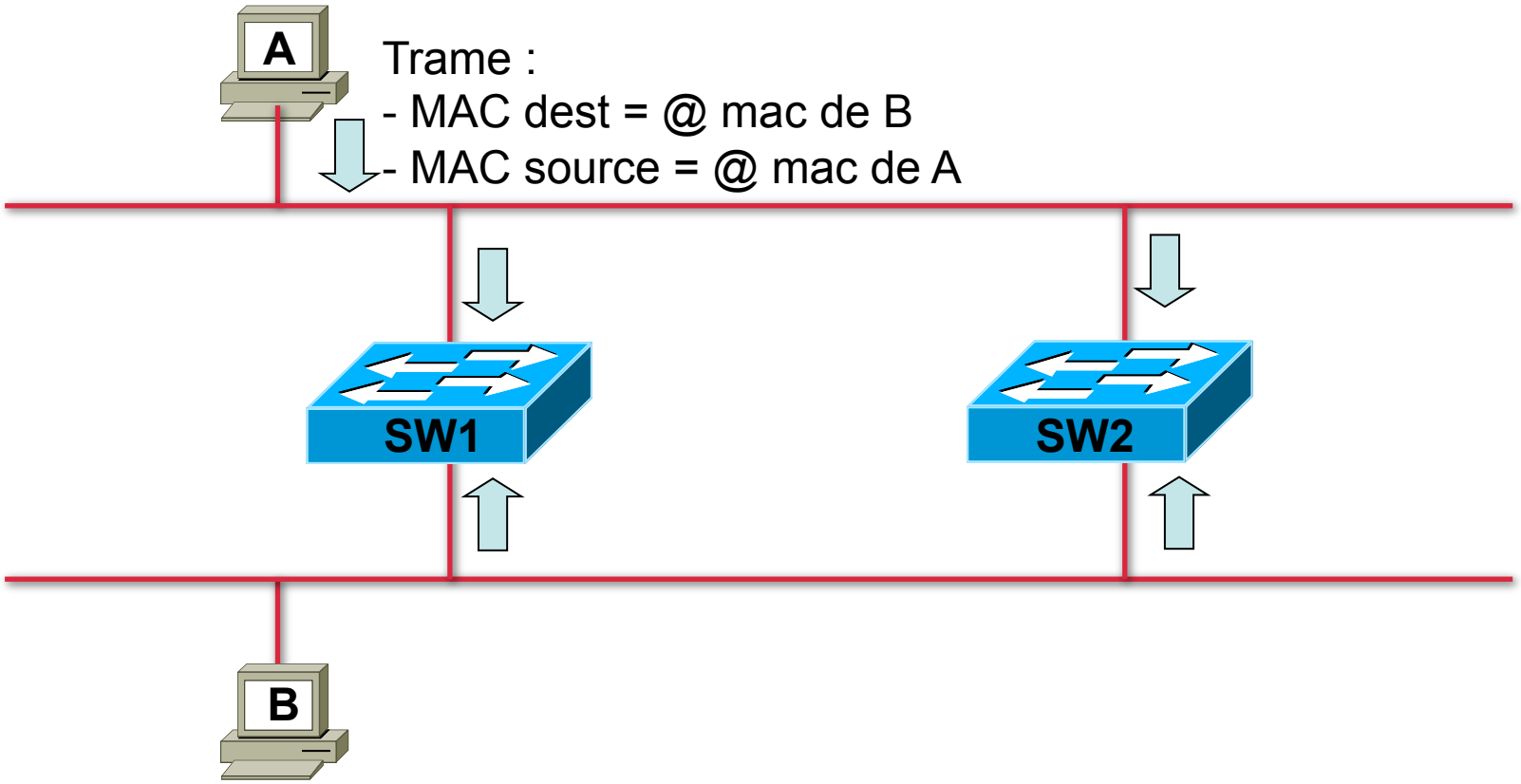
Et si le switch tombe …



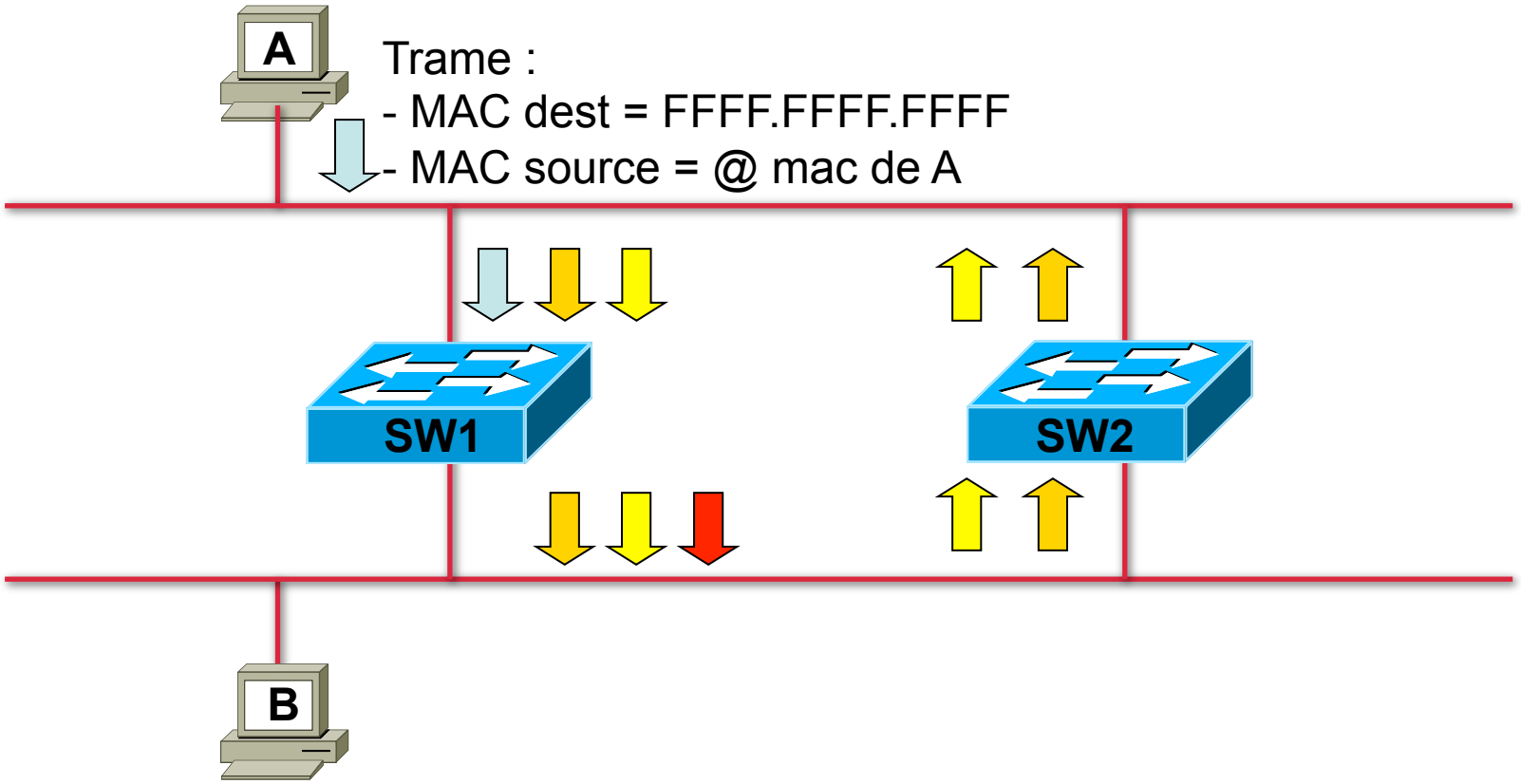
Redondance



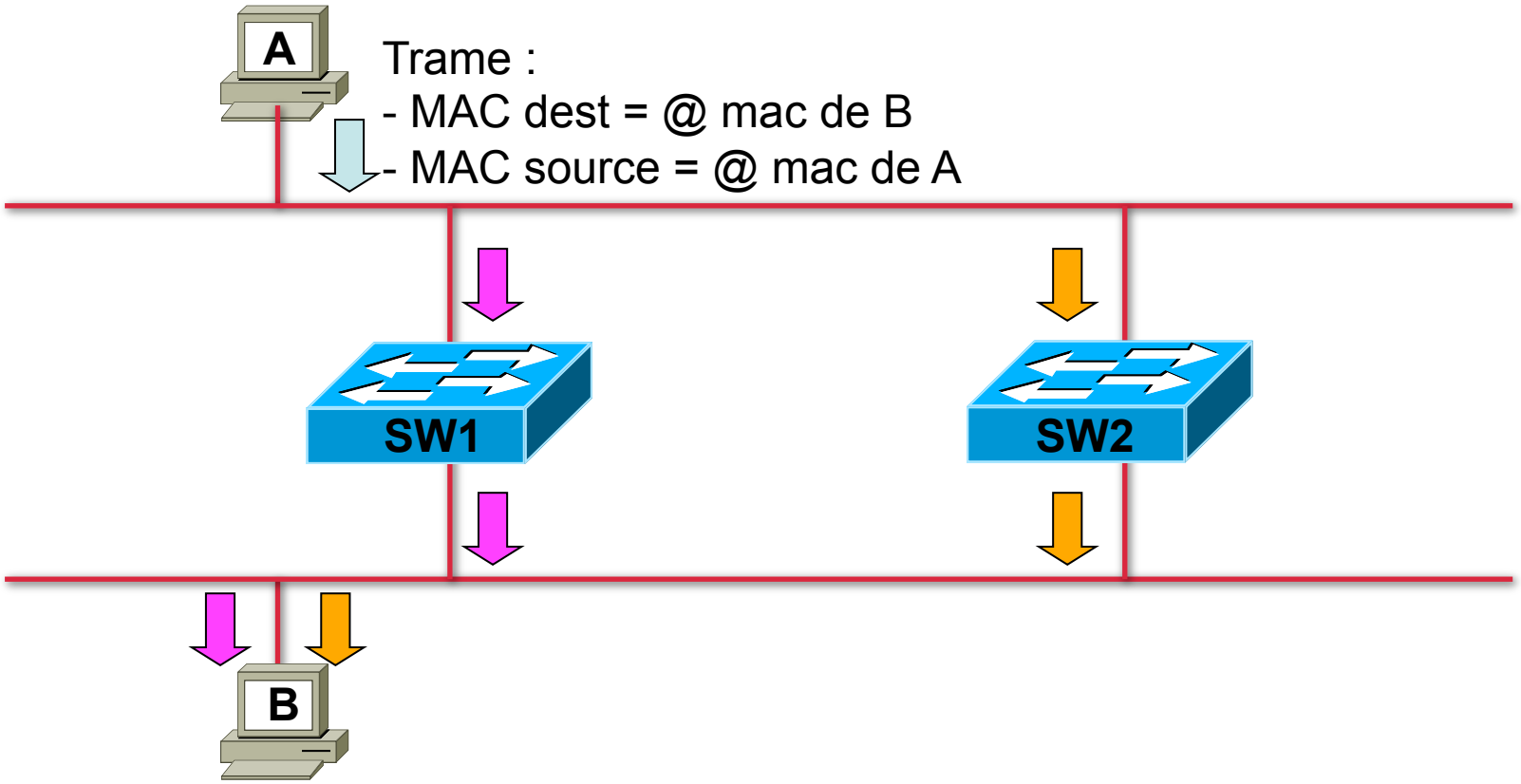
Instabilité de la table des @ MAC



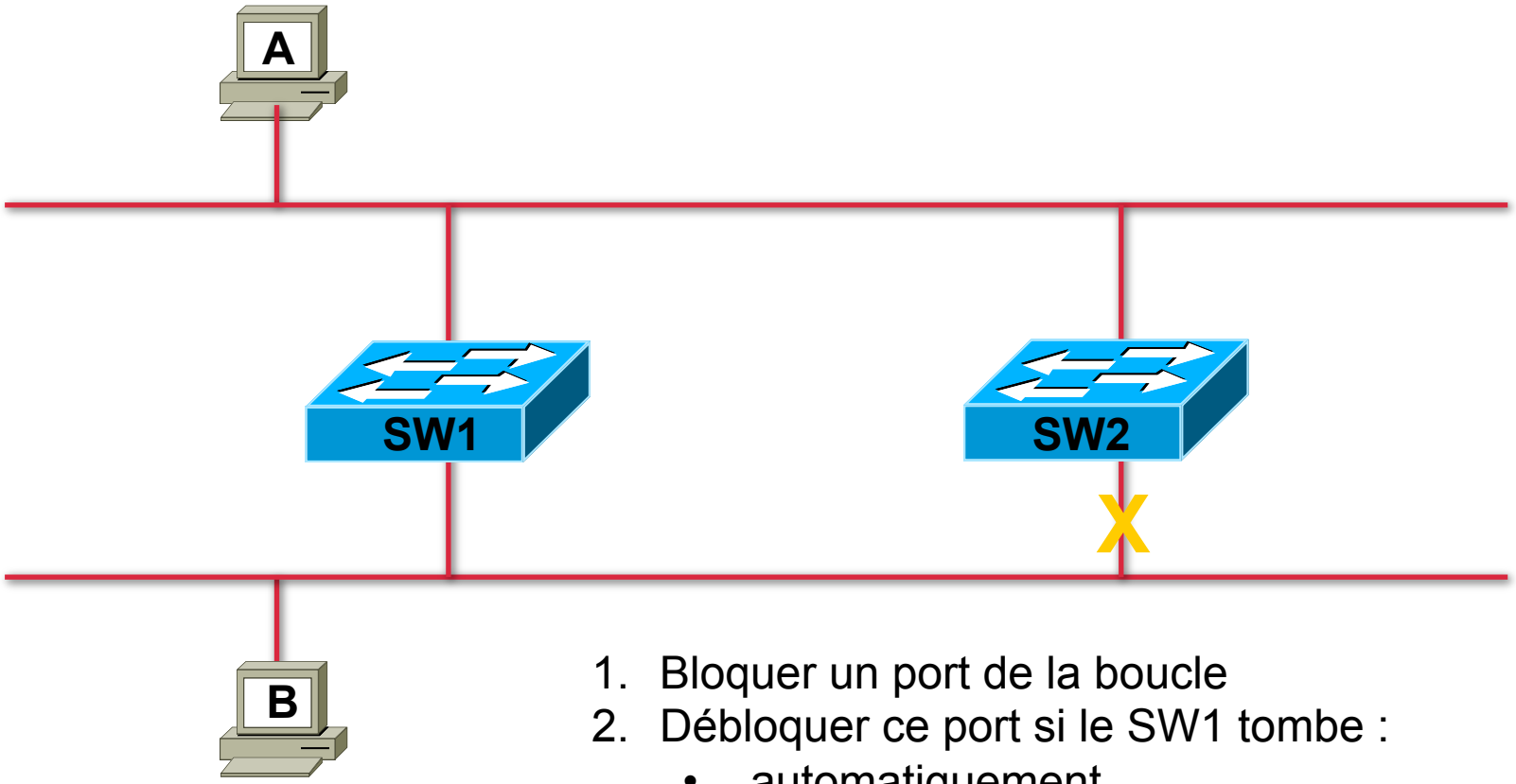
Tempête de broadcast



Duplication des trames



Solution : STP = 802.1d



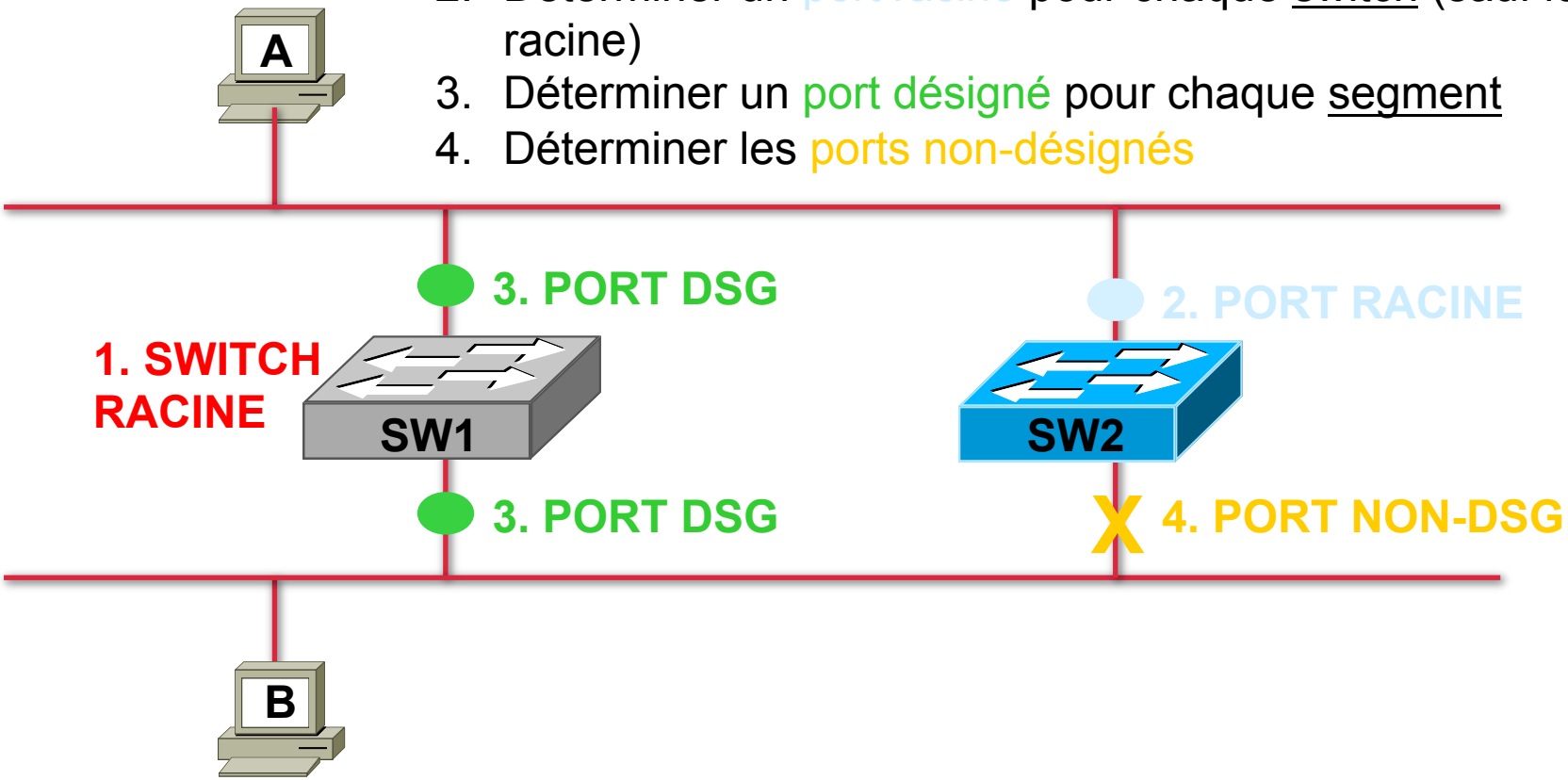
1. Bloquer un port de la boucle
2. Débloquer ce port si le SW1 tombe :
   - automatiquement
   - le plus rapidement possible

Méthodologie du STP

1. Déterminer le switch racine du réseau
2. Déterminer un port racine pour chaque switch (sauf le switch racine)
3. Déterminer un port désigné pour chaque segment
4. Bloquer les ports non-désignés

Exemple 1

1. Déterminer le switch racine du réseau
2. Déterminer un port racine pour chaque switch (sauf le sw racine)
3. Déterminer un port désigné pour chaque segment
4. Déterminer les ports non-désignés



Le BRIDGE-ID

- Bridge-ID = (Bridge PRIORITY ; MAC @)

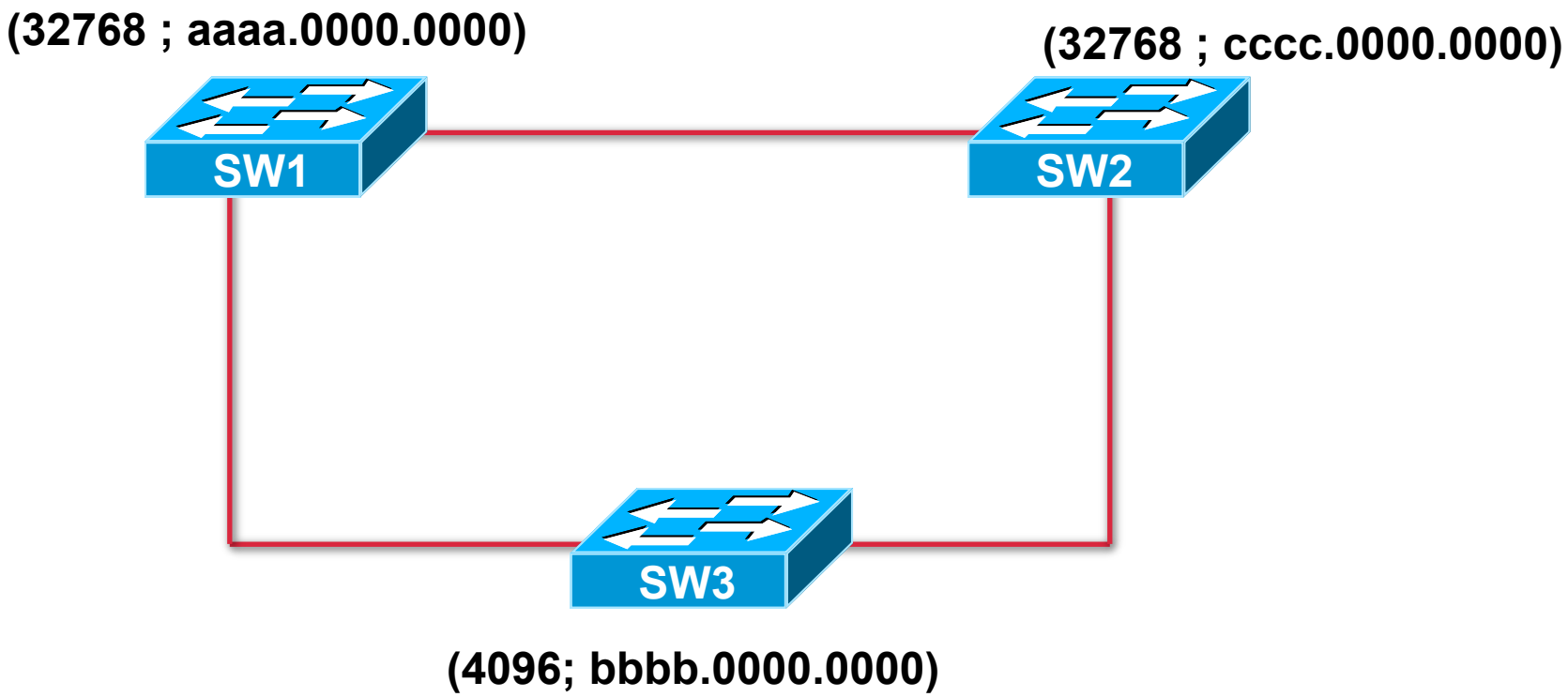
- Bridge PRIORITY :
  - entre 0 et 65535
  - par défaut 32768

Règle de l'étape 1

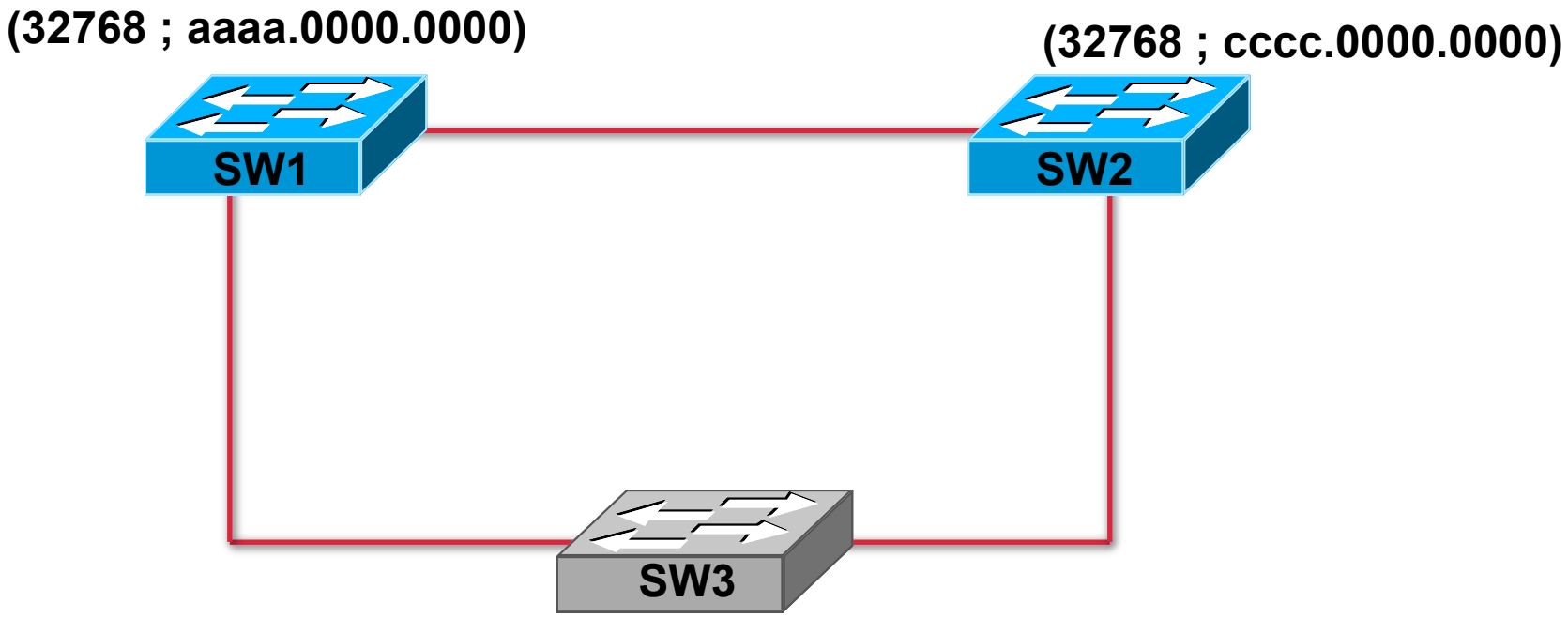
1. **Déterminer le switch racine du réseau**
2. Déterminer un port racine pour chaque switch (sauf le sw racine)
3. Déterminer un port désigné pour chaque segment
4. Déterminer les ports non-désignés

- Le switch racine est le switch dont le BRIDGE ID est le plus PETIT.

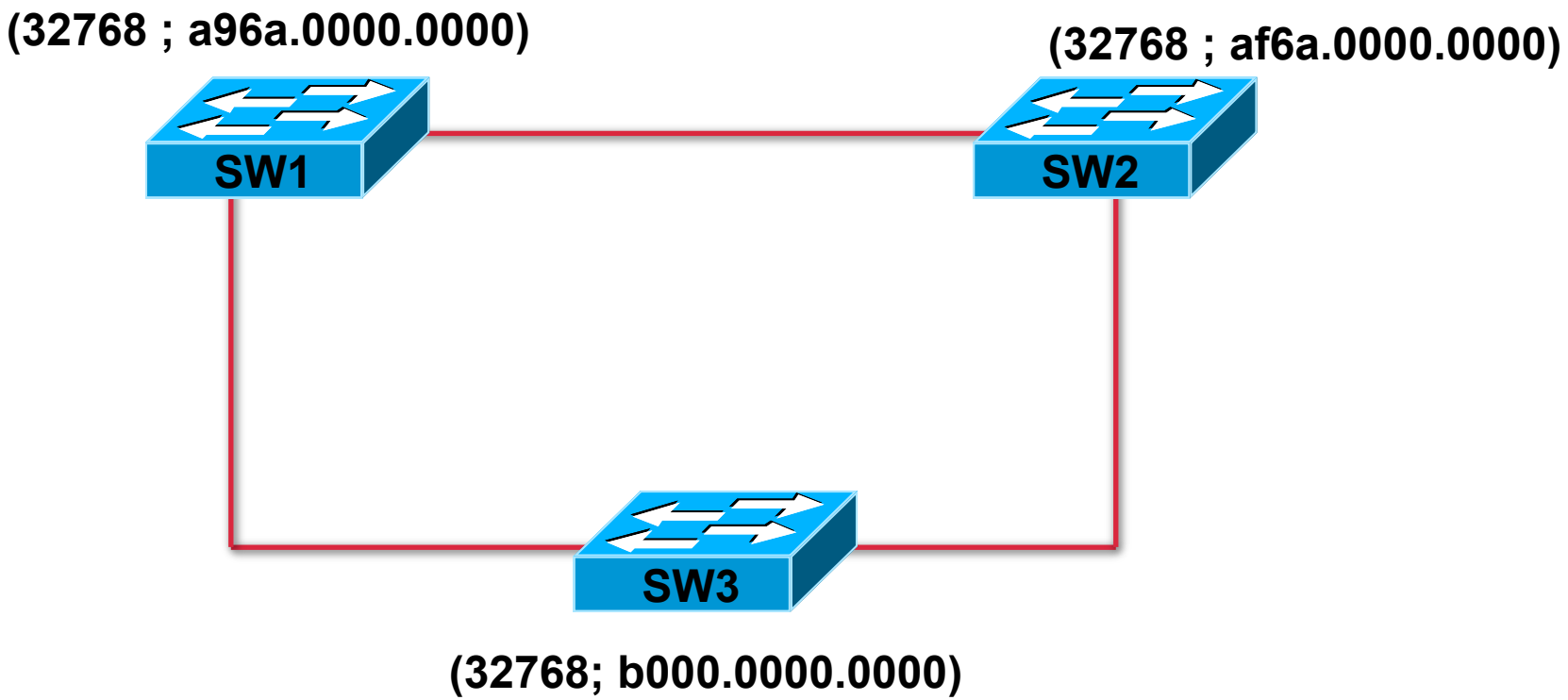
Exercice 1


(32768 ; aaaa.0000.0000)
(32768 ; cccc.0000.0000)
SW1
SW2
SW3
(4096; bbbb.0000.0000)

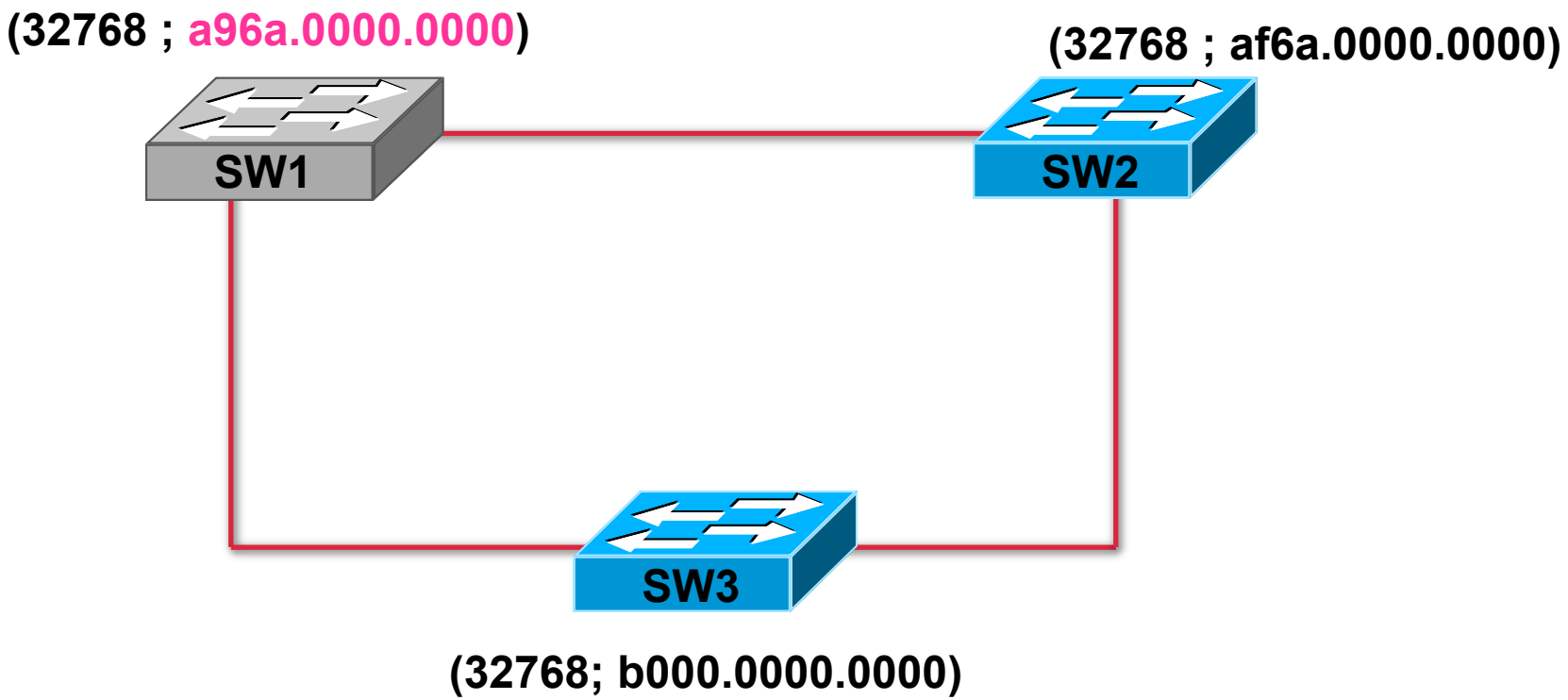
Solution 1


(32768 ; aaaa.0000.0000)
(32768 ; cccc.0000.0000)
SW1
SW2
SW3
(4096; bbbb.0000.0000)

Exercice 2

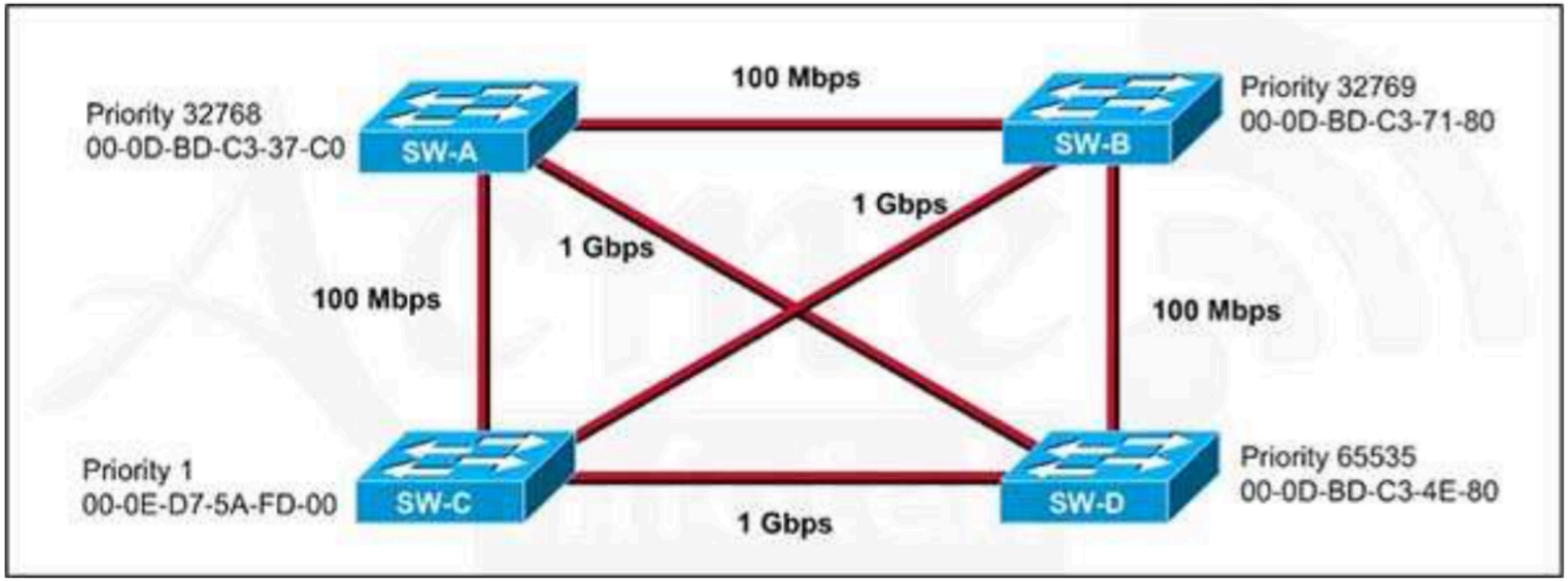

(32768 ; a96a.0000.0000)
(32768 ; af6a.0000.0000)
SW1
SW2
SW3
(32768; b000.0000.0000)

Solution 2


(32768 ; a96a.0000.0000)
(32768 ; af6a.0000.0000)
SW1
SW2
SW3
(32768; b000.0000.0000)

Test

- Qui sera élu switch racine ?



Test

- Qui sera élu switch racine ?

A. 32768: 11-22-33-44-55-66
B. 32768: 22-33-44-55-66-77
C. 32769:11-22-33-44-55-65
D. 32769: 22-33-44-55-66-78

Test

Pourquoi ce switch n'a pas été élu switch racine ?

```
Switch# show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    20481
              Address     0008.217a.5800
              Cost        38
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0008.205e.6600
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/4            Desg FWD 38        128.1    P2p
Fa0/11           Altn BLK 57        128.1    P2p
Fa0/13           Desg FWD 38        128.1    P2p
```

Règle de l'étape 2

1. Déterminer le switch racine du réseau
2. **Déterminer un port racine pour chaque switch (sauf le sw racine)**
3. Déterminer un port désigné pour chaque segment
4. Déterminer les ports non-désignés

- Le port racine est le port qui me mène le plus vite à la racine.
- C'est-à-dire dont le coût pour atteindre le Root est le moins élevé

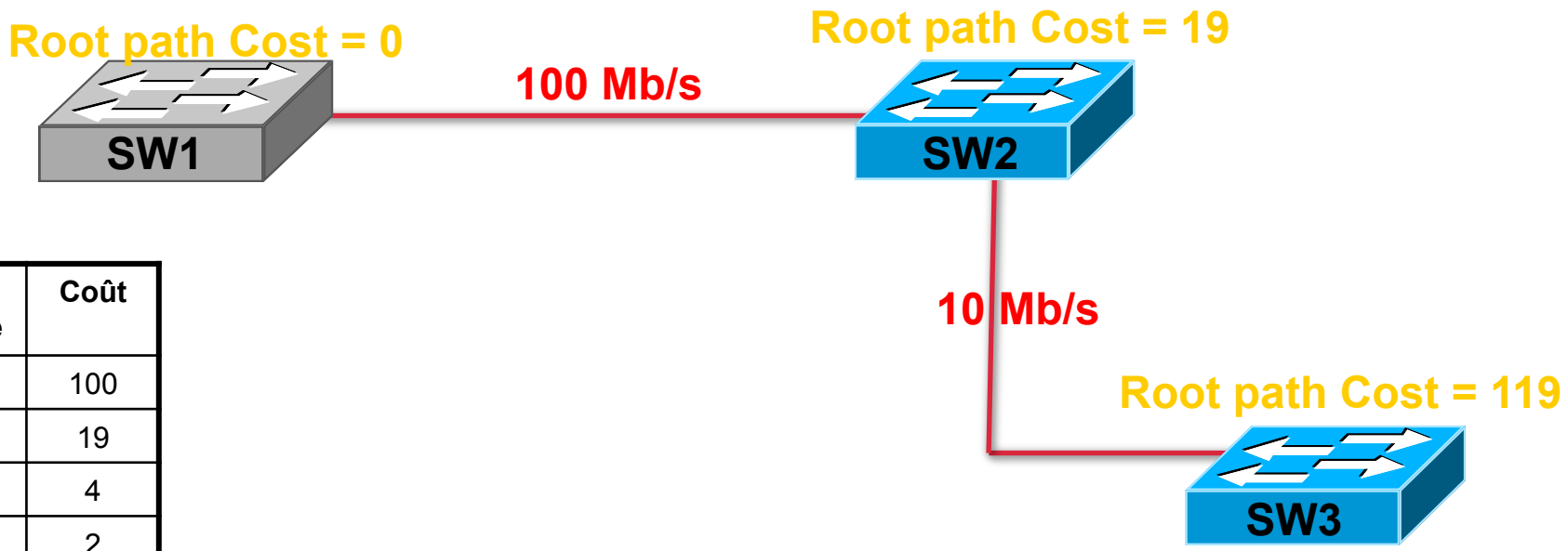
Coût de chaque liaison

- STP attribue un coût à chaque liaison
- Ce coût dépend de la Bande passante

Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

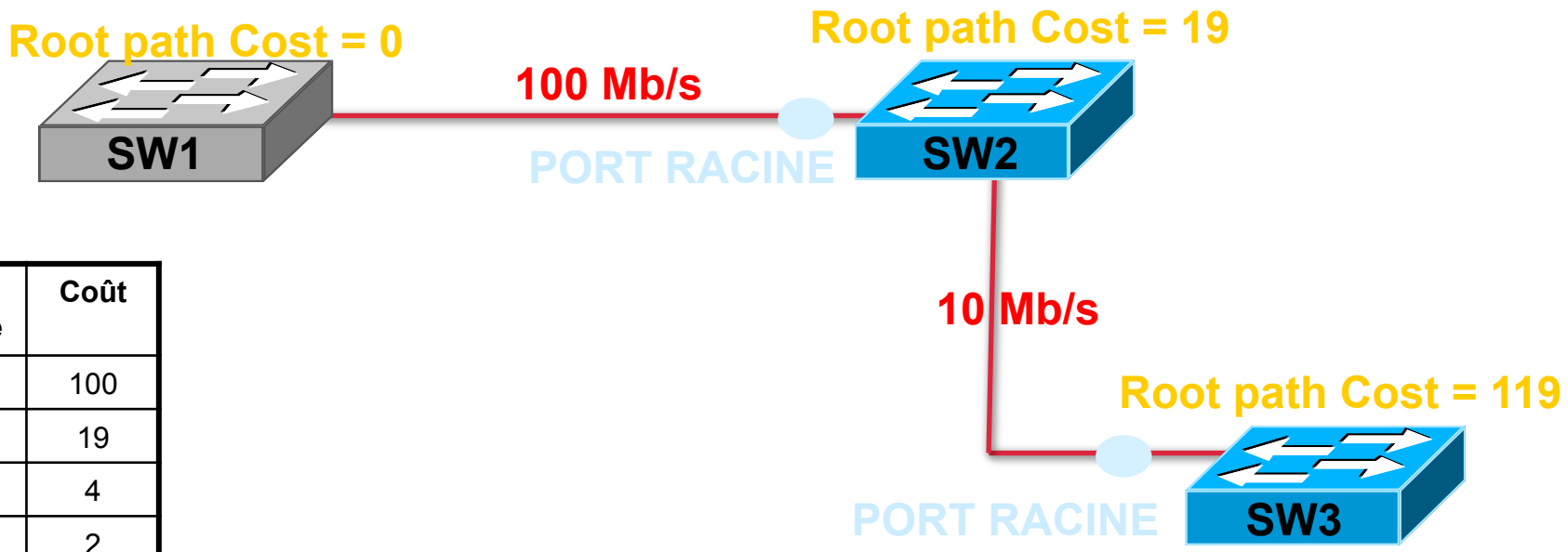
Root Path Cost

- Somme des coûts entre moi et le switch racine.



Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

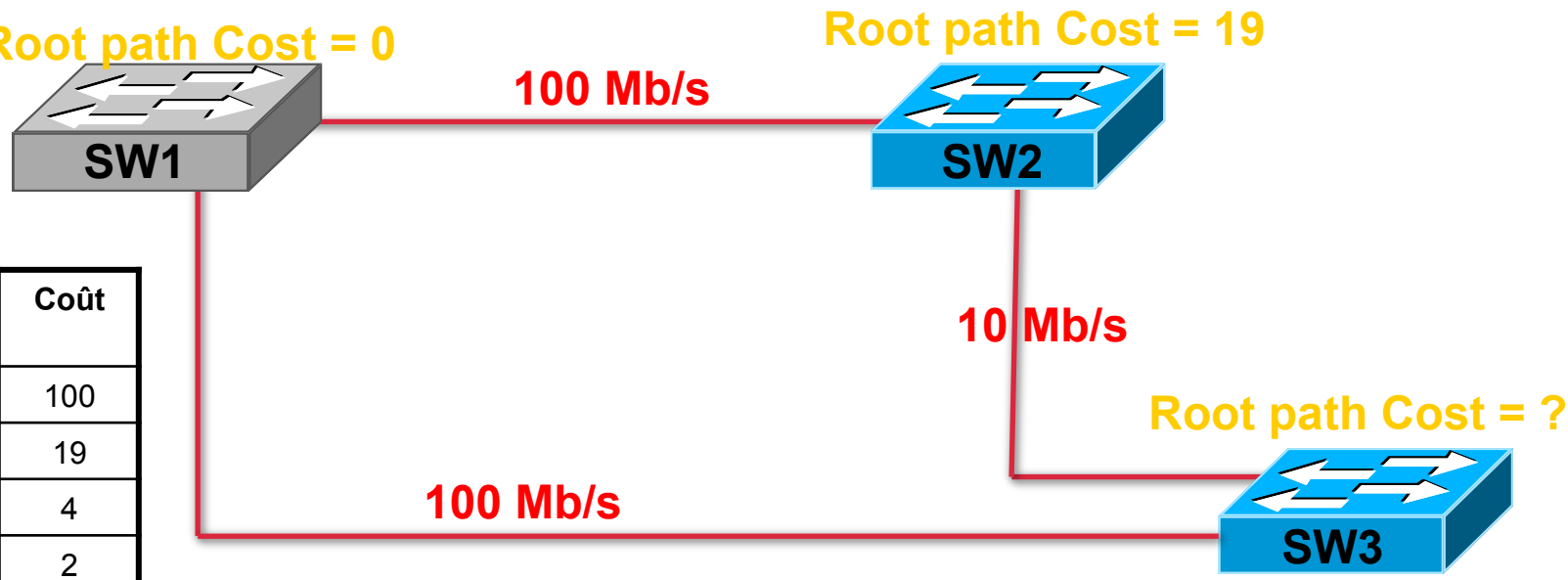
Port Racine (Root Port)



Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

Exercice 1

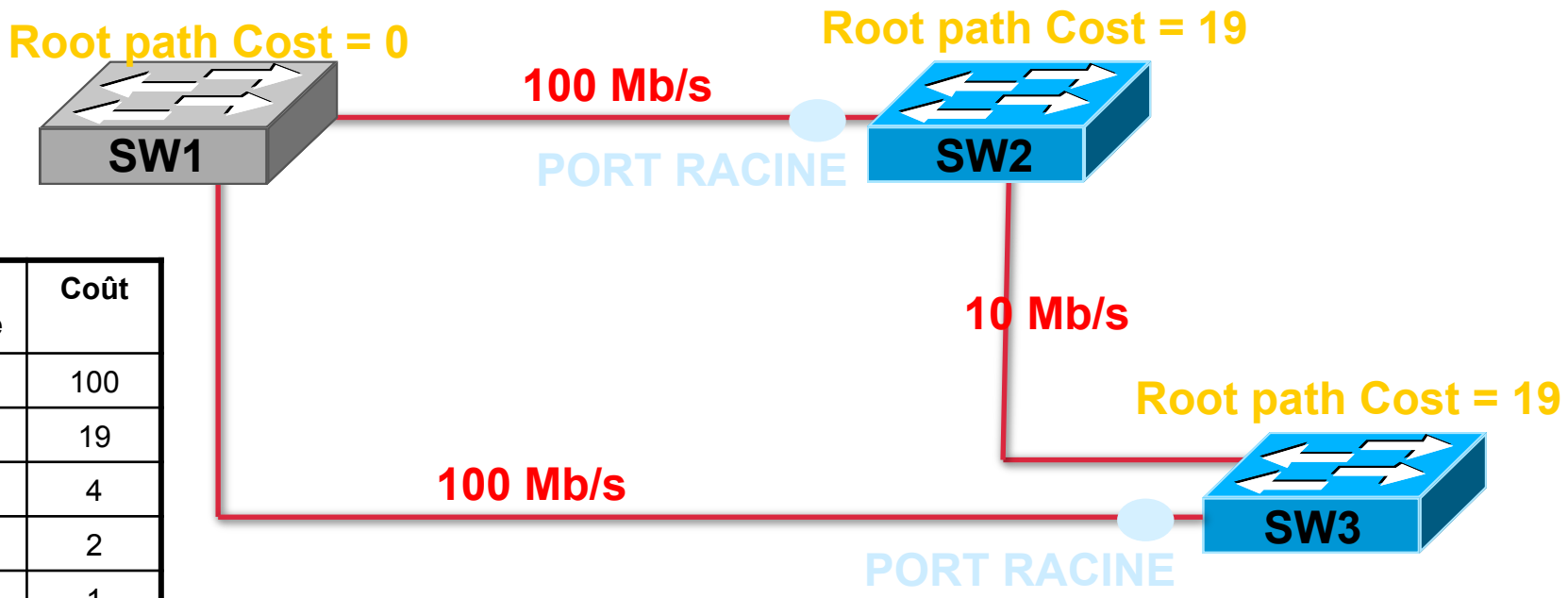
- Je cherche à atteindre ma racine par le chemin le plus rapide = bande passante maximale = root path cost minimal



Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

Solution

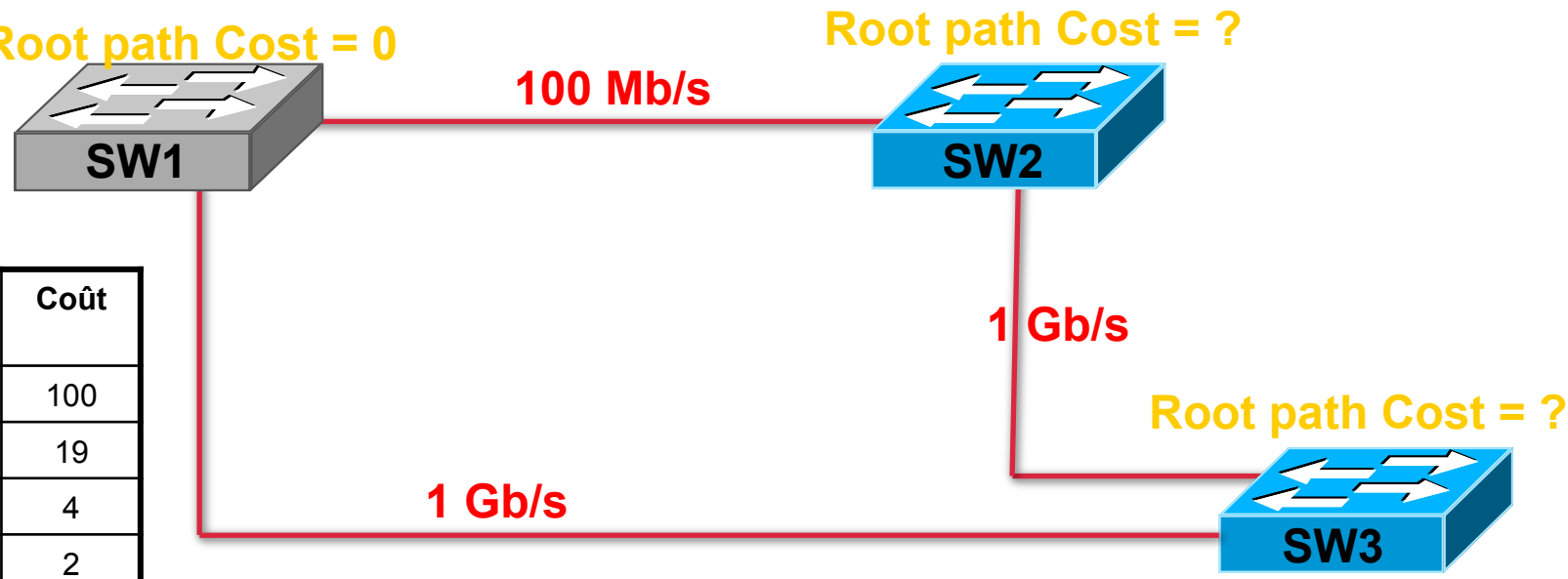
- Je cherche à atteindre ma racine par le chemin le plus rapide = bande passante maximale = root path cost minimal



Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

Exercice 2

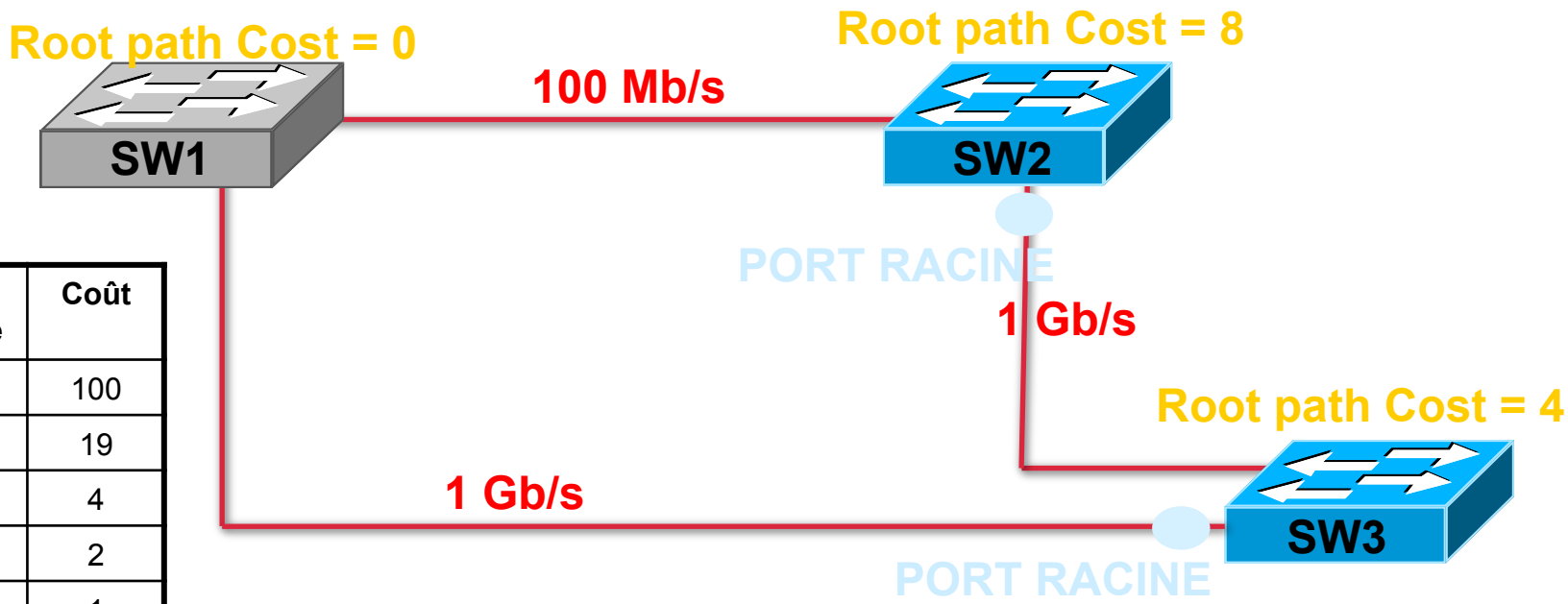
- Je cherche à atteindre ma racine par le chemin le plus rapide = bande passante maximale = root path cost minimal



Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

Solution

- Je cherche à atteindre ma racine par le chemin le plus rapide = bande passante maximale = root path cost minimal

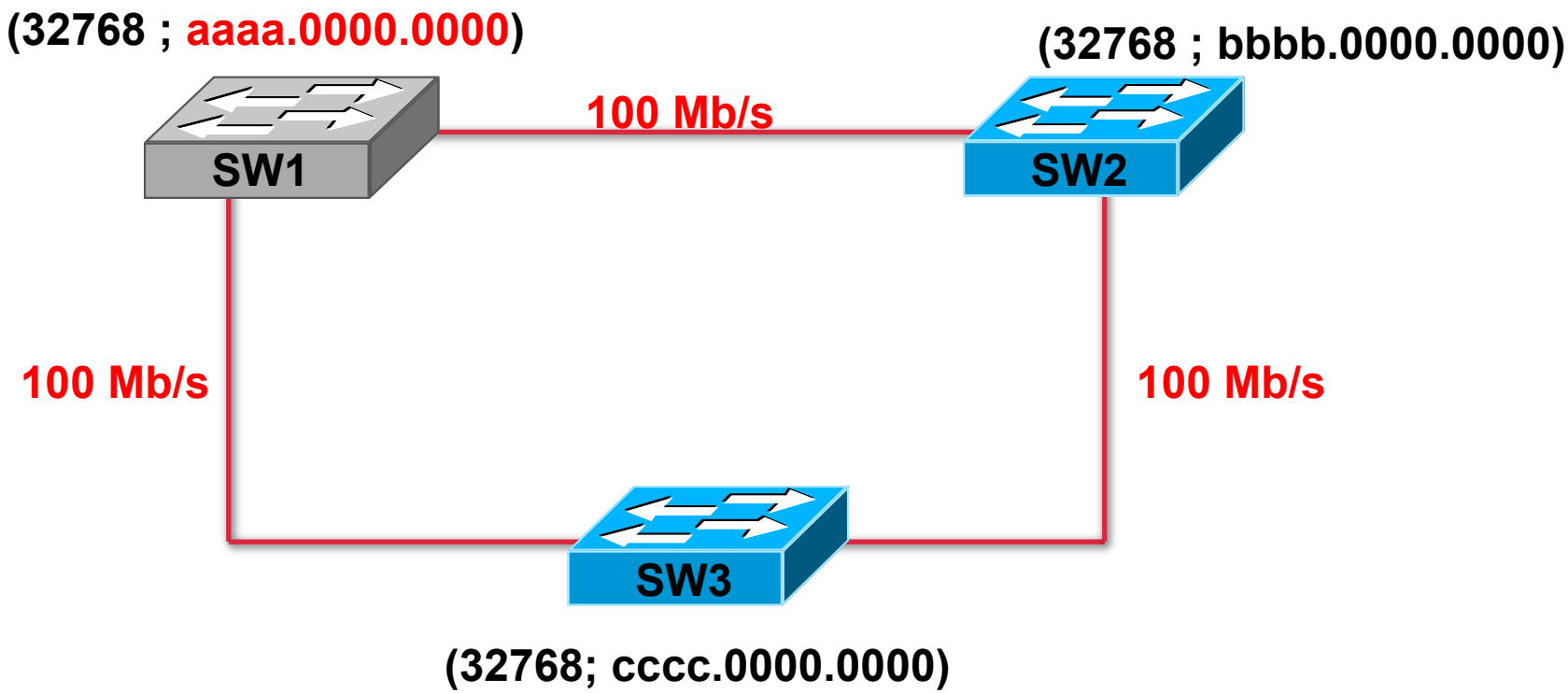


Bande passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

BPDU

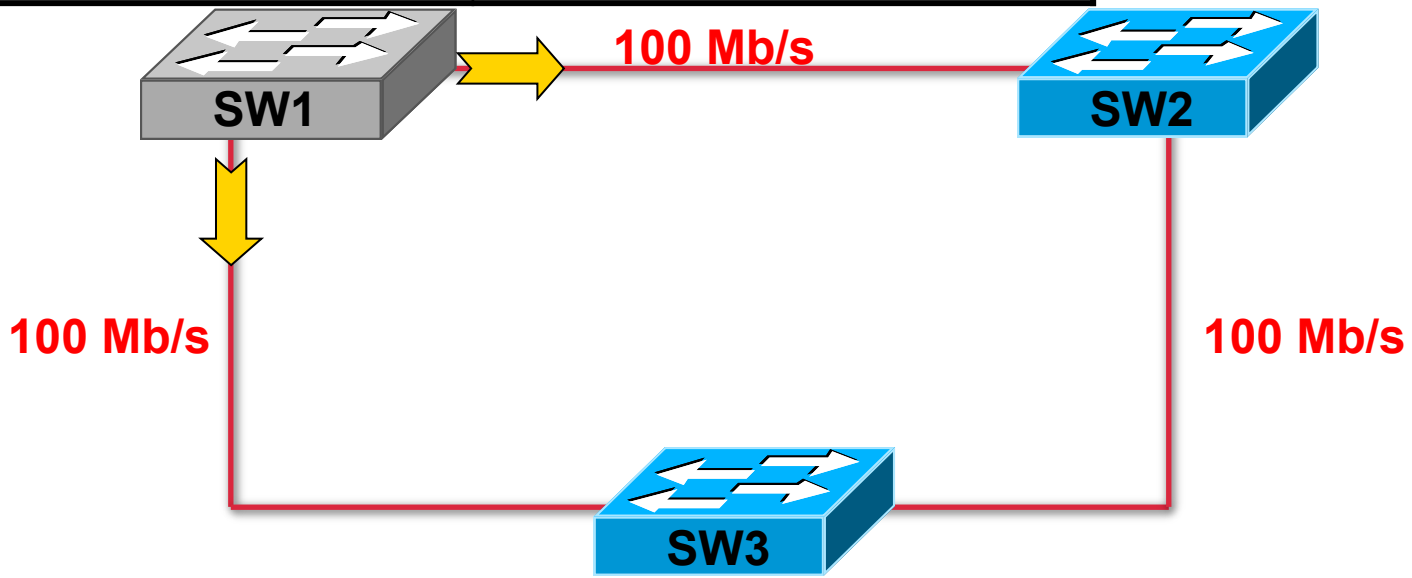
- Bridge Protocol Data Unit
- Générés par le switch racine
- Envoyé toutes les 2 secondes
- Sur toutes les interfaces
- 4 champs nous intéressent :
  - BRIDGE-ID du switch racine
  - BRIDGE-ID du switch local
  - ROOT PATH COST
  - PORT-ID

Exemple


(32768 ; aaaa.0000.0000)
(32768 ; bbbb.0000.0000)
100 Mb/s
SW1
SW2
100 Mb/s
100 Mb/s
SW3
(32768; cccc.0000.0000)

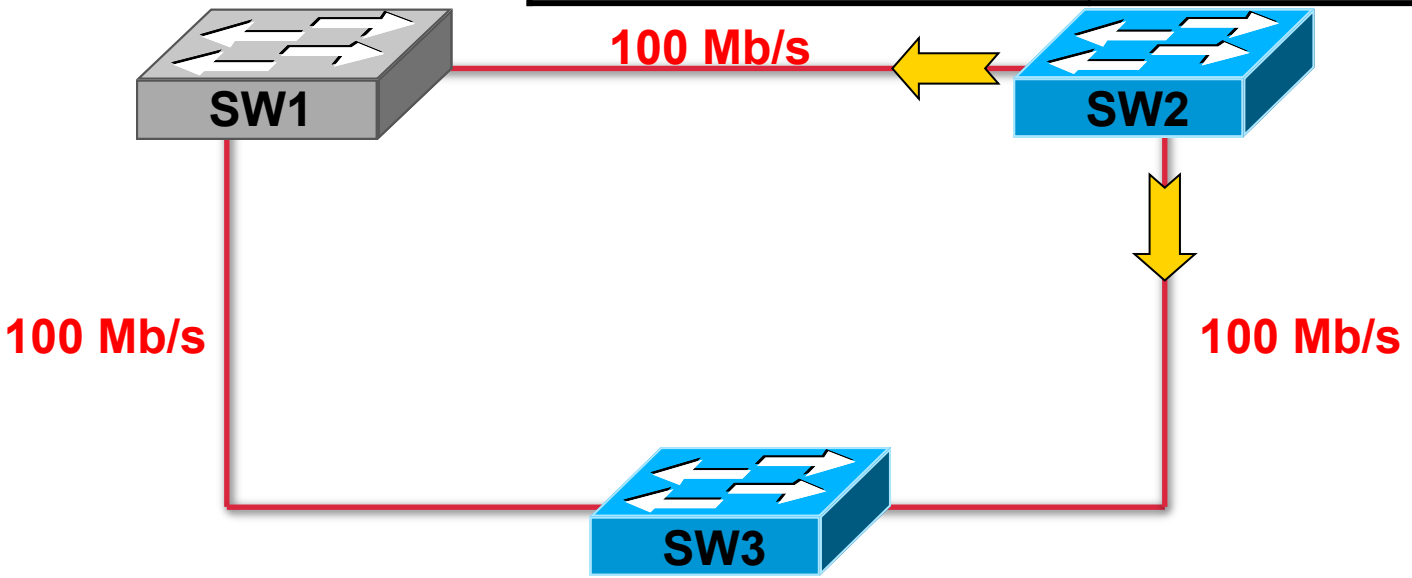
BPDU envoyés par SW1

Bridge-ID du sw racine :	**(32768 ; aaaa.0000.0000)**
Mon Bridge-ID :	**(32768 ; aaaa.0000.0000)**
Root Path Cost :	**0**

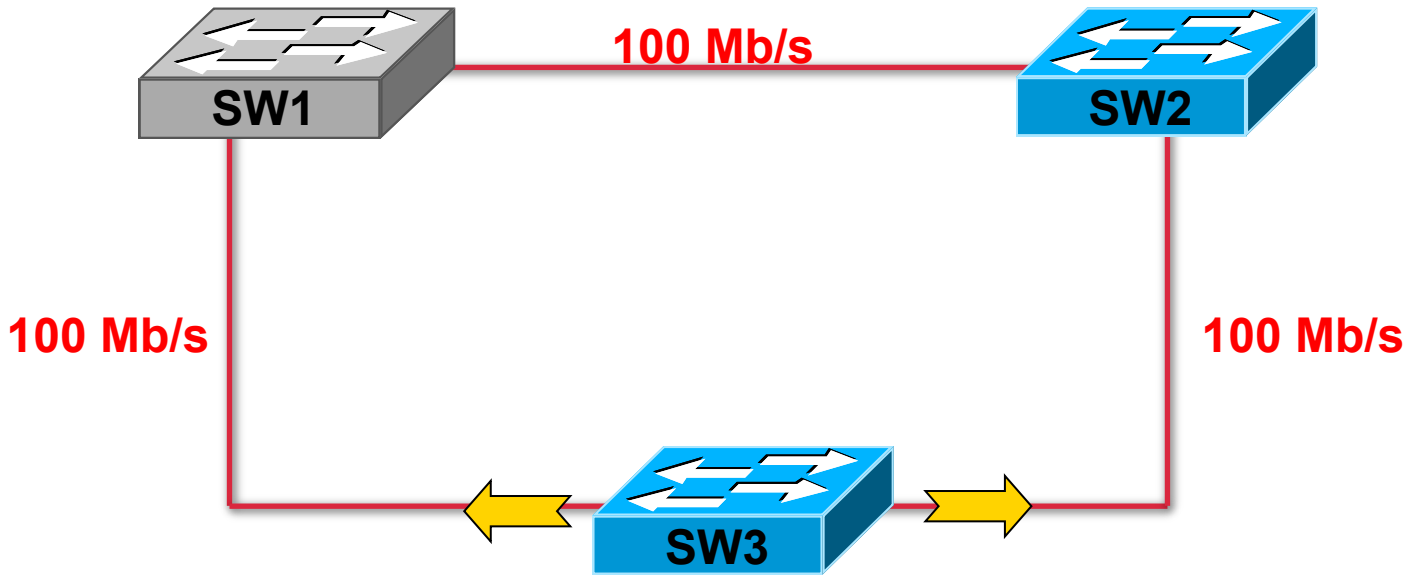


BPDU envoyés par SW2

Bridge-ID du sw racine :	(32768 ; aaaa.0000.0000)
Mon Bridge-ID :	(32768 ; bbbb.0000.0000)
Root Path Cost :	19



BPDU envoyés par SW3



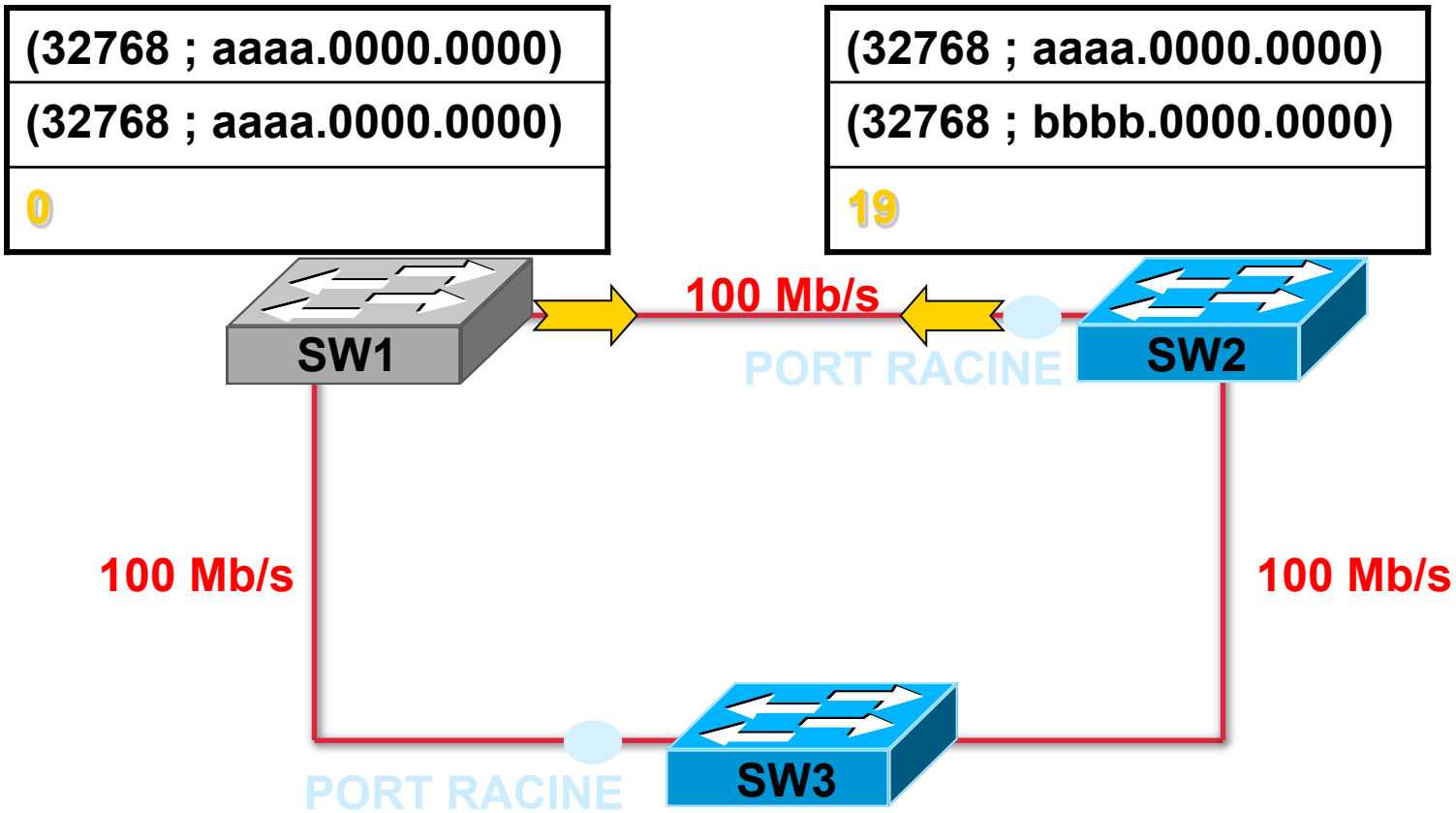
Bridge-ID du sw racine :	(32768 ; aaaa.0000.0000)
Mon Bridge-ID :	(32768 ; cccc.0000.0000)
Root Path Cost :	19

Règle de l'étape 3

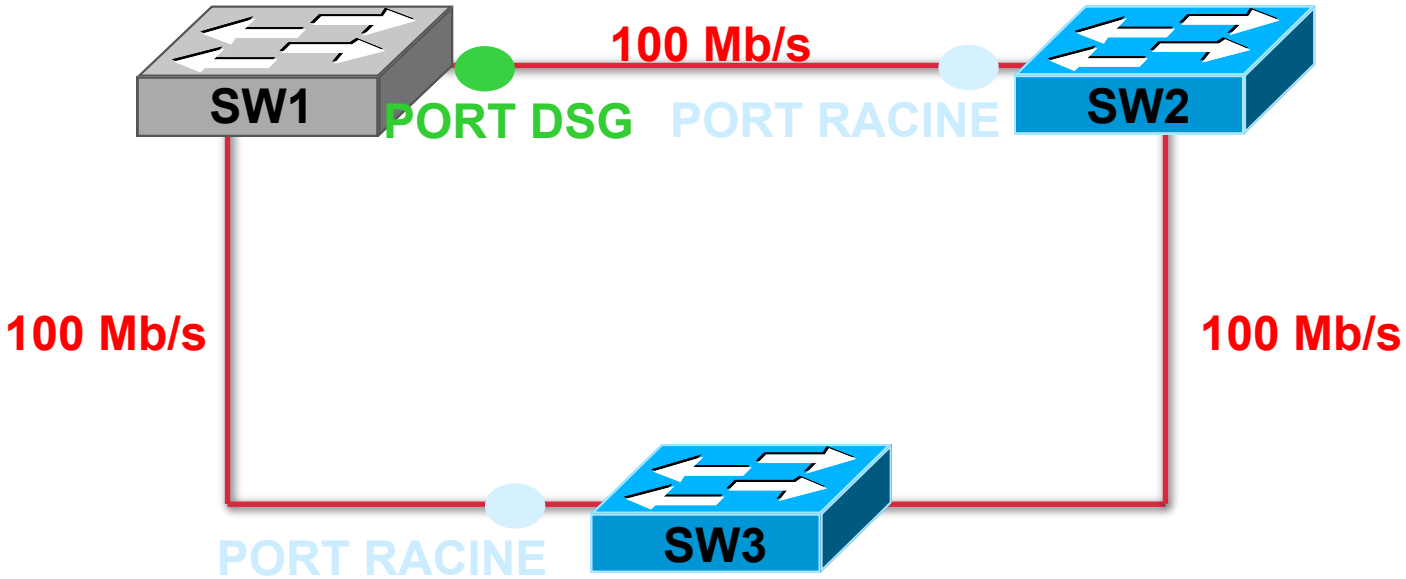
1. Déterminer le switch racine du réseau
2. Déterminer un port racine pour chaque switch (sauf le sw racine)
3. **Déterminer un port désigné pour chaque segment**
4. Déterminer les ports non-désignés

- Le port désigné est le port du Segment qui conduit le plus vite au Root
- C'est celui pour lequel le coût est le moins élevé

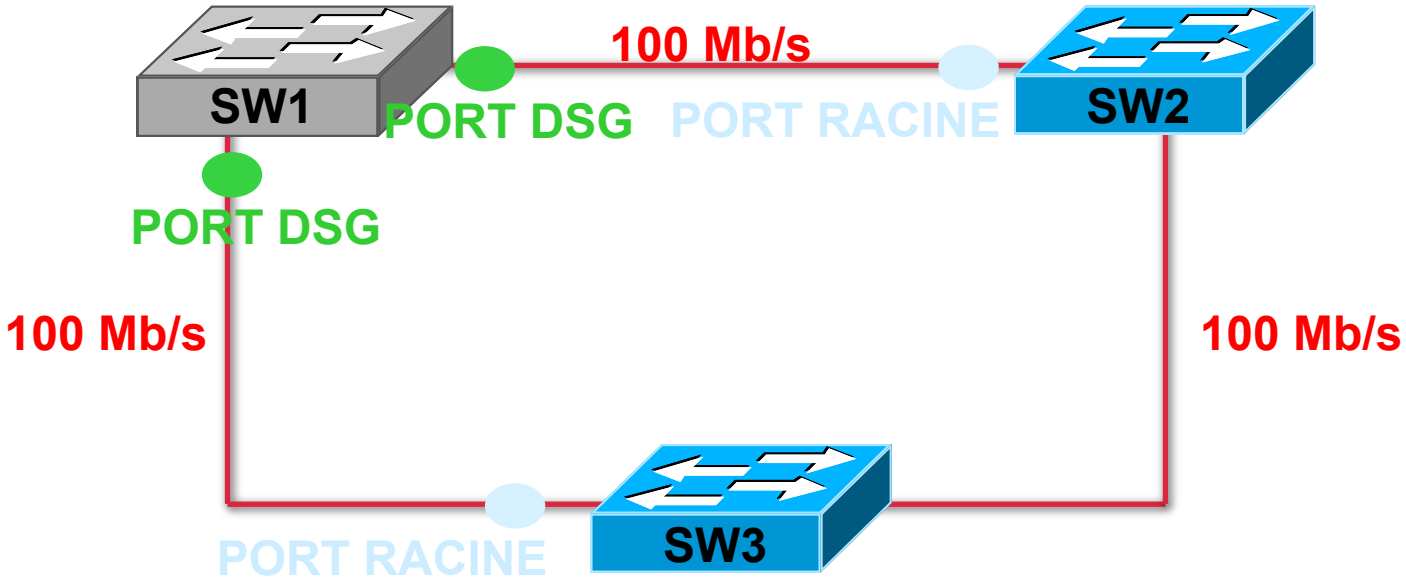
Port DSG sur segment 1-2



Port DSG sur segment 1-2

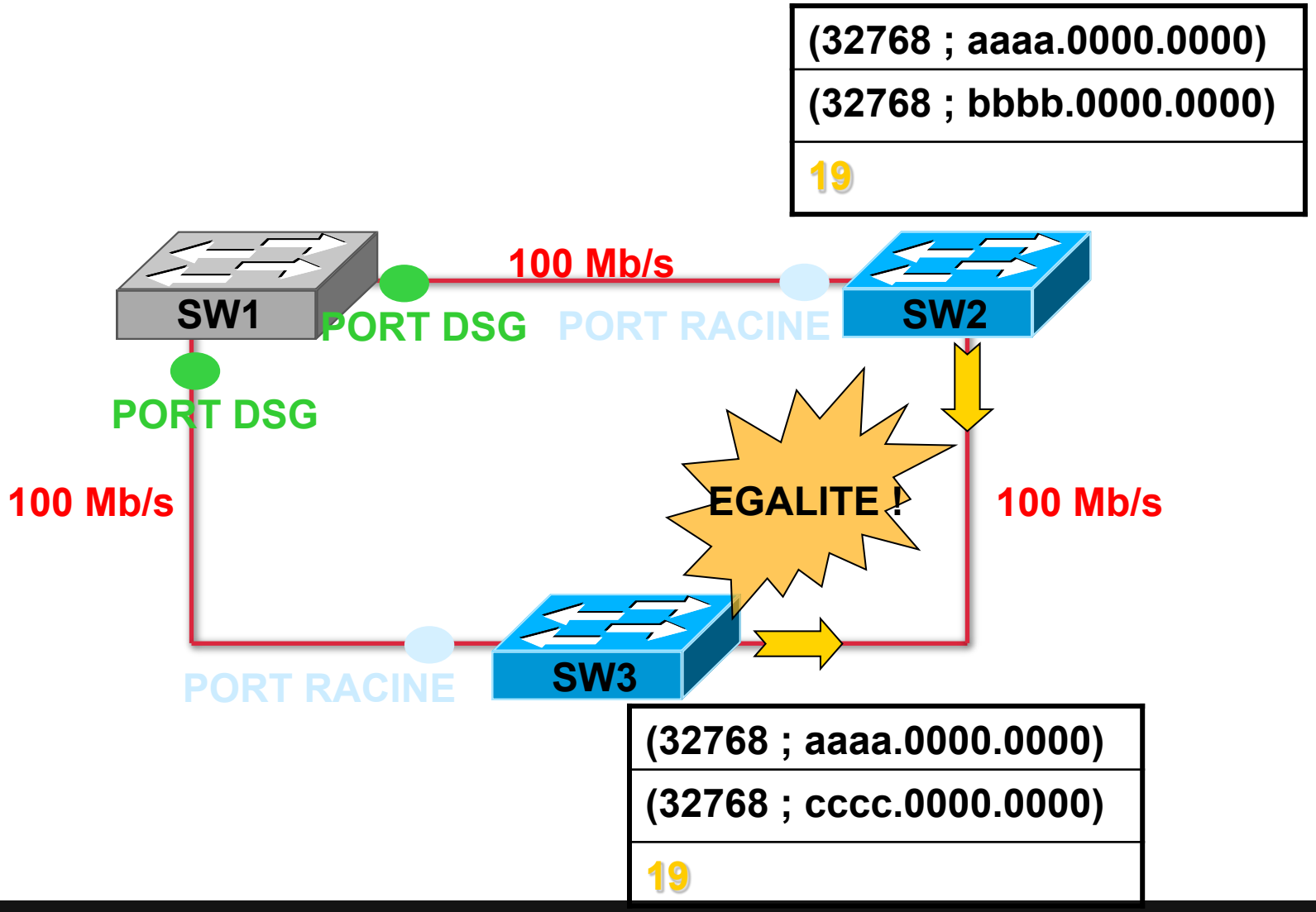


Port DSG sur segment 1-3



TOUS les ports du switch RACINE sont des ports DESIGNES

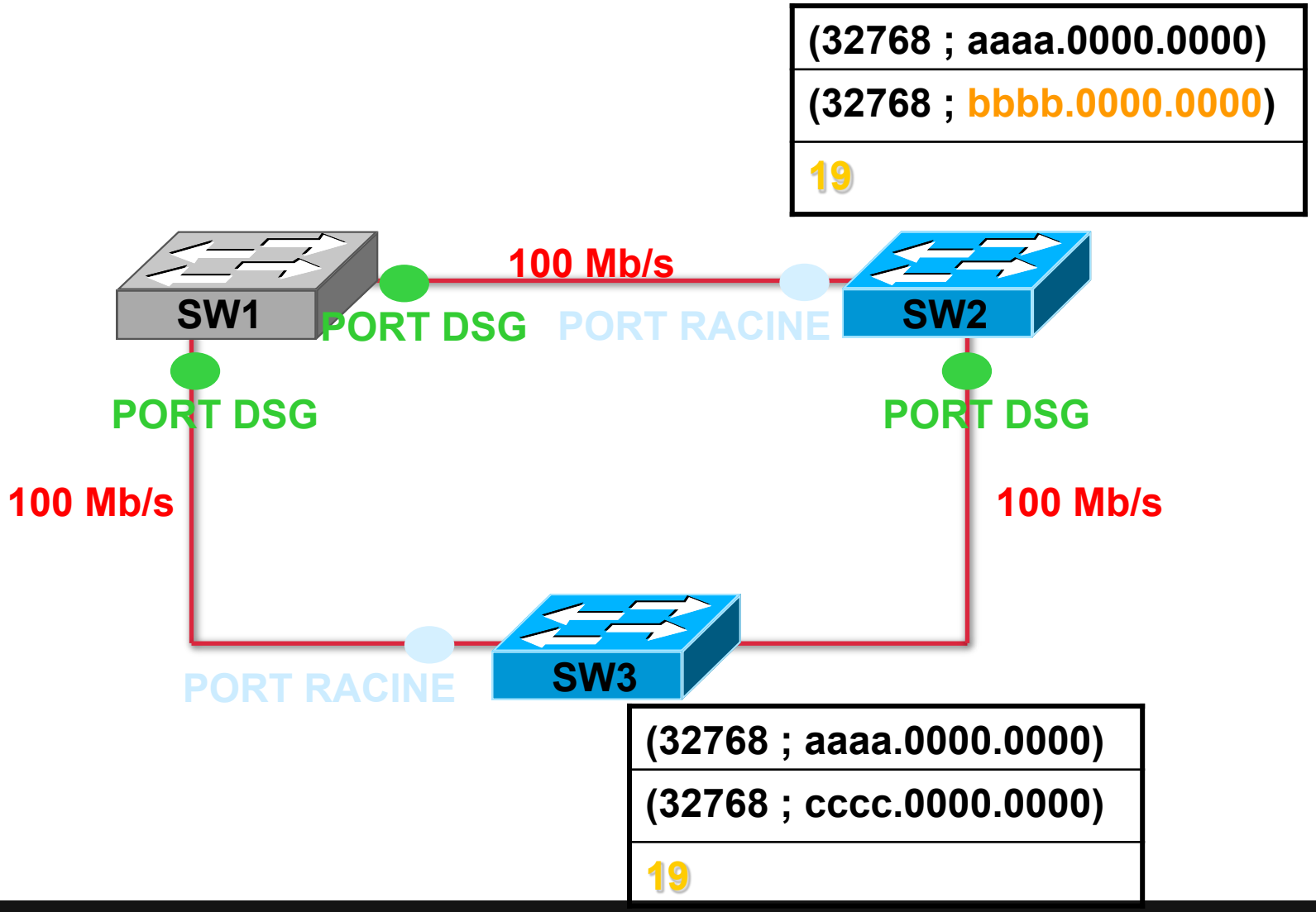
Port DSG sur segment 2-3



Le meilleur BPDU

- Celui dont le champ ROOT PATH COST est le plus petit.
- Si égalité :
  - Celui dont le champ MY BRIDGE-ID est le plus petit.

Port DSG sur segment 2-3

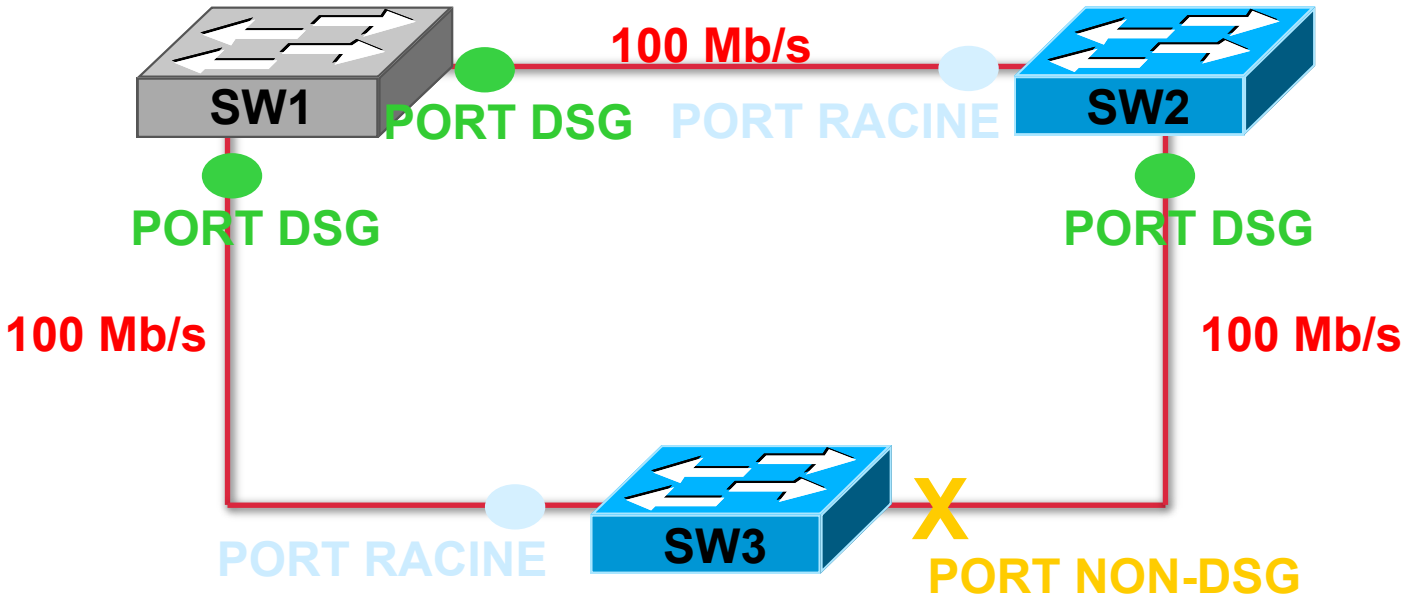


Règle de l'étape 4

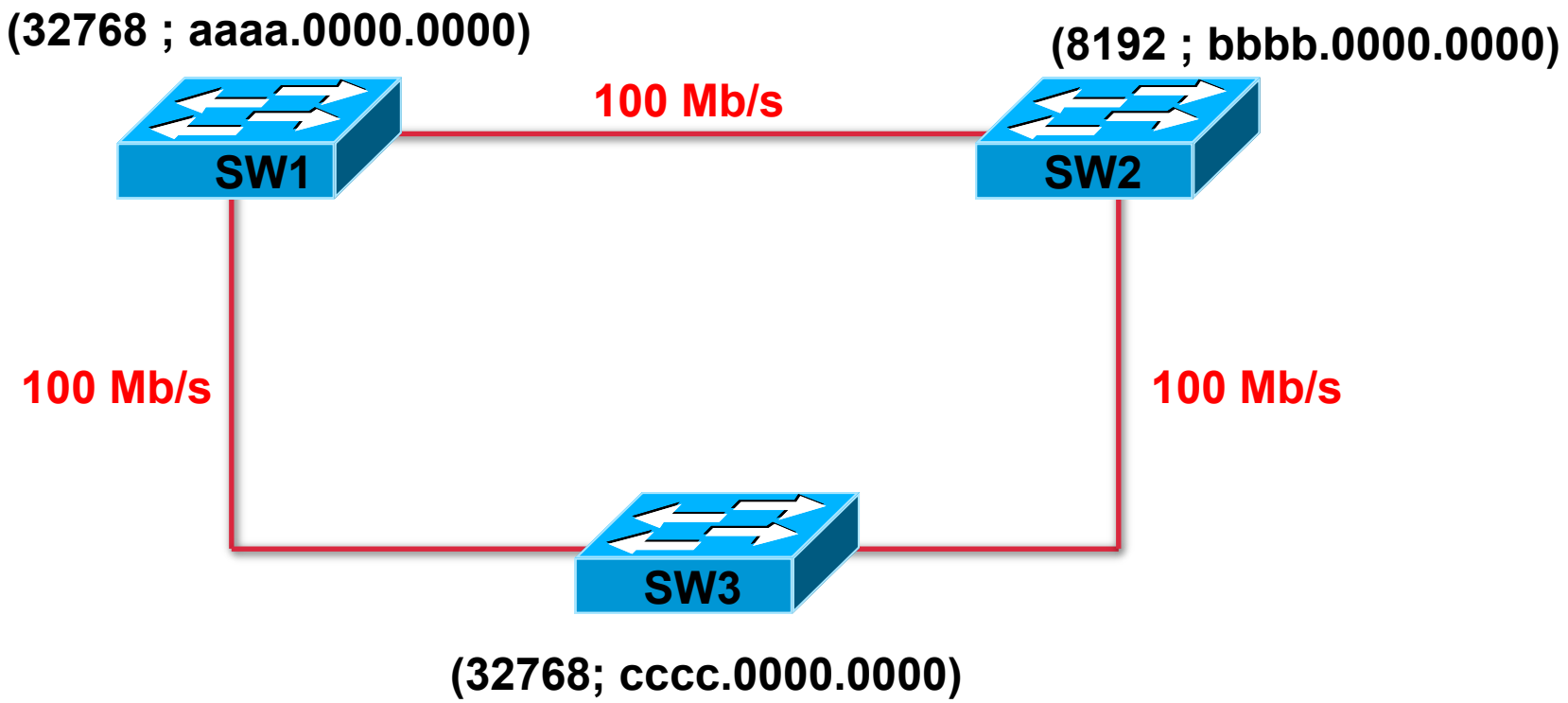
1. Déterminer le switch racine du réseau
2. Déterminer un port racine pour chaque switch (sauf le sw racine)
3. Déterminer un port désigné pour chaque segment
4. **Déterminer les ports non-désignés**

- Les ports non-désignés sont les ports qui ne sont ni RACINE ni DESIGNE

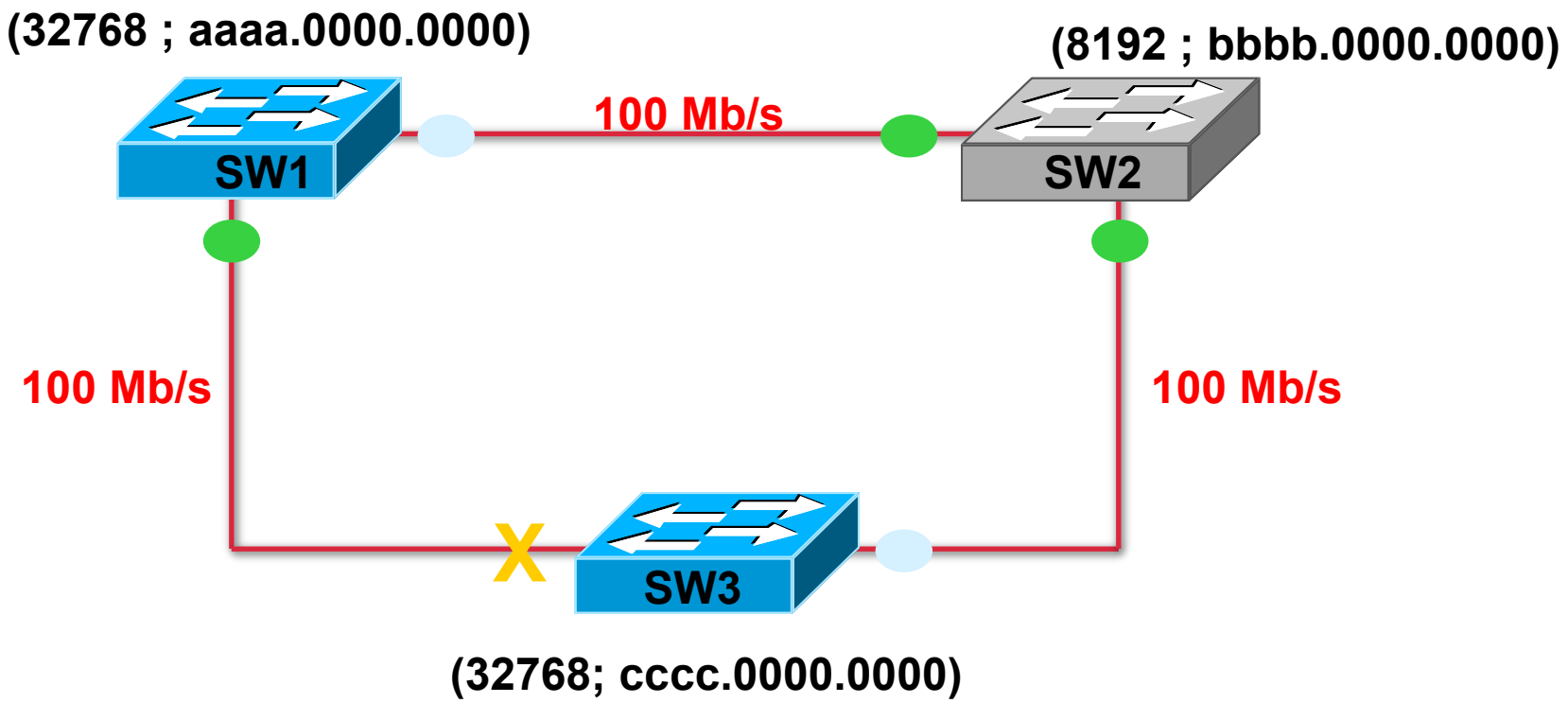
Port non désigné



Exercice 1


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
100 Mb/s
SW1
SW2
100 Mb/s
100 Mb/s
SW3
(32768; cccc.0000.0000)

Solution 1


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
100 Mb/s
SW1
SW2
100 Mb/s
100 Mb/s
X
SW3
(32768; cccc.0000.0000)

Exercice 2


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
100 Mb/s
10 Mb/s
SW1
SW2

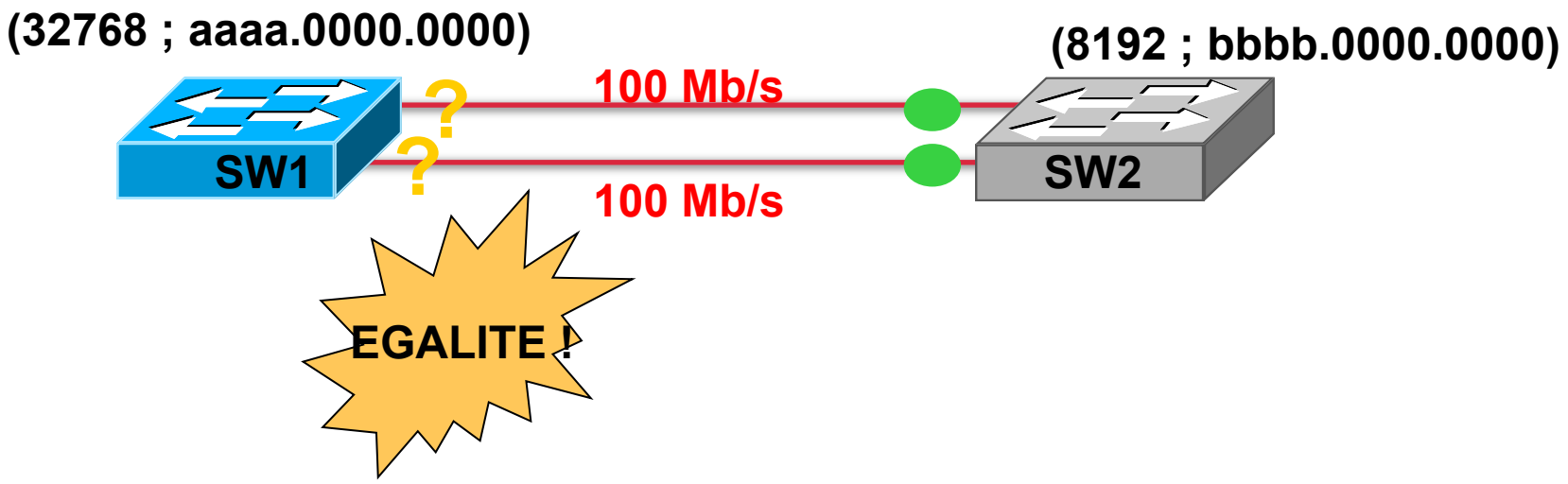
Solution 2


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
100 Mb/s
10 Mb/s
SW1
SW2

Exercice 3


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
100 Mb/s
100 Mb/s
SW1
SW2

Solution partielle 3



Le PORT-ID

- Port-ID = (Port PRIORITY ; n° de port [K])

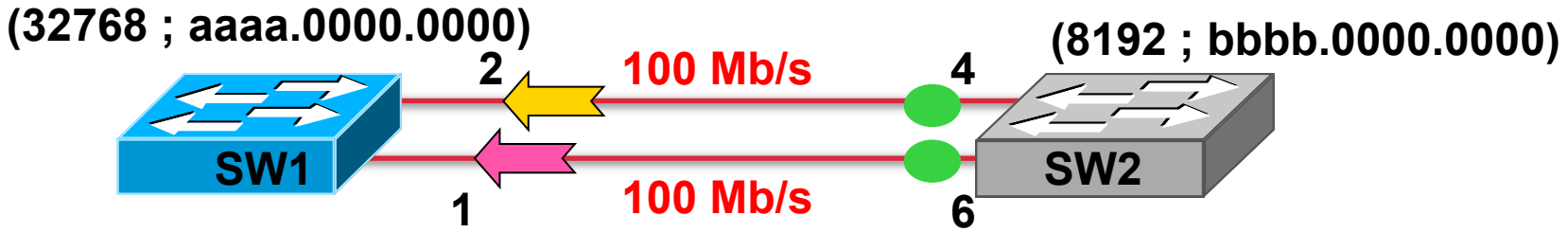
- Port PRIORITY :
  - entre 1 et 256
  - par défaut 128

Le meilleur BPDU

- Celui dont le champ ROOT PATH COST est le plus petit.
- Si égalité :
  - Celui dont le champ MY BRIDGE-ID est le plus petit.
  - Si égalité :
    - Celui dont le champ PORT-ID est le plus petit

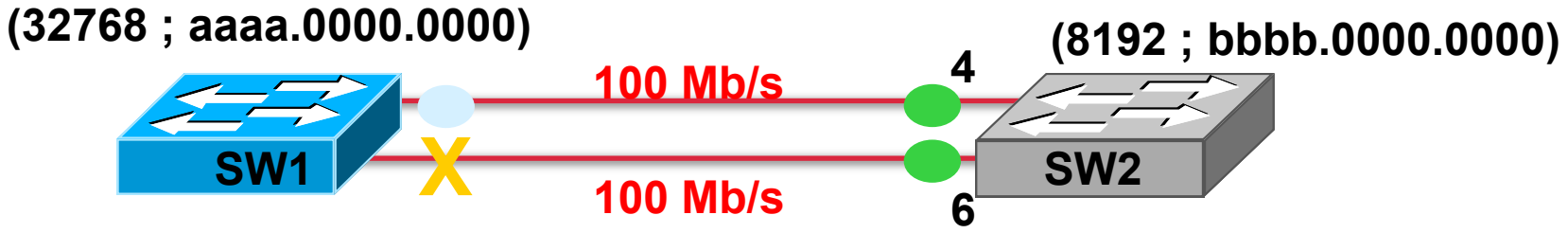
Quels Port-ID sont envoyés ?

(8192 ; bbbb.0000.0000)
(8192 ; bbbb.0000.0000)
0
(128 ; 4)



(8192 ; bbbb.0000.0000)
(8192 ; bbbb.0000.0000)
0
(128 ; 6)

Solution 3


(32768 ; aaaa.0000.0000)
(8192 ; bbbb.0000.0000)
SW1
SW2
100 Mb/s
100 Mb/s
4
6
X

Etats d'un port

- Racine — FORWARDING
- Désigné — FORWARDING
- Non désigné — BLOCKING

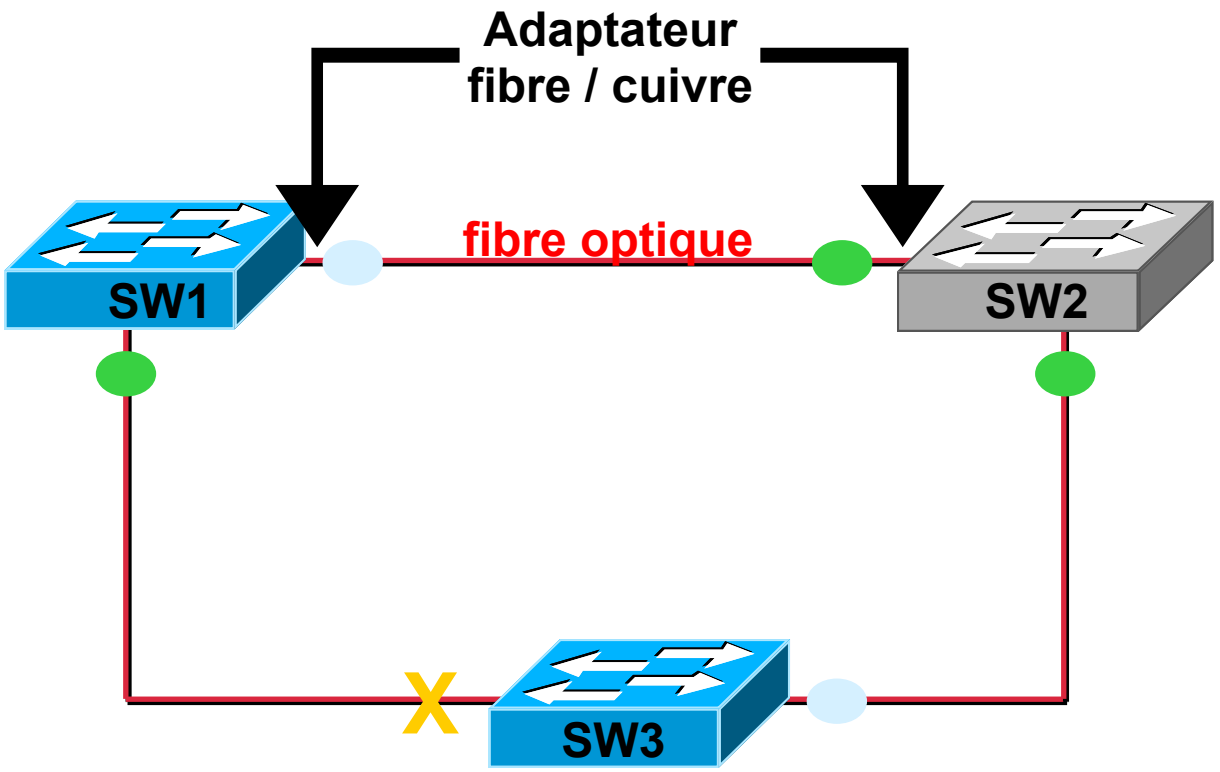
Passage en Forwarding

- N’est pas immédiat
- 15 secondes en LISTENING
  - pour valider que la décision prise est bien la bonne
- 15 secondes en LEARNING
  - pour enrichir la table des mac @
- puis passage en forwarding

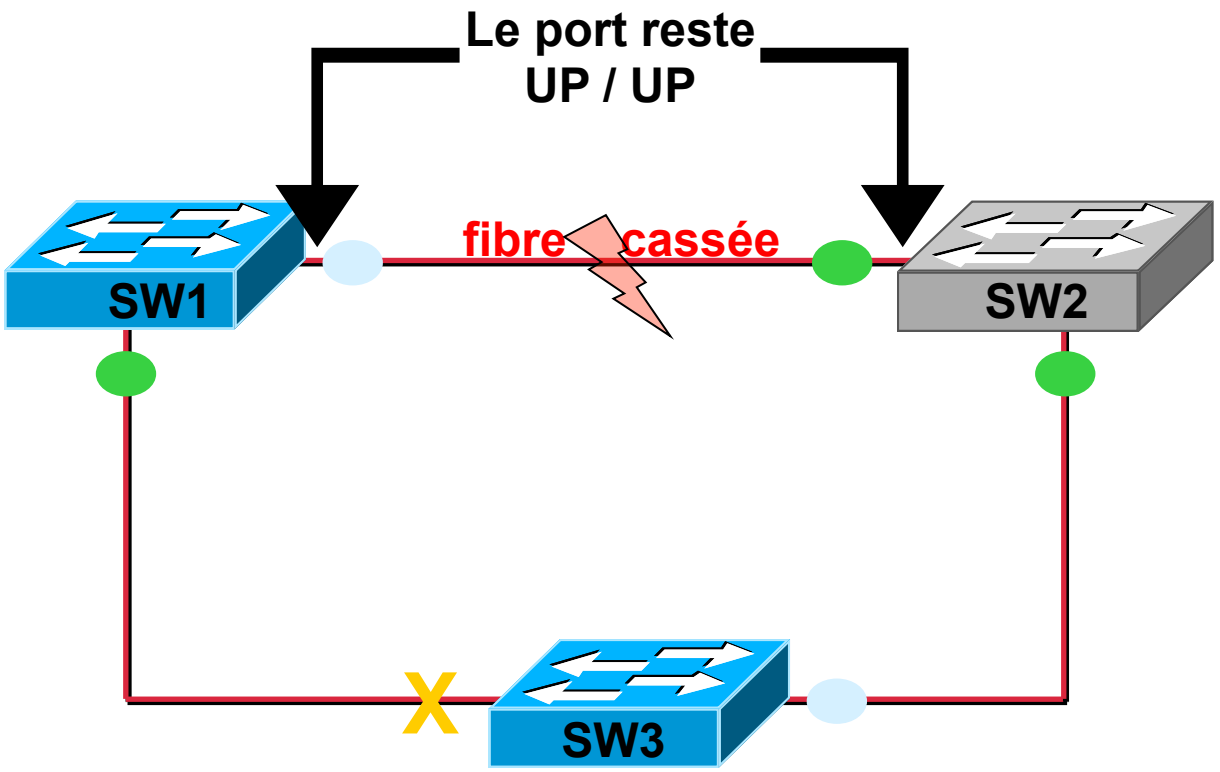
Timers STP

- HELLO 2 sec
  - fréquence à laquelle les BPDU sont générés par la racine
- FORWARD-DELAY 15 sec
  - temps d'attente dans les états listening et learning
- MAX-AGE 20 sec
  - durée de vie d'un BPDU

A quoi sert le ‘max-age’ ?



A quoi sert le ‘max-age’ ?



‘Max-age’ permet de détecter la perte du lien.

Vérifier STP sur le switch racine

```
Root_Switch#show spanning-tree vlan 1
VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     cc00.0000.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768
              Address     cc00.0000.0000
              Hello Time   2 sec  Max Age 20 sec
Forward Delay 15 sec
              Aging Time 300
Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID

-------------------- ------- ---- ----- --- ----- -------------

FastEthernet0/1      128.2    128    19 FWD     0 32768 cc00.0000.0000 128.2

FastEthernet0/10     128.11   128    19 FWD     0 32768 cc00.0000.0000 128.11
```

Vérifier STP sur le switch non-racine

```
Non_Root_Switch#show spanning-tree vlan 1

VLAN1
  Spanning tree enabled protocol ieee
 Root ID     Priority    32768
             Address     cc00.000c.0000
             Cost        19
             Port        11 (FastEthernet0/10)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768
             Address     cc03.0a4c.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet0/0      128.1    128    19 FWD    19 32768 cc03.0a4c.0000 128.1
FastEthernet0/1      128.2    128    19 BLK    19 32768 cc01.0a4c.0000 128.12
FastEthernet0/10     128.11   128    19 FWD     0 32768 cc00.000c.0000 128.11
```

15 secondes Statut LIS

```
Non_Root_Switch#sh spanning-tree vlan 1

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     cc00.000c.0000
              Cost        19
              Port        11 (FastEthernet0/10)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32768
              Address     cc03.0a4c.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet0/0      128.1    128    19 LIS    19 32768 cc03.0a4c.0000 128.1
FastEthernet0/1      128.2    128    19 BLK    19 32768 cc01.0a4c.0000 128.12
FastEthernet0/10     128.11   128    19 LIS     0 32768 cc00.000c.0000 128.11
```

15 secondes Statut LRN

```
Non_Root_Switch#sh spanning-tree vlan 1

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     cc00.000c.0000
              Cost        19
              Port        11 (FastEthernet0/10)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID  Priority    32768
              Address     cc03.0a4c.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet0/0      128.1    128    19 LRN    19 32768 cc03.0a4c.0000 128.1
FastEthernet0/1      128.2    128    19 BLK    19 32768 cc01.0a4c.0000 128.12
FastEthernet0/10     128.11   128    19 LRN     0 32768 cc00.000c.0000 128.11
```

Quelle affirmation est correcte ?

```
SwitchA# show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     0017.596d.2a00
              Cost        38
              Port        11(FastEthernet0/10)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 1)
              Address     0017.596d.1580
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

A. The Fa0/11 role confirms that SwitchA is the root bridge for VLAN 20.
B. VLAN 20 is running the Per VLAN Spanning Tree Protocol.
C. The MAC address of the root bridge is 0017.596d.1580.
D. SwitchA is not the root bridge, because not all of the interface roles are designated.

Port fast

- Pour passer immédiatement en FORWARDING.
- Certain qu'il n'y a pas de risque de boucle
- Exemple :
  - port connecté à un PC
  - port connecté à un serveur

Configurer Port Fast et activer Bpduguard

- conf t
- interface fa0/0
  - spanning-tree portfast
  - spanning-tree bpduguard enable
    - Désactive le lien sur réception d'un BPDU
    - Commande associée en général à la précdente
    - Le port passe en état « errdisabled »

Lenteur de 802.1d

- 50 secondes pour réagir :
  - 20 secondes de Max Age
  - 15 secondes en Listening
  - 15 secondes en Learning

Rapid STP = 802.1w

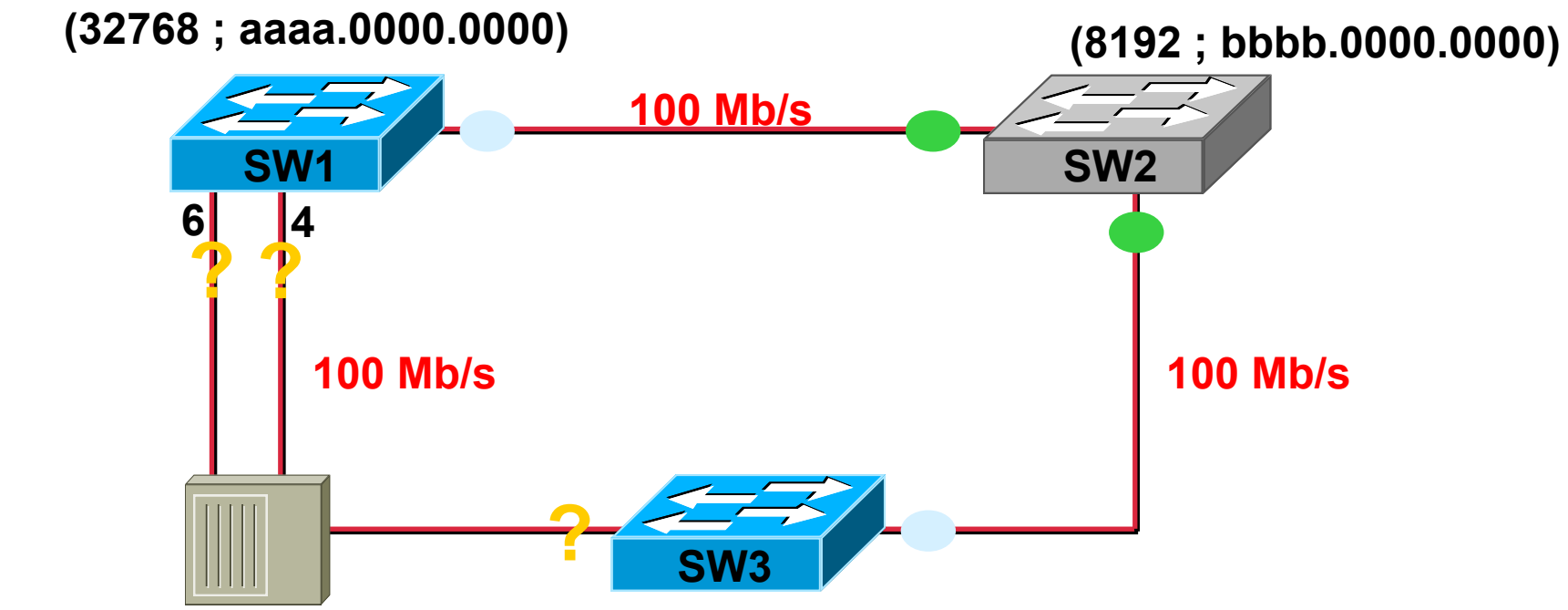
- **`conf t`**
- **`spanning-tree mode rapid-pvst`**

- Compatible avec STP.
- Les BPDU sont générés par chaque switch (et pas seulement par le switch racine).
  - Je n'attends plus 20 secondes pour réagir.
  - Je réagis dès que 3 BPDU ne sont pas arrivés

Rôles d'un port

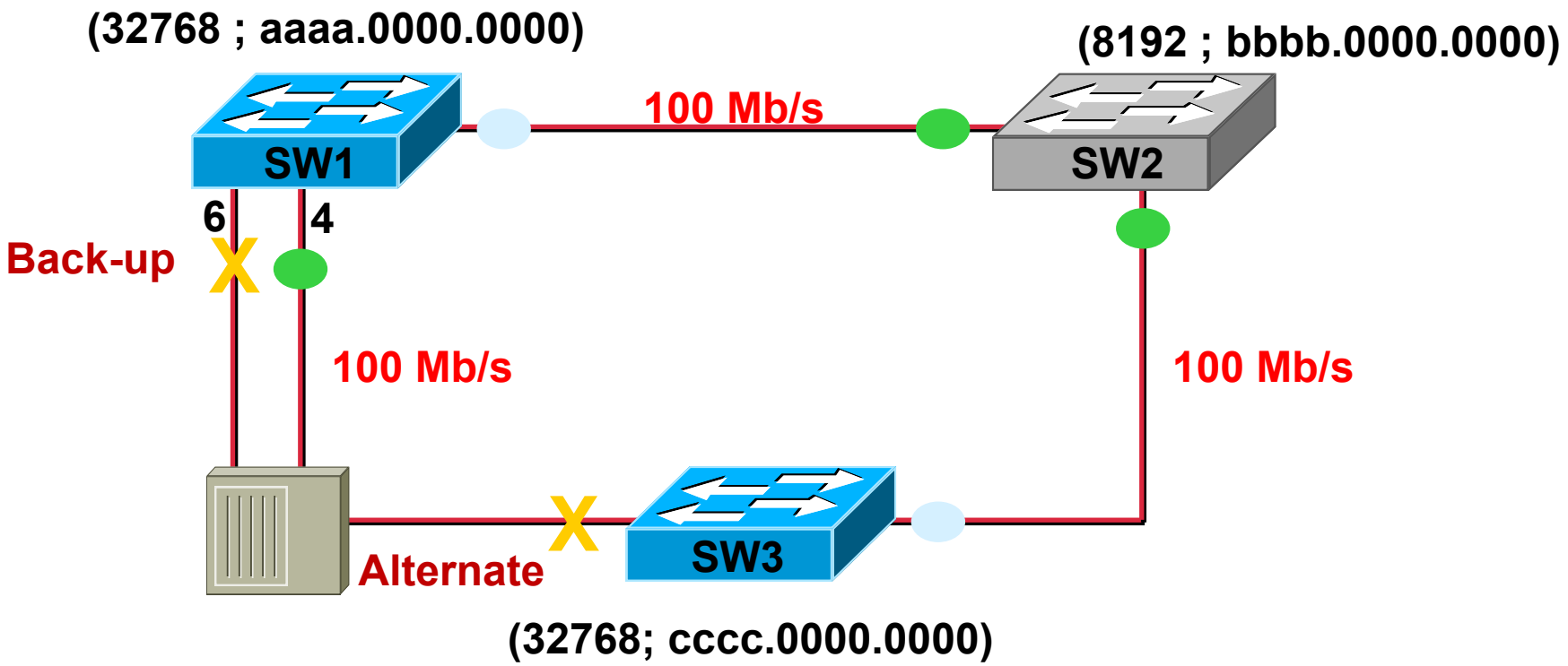
- Racine 
- Désigné
- Non désigné : X
  - Alternate
    - n'est pas sur le même switch que le port qui envoie le meilleur BPDU du segment
  - Back-up
    - est sur le même switch que le port qui envoie le meilleur BPDU du segment

Exemple pour ‘alternate / backup’

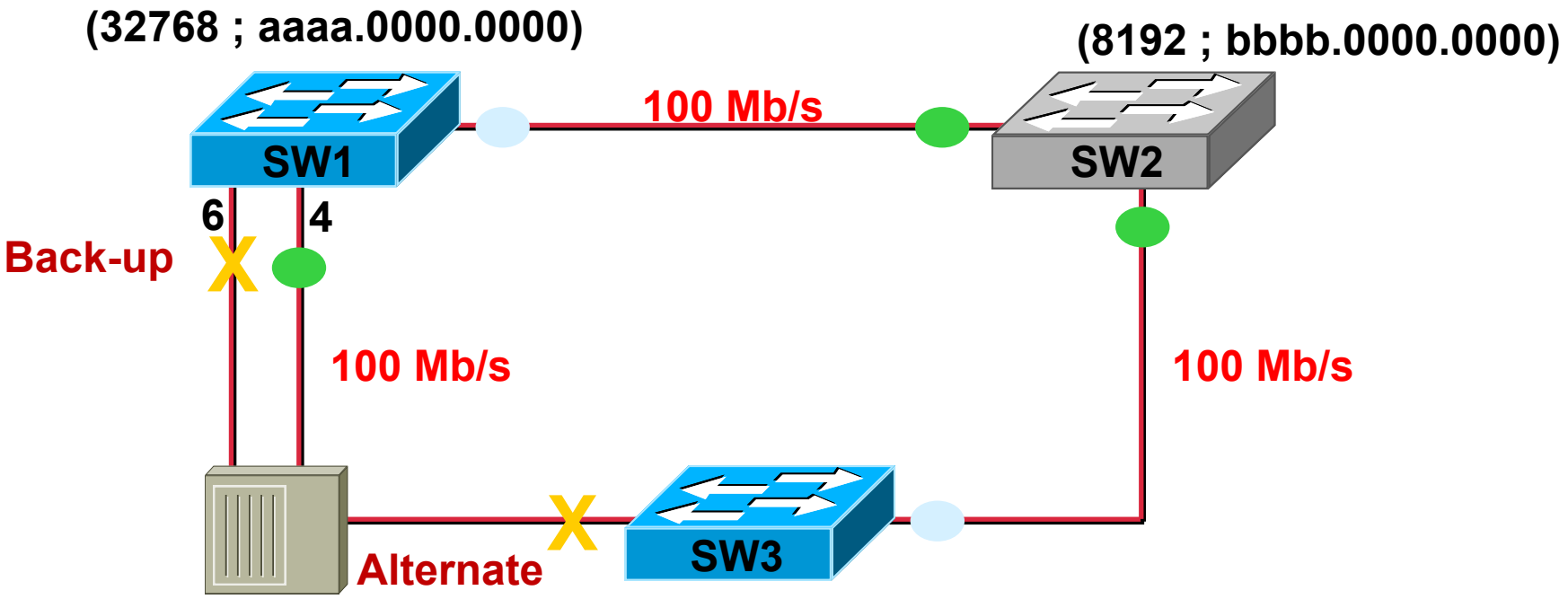


Quels sont les rôles de chaque port de ce segment ?

Exemple pour ‘alternate / backup’

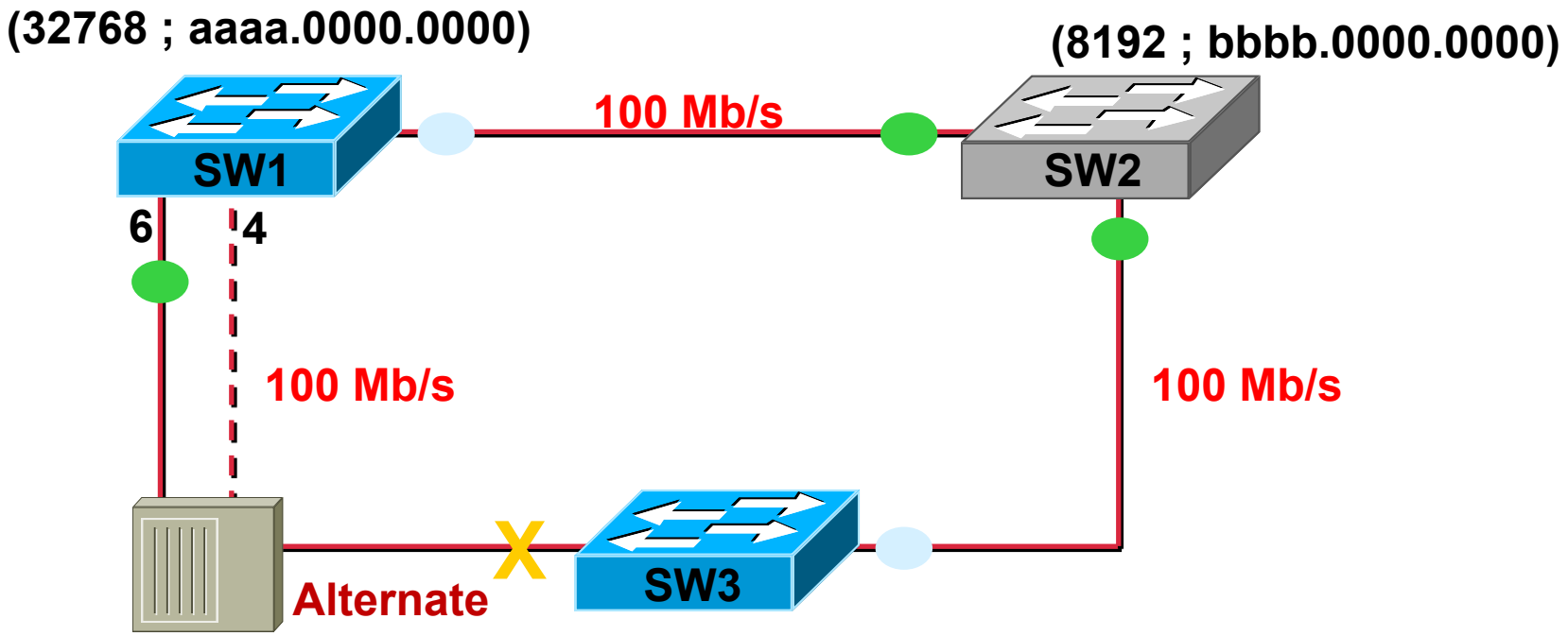


Exemple pour ‘alternate / backup’



Si le port désigné de ce segment tombe, qui prend la relève ?

Exemple pour ‘alternate / backup’



Le Back-up prend la relève.

RSTP : 3 types des ports

- « Point-to-Point »
  - Switch en full duplex
    - Convergence plus rapide avec RSTP
- « Shared »
  - Hub (half duplex)
- « Edge »
  - Connecté à un host
    - Configuré via PortFast

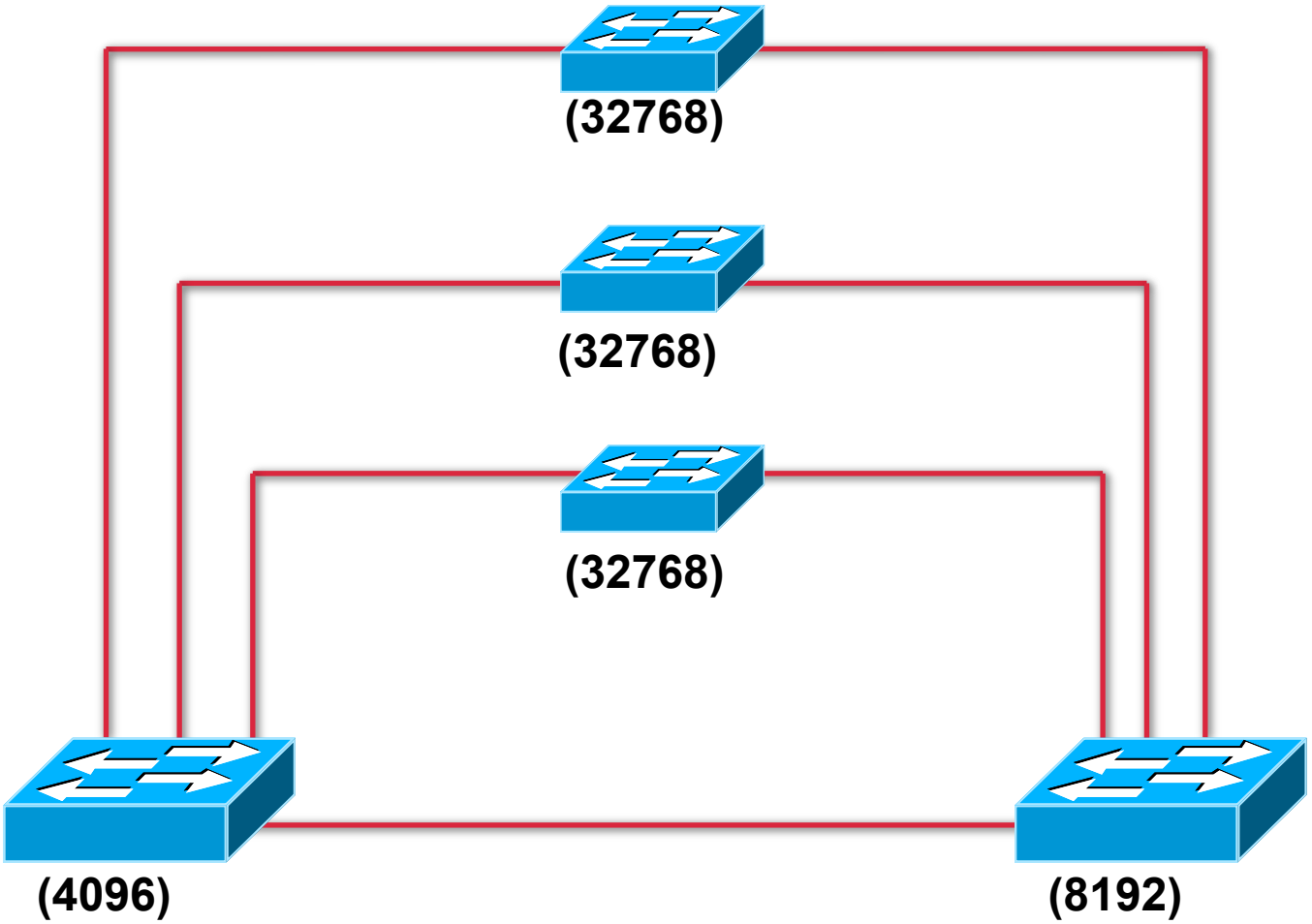
PVST+

- Per VLAN Spanning-Tree
- Un arbre de recouvrement pour CHAQUE vlan.
- Compatible avec Rapid-STP.

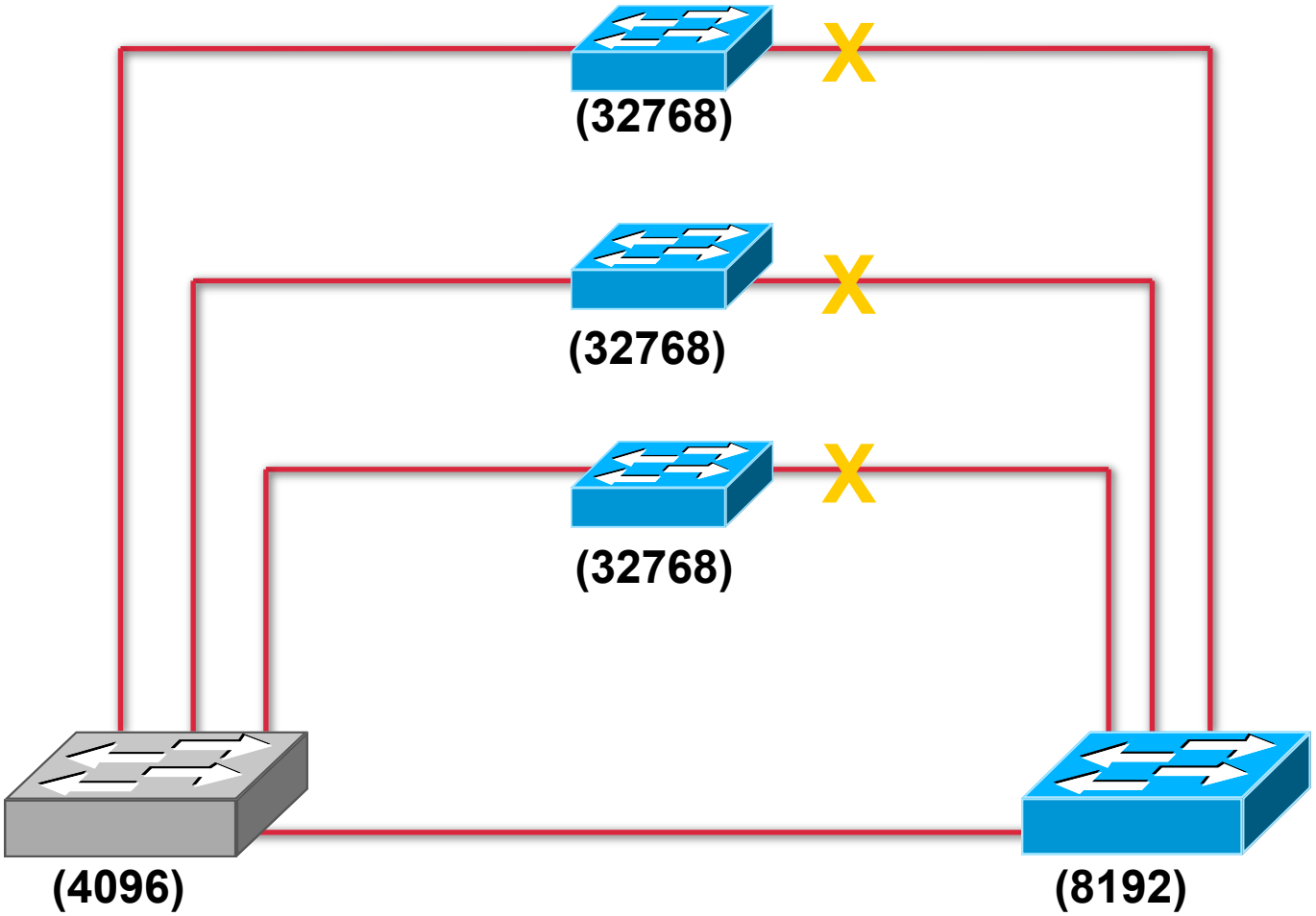
PVST

- Per VLAN Spanning-Tree
- Un arbre de recouvrement pour CHAQUE vlan

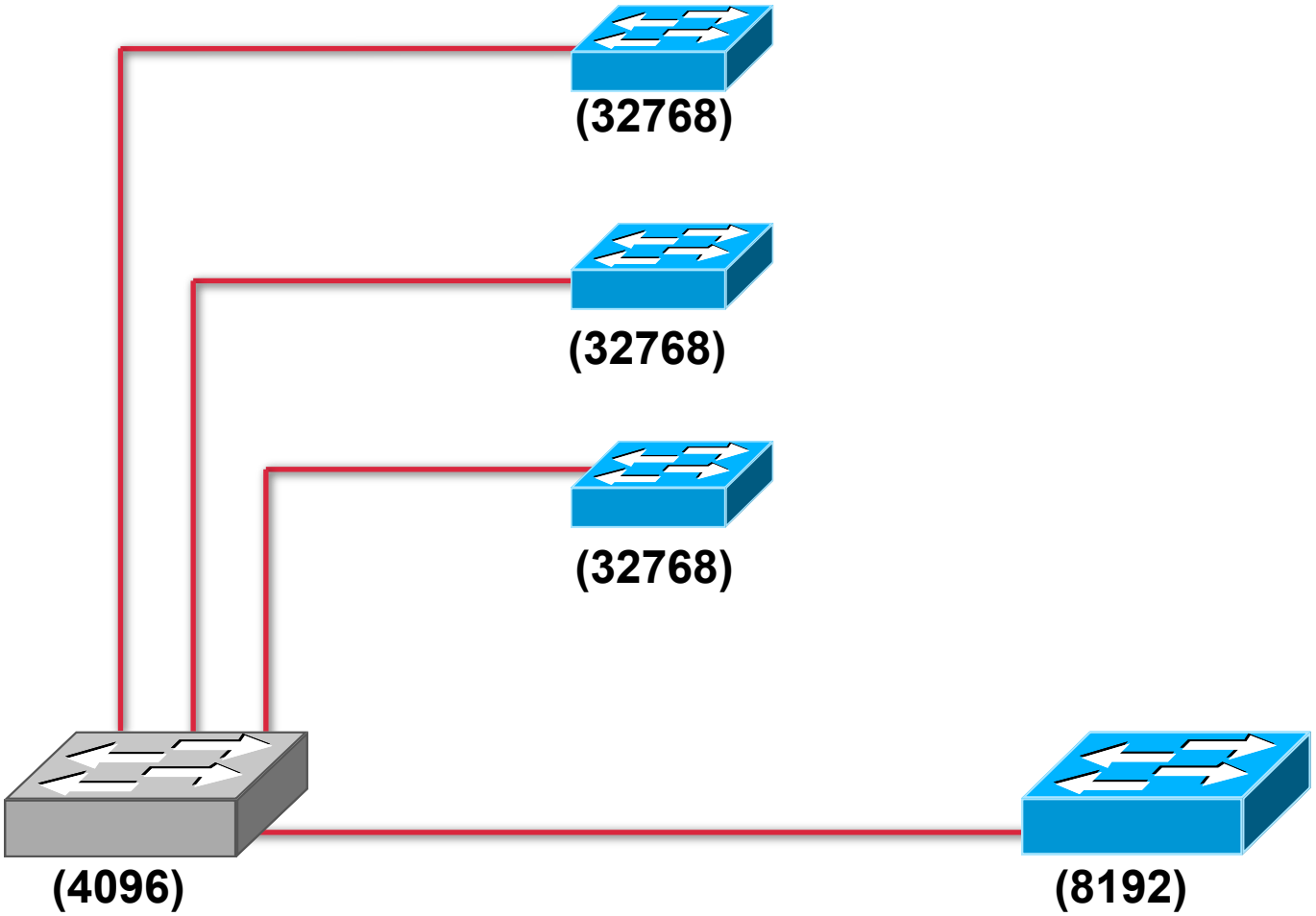
Batiment avec 3 étages



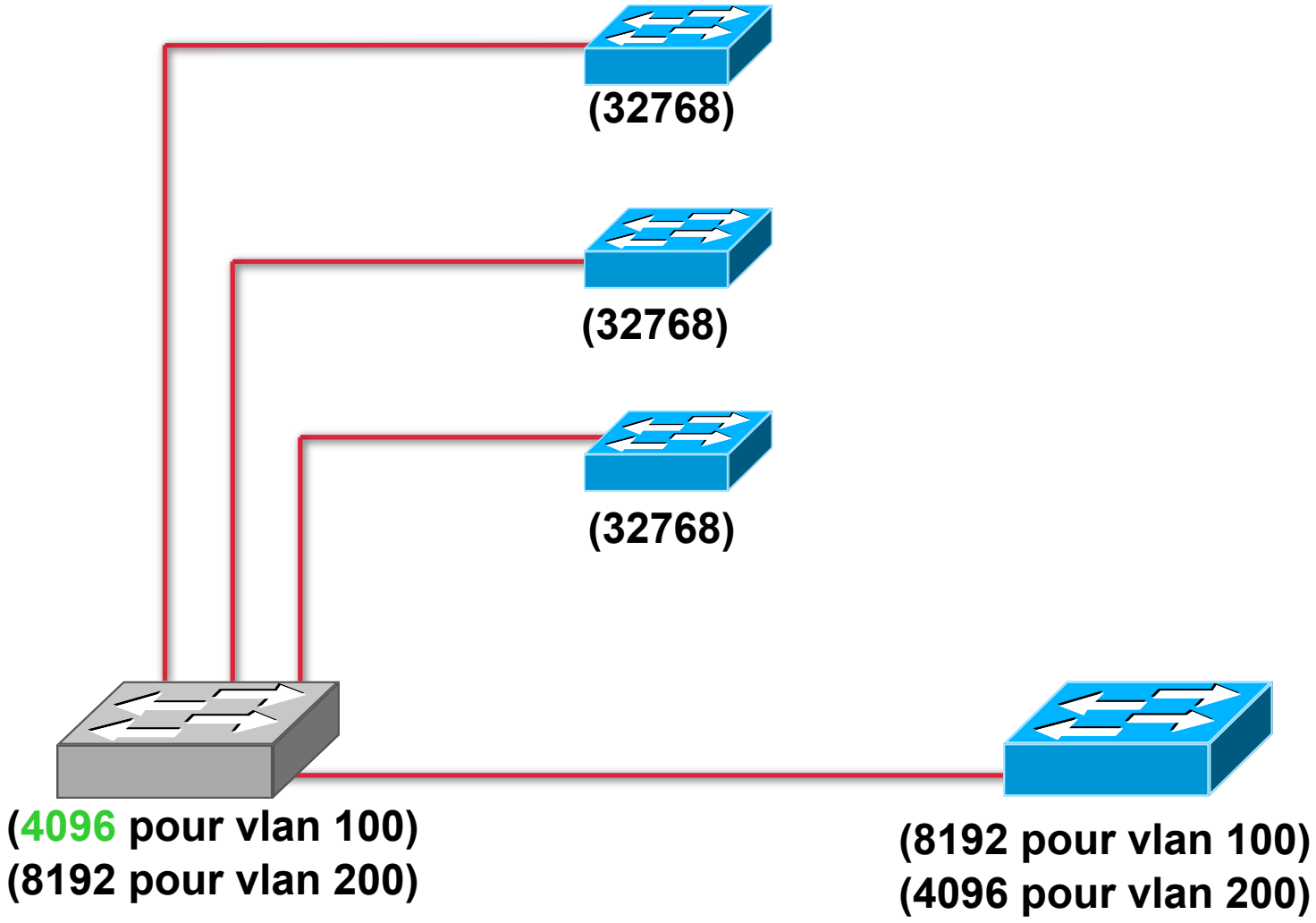
1 STP pour tous les VLANS



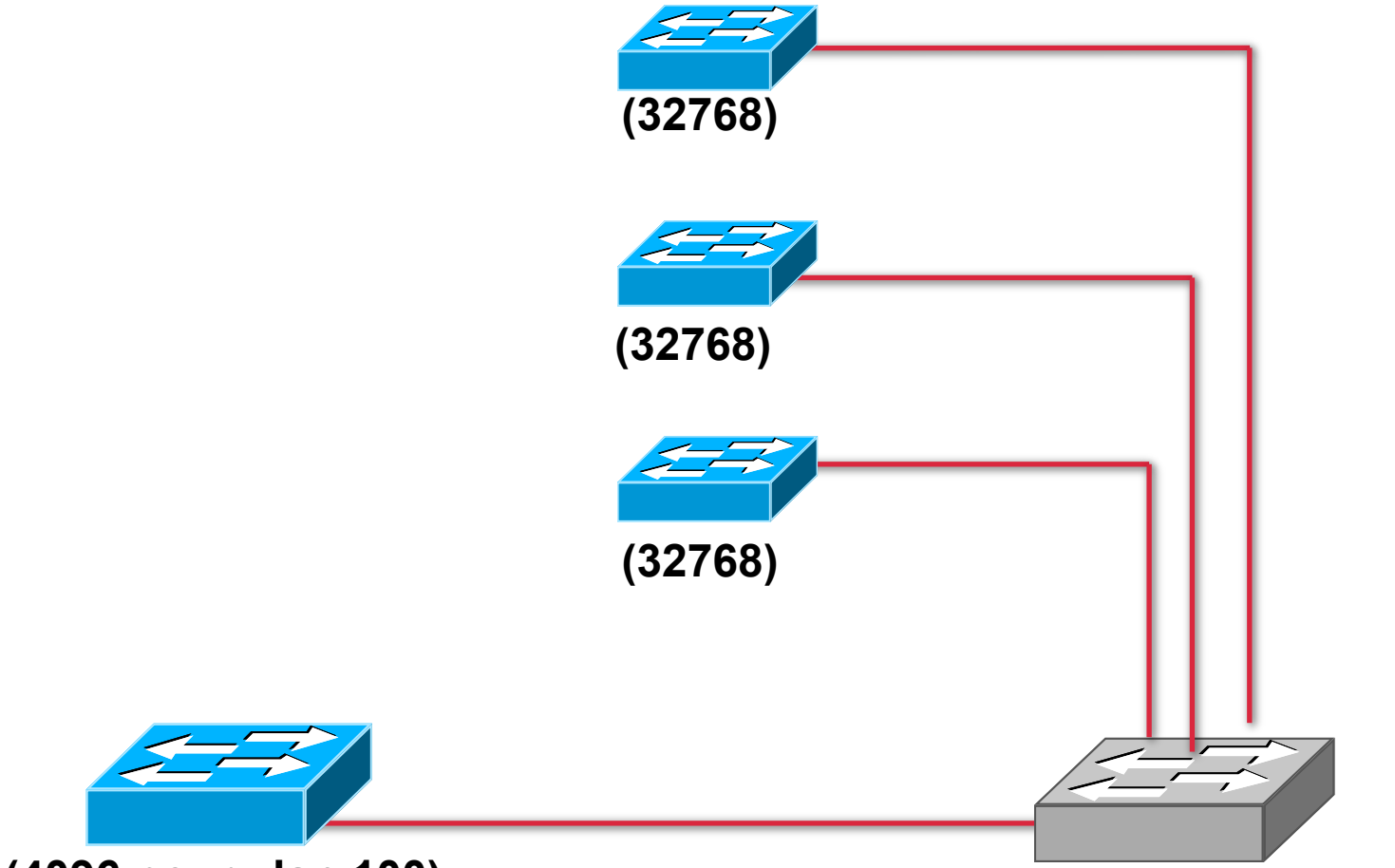
TOUT le trafic passe par ici…



PVSTP : trafic du VLAN 100



PVSTP : trafic du VLAN 200



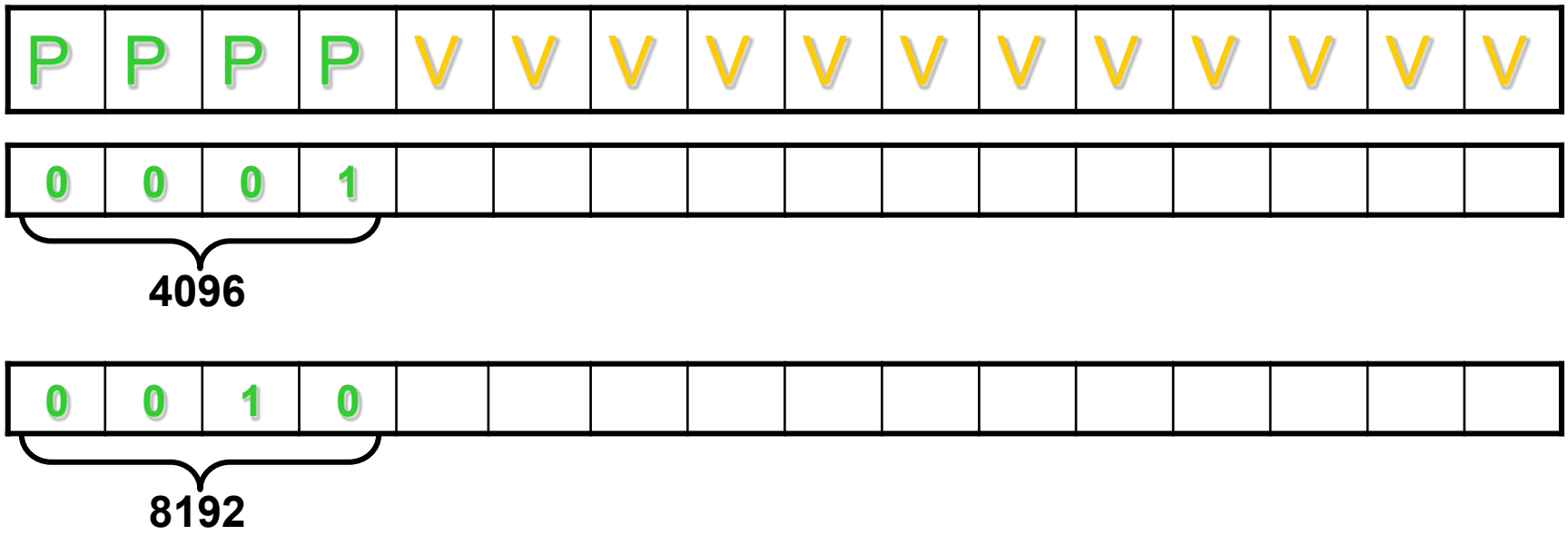
Positionner le sw racine

- Diminuer sa priorité.
- Par défaut, Bridge PRIORITY = 32768
- Pour diminuer :
  - conf t
  - spanning-tree vlan 100 priority 8192
    - obligatoirement un multiple de 4096

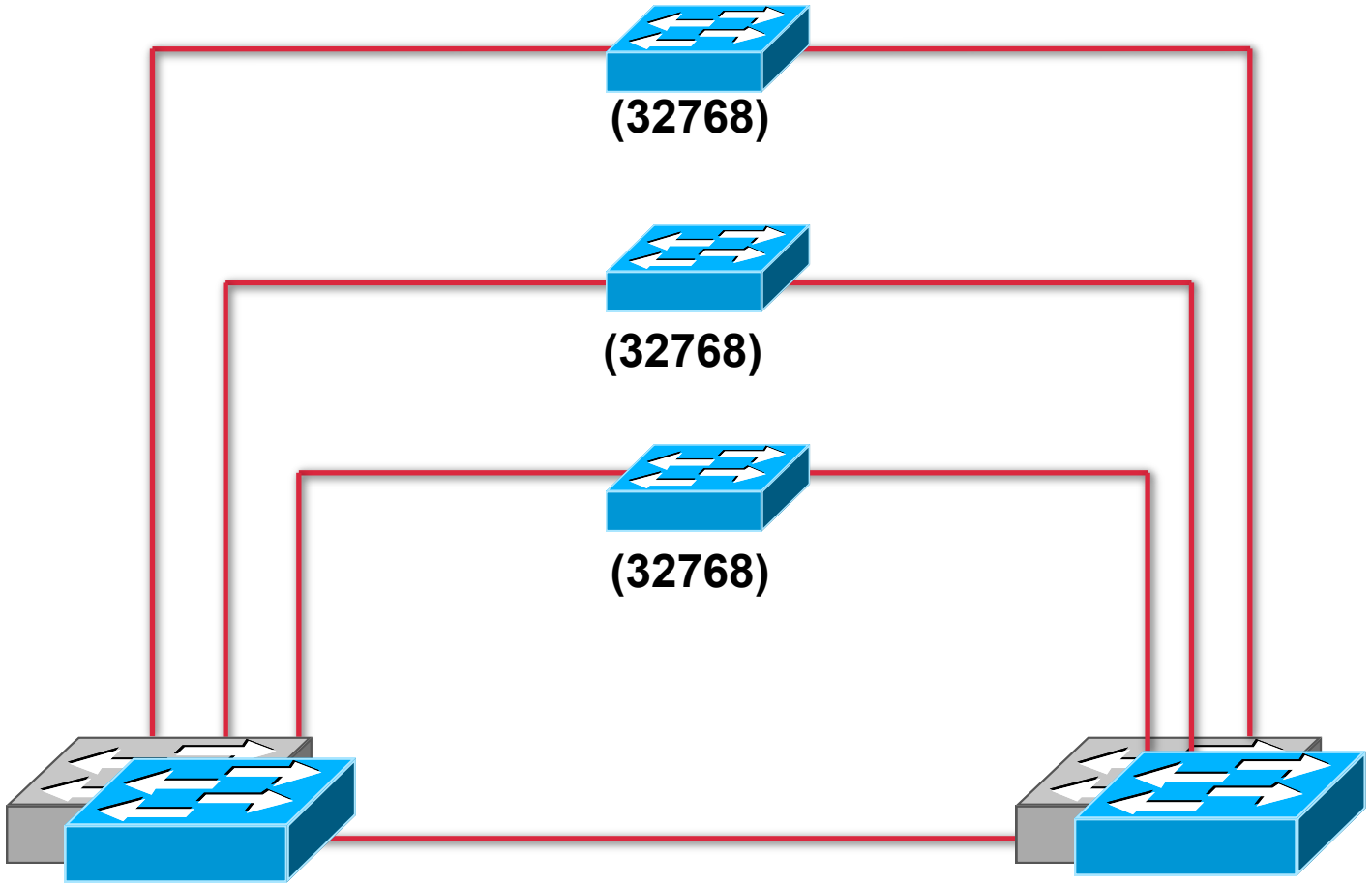
Le CHAMP bridge priority

Entre 0 et 65535 = 16 bits
Utilisé pour coder à la fois :

- le BRIDGE PRIORITY = 4 bits
- le n° du VLAN = 12 bits



Configuration PVSTP



spanning-tree vlan 100 priority 4096
spanning-tree vlan 200 priority 8192

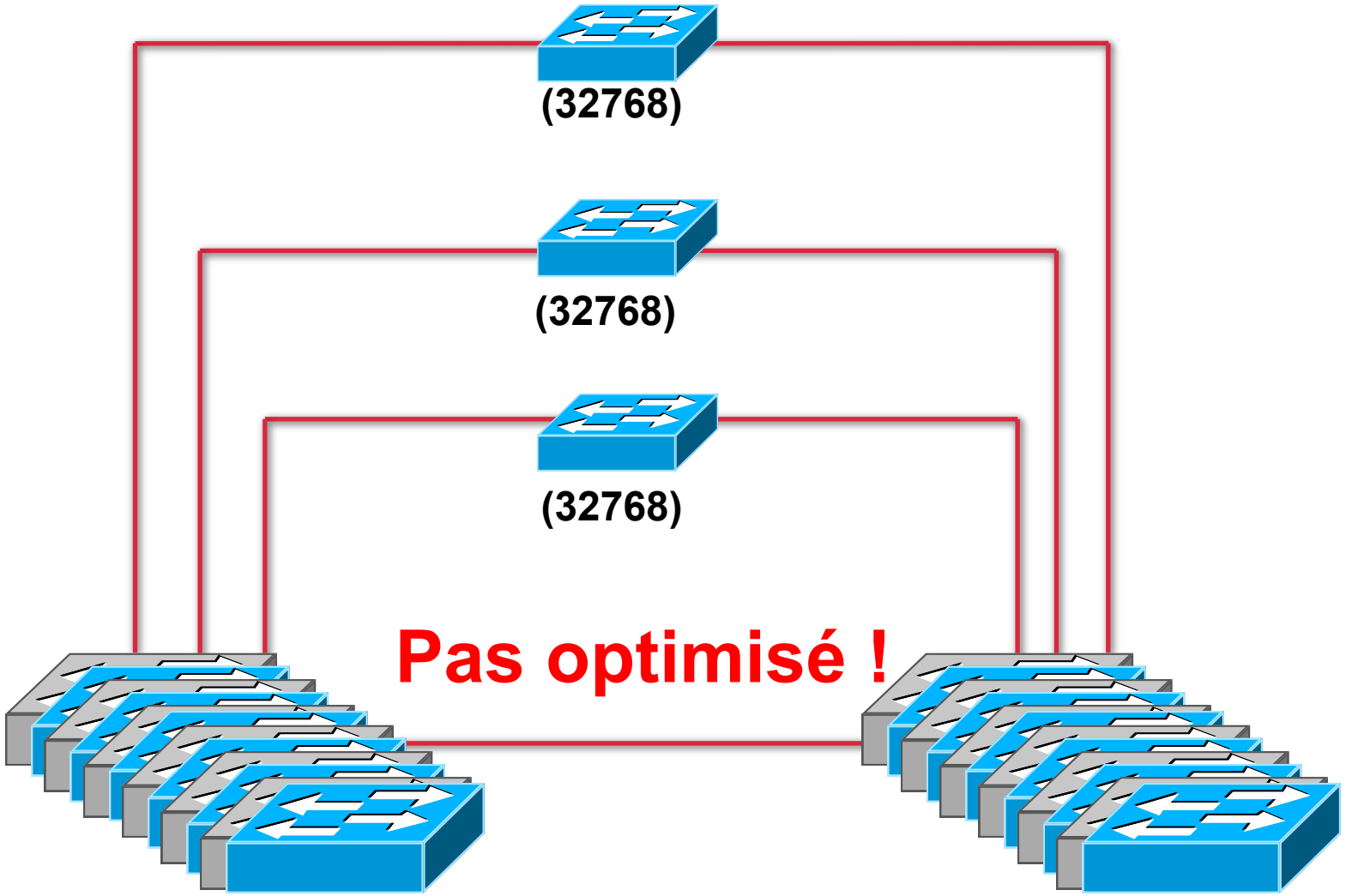
spanning-tree vlan 100 priority 8192
spanning-tree vlan 200 priority 4096

Macro

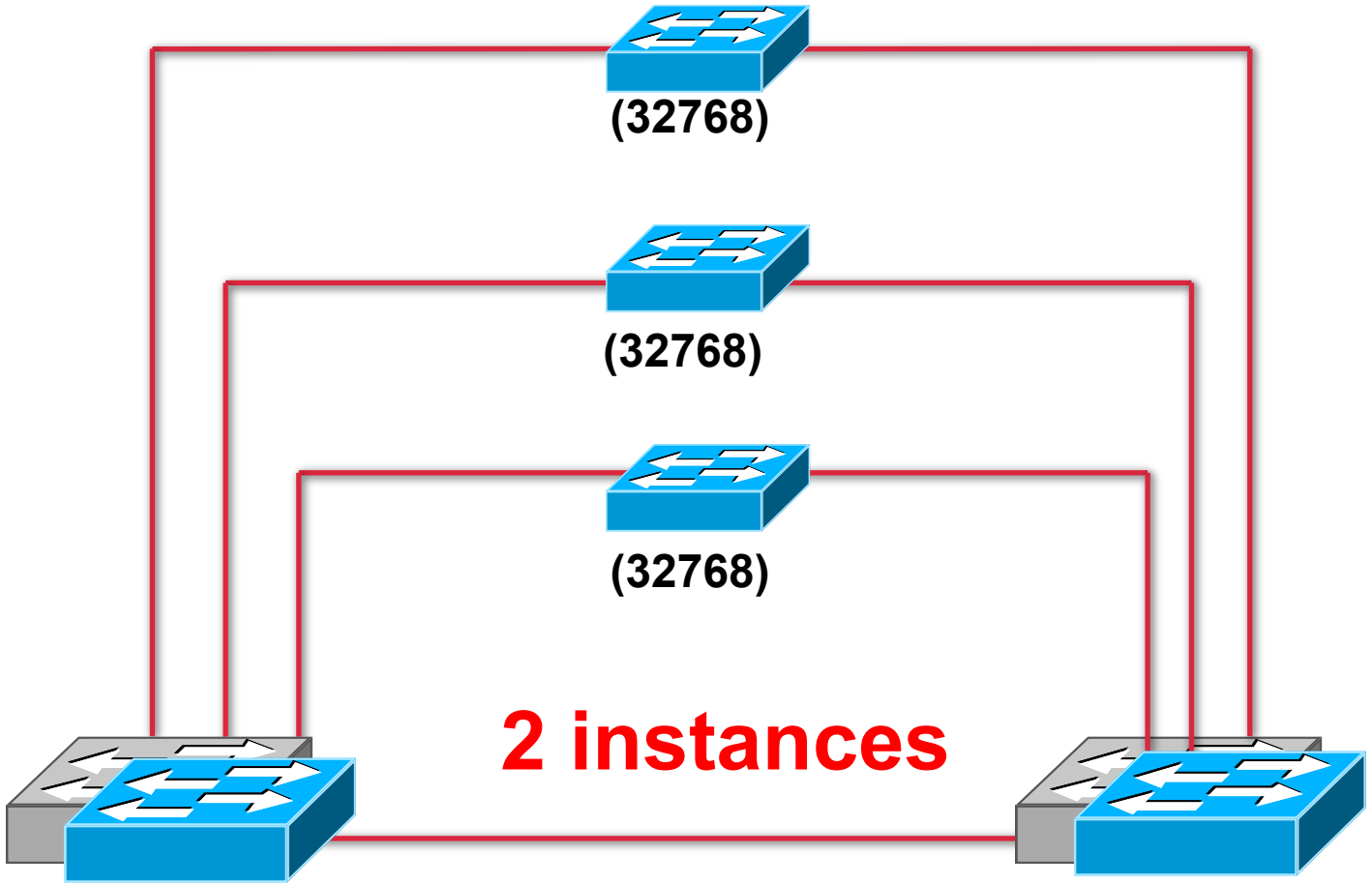
- spanning-tree vlan 100 root primary
  - IOS s' arrange pour prendre une priorité plus basse que toutes celles annoncées sur le réseau

- spanning-tree vlan 100 root secondary

Et si 50 vlans…



MSTP = Multiple STP = 802.1s



racine pour VLAN 1 à 50
back-up pour VLAN 51 à 100

back-up pour VLAN 1 à 50
racine pour VLAN 51 à 100

Types of Spanning-Tree Protocols

Spanning-tree standards:

- **IEEE 802.1D:** The legacy standard for bridging and STP
  - **CST:** Assumes one spanning-tree instance for the entire bridged network, regardless of the number of VLANs
- **PVST+:** A Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN that is configured in the network
- **802.1s (MSTP):** Maps multiple VLANs into the same spanning-tree instance
- **802.1w (RSTP):** Improves convergence over 1998 STP by adding roles to ports and enhancing BPDU exchanges
- **Rapid PVST+:** A Cisco enhancement of RSTP using PVST+

Comparison of Spanning-Tree Protocols

Protocol	Standard	Resources Needed	Convergence	Number of Trees
STP	802.1D	Low	Slow	One
PVST+	Cisco	High	Slow	One for every VLAN
RSTP	802.1w	Medium	Fast	One
Rapid PVST+	Cisco	Very high	Fast	One for every VLAN
MSTP	802.1s Cisco	Medium or high	Fast	One for multiple VLANs

Glossaire

Standard	Date	Description
802.3	1983	CSMA/CD Ethernet
802.3ad	2000	Aggrégation de liens LACP
802.1D	1998, 2004	Spanning Tree Protocol STP
802.1Q	1998, 2003, 2005 2011 2014	Virtual LANs
802.1s	*mutualisé avec 802.1Q-2003*	Multiple Spanning Trees
802.1w	*mutualisé avec 802.1D-2004*	Rapid Spanning Tree
802.1x	2001	Port Based Network Access
802.1ab	2005	LLDP

Test

Which spanning-tree protocol rides on top of another spanning-tree protocol?

A. MSTP
B. RSTP
C. PVST+
D. Mono Spanning Tree

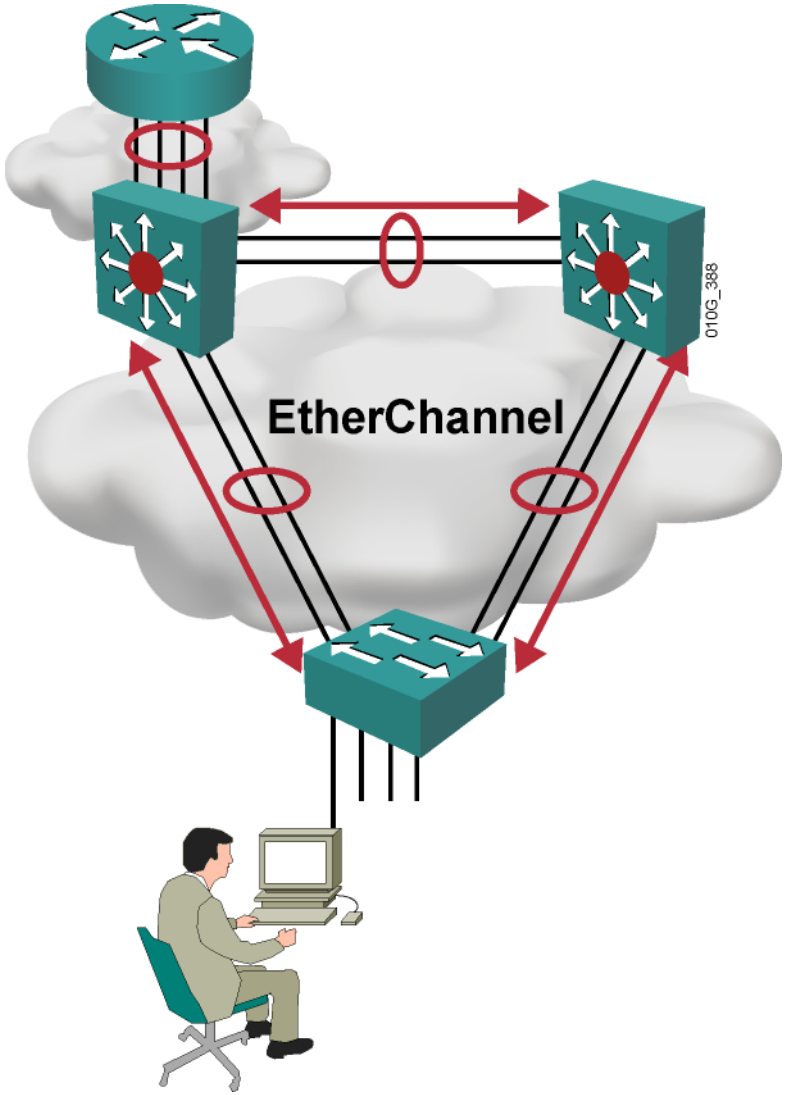
Correct Answer: A

Etherchannel

Aggrégation de liens

EtherChannel

- Aggrégation logique de liaisons similaires
- Partage de charge
- Considéré comme un seul port logique
- Redondance
- Jusque 8 liens simultannés



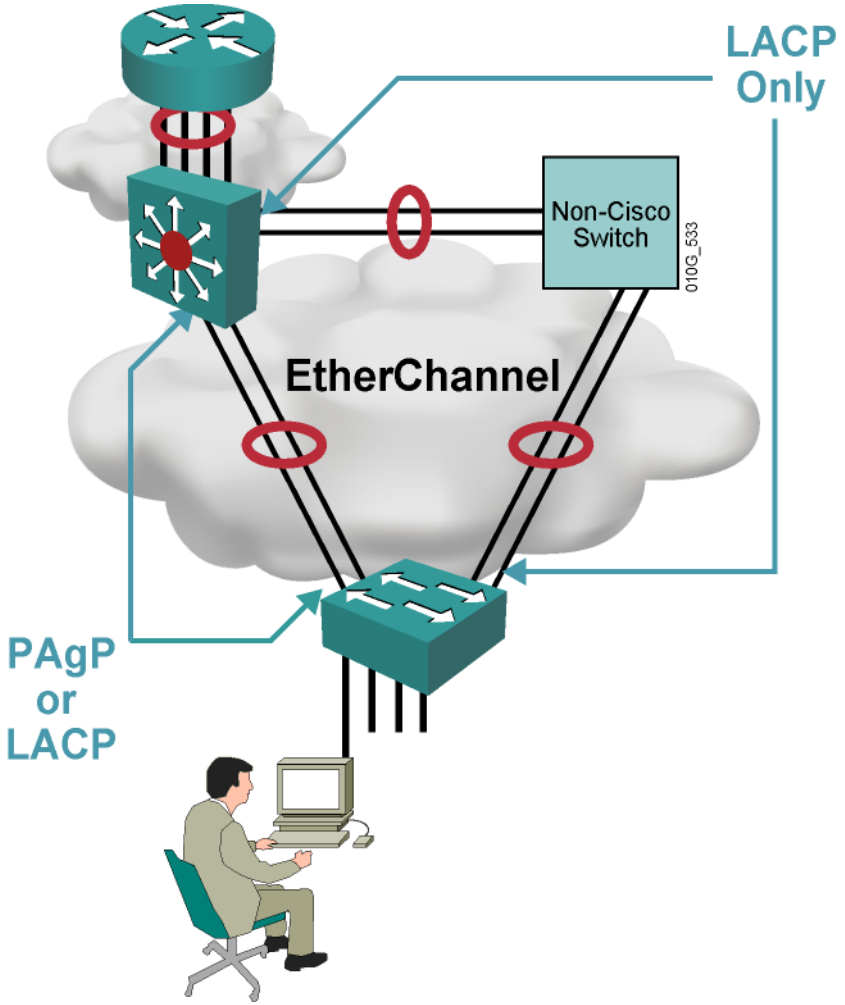
Protocoles de négociation dynamique

PAgP

- Propriétaire Cisco

LACP

- Standard IEEE 802.3ad



Terminologie de négociation

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Static Persistance

	On
On	Yes

Recommandations sur les EtherChannels

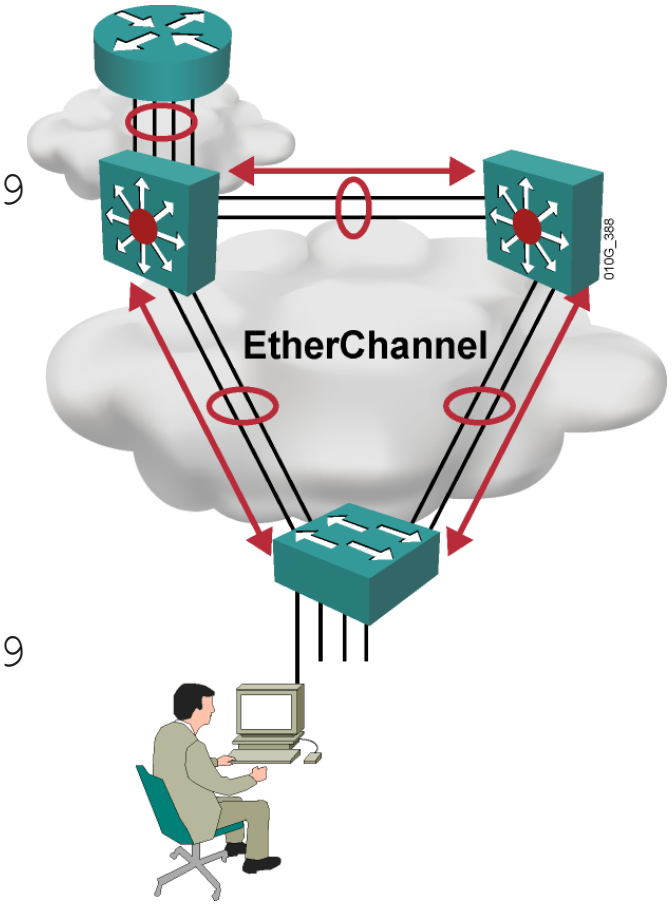
- Toutes les interfaces physiques d'un Etherchannel doivent être configurée avec la même **vitesse** et la même mode **duplex**.
- Toutes les interfaces physiques d'un Etherchannel doivent :
  - soit être rattachées au **même VLAN**,
  - soit fonctionner en **mode Trunk**.
- Si les interfaces physiques d'un Etherchannel sont en mode Trunk, alors elles doivent toutes autoriser **la même liste de VLANs**.

Recommandations sur les EtherChannels

- Les interfaces physiques d'un Etherchannel peuvent avoir des coûts STP différents.
- Toute modification de la configuration de l'interface logique impacte l'Etherchannel et donc les interfaces physiques
- Une modification de la configuration d'une interface physique n'impacte pas l'interface logique.

Recommandations sur les EtherChannels

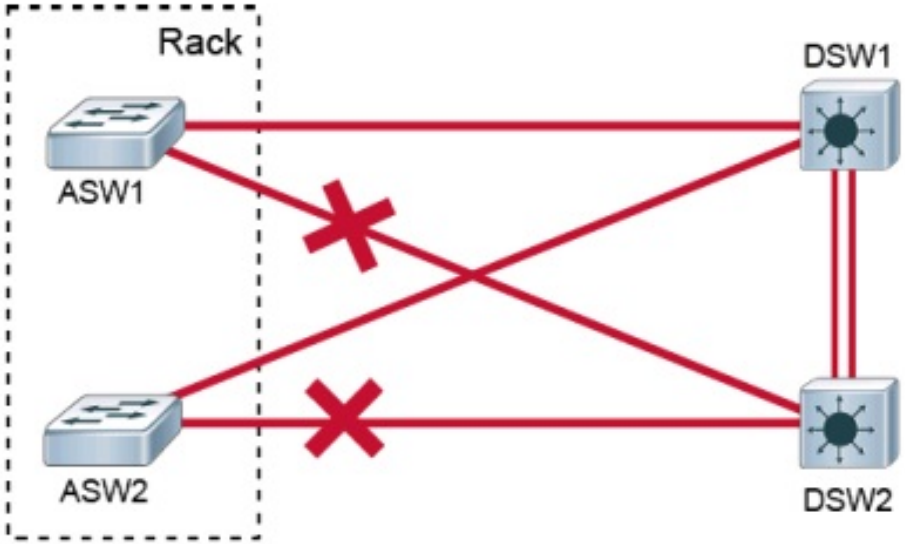
```
interface FastEthernet0/9
 description DSW121 0/9-10 - DSW122 0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,21-28
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 description DSW121 0/9-10 - DSW122 0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,21-28
 switchport mode trunk
 channel-group 2 mode desirable
```



Switch Stacking

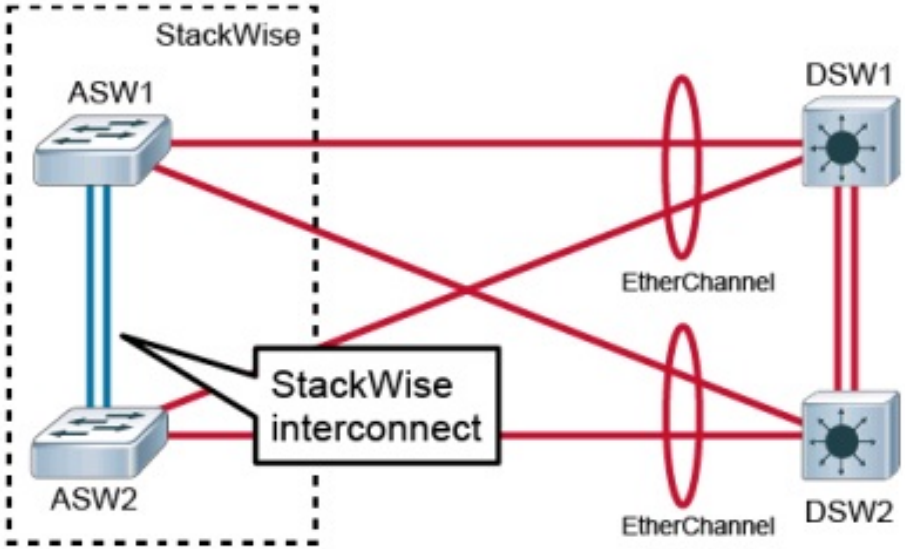
- StackWise provides a method to join multiple physical switches into a single logical switching unit.
- Switches are united by special interconnect cables.
- The master switch is elected.
- The stack is managed as a single object and has a single management IP address.

Switch Stacking (Cont.)



Typical switch topology:

- Management overhead.
- STP blocks half of the uplinks.
- No direct communication between access switches.



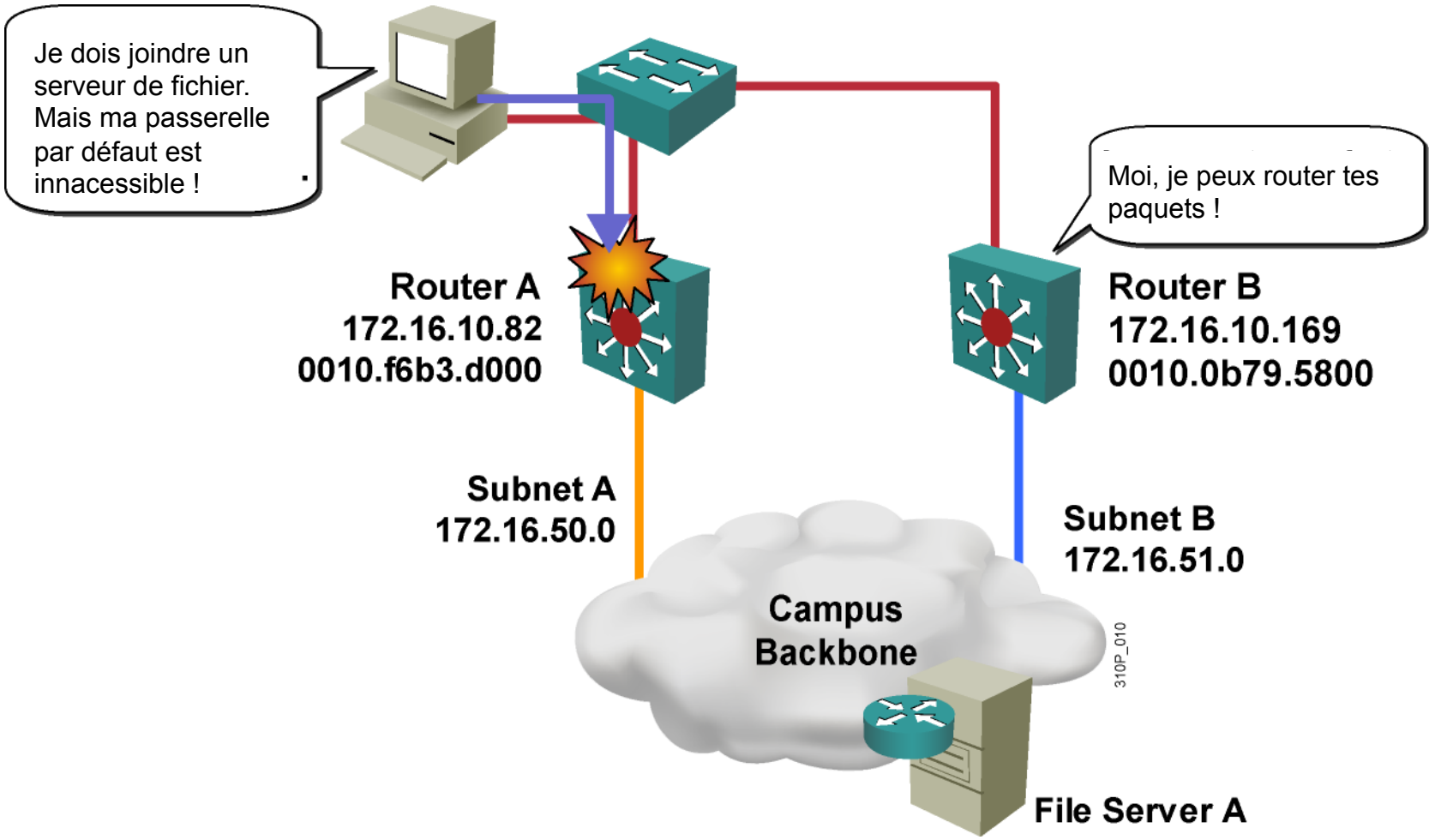
Topology using StackWise:

- Multiple access switches in the same rack.
- Reduced management overhead.
- Stack interconnect.
- Multiple switches can create an EtherChannel connection.

Configurer la haute disponibilité dans un réseau d'entreprise

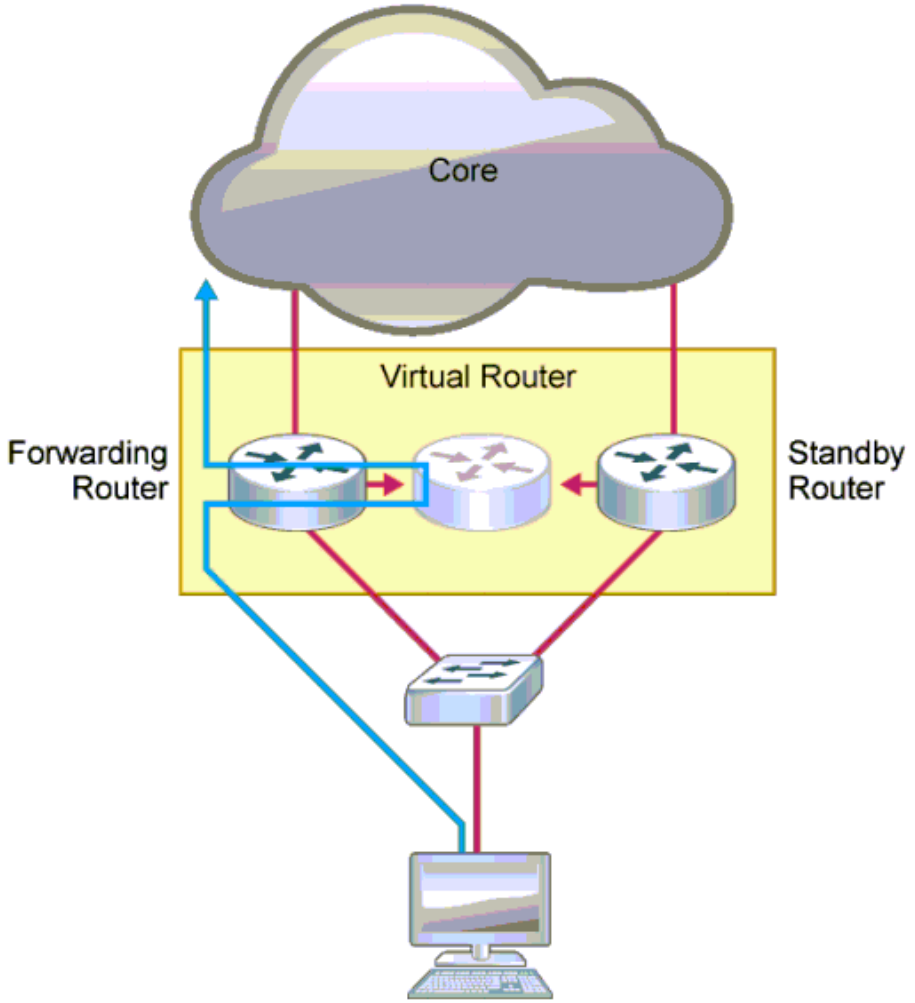
Configurer la redondance de la passerelle par défaut avec HSRP

Indisponibilité de la passerelle par défaut

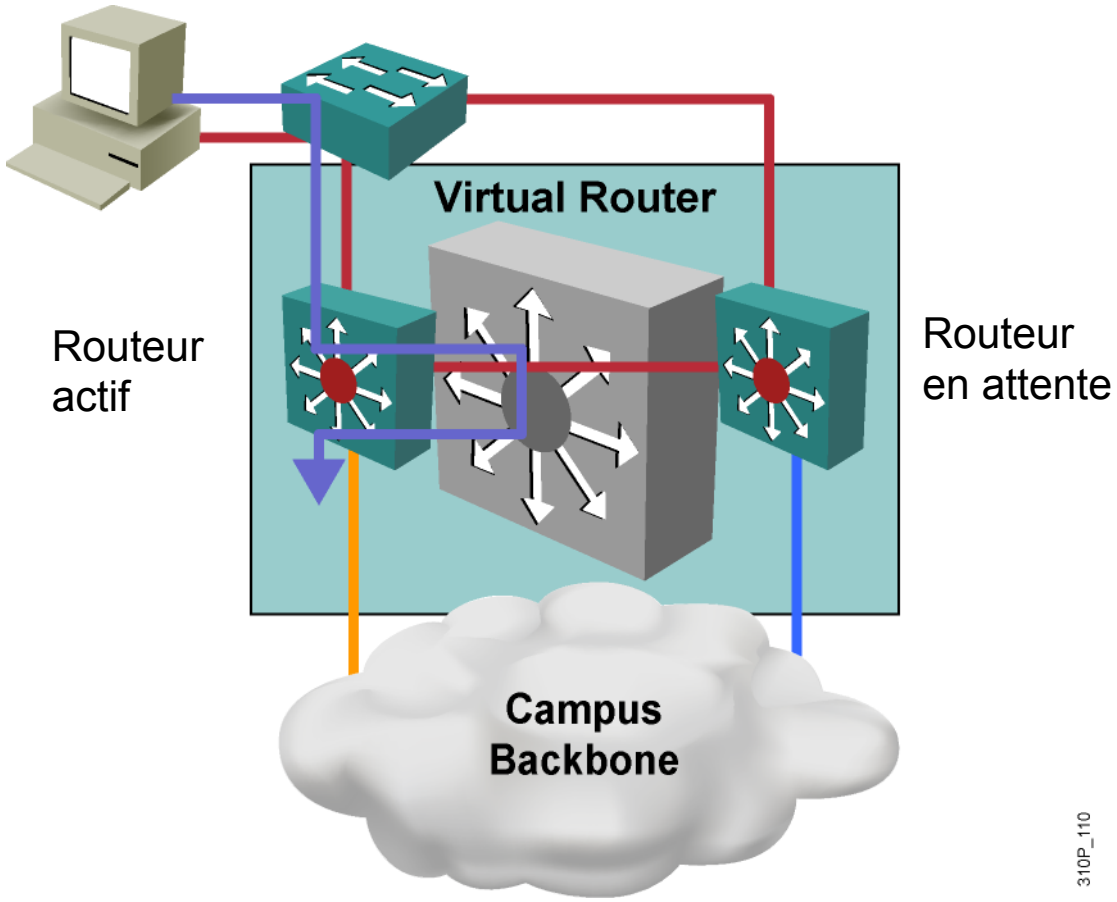


First Hop Redundancy Protocol

Understanding FHRP

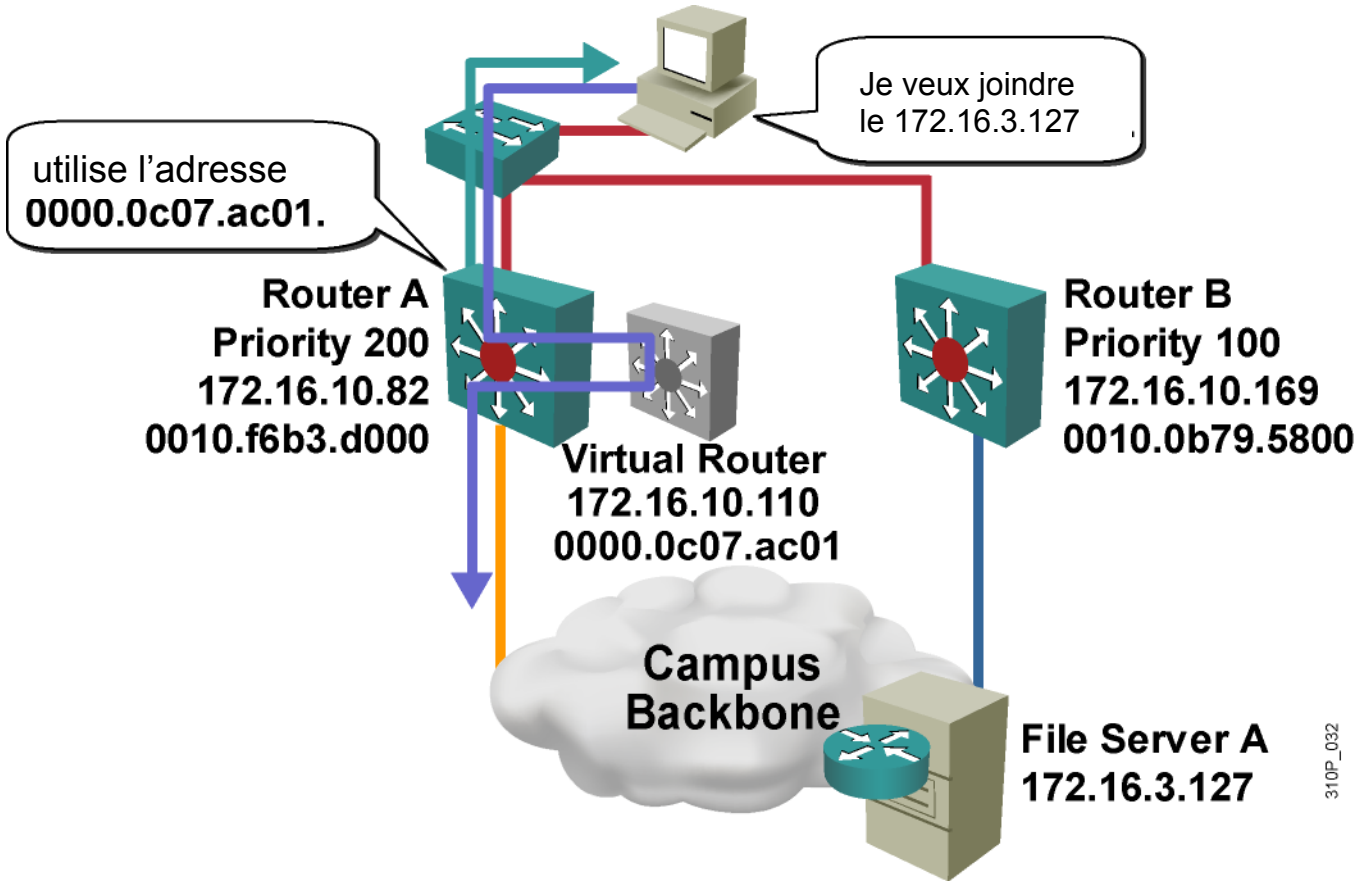


Cisco HSRP (Hot Standby Routing Protocol)



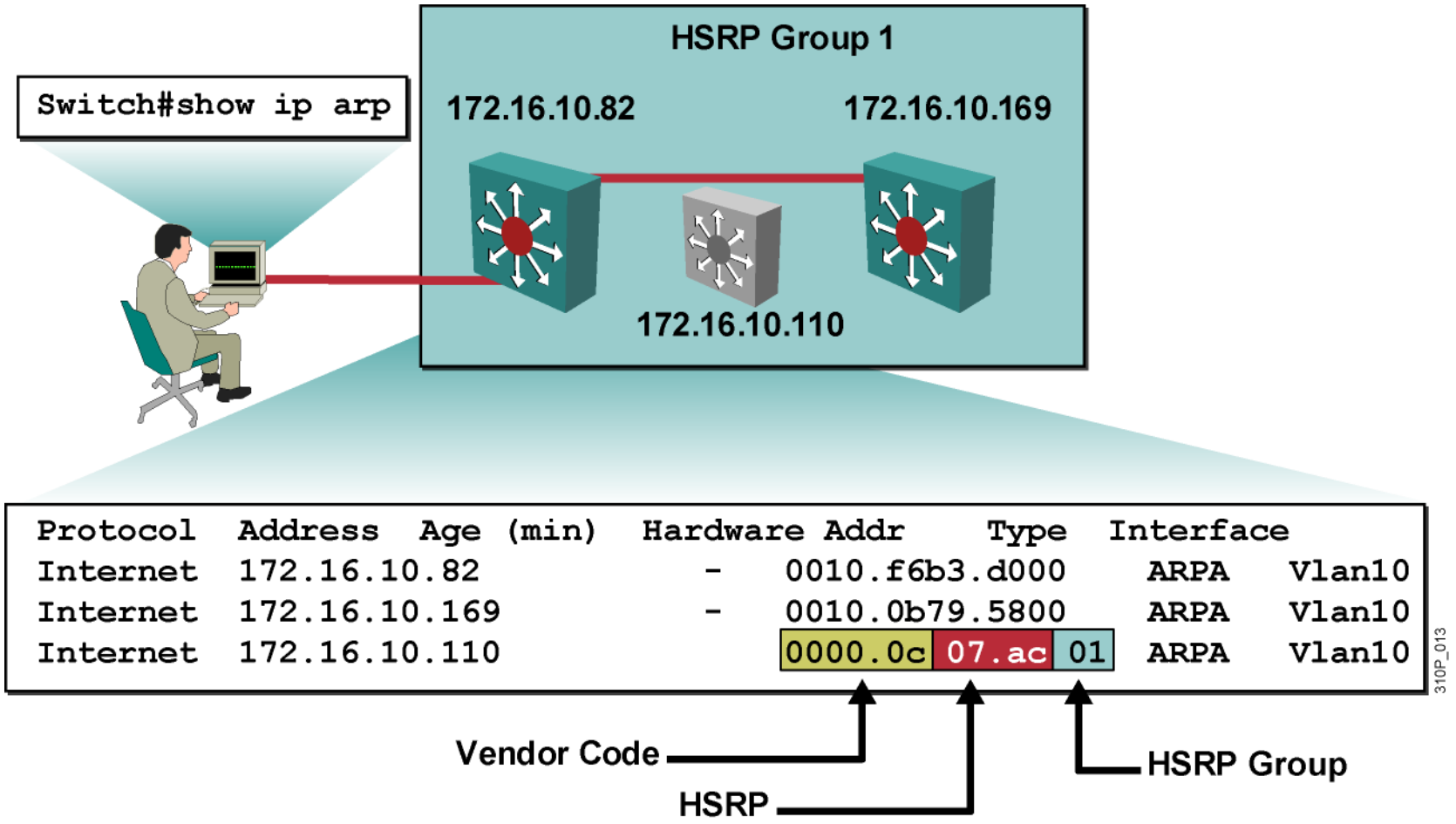
Un ensemble de routeurs, en secours d'un routeur actif, est appelé groupe HSRP

Le routeur Actif

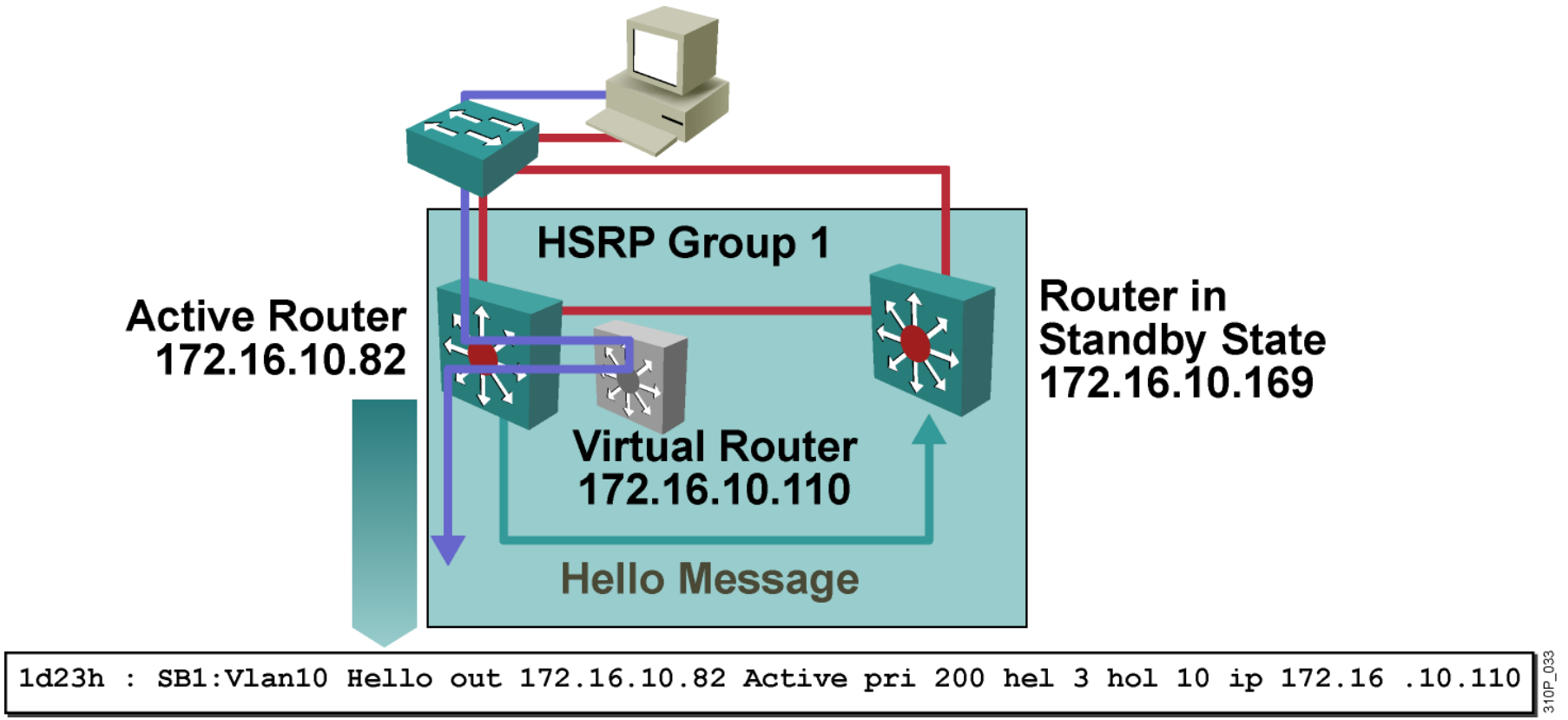


Le routeur actif répond aux requêtes ARP avec l'adresse MAC virtuelle du routeur virtuel

Adresse MAC virtuelle

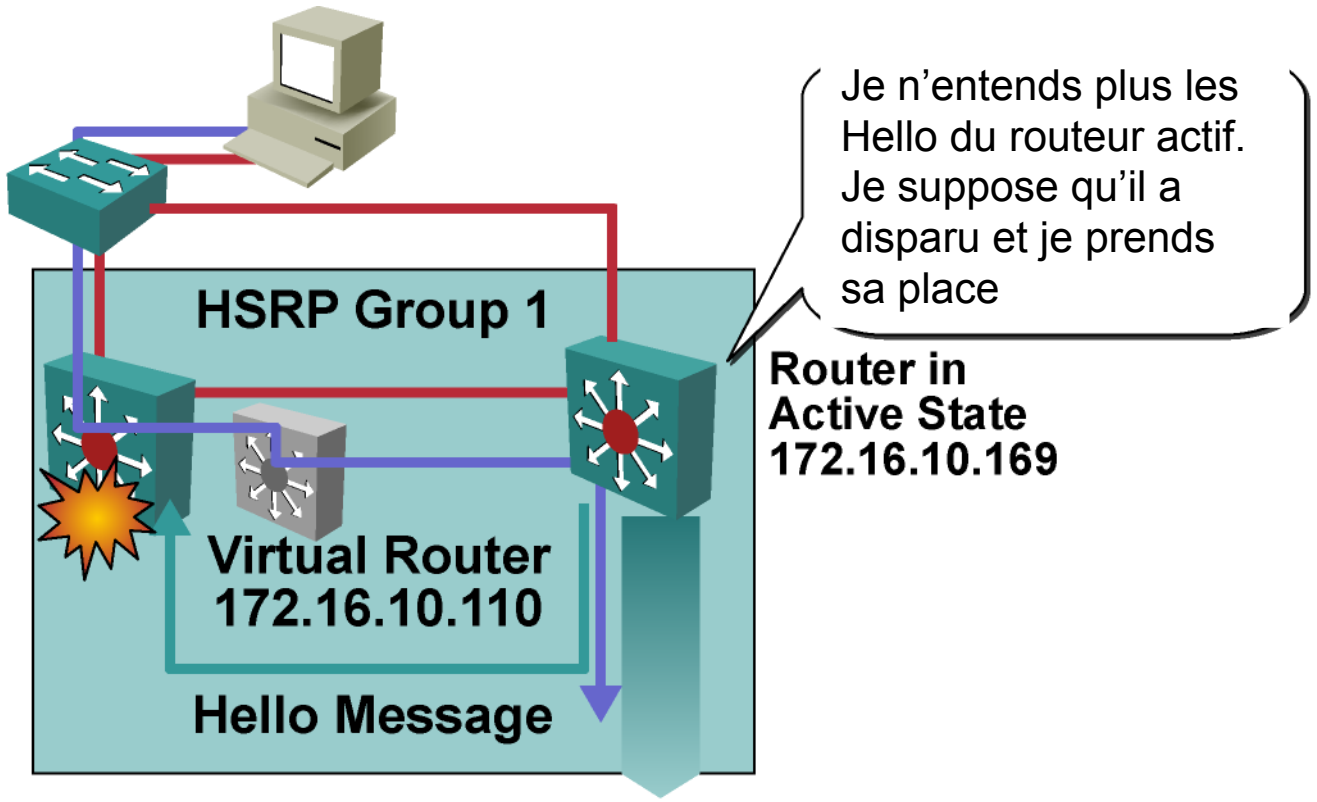


Le routeur Standby



Le routeur Standby écoute les hellos périodiques sur 224.0.0.2.

Si le routeur actif n'entend plus le Stanby

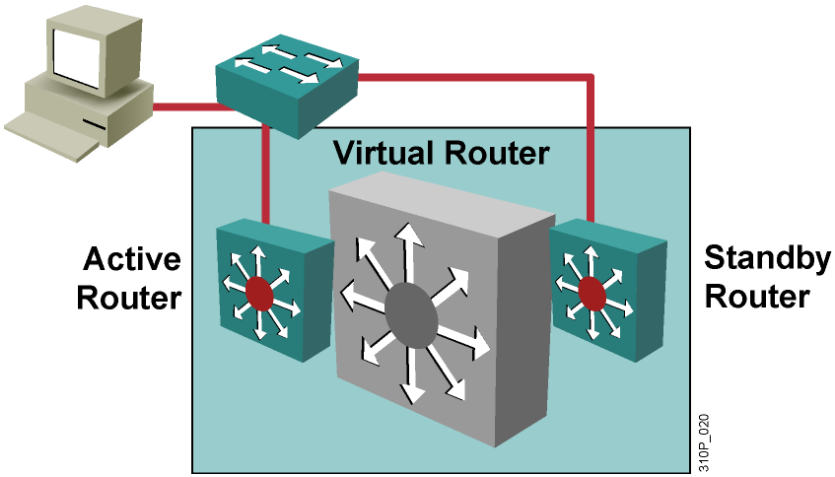



```
1d23h: SB1:Vlan10 Hello out 172.16.10.169 Active pri 100 hel 3 hol 10 ip 172.16 .10.110
```

310P_034

Les commandes de configuration

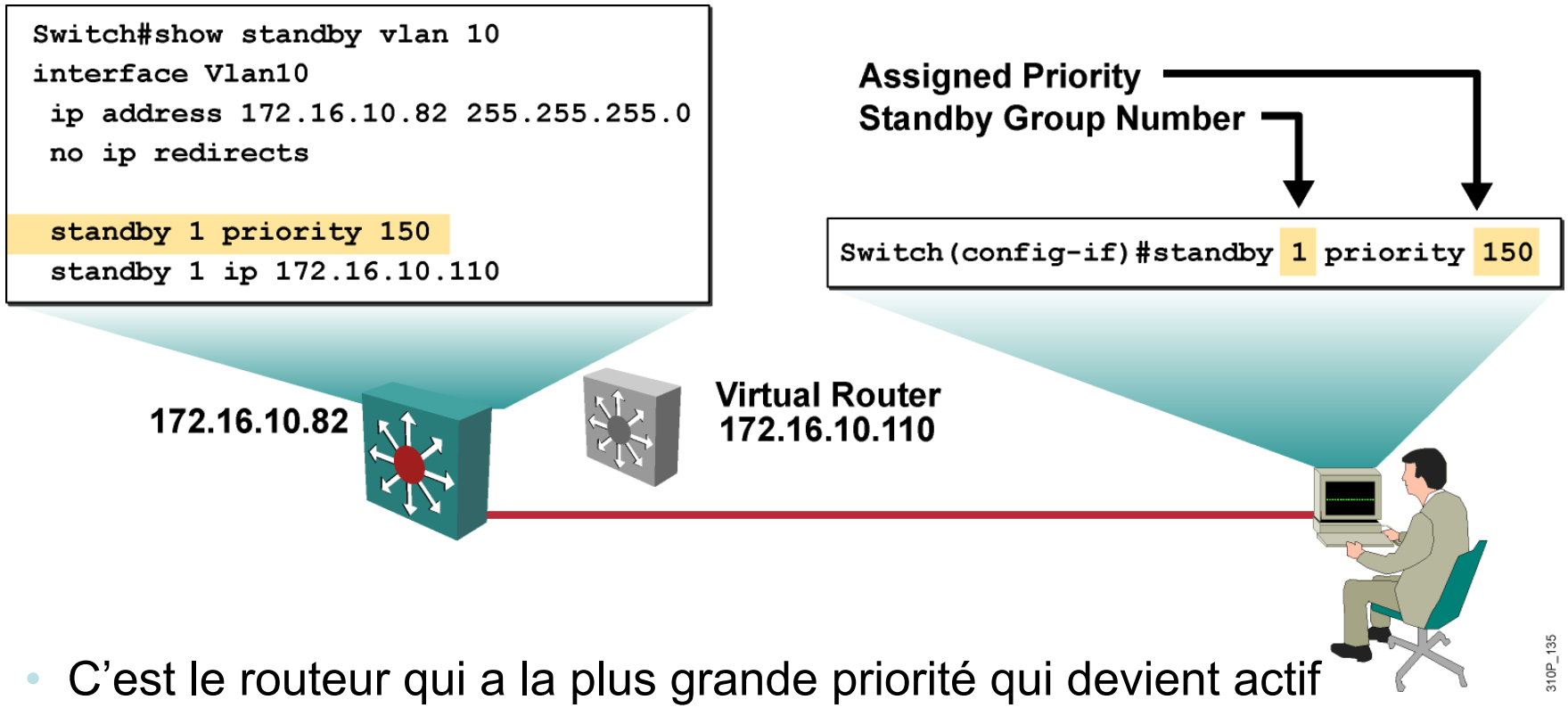
- Configuration
  (config-if)# standby 1 ip 172.16.10.110



- Verification
  - show running-config
  - show standby

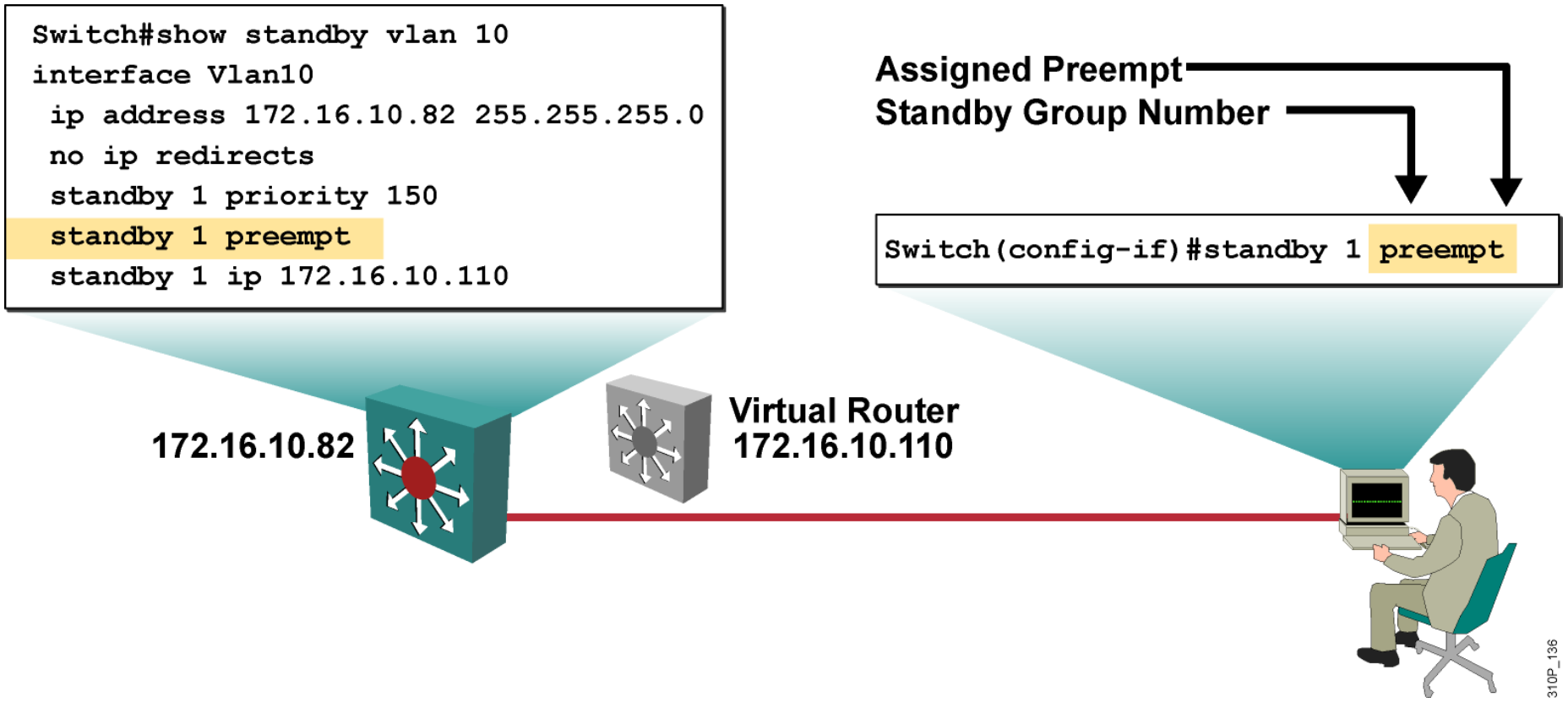
```
Switch#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Vl11        10  110    Active   local           172.16.10.169   172.16.10.110
```

Configuration des priorités HSRP



- C’est le routeur qui a la plus grande priorité qui devient actif
- La priorité par défaut est 100
- En cas d’égalité, c’est le routeur avec la plus grande adresse IP qui devient actif.

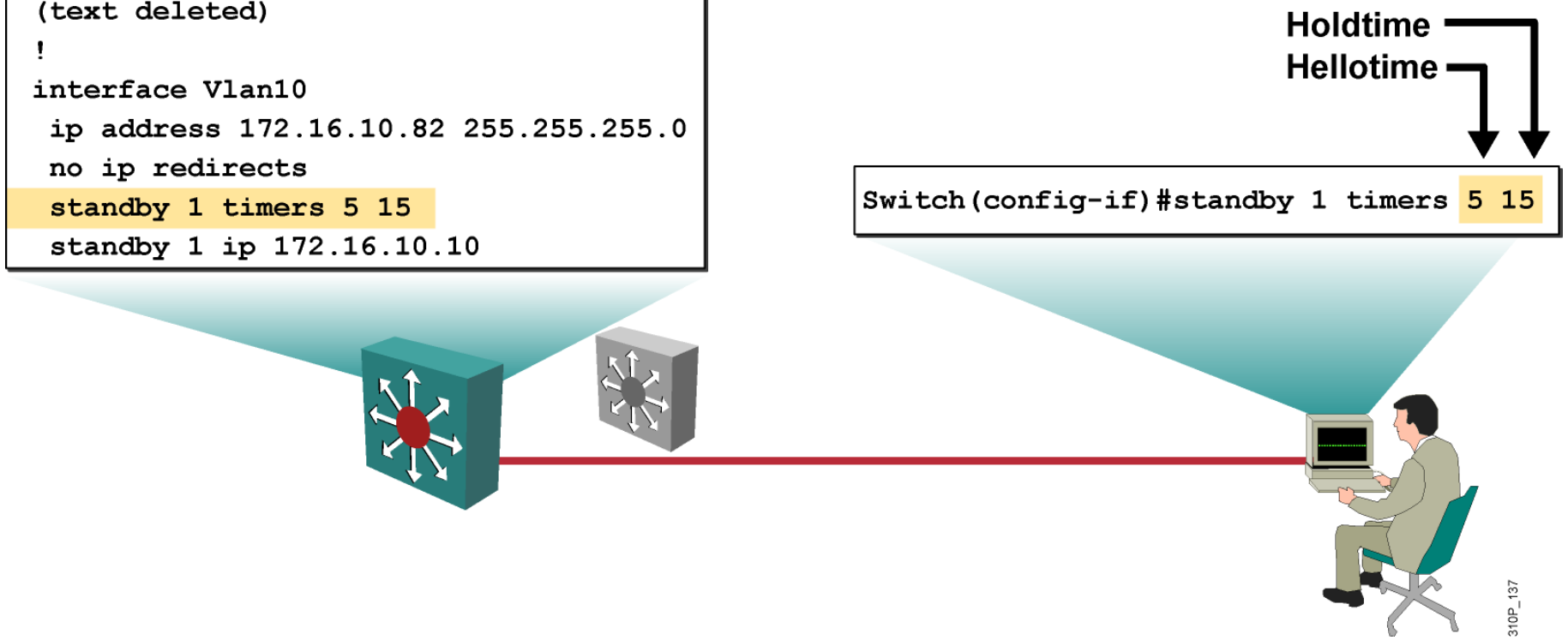
Configuration HSRP de la préemption



La préemption permet au routeur actif de reprendre la main lorsqu'il reprend du service

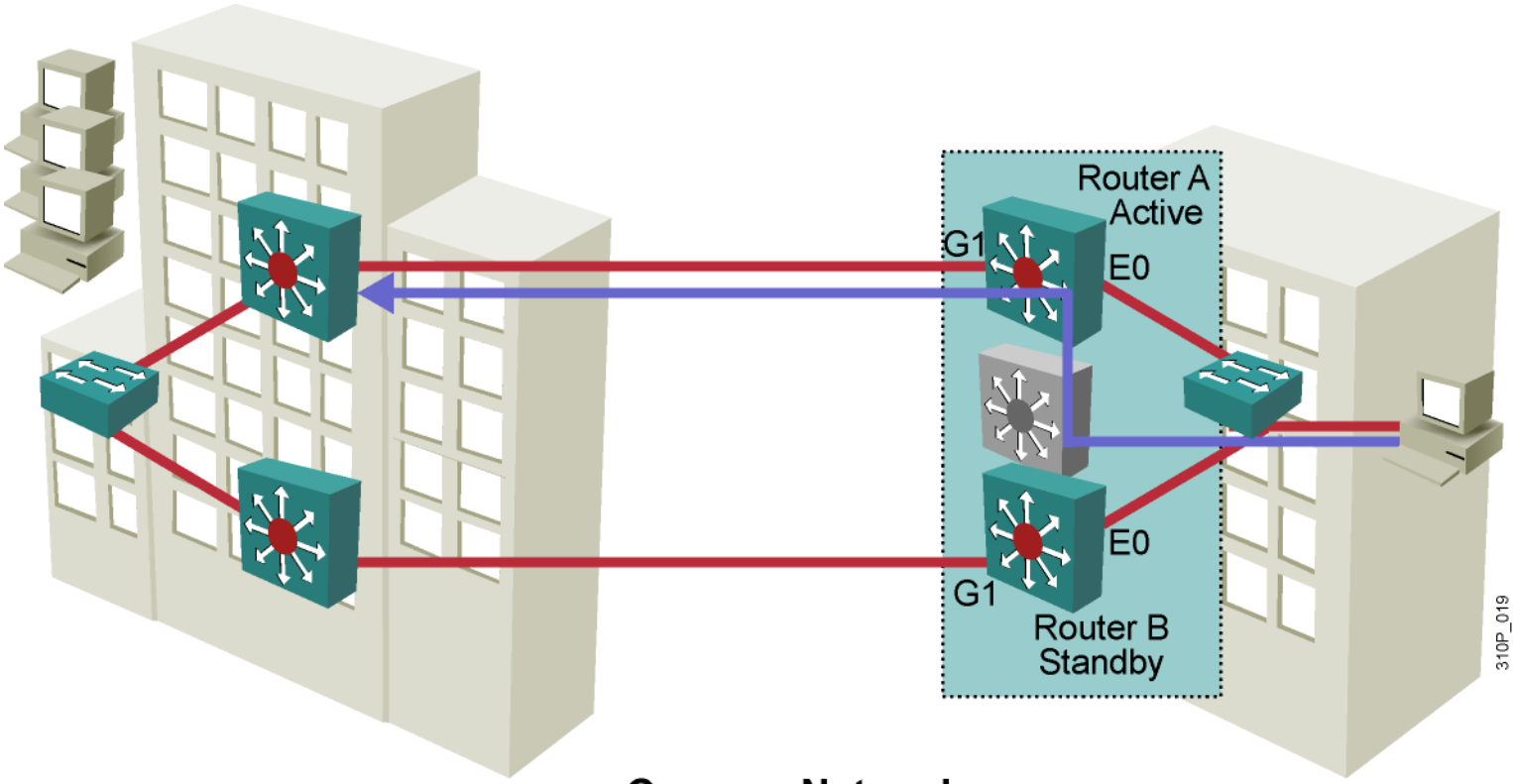
Configuration des Timers

```
Building configuration...

Current configuration:
(text deleted)
!
interface Vlan10
 ip address 172.16.10.82 255.255.255.0
 no ip redirects
 standby 1 timers 5 15
 standby 1 ip 172.16.10.10
```



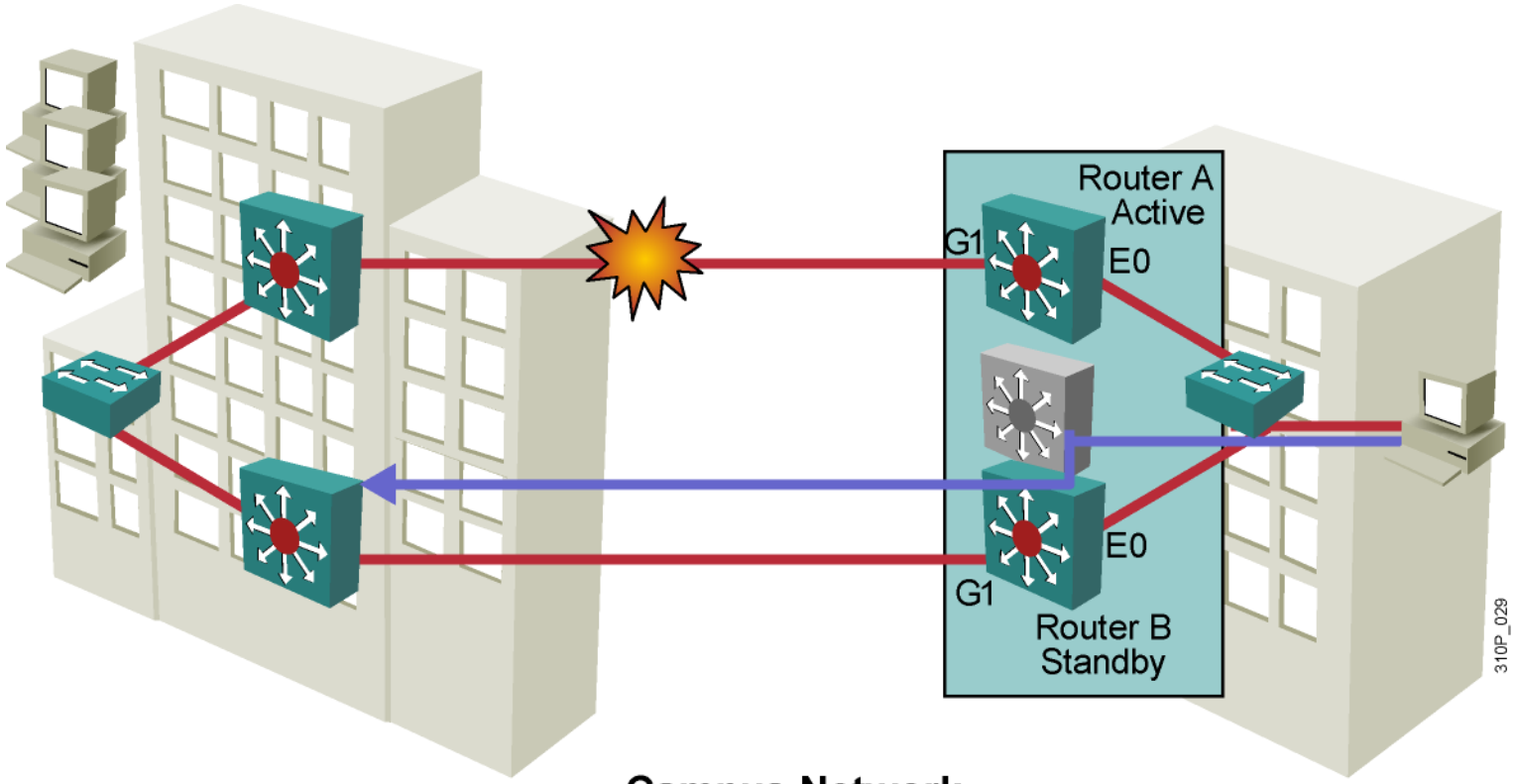
Le Holdtime doit être supérieur à 3 fois le Hello

Supervision du lien



Campus Network

Un lien tombe et le trafic bascule



Campus Network

Configuration de la supervision

```
Switch(config-if)#standby [group-number] track type number
[interface-priority]
```

- Configuration de la supervision

```
Switch(config)#interface vlan 10
Switch(config-if)#standby 1 track GigabitEthernet 0/7 50
Switch(config-if)#standby 1 track GigabitEthernet 0/8 60
```

- Example de configuration

Note: la préemption doit être configurée sur tous les membres d'un groupe

IP v6

L'adresse IPv6

Rappel sur IPv4:

- Longueur : 4 octets
- Exprimée en : Décimal
- Exemple : 192.168.10.1
- Masque : 4 octets, en décimal, 255.255.255.0

IPv6 :

- Longueur : **16** octets
- Exprimée en : **Hexadécimal**
- Exemple : 1111:2222:3333:4444:5555:6666:7777:FFFF
- Masque : 16 octets, exprimé en /X, exemple : **/64**
- **Plusieurs** adresses IPv6 sur une **même** interface

Règles de simplification

- Toute suite de 0000 peut être remplacée par **::**
  - :0000: ::
  - :0000:0000: ::
  - :0000:0000:0000 ::
- Ce remplacement ne peut être effectué **qu'une seule** fois.
- Les 0 en **début** de section peuvent être supprimés.
  - :0001: :1:
  - :0123: :123:
- Les 0 en **fin** de section ne peuvent pas être supprimés.
  - :1000: :1000:
  - :1100: :1100:

Simplifier une adresse

Adresse initiale	0011:	2020 :	0000:	0000:	00aa:	0000:	3330:	2000
OK	0011:	2020 :		:	00aa:	0000:	3330:	2000
OK	0011:	2020:	0000:	0000:	00aa :	:	3330:	2000
KO	0011:	2020 :		:	00aa :	:	3330:	2000
OK	11:	2020:	0000:	0000:	aa:	0000:	3330:	2000
KO	0011:	202 :	0000:	0000:	00aa:	0000:	333 :	2
Adresse finale	11:	2020:		:	aa:	0 :	3330:	2000

Catégories de paquets

Rappel sur IPv4:

- Unicast
- Multicast
  - classe D : 224.0.0.0 à 239.255.255.255
- Broadcast

IPv6 :

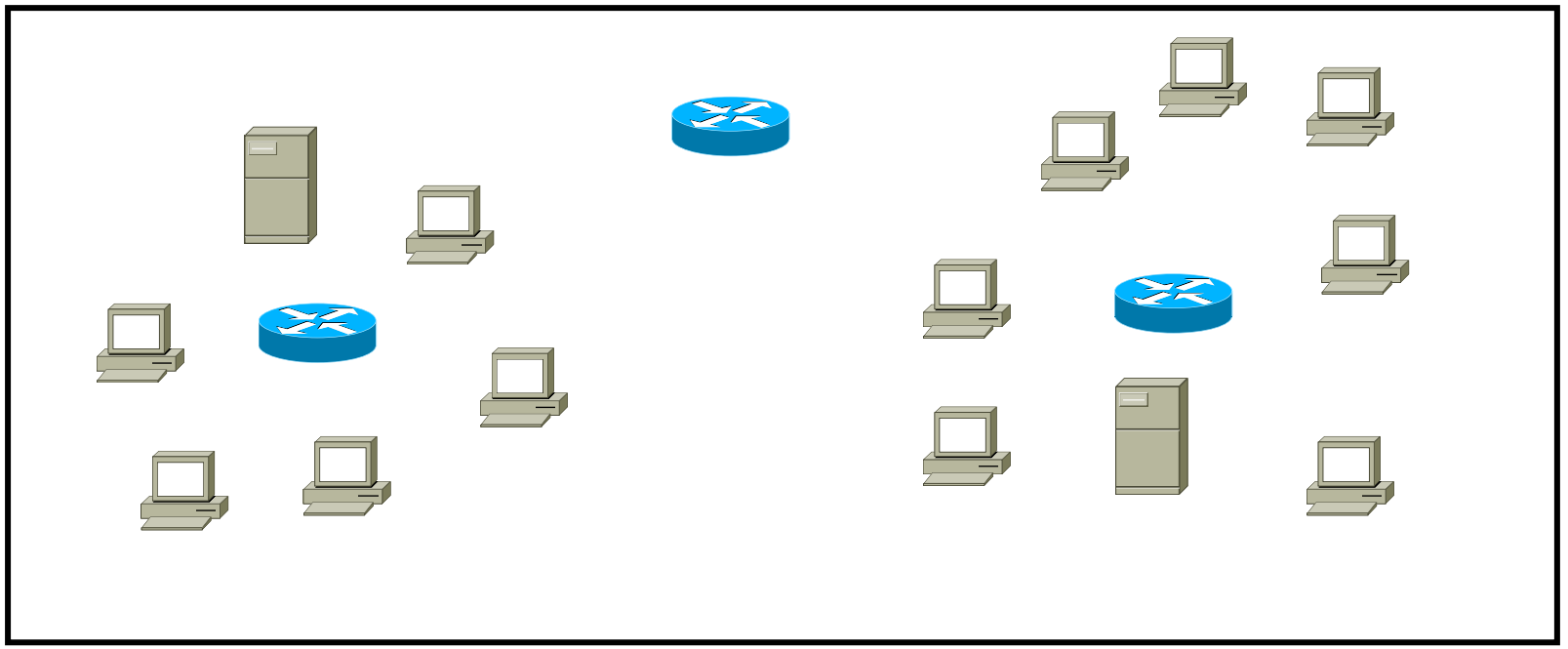
- Unicast
- Multicast
  - FF00::/8
- Anycast
  - « One-to-nearest »

Exemples multicast IPv6

Adresse IPv4	Adresse IPv6	Signification
224.0.0.1	FF02::1	Tous les hosts
224.0.0.2	FF02::2	Tous les routeurs
224.0.0.5 et 6	FF02::5 et 6	Tous les routeurs OSPF
224.0.0.9	FF02::9	Tous les routeurs RIP
224.0.0.10	FF02::A	Tous les routeurs EIGRP

Anycast

- La même adresse IPv6 configurée sur 2 équipements distincts.
- Modèle de communication « one-to-nearest ».



Plages réservées

Rappel sur IPv4:

- Privées = site local:
  - Classe A : 10.0.0.0/8
  - Classe B : 172.16.0.0. à 172.31.0.0 /16
  - Classe C : 192.168.0.0 à 192.168.255.0 /24
- Publiques
- 127.0.0.1 = adresse de loopback

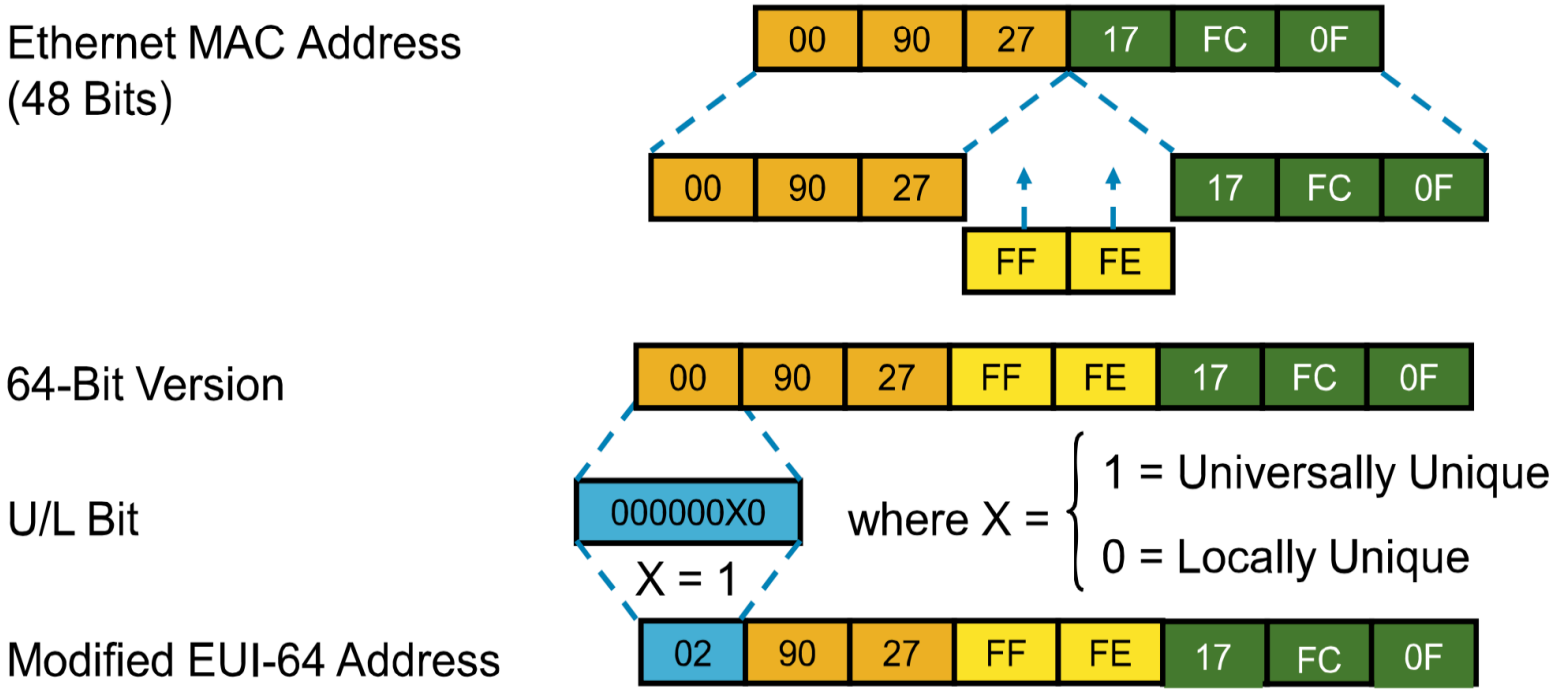
IPv6 :

- Privées :
  - Link local = FE80::/10
  - Unique Local Address = FC::0/7
- Publiques = uniques globalement :
  - 2000::/3 =001x xxxx xxxx xxxx ::
- ::1 = adresse de loopback
- :: = adresse non spécifiée (par exemple source de paquet DHCPv6)

IPv6 Unicast Addresses

Address	Value	Description
Global	2000::/3	Assigned by the IANA and used on public networks. They are equivalent to IPv4 global (public) addresses. ISPs summarize these to provide scalability on the Internet.
Unique-Local	FC00::/7	Unique local unicast addresses are analogous to private IPv4 addresses in that they are used for local communications. The scope is entire site or organization.
Link-local	FE80::/10—FEB0::/10	An automatically configured IPv6 address on an interface, the scope is only on the physical link. The first two digits are FE, and the third digit can range from 8 to B.
Reserved	(range)	Used for specific types of anycast and also for future use. Currently, about 1/256 of the IPv6 address space is reserved.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:0:1, or ::1, is used for local testing functions. Unlike IPv4, which dedicates a complete A class block of addresses for local testing, IPv6 uses only one.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this address is represented by 0:0:0:0:0:0:0:0, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

Le format EUI-64



Exemple EUI-64

Avec une Mac address **1111.2222.3333 :**

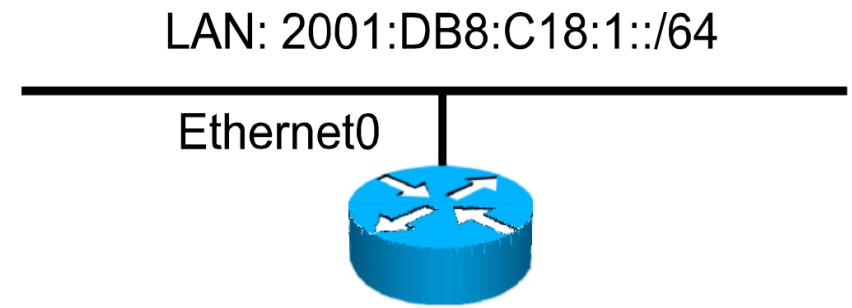
1111.22 est l'OUI = Organizational Unique Identifier

22.3333 est le numéro de série

Adresse réseau	2001							
Adresse MAC					**1111:**	**22**	**22:**	**3333**
Adresse eui-64					**1311:**	**22FF:**	**FE22:**	**3333**
Adresse réseau	2001				**1311:**	**22FF:**	**FE22:**	**3333**

- `int fa0/0`
- `ipv6 address 2001:: /64 eui-64`
- `show ipv6 address`
  - **2001::1311:22FF:FE22:3333/64**

Exemple de configuration



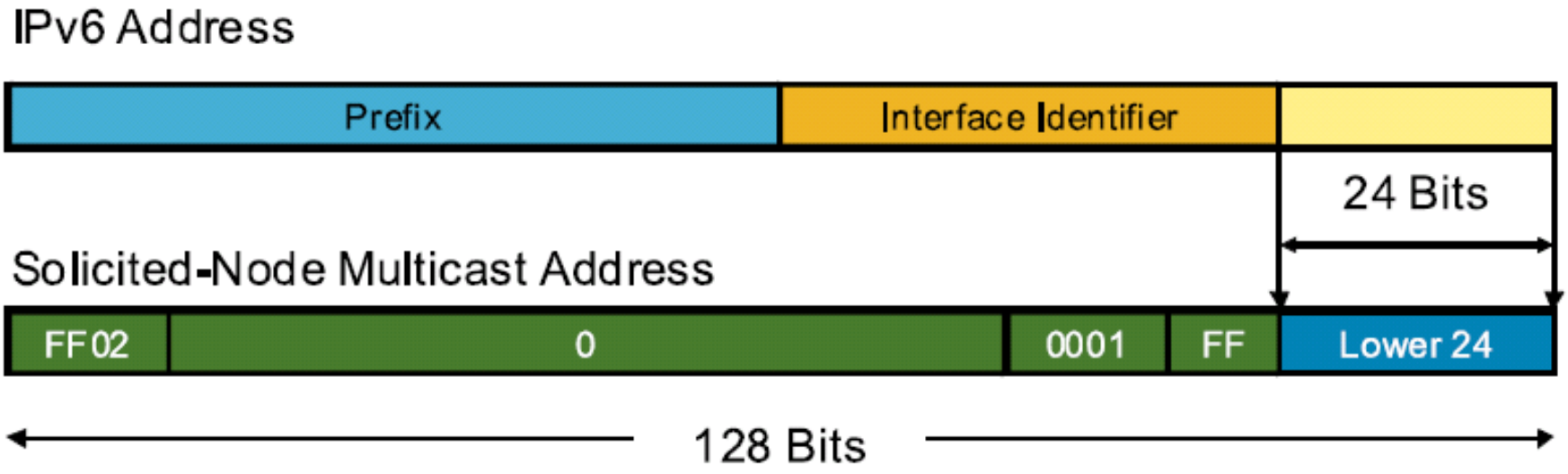

```
ipv6 unicast-routing
interface Ethernet0
 ipv6 address 2001:db8:c18:1::/64 eui-64
```

MAC Address: 0060.3E47.1530

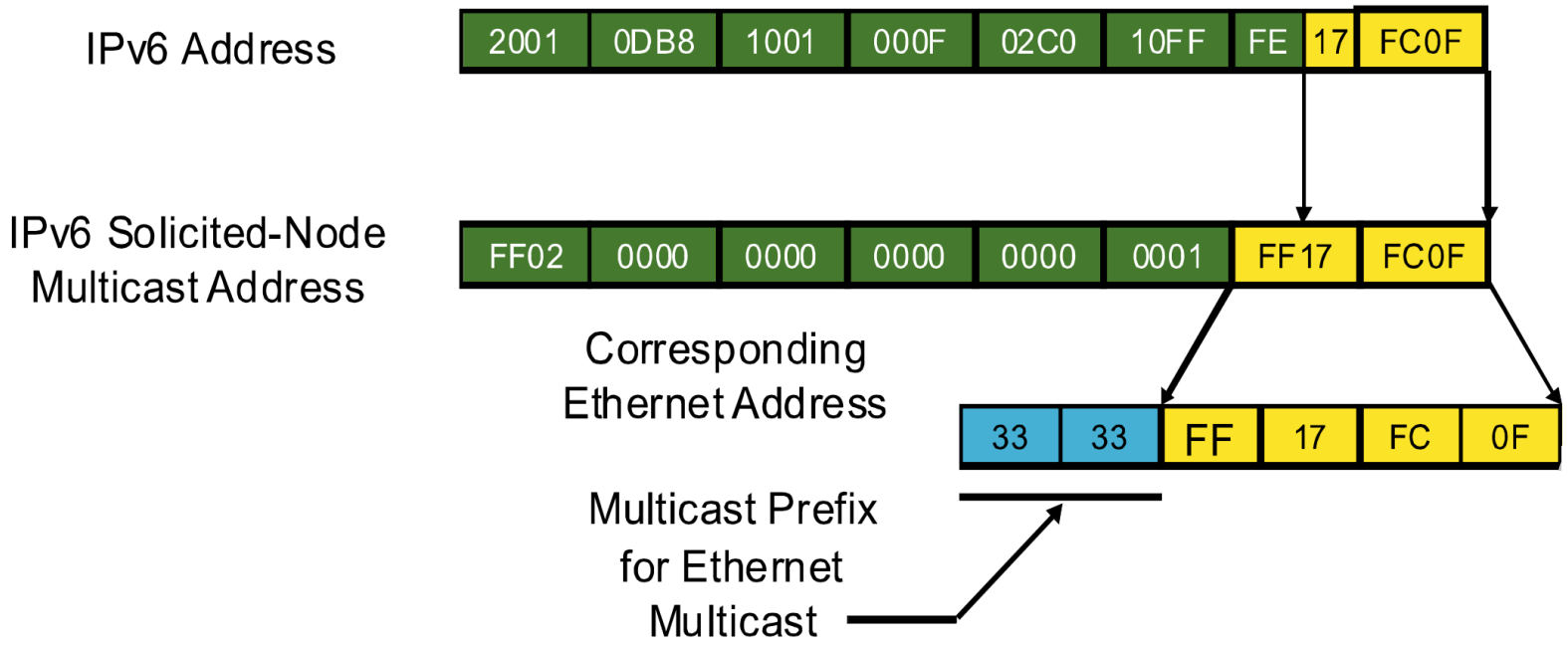
```
router# show ipv6 interface Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
    2001:DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:DB8:C18:1::/64
  Joined group address(es):
    FF02::1:FF47:1530
    FF02::1
    FF02::2
  MTU is 1500 bytes
```

Solicited Node Multicast Address

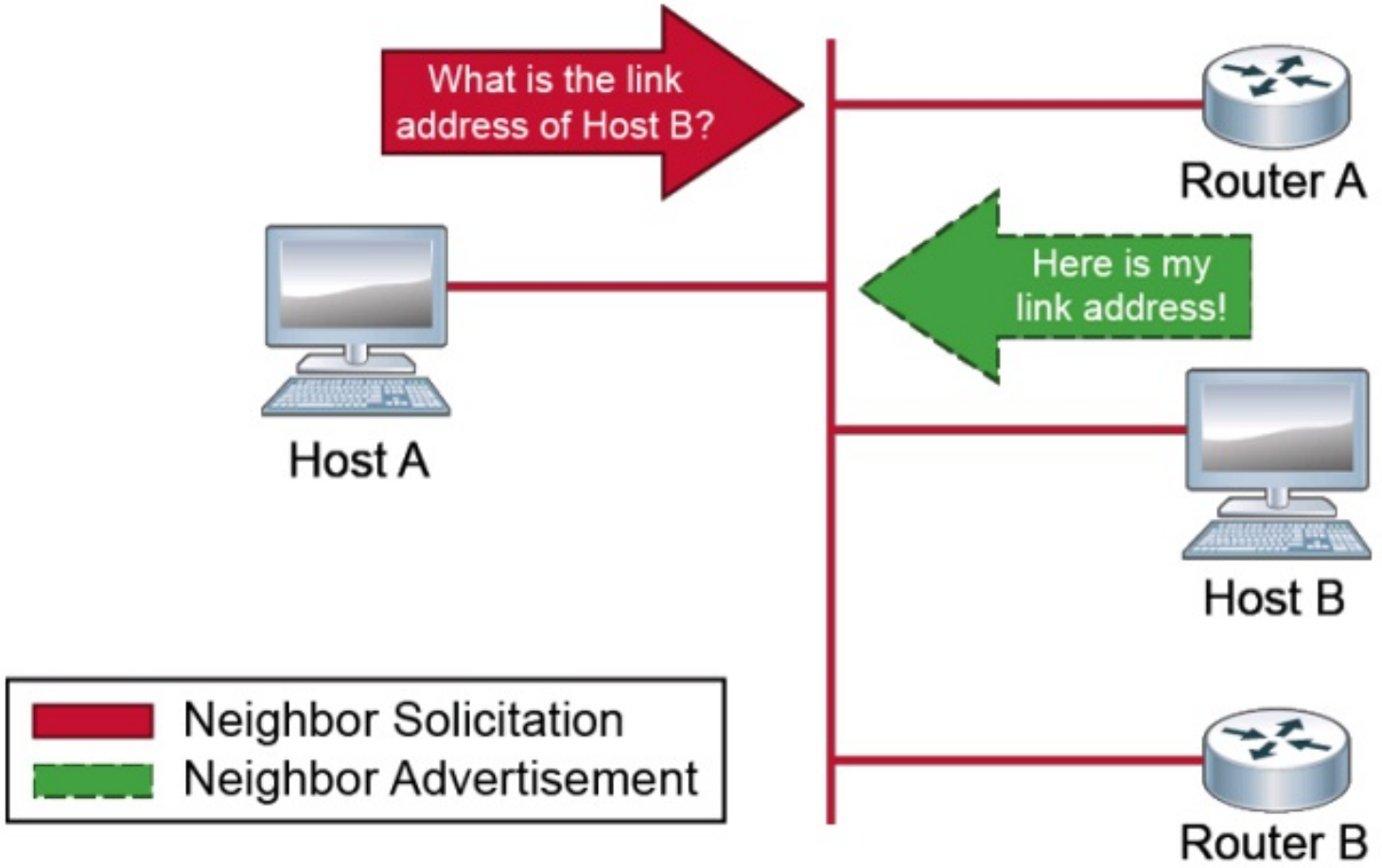
- A chaque adresse unicast correspond une adresse dite SNMA.
- L'équipement doit joindre les groupes multicast correspondant à chacune de ses SNMA
  - « écouter ces paquets »



Exemple SNMA



Neighbor Discovery



Neighbor discovery performs the same functions in IPv6 as ARP does in IPv4.

Corrélation couches 2 et 3

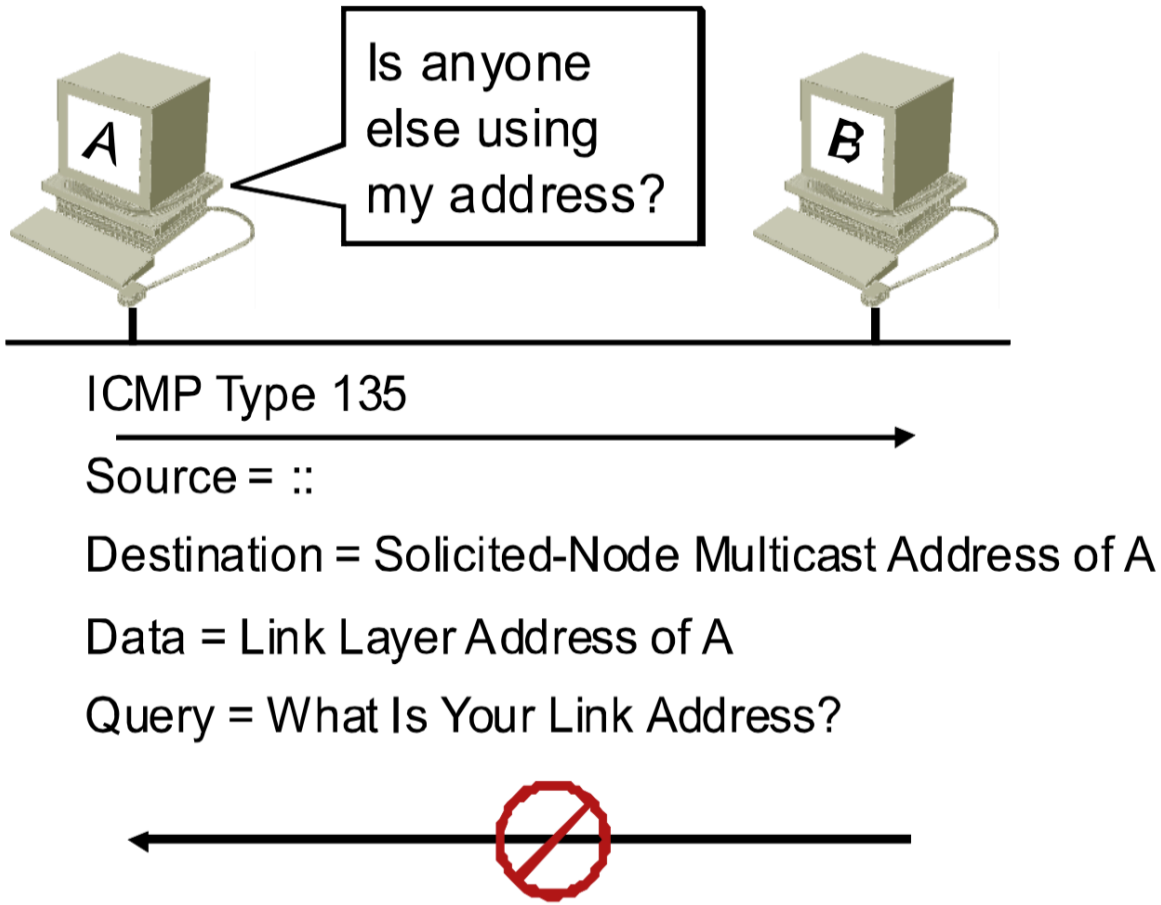
- IPv4:
  - **ARP**, Adress Resolution Protocol
- IPv6:
  - **NDP**, Neighbor Discovery Protocol
    - deux paquets ICMPv6:
      - **NS, Neighbor Sollicitation** = paquet ICMPv6 type 135
        - » multicast vers *Solicited Node Multicast Address*
      - **NA, Neighbor Advertisement** = paquet ICMPv6 type 136
        - » unicast
    - mécanisme **DAD, Duplicate Address Detection**

Exemple NS & NA

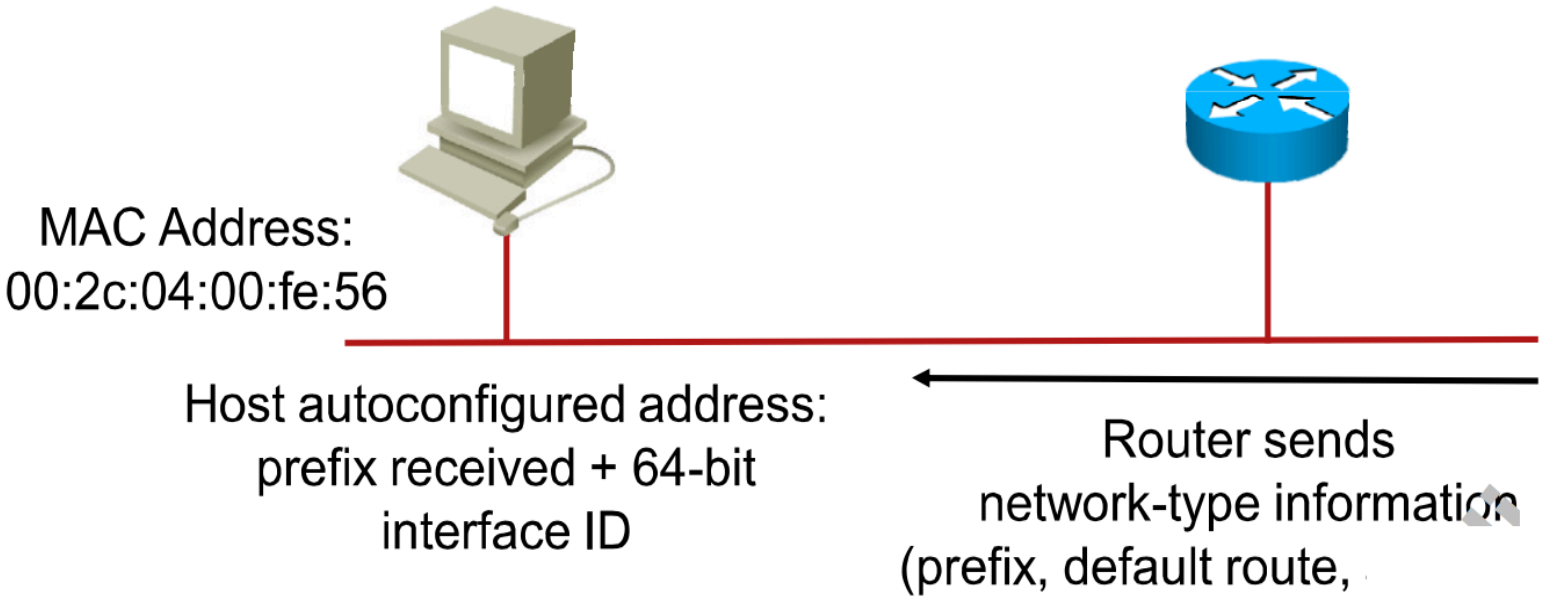
ICMP Type = 135
Src = A
Dst = Solicited-node Multicast of B
Data = Link Layer Address of A
Query = What Is Your Link Address?

ICMP Type = 136
Src = B
Dst = A
Data = Link Layer Address of B

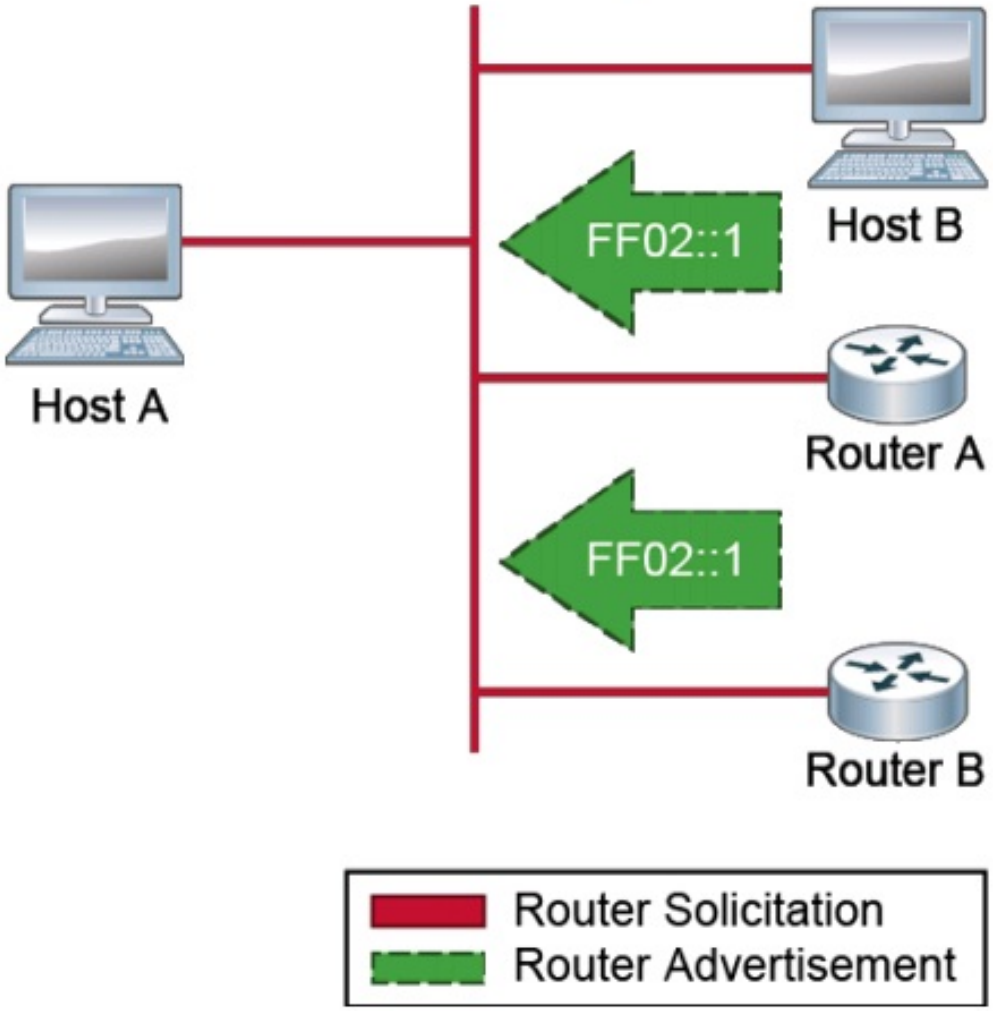
Duplicate Address Detection



Stateless auto-configuration



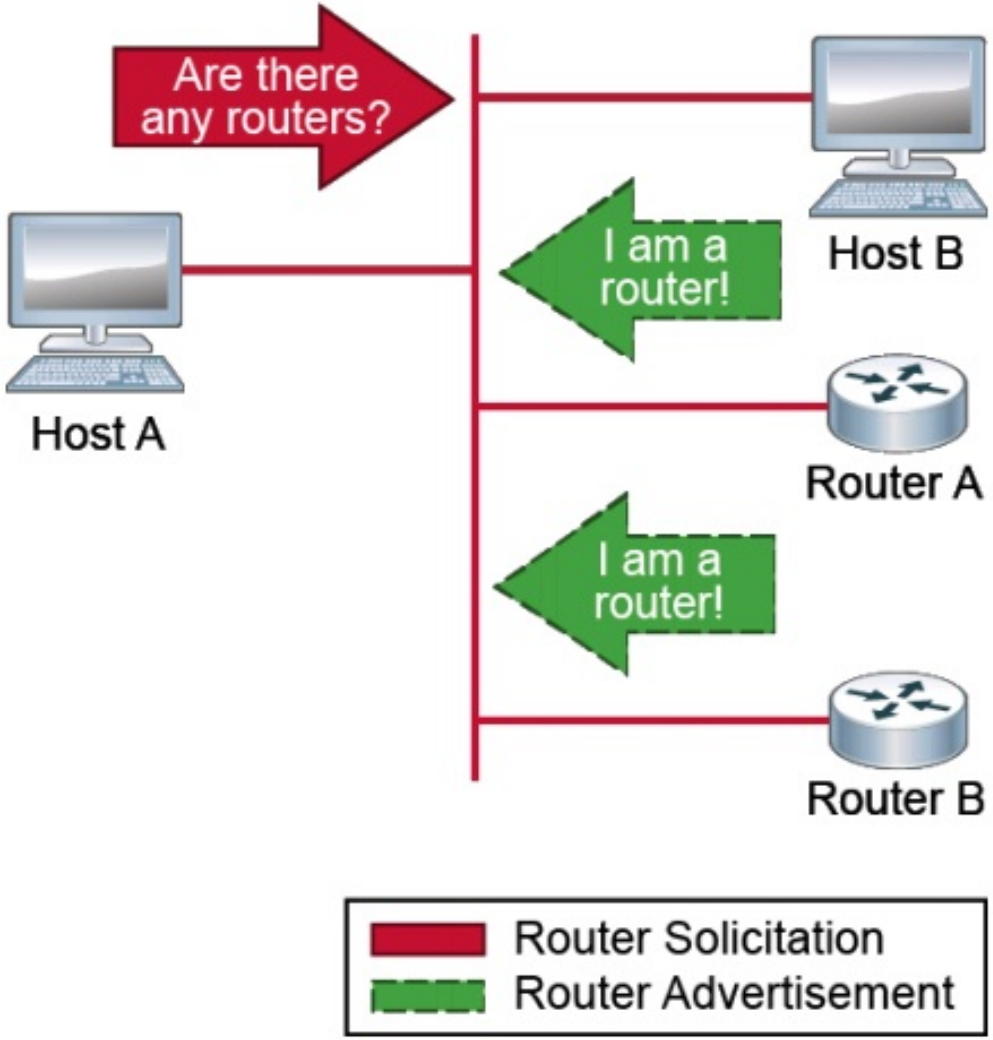
Stateless Autoconfiguration



The router advertisement packet:

- **ICMP type:** 134
- **Source:** Router link-local address
- **Destination:** FF02::1 (all-nodes multicast address)
- **Data:** Options, prefix, lifetime, autoconfiguration flag

Stateless Autoconfiguration (Cont.)



The router solicitation packet:

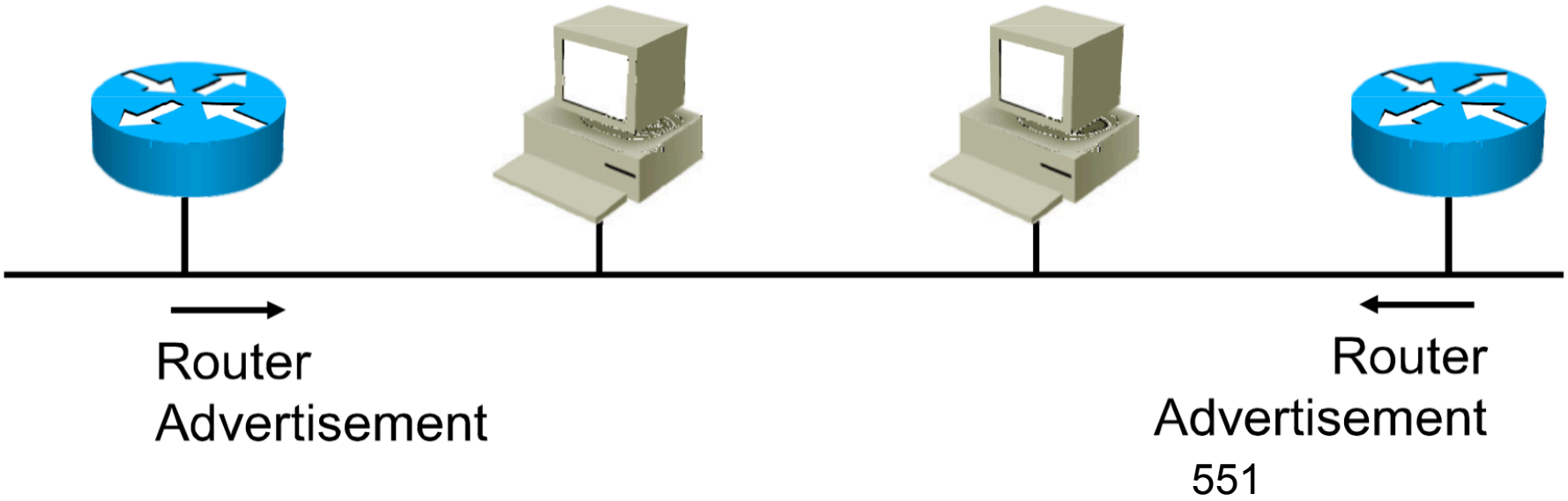
- **ICMP type:** 133
- **Source:** Unspecified address (::)
- **Destination:** FF02::2 (all-routers multicast address)

NDP RS & RA

- **NDP**, Neighbor Discovery Protocol
  - deux paquets ICMPv6:
    - **RS, Router Sollicitation** = paquet ICMPv6 type 133
      - multicast vers FF02::2
      - demande aux routeurs d'envoyer un RA
      - ne peut être envoyé que 3 fois, au boot
    - **RA, Router Advertisement** = paquet ICMPv6 type 134
      - multicast vers FF02::1 (unicast si en réponse à un RS)
      - **Prefix information =** les sous-réseaux disponibles sur le lien
      - **Gateway**

Exemple RA

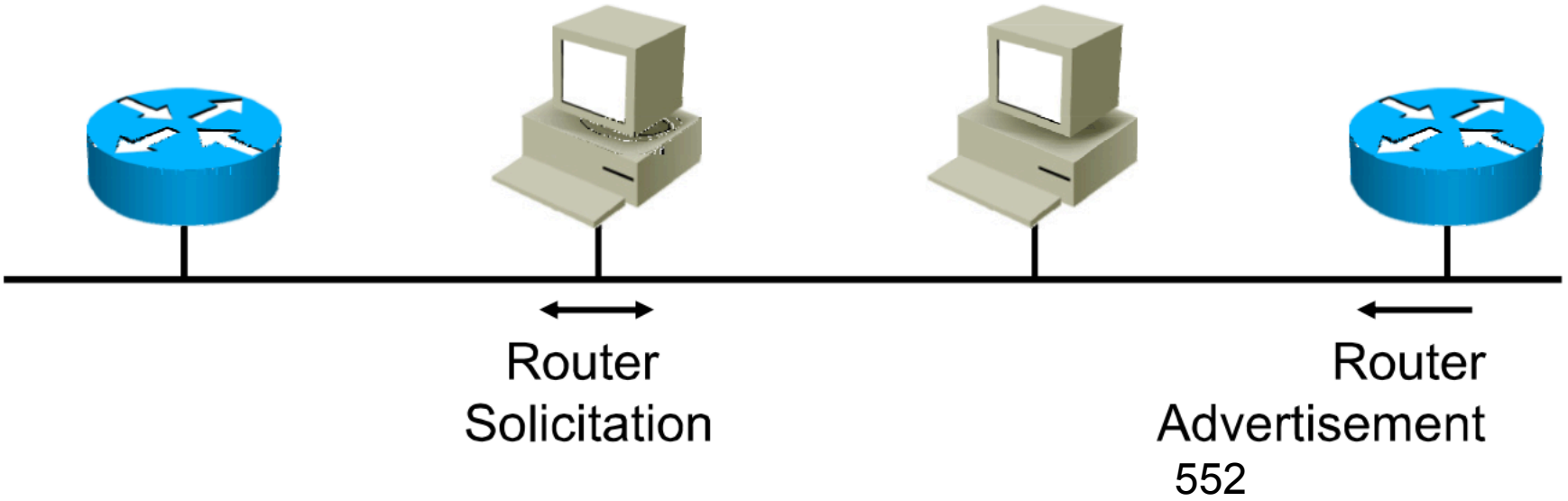
- ICMPv6 type 134
  - Adresse source = Link-local du routeur
  - Adresse destination = FF02::1 (tous les nœuds)
  - Data = Prefix, gateway, lifetime, flags



551

Exemple RS

- ICMPv6 type 133
  - Adresse source = ::
  - Adresse destination = FF02::2 (tous les routeurs)



552

Bilan des méthodes de config

link-local	statique		`ipv6 address FE80::1 link-local`
	eui 64		*[automatique]*
routable	statique		`ipv6 address 2001:abcd::1/64` `ipv6 unnumbered Loopback0`
	eui 64		`ipv6 address 2001:abcd::/64 eui-64`
	dyna-mique	auto-config	`ipv6 address autoconfig`
		DHCPv6	`ipv6 address dhcp`

Entête IPv6

- Simplifié
  - moitié des champs IPv4 supprimés
  - consomme moins de ressources pour processer
  - amélioré les performances et l'efficacité du routage
- Aligné sur 64 bits (IPv4 sur 32 bits)
  - meilleur processing en hardware
- Plus de Checksum:
  - le routage n'a plus besoin de recalculer
  - détection d'erreur au niveaux 2 et 4

Subnetting

Seconde partie

Le subnetting :

1. **L’adresse IP et son masque**
2. **Les adresses réservées**
3. **Les classes**
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

Définition des 5 classes d'adresses IP

Classe	Définition en binaire			
A	0xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
B	10xxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
C	110xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
D	1110xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
E	1111xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Définition des 5 classes d'adresses IP

Classe	Définition en décimal			
A	0 à 127	xxxxxxxx	xxxxxxxx	xxxxxxxx
B	128 à 191	xxxxxxxx	xxxxxxxx	xxxxxxxx
C	192 à 223	xxxxxxxx	xxxxxxxx	xxxxxxxx
D	224 à 239	xxxxxxxx	xxxxxxxx	xxxxxxxx
E	240 à 255	xxxxxxxx	xxxxxxxx	xxxxxxxx

Explications

classe	128	64	32	16	8	4	2	1		décimal
A	0	0	0	0	0	0	0	1	=	1
A	0	0	1	1	1	1	1	1	=	63
A	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**=**	**127**
B	1	0	0	0	0	0	0	0	=	128
B	1	0	0	0	0	0	0	1	=	129
B	1	0	1	1	1	1	1	0	=	190
B	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**=**	**191**
C	1	1	0	0	0	0	0	0	=	192
C	1	1	0	0	0	0	0	1	=	193
C	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**=**	**223**
D	1	1	1	0	0	0	0	0	=	224
D	1	1	1	0	1	1	1	1	=	239

Masque des 5 classes

Classe	Masque			
A	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
B	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
C	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
D	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
E	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX

Masque des 3 classes

Classe	Masque	
A	/8	255.0.0.0
B	/16	255.255.0.0
C	/24	255.255.255.0
D	Multicast	
E	Recherche	

Adresses privées de chaque classe

A	10.0.0.0
B	172.16.0.0 à 172.31.0.0
C	192.168.0.0 à 192.168.255.0

Le subnetting :

1. L’adresse IP et son masque
2. Les adresses réservées
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

Pour les réseaux de Classe C

- Regardons la longueur du masque :
  - Masque : 255.255.255.0 i.e. /24
  - Nombre de bits pour la partie hôte = 8
- Exemple : 200.10.20.0
  - Adresse réseau : 200.10.20.0
  - Première adresse disponible : 200.10.20.1
  - Dernière adresse disponible : 200.10.20.254
  - Adresse broadcast : 200.10.20.255
  - **Nombre d'adresses disponibles : 254**
    - **254 = 256 - 2 = 2^8 - 2**

La Classe B

- Regardons la longueur du masque :
  - Masque : 255.255.0.0 i.e. /16
  - Nombre de bits pour la partie hôte = 16
- Exemple : 151.1.0.0
  - Adresse réseau : 151.1.0.0
  - Première adresse disponible : 151.1.0.1
  - Dernière adresse disponible : 151.1.255.254
  - Adresse broadcast : 151.1.255.255
  - **Nombre d'adresses disponibles : 65 534**
    - **(256 x 256) - 2 = 65 534 = 2^{16} - 2**

La Classe A

- Propriétés :
  - Masque : 255.0.0.0 i.e. /8
  - Nombre de bits pour la partie hôte = 24
- Exemple : 5.0.0.0
  - Adresse réseau : 5.0.0.0
  - Première adresse disponible : 5.0.0.1
  - Dernière adresse disponible : 5.255.255.254
  - Adresse broadcast : 5.255.255.255
  - **Nombre d'adresses disponibles** : 16 777 216
    - **(256 x 256 x 256) - 2 = 2^{24} - 2**

Exercice

Adresse	Classe	Adresse réseau	1ère adresse disponible	Dernière adresse disponible	Adresse broadcast
2.2.2.2					
200.2.2.2					
222.2.2.2					
182.2.2.2					
191.1.1.1					

Solution

Adresse	Classe	Adresse réseau	1ère adresse disponible	Dernière adresse disponible	Adresse broadcast
2.2.2.2	A	2.0.0.0	2.0.0.1	2.255.255.254	2.255.255.255
200.2.2.2	C	200.2.2.0	200.2.2.1	200.2.2.254	200.2.2.255
222.2.2.2	C	222.2.2.0	222.2.2.1	222.2.2.254	222.2.2.255
182.2.2.2	B	182.2.0.0	182.2.0.1	182.2.255.254	182.2.255.255
191.1.1.1	B	191.1.0.0	191.1.0.1	191.1.255.254	191.1.255.255

Tableau récapitulatif

Masque	Nombre de bits dans la partie réseau	Nombre de bits dans la partie hôte	Nombre de combinaisons possibles	Nombre d'@ interdites	**Nombres d'@ disponibles**
/8	8	24	2^{24}	2	**$2^{24}-2$**
/16	16	16	2^{16}	2	**$2^{16}-2$**
/24	24	8	2^{8}	2	**$2^{8}-2$**

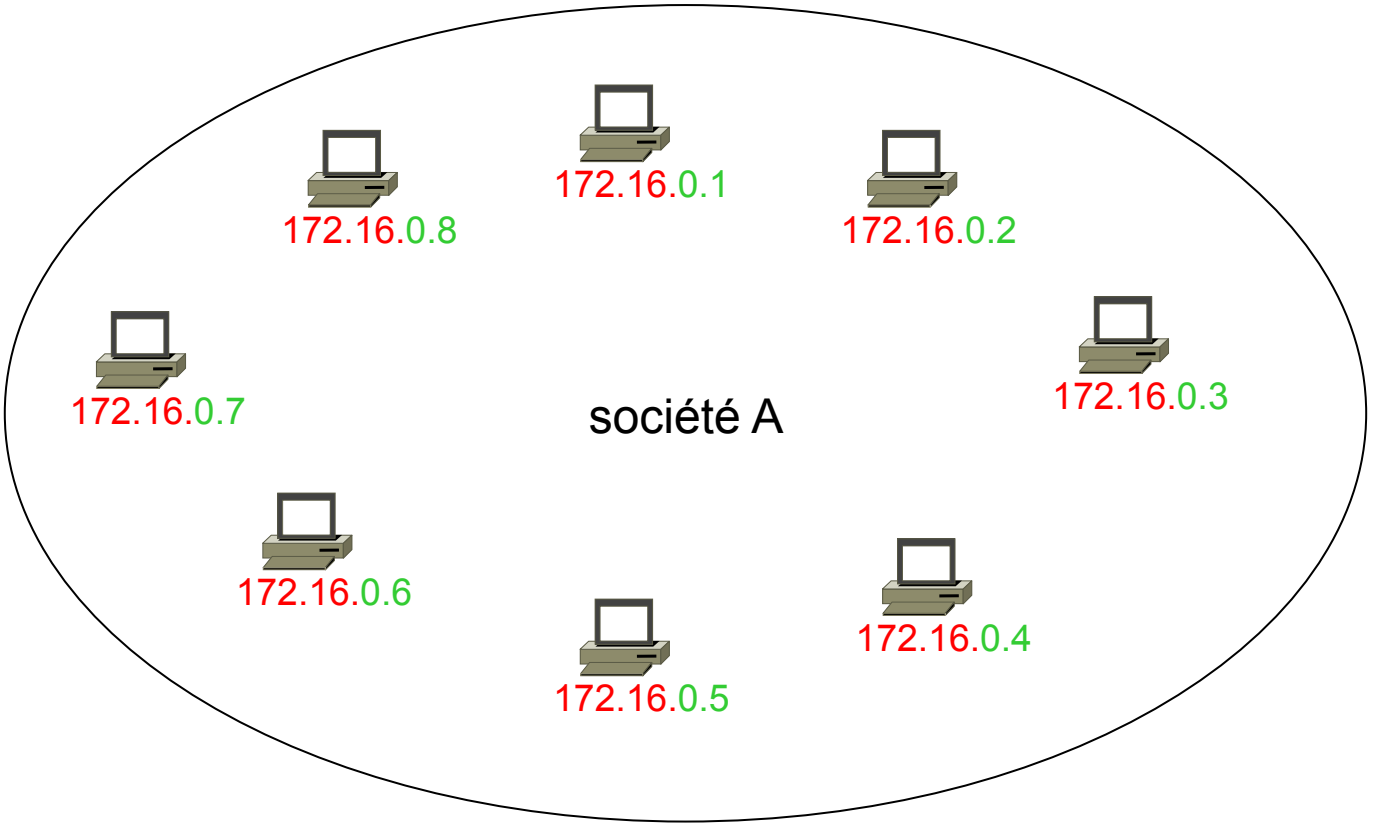
Identifier avec la « Largeur de bloc »

Masque		Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	2^8=256	254
/16	255.255.0.0	2^{16}=65 536	65 534
/8	255.0.0.0	2^{24}=16 777 218	16 777 216

Le subnetting :

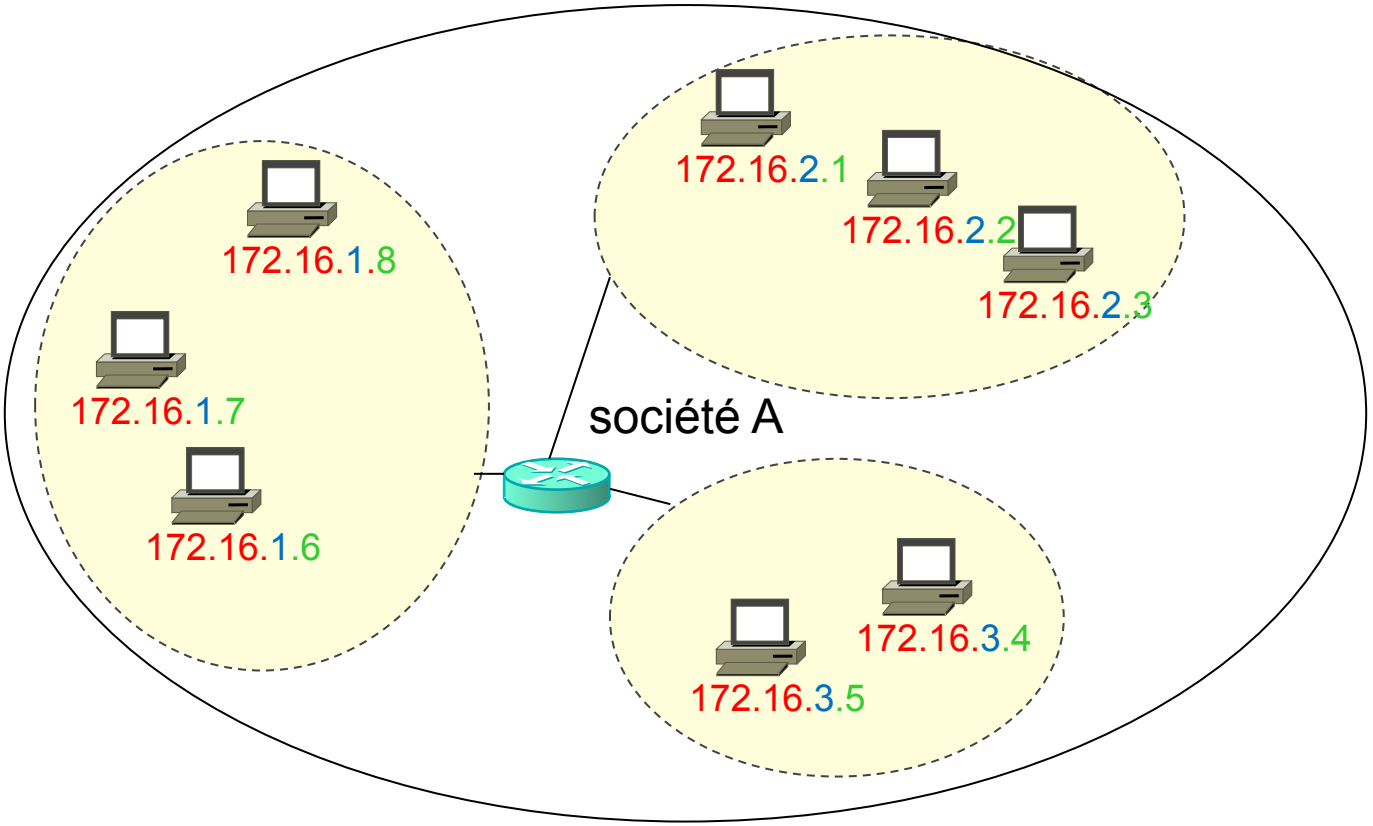
1. L’adresse IP et son masque
2. Les adresses réservées
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

Les broadcast sans sous-réseau



- Avec le masque de la classe /16 :
  - Les broadcast sont diffusés sur tout le réseau 172.16.0.0/16.
  - Ils innondent le réseau.

Les broadcast avec sous-réseau



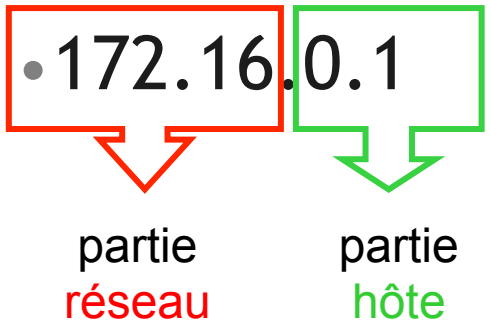
- Avec un masque de sous-réseau en /24 :
  - Les broadcast sont confinés dans chaque sous-réseau.

Créer un sous-réseau

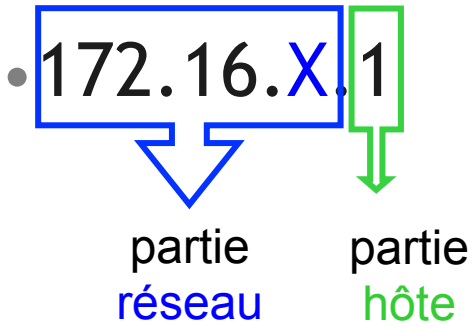
- Pour créer un sous-réseau :
  - on **allonge** la taille du masque initial
- Exemple :
  - masque initial : /16
  - masque final : /24
- En binaire :
  - masque initial : 11111111.11111111.00000000.00000000
  - masque final : 11111111.11111111.11111111.00000000

Le sous-réseau

- Avec le masque **initial** :



- Avec un masque **allongé** (plusieurs possibilités selon X) :



Avec le masque initial en /16

172.16.0.0	Adresse réseau
172.16.0.1	1ère adresse disponible
172.16.0.2	2ème adresse disponible
172.16.0.3	3ème adresse disponible
172.16.0.…	etc..
172.16.255.254	Dernière adresse disponible
172.16.255.255	Adresse de broadcast

Avec un masque rallongé en /24

172.16.0.0	Adresse réseau	1er sous-réseau
172.16.0.1	1ère adresse disponible	
172.16.0.2	2ème adresse disponible	
172.16.0.…	etc…	
172.16.0.254	Dernière adresse disponible	
172.16.0.255	Adresse de broadcast	
172.16.1.0	Adresse réseau	2ème sous-réseau
172.16.1.1	1ère adresse disponible	
172.16.1.2	2ème adresse disponible	
172.16.1.…	etc…	
172.16.1.254	Dernière adresse disponible	
172.16.1.255	Adresse de broadcast	
172.16.2.0	Adresse réseau	3ème sous-réseau
172.16.2.1	1ère adresse disponible	
172.16.2.2	2ème adresse disponible	
172.16.2.…	etc…	
172.16.2.254	Dernière adresse disponible	
172.16.2.255	Adresse de broadcast	

Combien de sous-réseaux créés ?

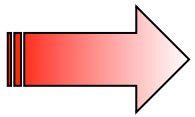
172.16.**0**.0	Adresse réseau	1er sous-réseau
172.16.**1**.0	Adresse réseau	2ème sous-réseau
172.16.**2**.0	Adresse réseau	3ème sous-réseau
172.16.**3**.0	Adresse réseau	4ème sous-réseau
172.16.**4**.0	Adresse réseau	5ème sous-réseau
172.16.**5**.0	Adresse réseau	6ème sous-réseau
172.16.**254**.0	Adresse réseau	255ème sous-réseau
172.16.**255**.0	Adresse réseau	256ème sous-réseau

Conclusion

- Lorsqu'on rallonge le masque de **8 bits :**
- Exemple :
  - de /16 = 11111111.11111111.00000000.00000000
  - à /24 = 11111111.11111111.11111111.00000000
- Nombre de sous-réseaux créés : 256 = 2^8
  - C'est le nombre de combinaisons possibles pour le 3ème octet

Le subnetting :

1. L’adresse IP et son masque
2. Les adresses réservées
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel



Subnetting sur octet entier ou partiel ?

- Sur un octet **entier** :
  - rallonger le masque de **8 ou 16 bits**
  - par exemple :
    - de /16 = 11111111.11111111.00000000.00000000
    - à /24 = 11111111.11111111.11111111.00000000
- Sur un octet **partiel** :
  - rallonger le masque de **1, 2, … 5 … X bits**
  - par exemple :
    - de /16 = 11111111.11111111.00000000.00000000
    - à /20 = 11111111.11111111.11110000.00000000

Rallonger de 1 bit

- Lorsqu'on rallonge le masque de **1 bit :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
  - à /25 = 11111111.11111111.11111111.10000000
- Nombre de sous-réseaux créés : $2^1 = 2$

Rallonger de 2 bits

- Lorsqu'on rallonge le masque de **2 bits :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
  - à /26 = 11111111.11111111.11111111.**11**000000
- Nombre de sous-réseaux créés : $2^2 = 4$

Rallonger de N bits

- Lorsqu'on rallonge le masque de **N bits :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
  - à /24+**N** = 11111111.11111111.11111111.**1...1**0...0

- Nombre de sous-réseaux créés : 2^{N}

Comment écrire le masque en décimal ?

- Exemple :
  - Le masque /24 = 11111111.11111111.11111111.00000000
    255 . 255 . 255 . 0
  - Le masque /25 = 11111111.11111111.11111111. 10000000
    255 . 255 . 255 . 128
  - Le masque /26 = 11111111.11111111.11111111. 11000000
    255 . 255 . 255 . 192

Rappel de conversion d'octet

128	64	32	16	8	4	2	1		en décimal
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Exercice 1 : écrivez le masque

255	255	255	0	=	/24
255	255	255	128	=	?
255	255	255	192	=	?
255	255	255	224	=	?
255	255	255	240	=	?
255	255	255	248	=	?
255	255	255	252	=	?
255	255	255	254	=	?
255	255	255	255	=	?

Solution 1

255	255	255	0	=	/24
255	255	255	128	=	/25
255	255	255	192	=	/26
255	255	255	224	=	/27
255	255	255	240	=	/28
255	255	255	248	=	/29
255	255	255	252	=	/30
255	255	255	254	=	/31
255	255	255	255	=	/32

Exercice 2 : écrivez le masque

255	255	?	?	=	/16
255	255	?	?	=	/17
255	255	?	?	=	/18
255	255	?	?	=	/19
255	255	?	?	=	/20
255	255	?	?	=	/21
255	255	?	?	=	/22
255	255	?	?	=	/23
255	255	?	?	=	/24

Solution 2

255	255	0	0	=	/16
255	255	128	0	=	/17
255	255	192	0	=	/18
255	255	224	0	=	/19
255	255	240	0	=	/20
255	255	248	0	=	/21
255	255	252	0	=	/22
255	255	254	0	=	/23
255	255	255	0	=	/24

Taille d'un réseau

- Lorsqu'on rallonge le masque de **1 bit :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
    - pour ce réseau initial :
    - nombre d'@ consommées = **256** = 2^8
    - nombre d'@ disponibles = **254** = 2^8 -2
  - à /25 = 11111111.11111111.11111111.10000000
    - pour chaque nouveau réseau :
    - nombre d'@ consommées = **128** = 2^7
    - nombre d'@ disponibles = **126** = 2^7 -2

Taille d'un réseau

- Lorsqu'on rallonge le masque de **2 bits :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
    - pour ce réseau initial :
    - nombre d'@ consommées = **256** = 2^8
    - nombre d'@ disponibles = **254** = 2^8 -2
  - à /26 = 11111111.11111111.11111111.11000000
    - pour chaque nouveau réseau :
    - nombre d'@ consommées = **64** = 2^6
    - nombre d'@ disponibles = **62** = 2^6 -2

Taille d'un réseau

- Lorsqu'on rallonge le masque de **N bits :**
- Exemple :
  - de /24 = 11111111.11111111.11111111.00000000
    - pour ce réseau initial :
    - nombre d'@ consommées = **256** = 2^8
    - nombre d'@ disponibles = **254** = 2^8 -2
  - à /24+N = 11111111.11111111.11111111.**1**...**1**0...00
    - pour chaque nouveau réseau :
    - nombre d'@ consommées = $2^{(8-\mathbf{N})}$
    - nombre d'@ disponibles = $2^{(8-\mathbf{N})}$ -2

Apprendre par coeur

	Masque	Largeur du bloc = @ consommées	Nombre d'hôtes = @ disponibles
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/26	255.255.255.192	2^6=64	62
/27	255.255.255.224	2^5=32	30
/28	255.255.255.240	2^4=16	14
/29	255.255.255.248	2^3=8	6
/30	255.255.255.252	2^2=4	2
/31	255.255.255.254	2^1=2	0

VLSM

- Variable Length Subnet Mask
- Tous les sous-réseaux n’ont pas le même masque.
- Exemple :
  - 192.168.0.0 /25 pour le VLAN A
  - 192.168.0.128 /26 pour le VLAN B
  - 192.168.0.192 /28 pour le VLAN C

Le plus petit sous-réseau

- Utilisé pour des réseaux point à point
  - exemple : WAN

- Masque en /30
  - Exemple : 10.1.1.0/30
    - Première adresse IP disponible : 10.1.1.1
    - Seconde adresse IP disponible : 10.1.1.2
    - Adresse broadcast : 10.1.1.3
  - Sous-réseau suivant : 10.1.1.4 /30

Exercice 1

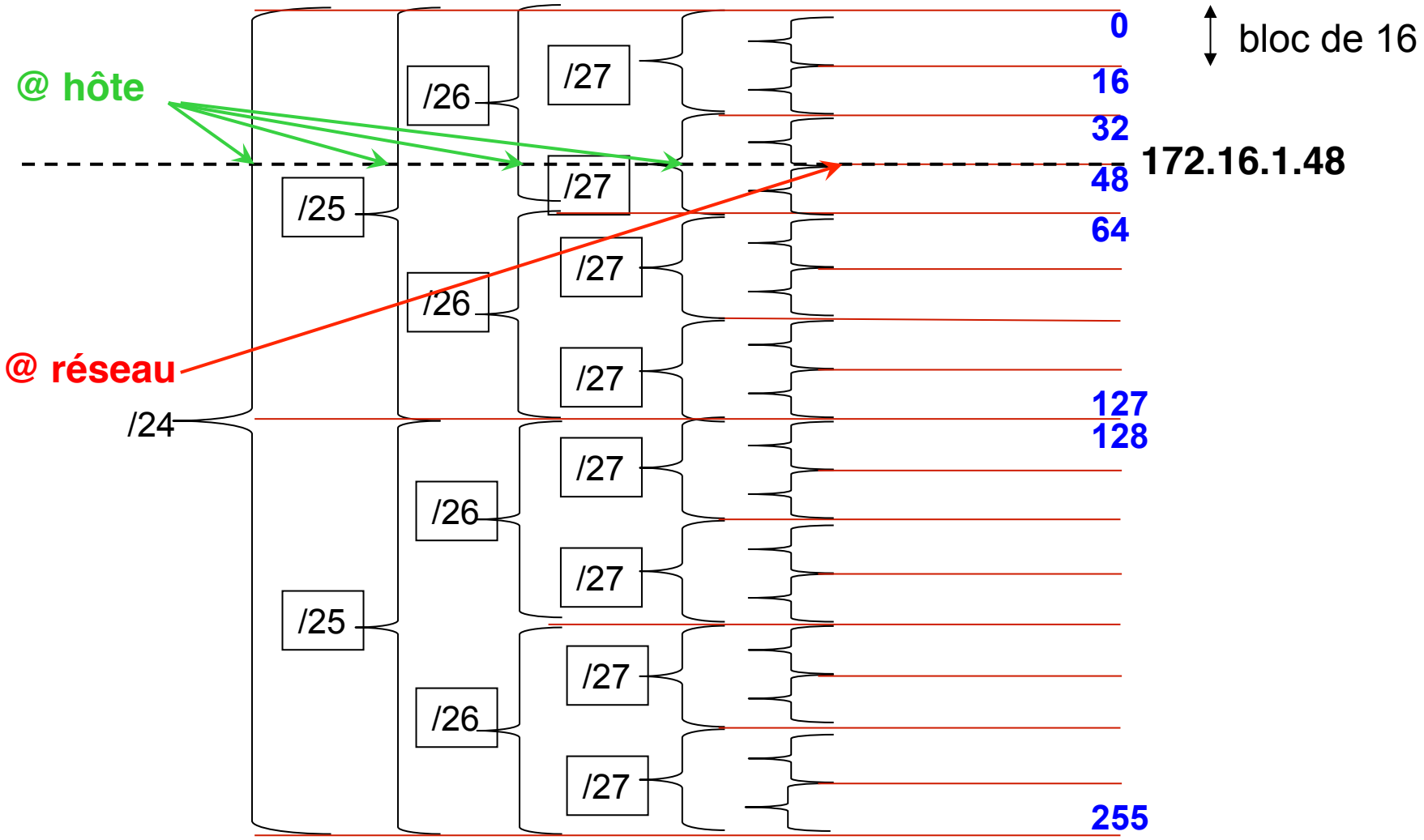
- Est-ce que 172.16.1.48 est :
  - une adresse réseau ?
  - une adresse disponible pour un hôte ?
  - une adresse broadcast ?

Exercice 1

- Tout dépend du masque !!
- 172.16.1.48 /24
- 172.16.1.48 /25
- 172.16.1.48 /26
- 172.16.1.48 /27
- 172.16.1.48 /28

Masque		Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/26	255.255.255.192	2^6=64	62
/27	255.255.255.224	2^5=32	30
/28	255.255.255.240	2^4=16	14

Explications 1



Solution 1

- 172.16.1.48 /24 adresse hôte
- 172.16.1.48 /25 adresse hôte
- 172.16.1.48 /26 adresse hôte
- 172.16.1.48 /27 adresse hôte
- 172.16.1.48 /28 adresse réseau

Exercice 2 : identifier l'adresse réseau

Adresse	Masque	Adresse sous-réseau
172.16.2.10	255.255.255.0	
10.6.24.20	255.255.240.0	
10.30.36.12	255.255.255.0	
192.168.1.129	255.255.255.128	

Masque		Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/28	255.255.255.240	2^4=16	14

Solution 2

Adresse	Masque	Adresse sous-réseau
172.16.2.10	255.255.**255**.0	172.16.2.0
10.6.24.20	255.255.**240**.0	10.6.16.0
10.30.36.12	255.255.**255**.0	10.30.36.0
192.168.1.129	255.255.255.**128**	192.168.1.128

	Masque	Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/28	255.255.255.240	2^4=16	14

Exercice 3 : identifier les @ réseau & br

Adresse	Masque	Adresse sous-réseau	Adresse broadcast
201.222.10.60	255.255.255.**248**		
15.16.193.6	255.255.**248**.0		
128.16.32.13	255.255.255.**252**		
153.50.6.27	255.255.255.**128**		

	Masque	Largeur du bloc = @ consommées	Nombre d'hôtes = @ disponibles
/25	255.255.255.128	2^7=128	126
/29	255.255.255.248	2^3=8	6
/30	255.255.255.252	2^2=4	2

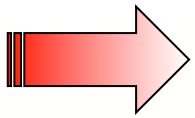
Solution 3

Adresse	Masque	Adresse sous-réseau	Adresse broadcast
201.222.10.60	255.255.255.248	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	153.50.6.0	153.50.6.127

	Masque	Largeur du bloc = @ consommées	Nombre d'hôtes = @ disponibles
/25	255.255.255.128	2^7=128	126
/29	255.255.255.248	2^3=8	6
/30	255.255.255.252	2^2=4	2

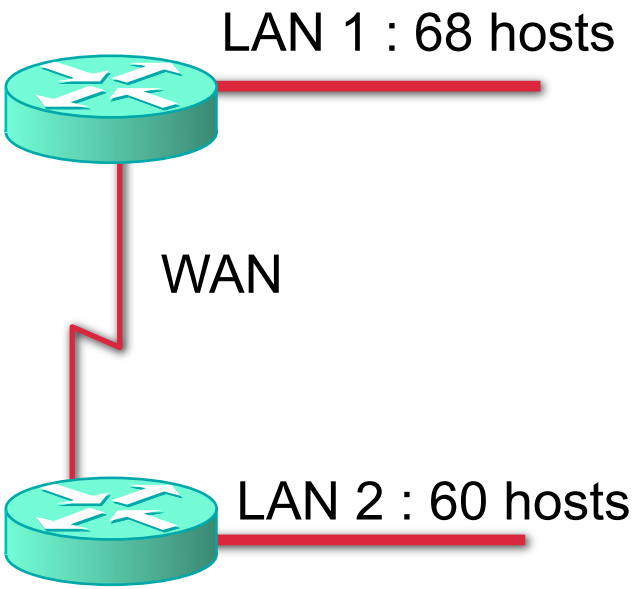
Le subnetting :

1. L’adresse IP et son masque
2. Les adresses réservées
3. Les classes
4. Le nombre d’adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel
7. Cas pratiques



Cas concrêt

- On vous a attribué le sous-réseau 172.16.1.0 /24
- Choisir un sous-réseau pour :



	Masque	Largeur du bloc	Nombre d'hôtes	
/24	255.255.255.0	2^8=256	254	
/25	255.255.255.128	2^7=128	126	ok pour 68 hosts
/26	255.255.255.192	2^6=64	62	ok pour 60 hosts
/27	255.255.255.224	2^5=32	30	
/28	255.255.255.240	2^4=16	14	
/29	255.255.255.248	2^3=8	6	
/30	255.255.255.252	2^2=4	2	ok pour 2 hosts
/31	255.255.255.254	2^1=2	0	

Solution 3

- LAN 1 = 172.16.1.X /25 : largeur de bloc = 128
- LAN 2 = 172.16.1.X /26 : largeur de bloc = 64
- WAN = 172.16.1.X /30 : largeur de bloc = 4

Solution 3

172	16	1	0	Adresse réseau	Un bloc de 128 pour le LAN 1 avec 68 hôtes
			1	1ère adresse disponible	
			…	2ème adresse disponible	
				3ème adresse disponible	
			63		
			64		
			65		
			…		
			126	Dernière adresse disponible	
			127	Adresse de broadcast	
			128		
			129		
			…		
			190		
			191		
			192		
			193		
			…		
			255		

Solution 3

172	16	1	0	Adresse réseau	Un bloc de **128** pour le LAN 1 avec 68 hôtes
			1	1ère adresse disponible	
			…	2ème adresse disponible	
				3ème adresse disponible	
			63		
			64		
			65		
			…		
			126	Dernière adresse disponible	
			127	Adresse de broadcast	
			128	Adresse réseau	Un bloc de **64** pour le LAN 2 avec 60 hôtes
			129	1ère adresse disponible	
			…		
			190	Dernière adresse disponible	
			191	Adresse de broadcast	
			192		
			193		
			…		
			255		

Solution 3

- LAN 1 = 172.16.1.0 /25
- LAN 2 = 172.16.1.128 /26
- WAN = 172.16.1.192 /30

Test

You have been asked to come up with a subnet mask that will allow all three web servers to be on the same network while providing the maximum number of subnets. Which network address and subnet mask meet this requirement?

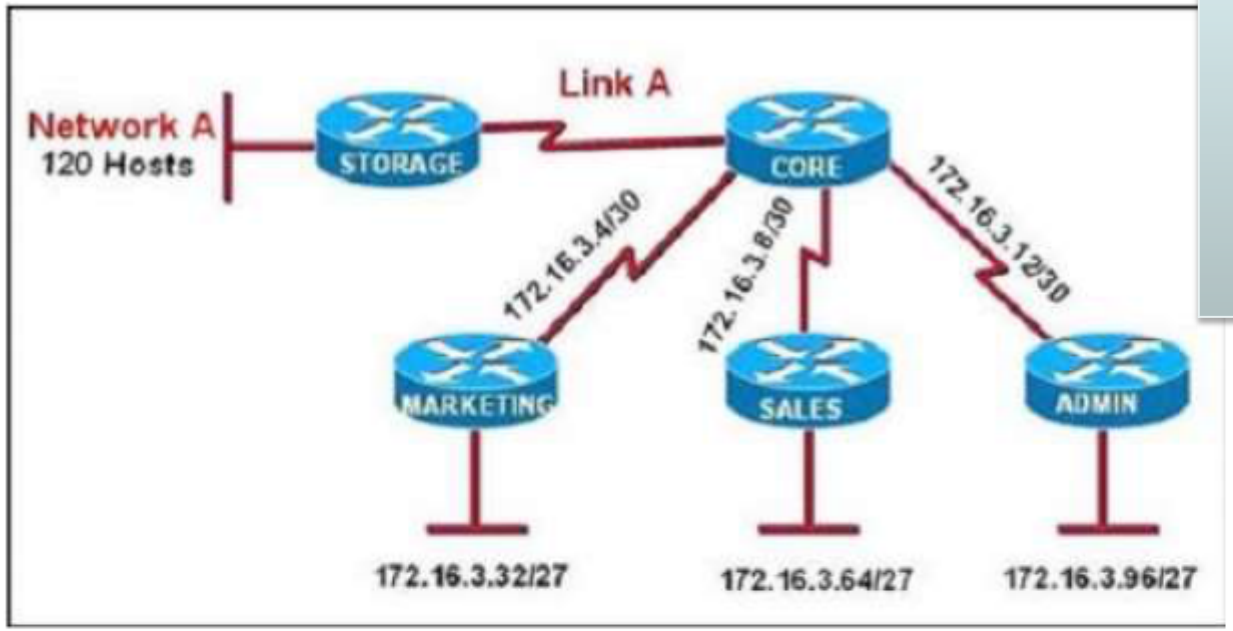
A. 192.168.252.0 255.255.255.252
B. 192.168.252.8 255.255.255.248
C. 192.168.252.8 255.255.255.252
D. 192.168.252.16 255.255.255.240
E. 192.168.252.16 255.255.255.252

Correct Answer: B

	Masque	Largeur du bloc	Nombre d'hôtes	
/24	255.255.255.0	2^8=256	254	
/25	255.255.255.128	2^7=128	126	
/26	255.255.255.192	2^6=64	62	
/27	255.255.255.224	2^5=32	30	
/28	255.255.255.240	2^4=16	14	
/29	255.255.255.248	2^3=8	6	ok pour 3 hosts
/30	255.255.255.252	2^2=4	2	
/31	255.255.255.254	2^1=2	0	

Test

	Masque	bloc	hôtes
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/26	255.255.255.192	2^6=64	62
/27	255.255.255.224	2^5=32	30
/28	255.255.255.240	2^4=16	14
/29	255.255.255.248	2^3=8	6
/30	255.255.255.252	2^2=4	2
/31	255.255.255.254	2^1=2	0



All of the routers in the network are configured with the ip subnet-zero command. Which network addresses should
be used for Link A and Network A? (Choose two.)

A. Link A – 172.16.3.0/30
B. Link A – 172.16.3.112/30
C. Network A – 172.16.3.48/26
D. Network A – 172.16.3.128/25
E. Link A – 172.16.3.40/30
F. Network A – 172.16.3.192/26

Correct Answer: AD

Test

How many usable host are there per subnet if you have the address of 192.168.10.0 with a subnet mask of 255.255.255.240?

A. 4
B. 8
C. 16
D. 14

Correct Answer: D

	Masque	Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	2^8=256	254
/25	255.255.255.128	2^7=128	126
/26	255.255.255.192	2^6=64	62
/27	255.255.255.224	2^5=32	30
/28	255.255.255.240	2^4=16	14
/29	255.255.255.248	2^3=8	6
/30	255.255.255.252	2^2=4	2
/31	255.255.255.254	2^1=2	0

ROUTAGE

Routage statique

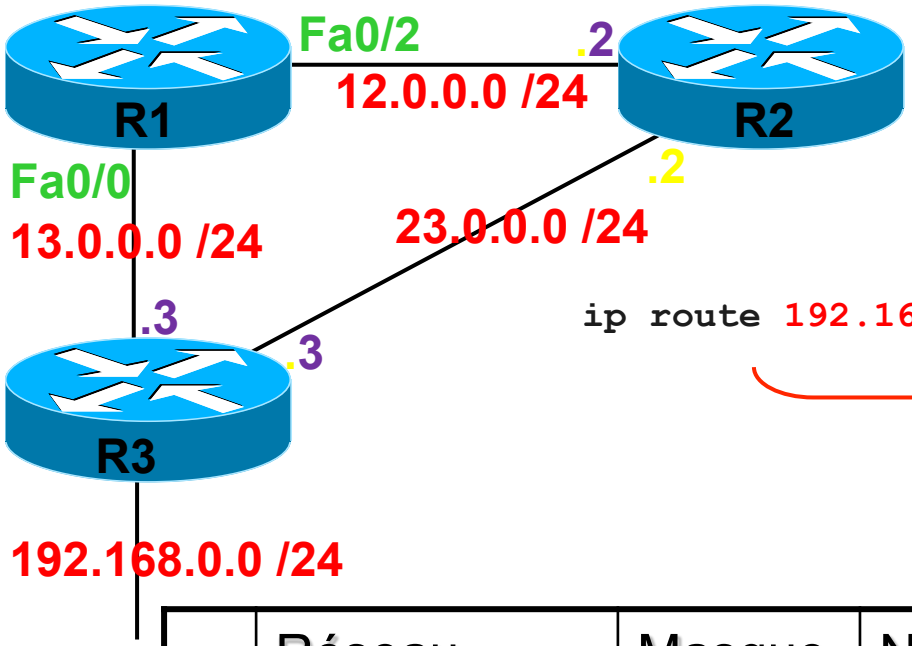
Introduction

Enrichir la table de routage

- Route statique :
  - saisie manuellement par l'administrateur
    - Sécurité car seul l' administrateur peut changer les tables de routage
  - aucune charge sur l' utilisation de la bande passante
  - administration fastidieuse
  - la distance administrative d' une route statique est égale à 1 par défaut.

- Protocole de routage :
  - il suffit d'activer un protocole de routage
  - adaptation automatique en cas de modification de la topologie du réseau

Route statique pour 192 à partir de R1



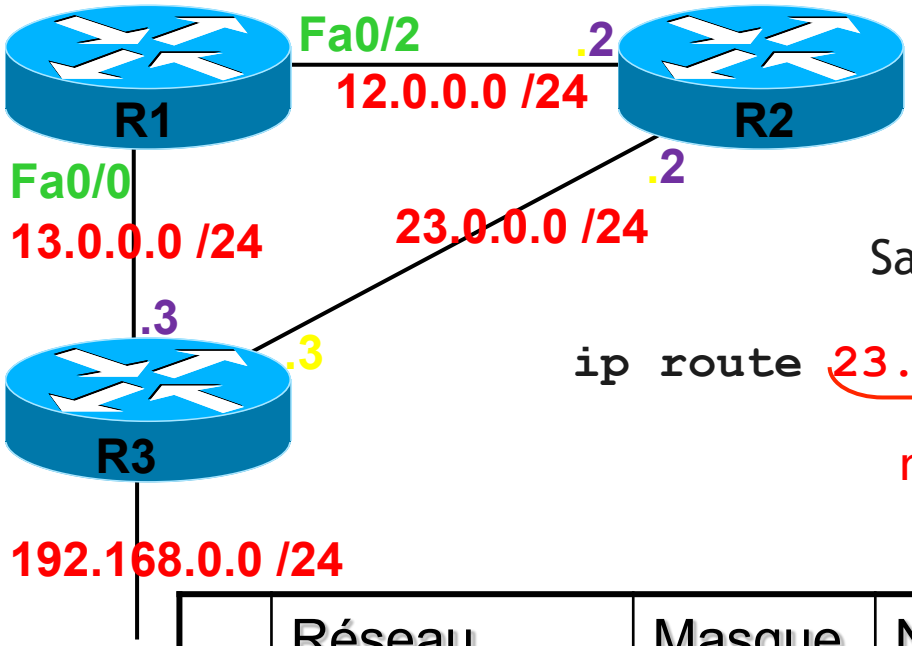
Saisir cette commande sur R1 :

```
ip route 192.168.0.0 255.255.255.0        13.0.0.3
```

réseau destination — next-hop

	Réseau	Masque	Next-Hop	Interface
C	12.0.0.0	/24		Fa0/2
C	13.0.0.0	/24		Fa0/0
S	192.168.0.0	/24	via 13.0.0.3	

Route statique pour 23 à partir de R1



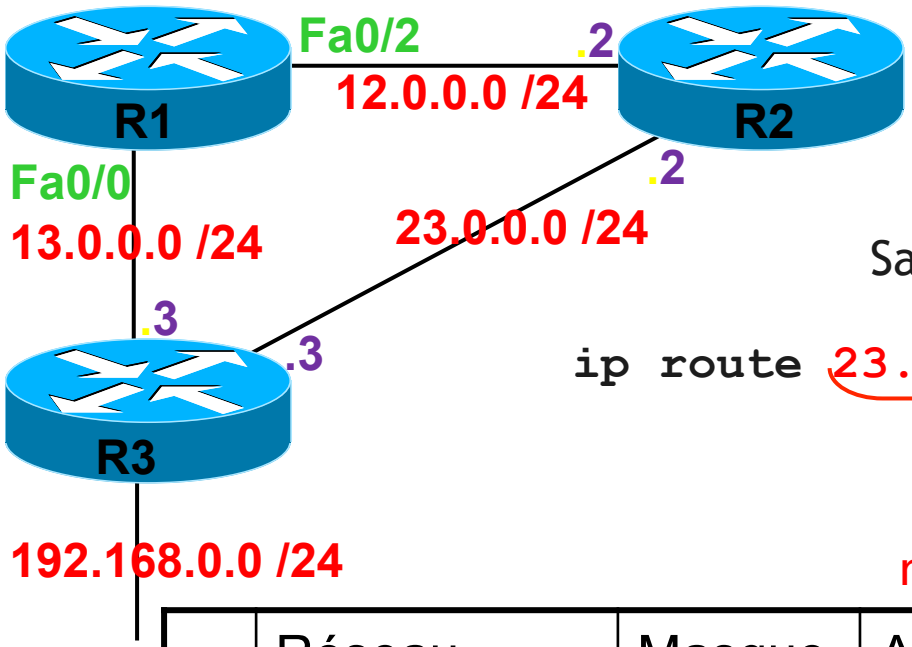
Saisir cette commande sur R1 :

```
ip route 23.0.0.0 255.255.255.0 13.0.0.3
```

réseau destination — next-hop

	Réseau	Masque	Next-Hop	Interface
C	12.0.0.0	/24		Fa0/2
C	13.0.0.0	/24		Fa0/0
S	23.0.0.0	/24	via 13.0.0.3	
S	192.168.0.0	/24	via 13.0.0.3	

Seconde route statique pour 23



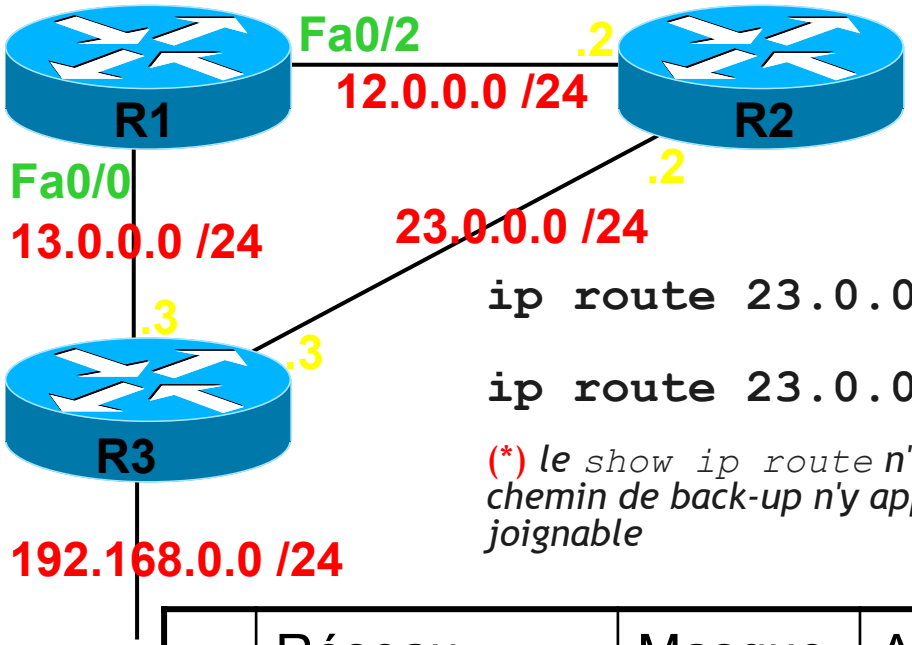
Saisir cette commande sur R1 :

```
ip route 23.0.0.0 255.255.255.0 12.0.0.2
```

réseau destination next-hop

	Réseau	Masque	AD	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
S	23.0.0.0	/24	1 1	via 13.0.0.3 via 12.0.0.2	
S	192.168.0.0	/24	1	via 13.0.0.3	

Route statique flottante pour 192




```
ip route 23.0.0.0 255.255.255.0 13.0.0.3

ip route 23.0.0.0 255.255.255.0 12.0.0.2 2
```

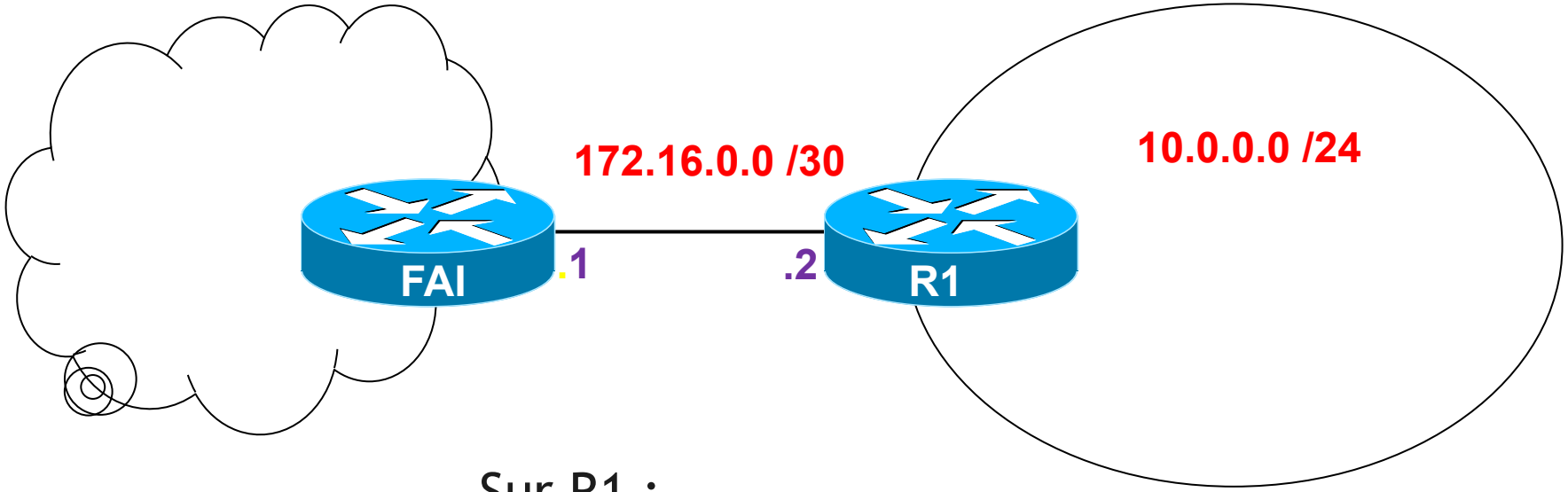
(*) *le* `show ip route` *n'indique que le meilleur chemin, par conséquent le chemin de back-up n'y apparaît que lorsque le meilleur chemin n'est plus joignable*

	Réseau	Masque	AD	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
S	23.0.0.0	/24	1	via 13.0.0.3	
S	192.168.0.0	/24	1	via 13.0.0.3	

Routage statique

Route par défaut

Route statique par défaut



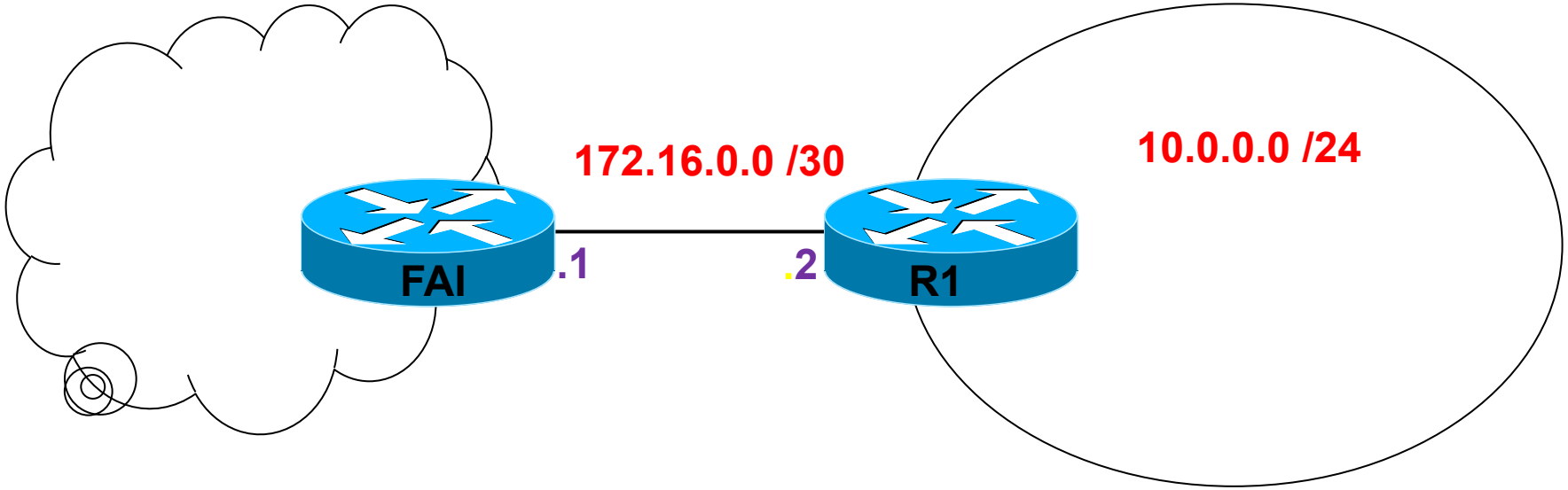
Sur R1 :

```
ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

Sur FAI :

```
ip route 10.0.0.0 255.255.255.0 172.16.0.2
```

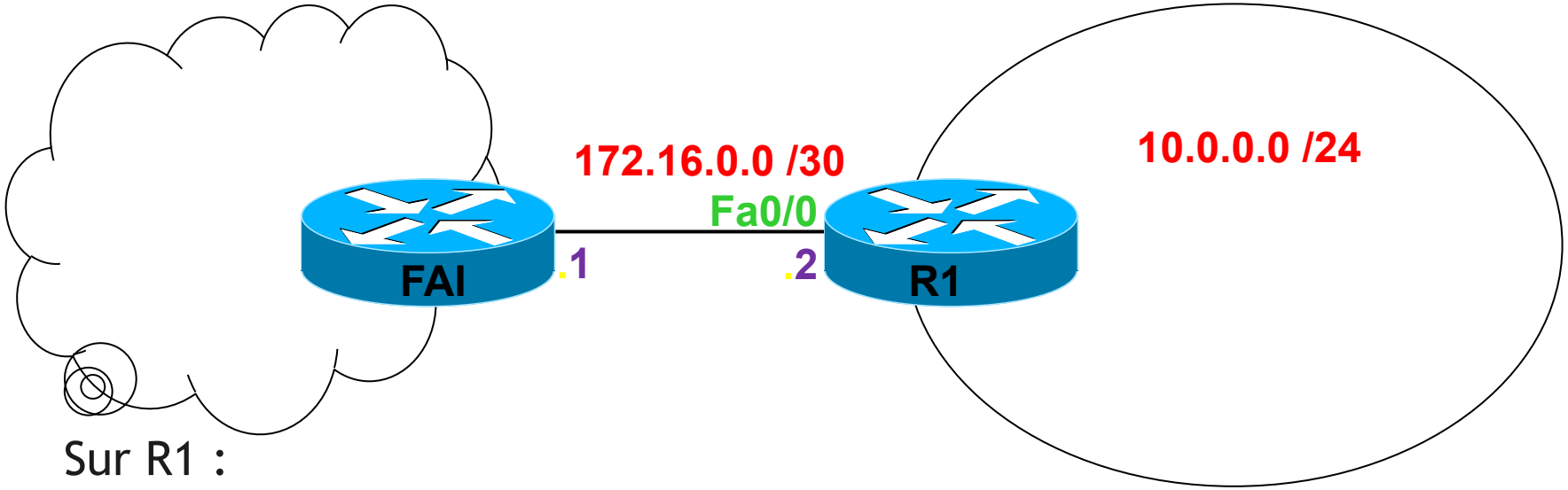
Route statique par défaut



Sur R1, **`show ip route :`**

	Réseau	Masque	AD	Next-Hop	Interface
C	10.0.0.0	/24			Fa0/2
C	172.16.0.0	/24			Fa0/0
S*	0.0.0.0	/0	1	via 172.16.0.1	

Route statique sans next hop



Sur R1 :

```
ip route 0.0.0.0 0.0.0.0 Fa0/0
```

La distance administrative de cette route statique sera égale à 0.

Routage dynamique

Types et familles de protocoles

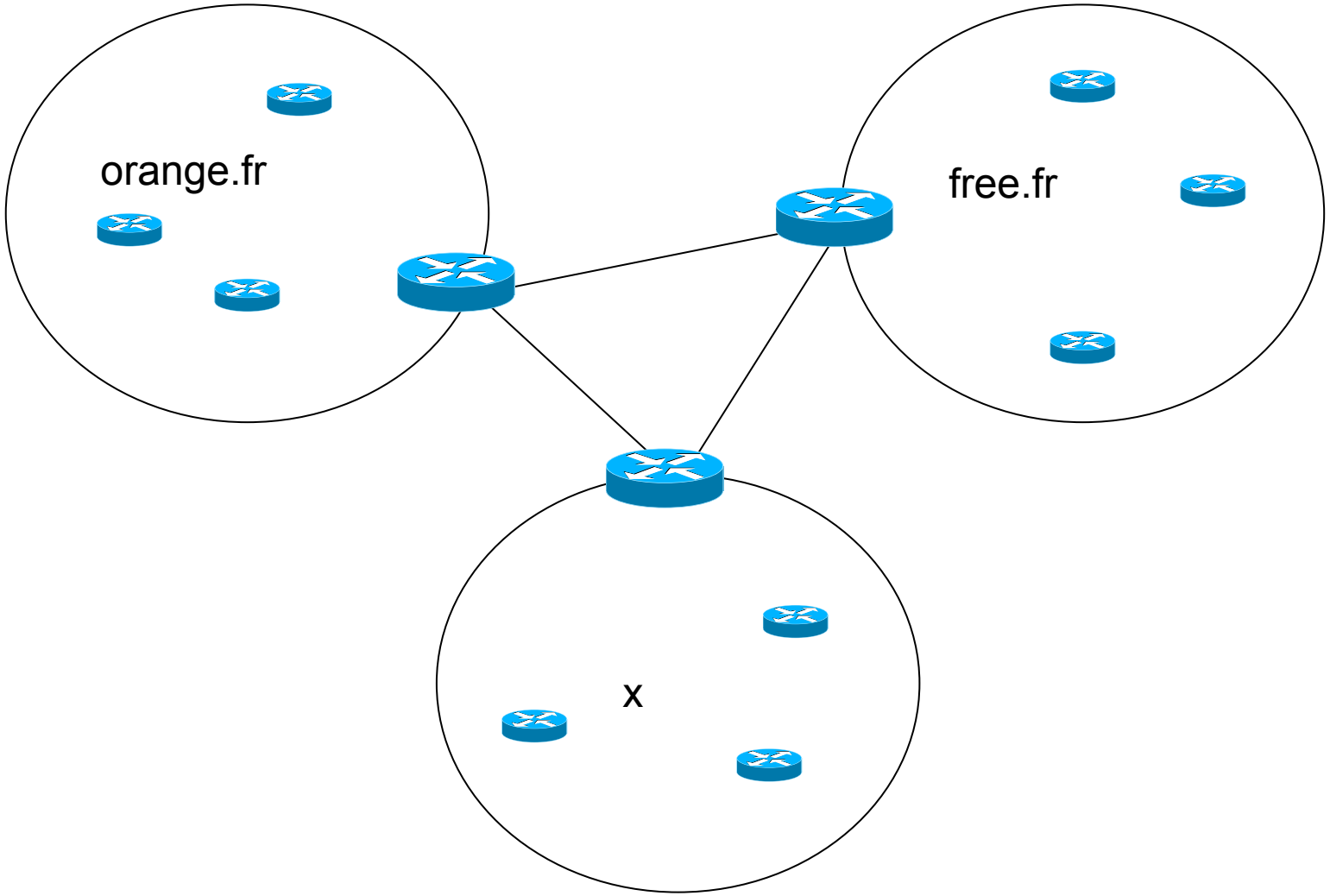
Principe des Protocoles de routage

- Les routeurs échangent des informations.
- Ces échanges leur permettent d'enrichir de manière automatique leurs tables de routages.
- En cas de modification de la topologie du réseau, les tables de routage sont mises à jour de manière dynamique.

Le Système Autonome

- C’est un ensemble de réseaux gérés par une seule et même entité administrative.
- C’est donc un ensemble de réseaux possédant une politique de routage qui lui est propre et indépendante.
- Internet est constitué de Systèmes Autonomes.
- Un AS est identifié par un numéro entre 1 et 65535.

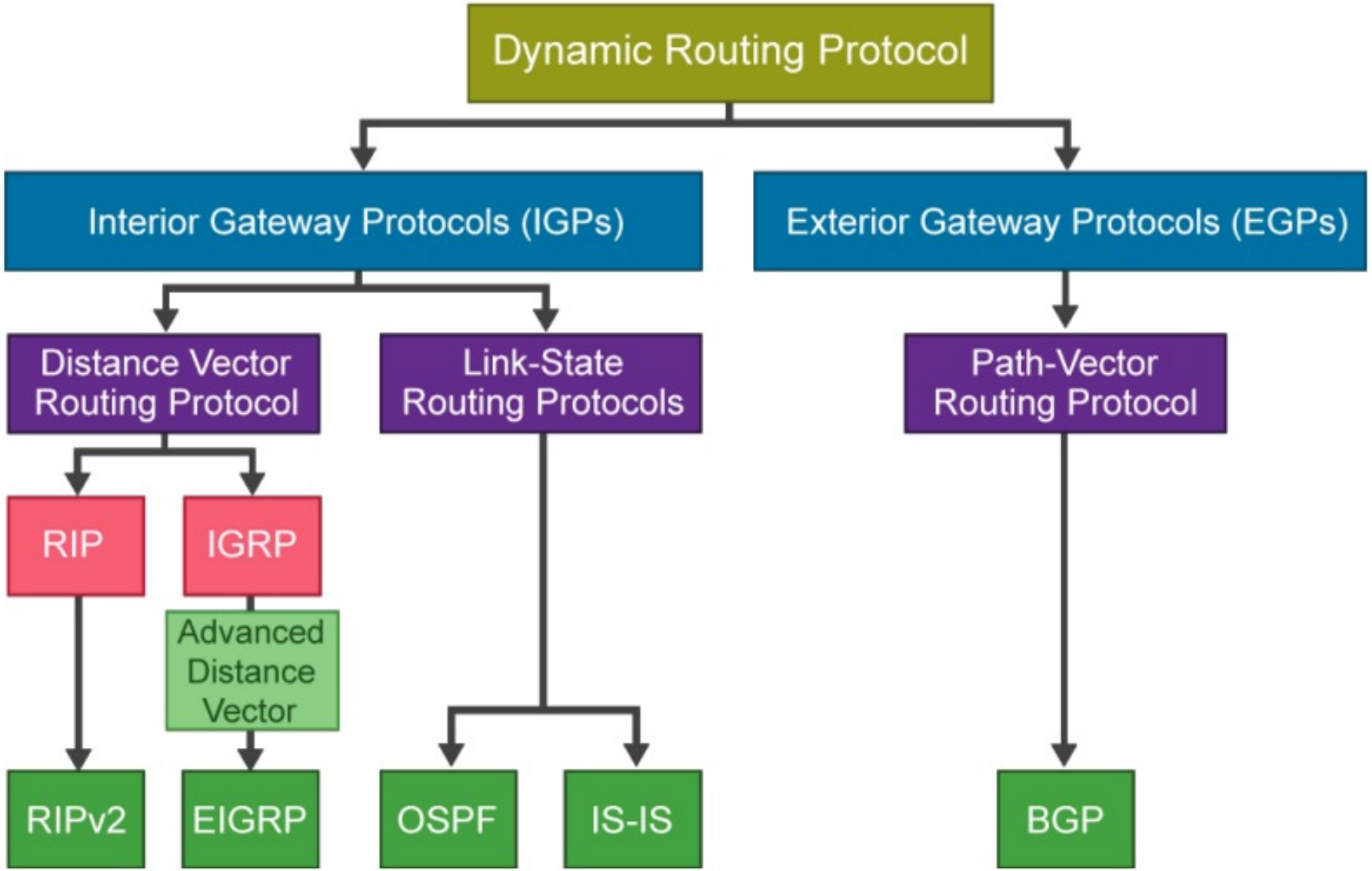
Exemple



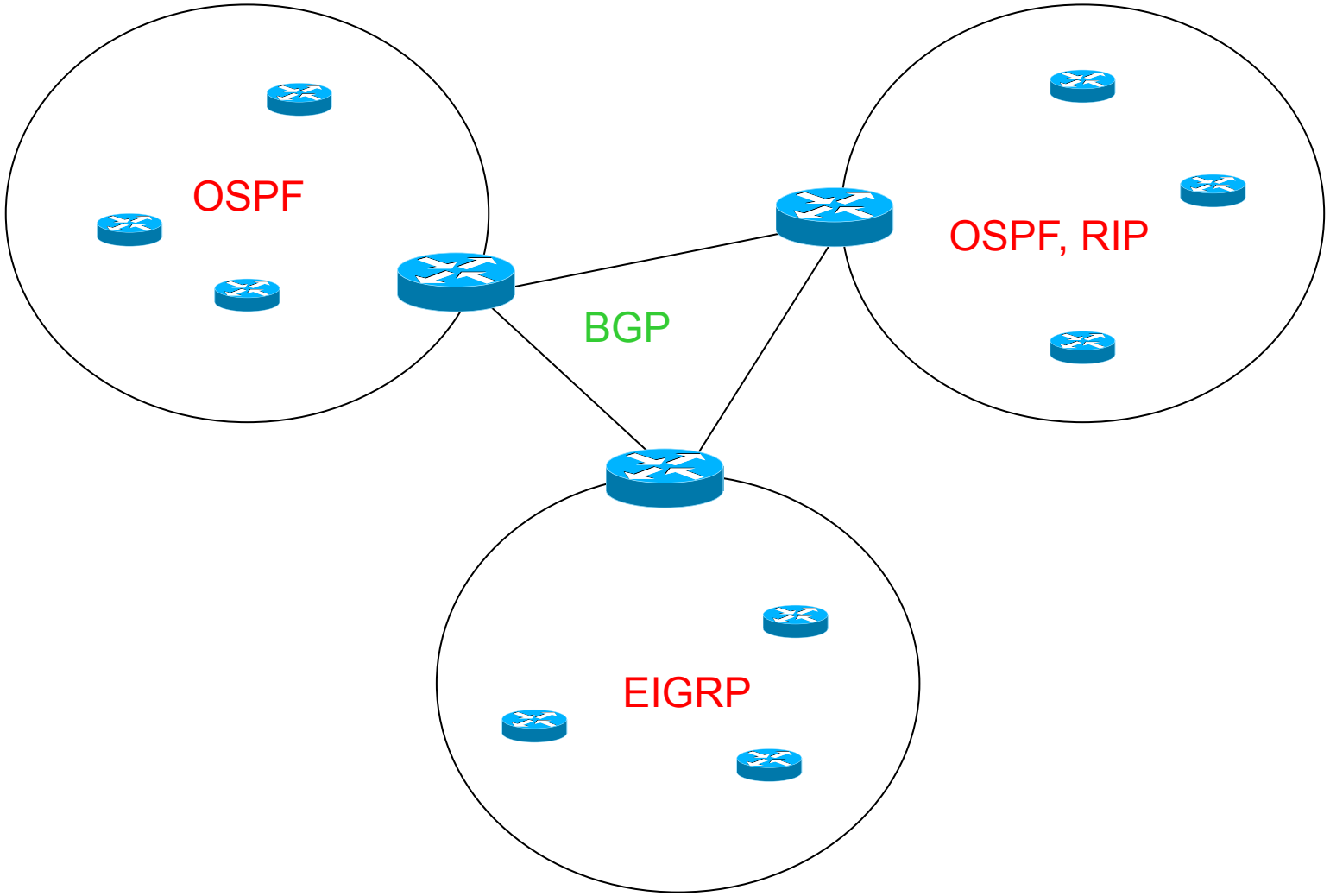
2 familles de protocoles de routage

- IGP Interior Gateway Protocol
  - protocoles de routage utilisés au sein d'un même AS
  - Exemples :
    - RIP
    - OSPF
    - EIGRP
- EGP Exterior Gateway Protocol
  - protocole de routage utilisé entre 2 AS
    - BGP

Distance Vector and Link-State Routing Protocols



2 familles de protocoles de routage



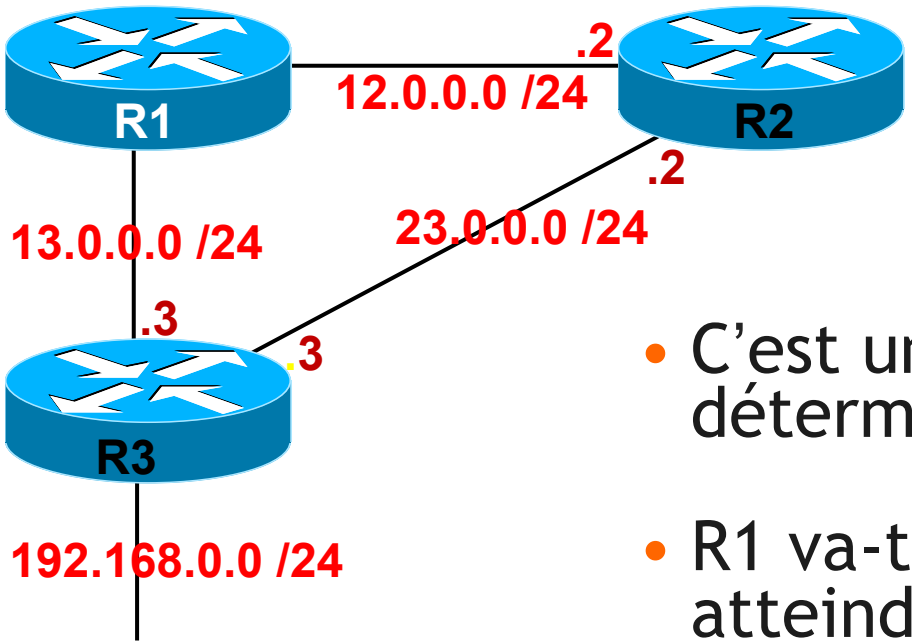
2 types de protocoles de routage

- Les protocoles à vecteur de distance :
  - Routage par « rumeur »
  - Le routeur envoie à son voisin une copie de sa table de routage.
  - Exemple : RIP (Routing Information Protocol)
- Les protocoles à état de lien :
  - Cartographie du réseau
  - Le routeur fait suivre à son voisin les informations détaillées reçues d'autres voisins.
  - Exemple : OSPF (Open Shortest Path First)

Routage dynamique

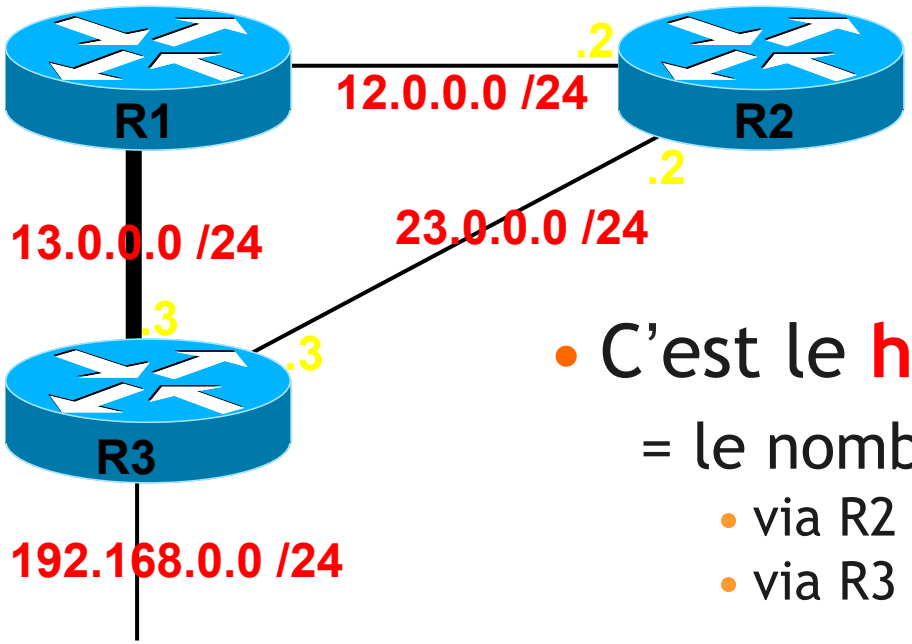
Métrique et AD

La métrique



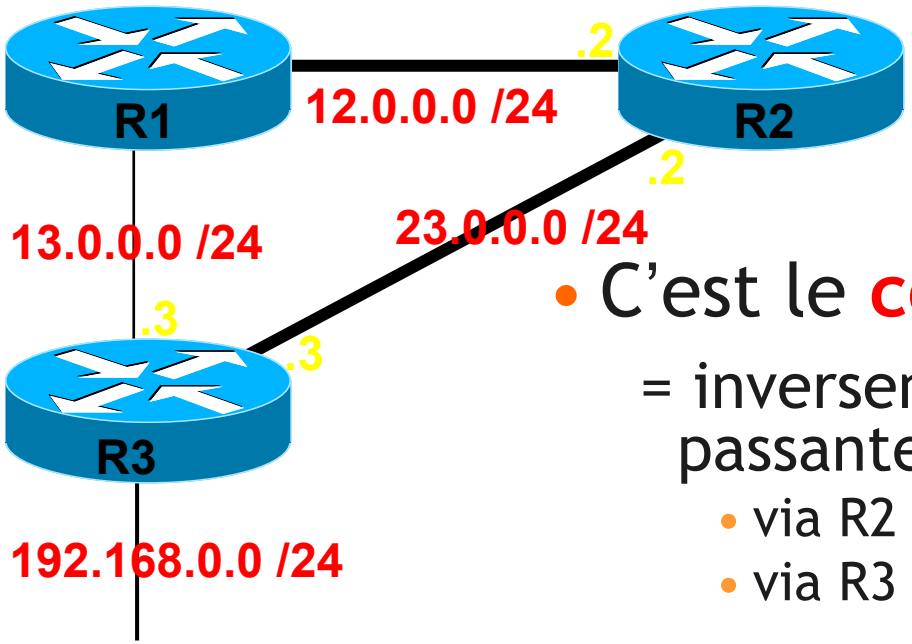
- C'est un critère utilisé pour déterminer le 'meilleur' chemin.
- R1 va-t-il passer par R2 ou R3 pour atteindrer le réseau 192.168.0.0/24 ?
- R1 prendra le chemin dont la métrique est la plus **petite**.

La métrique de RIP



- C'est le **hop-count** :
  = le nombre de routeurs à traverser.
  - via R2 : métrique = 2
  - via R3 : métrique = 1
- RIP indique à R1 de passer par R3.
- Se peut-il que RIP lui indique de passer par R2 ?

La métrique d'OSPF



- C'est le **coût** :

  = inversement proportionel à la bande passante de chaque segment traversé
  - via R2 : métrique = 2
  - via R3 : métrique = 10

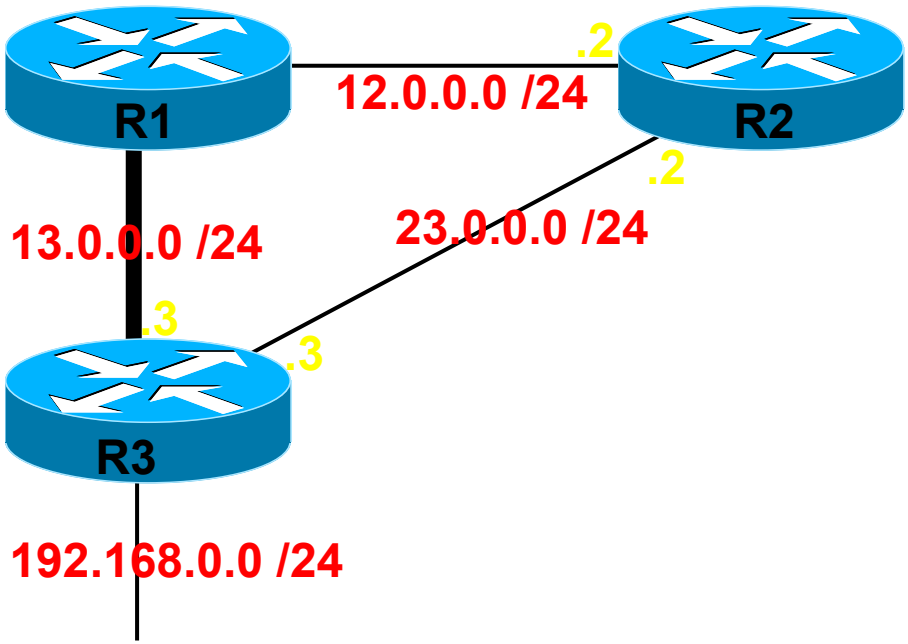
- OSPF indique à R1 de passer par R2.

- R1 reçoit donc 2 informations **contradictoires**

Comparer 2 protocoles de routage

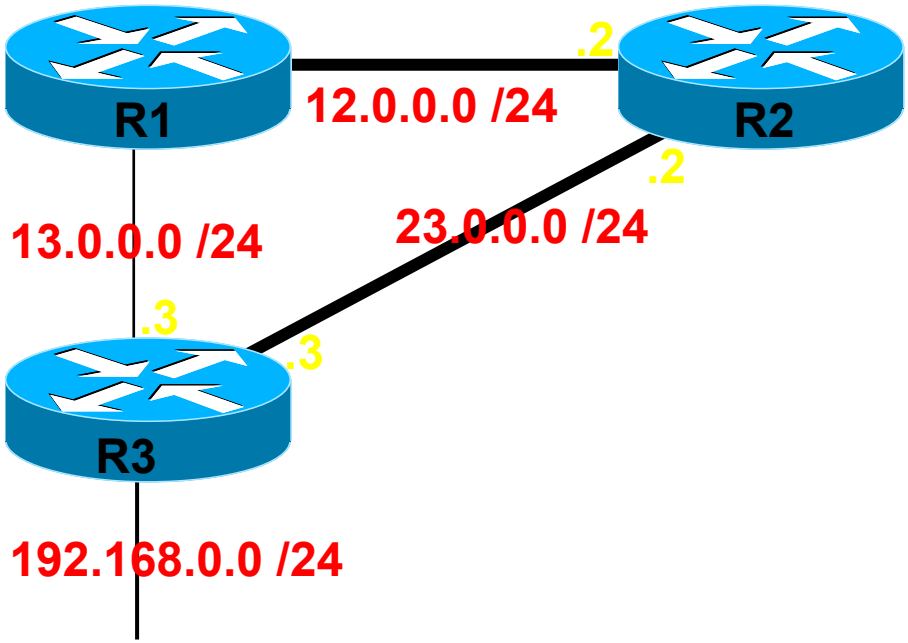
- A chaque protocole est attribué une **Distance administrative** arbitraire.
- Si 2 protocoles sont en concurrence, le routeur préfère le chemin dont la Distance administrative est la plus **petite**.
  - RIP = 120
  - OSPF = 110
  - EIGRP=90
- La distance administrative d'une route statique :
  - avec next-hop est égale à 1.
  - sans next-hop (sur une interface) est égale à 0.

Show ip route avec RIP



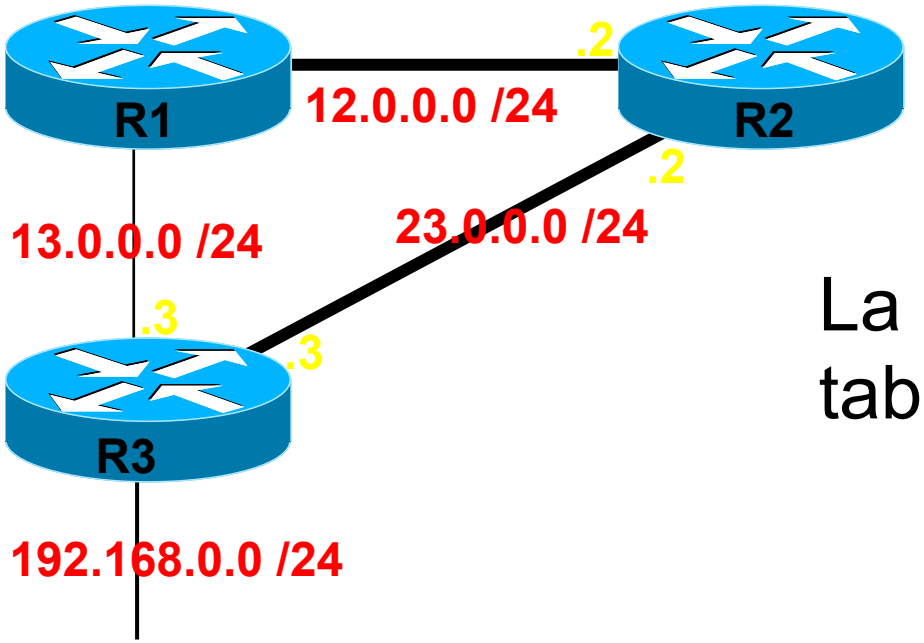
	Réseau	Masque	AD / métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	192.168.0.0	/24	[120 / 1]	via 13.0.0.3	

Show ip route avec OSPF



	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
O	192.168.0.0	/24	[110 / 2]	via 12.0.0.2	

Show ip route avec RIP et OSPF



La ligne RIP a disparu de la table de routage.

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
O	192.168.0.0	/24	[110 / 2]	via 12.0.0.2	

Règle de sélection du meilleur chemin.

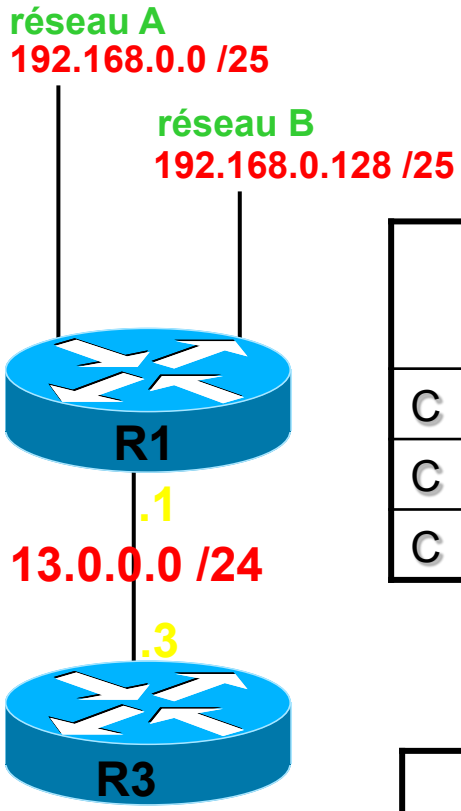
1. Chemin dont **AD** est le plus petit.
2. Chemin dont la **métrique** est la plus petite

- Cette règle est partielle.
- Elle sera complétée ultérieurement.

Routage dynamique

Summarization

Sans summarization



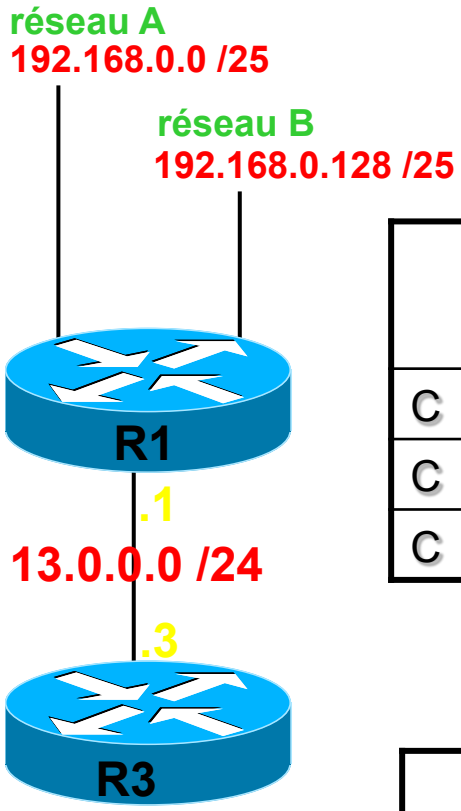
R1, `show ip route` :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	13.0.0.0	/24			Fa0/2
C	192.168.0.0	/25			Fa0/0
C	192.168.0.128	/25			Fa0/1

R3, `show ip route` :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	13.0.0.0	/24			Fa0/2
R	192.168.0.0	/25	[120 / 1]	13.0.0.1	
R	192.168.0.128	/25	[120 / 1]	13.0.0.1	

Avec summarization



R1, `show ip route` :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	13.0.0.0	/24			Fa0/2
C	192.168.0.0	/25			Fa0/0
C	192.168.0.128	/25			Fa0/1

R3, `show ip route` :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	13.0.0.0	/24			Fa0/2
R	192.168.0.0	/24	[120 / 1]	13.0.0.1	

Une seule ligne apprise par R3.

Avantages et prérequis

- La summarization permet de fusionner plusieurs sous-réseaux d'un même réseau majeur.
- Le protocole de routage annoncera le réseau fusionné au lieu d'annoncer chacun des sous-réseaux.
- Avantage : Réduction de la taille des tables de routage.
- Prérequis : Nécessite un plan d'adressage judicieusement défini.

Fusion exacte

- Sous-réseaux initiaux :
  - 10.0.0.0 /24
  - 10.0.1.0 /24
- Après fusion, annonce du réseau :
  - 10.0.0.0 /23
- La réseau fusionné est bien la somme des 2 sous-réseaux initiaux.

Fusion inexacte

- Sous-réseaux initiaux :
  - 10.0.0.0 /24
  - 10.0.1.0 /24
- Après fusion, annonce du réseau :
  - 10.0.0.0 /16
- La réseau fusionné contient bien d'autres réseaux que les 2 sous-réseaux initiaux.

Exercice 1

- Sous-réseaux initiaux :
  - 192.168.0.0/24
  - 192.168.1.0/24
- La meilleure summarization possible est :
  - 192.168.0.0/23

Exercice 2

- Sous-réseaux initiaux :
  - 192.168.2.0/24
  - 192.168.3.0/24
- La meilleure summarization possible est :
  - 192.168.2.0/23

Exercice 3

- Sous-réseaux initiaux :
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.3.0/24
- La meilleure summarization possible est :
  - 192.168.0.0/22

Exercice 4

- Sous-réseaux initiaux :
  - 192.168.0.0/25
  - 192.168.0.128/25
- La meilleure summarization possible est :
  - 192.168.0.0/24

Exercice 5

- Sous-réseaux initiaux :
  - 192.168.0.0/26
  - 192.168.0.64/26
- La meilleure summarization possible est :
  - 192.168.0.0/25

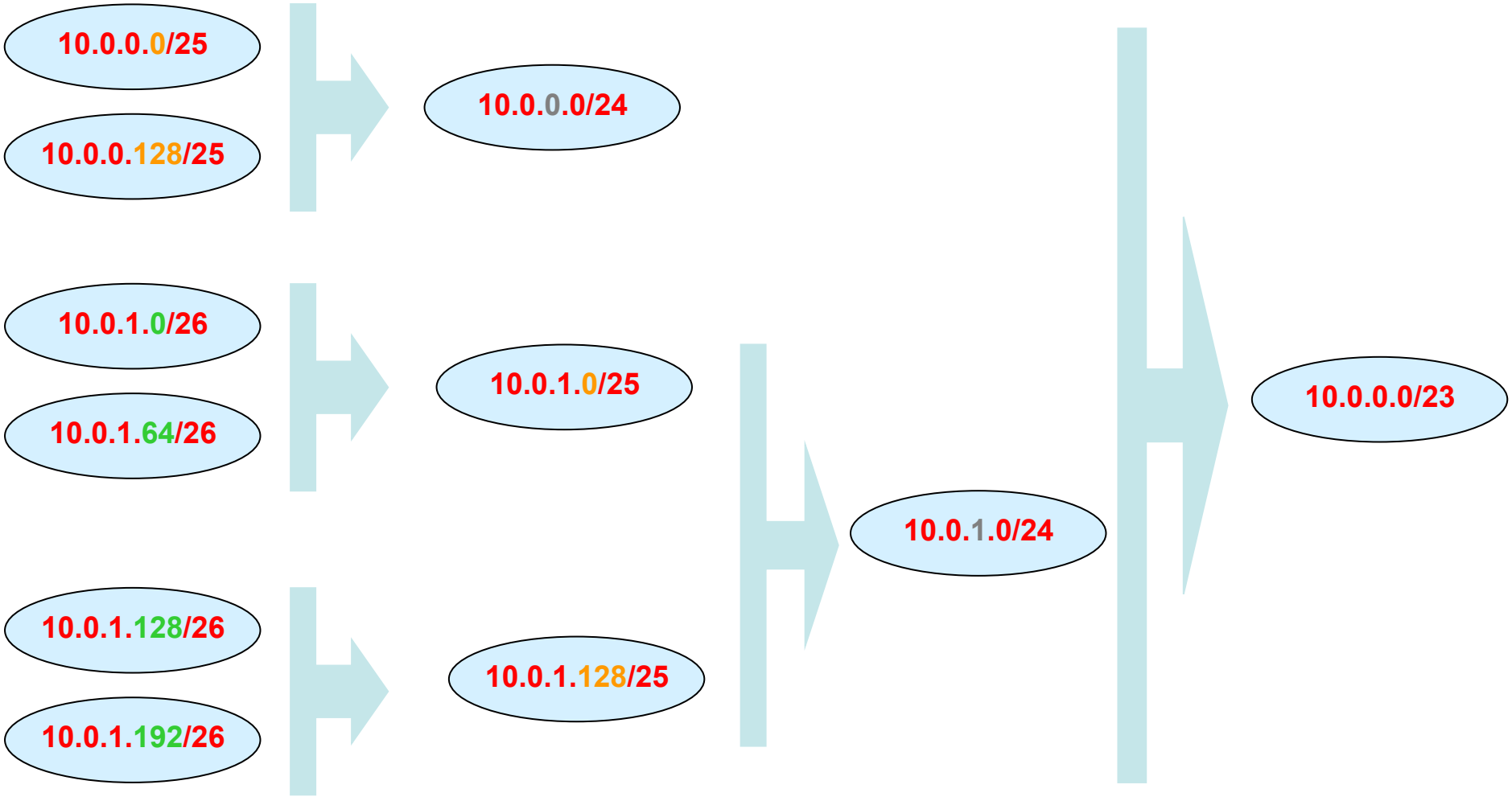
Exercice 6

- Sous-réseaux initiaux :
  - 192.168.0.128/26
  - 192.168.0.192/26
- La meilleure summarization possible est :
  - 192.168.0.128/25

Exercice 7

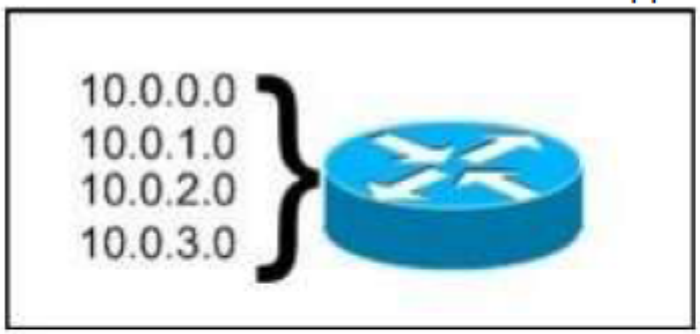
- Sous-réseaux initiaux :
  - 192.168.0.0/26
  - 192.168.0.64/26
  - 192.168.0.128/26
  - 192.168.0.192/26
- La meilleure summarization possible est :
  - 192.168.0.0/24

Summarizations hiérarchiques



Test

Refer to the exhibit. What is the most appropriate summarization for these routes?



A. 10.0.0.0 /21
B. 10.0.0.0 /22
C. 10.0.0.0 /23
D. 10.0.0.0 /24

Correct Answer: B

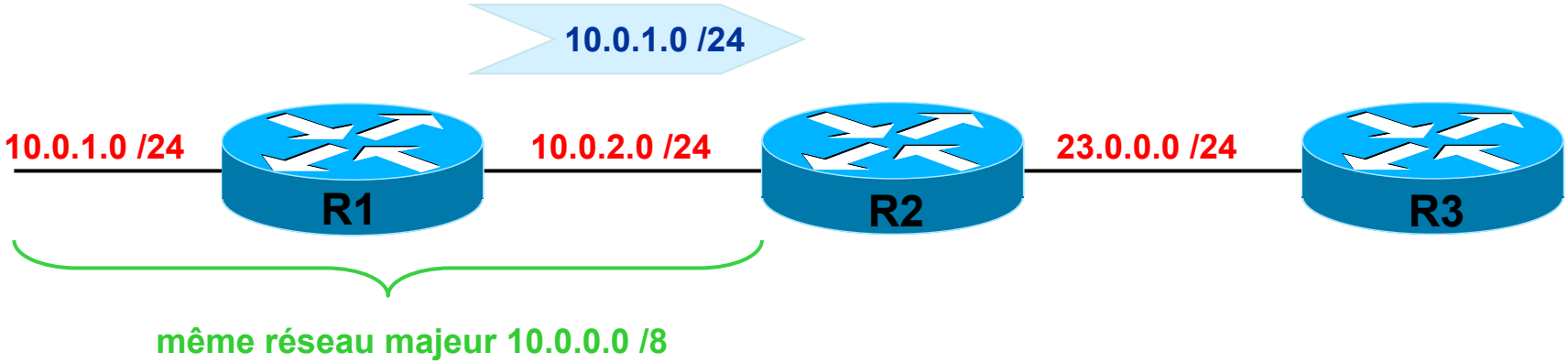
Routage dynamique

Summarization automatique

Principe

- Pour réduire la taille des tables de routage, certains protocoles effectuent de manière automatique une summarization à la frontière des réseaux majeurs.
- Ce sont les protocoles RIP et EIGRP.

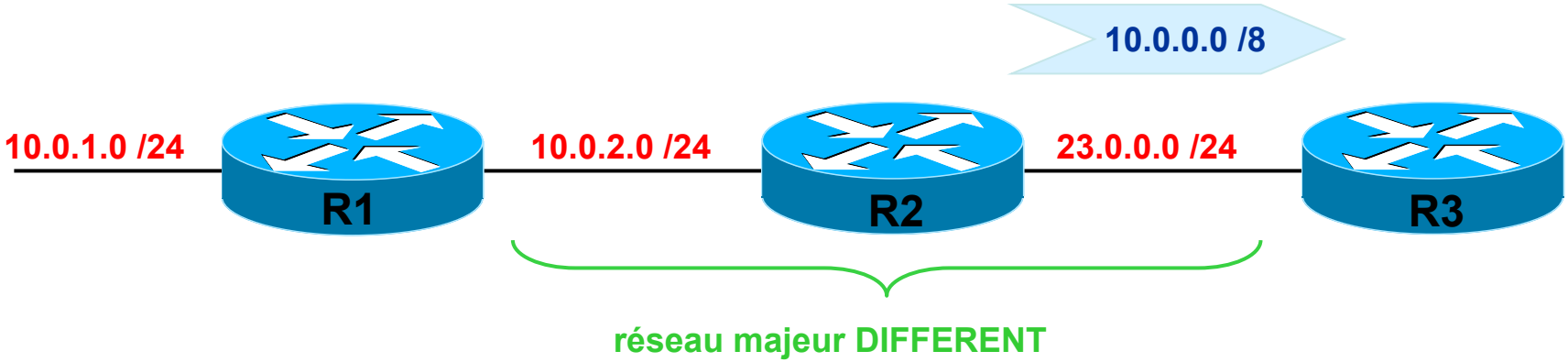
Exemple



Annonce du réseau 10.0.1.0/24 de R1 à R2 :

- R1 envoie cette annonce à R2.
- Le sous-réseau entre R1 et R2 est 10.0.2.0 /24.
- 10.0.1.0/24 et 10.0.2.0 /24 appartiennent au même réseau majeur.
- R1 n'applique pas de summarization automatique.
- R1 annonce donc 10.0.1.0 /24 à R2

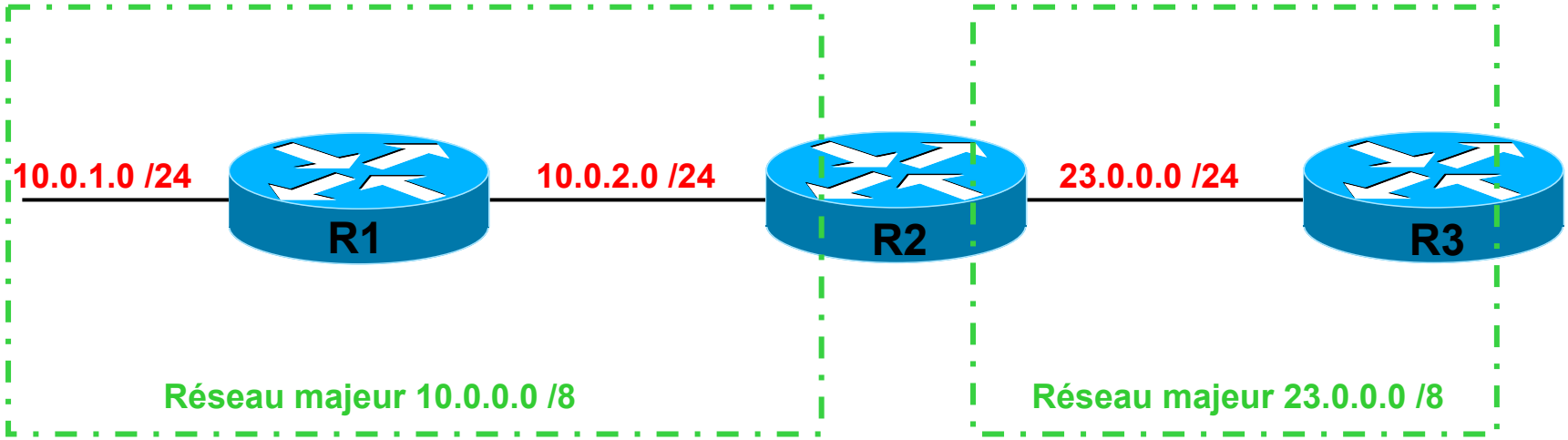
Exemple, suite



Annonce du réseau 10.0.1.0/24 de R2 à R3 :

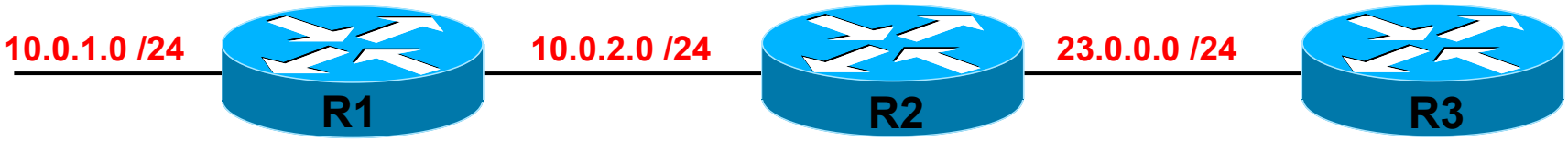
- R2 envoie cette annonce à R3.
- Le sous-réseau entre R2 et R3 est 23.0.0.0 /24.
- 10.0.1.0/24 et 23.0.0.0 /24 n'appartiennent pas au même réseau majeur.
- R2 applique DONC la summarization automatique.
- R2 annonce donc 10.0.0.0 /8 à R2

Frontière des réseaux majeurs



La summarization automatique ne concerne que les annonces qui traversent les frontières de réseaux majeurs.

show ip route



	Réseau	Masque
C	10.0.1.0	/24
C	10.0.2.0	/24
X	23.0.0.0	/24

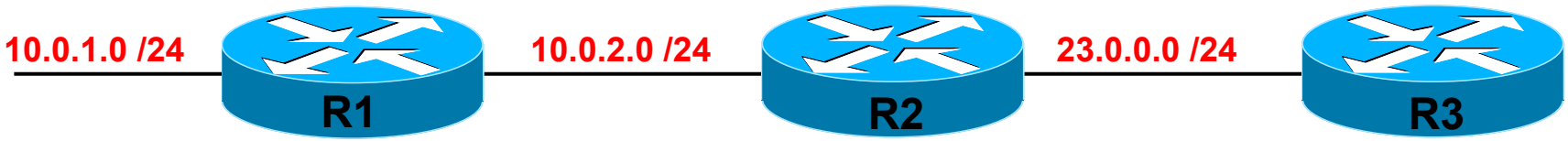
	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24

	Réseau	Masque
R	10.0.0.0	/8
C	23.0.0.0	/24

Désactiver

- Par défaut, RIP et EIGRP effectuent la summarization automatique.
- Elle peut être désactivée avec la commande suivnate :
  - `no auto-summary`
- et re-activée par :
  - `auto-summary`

Avec no auto-summary

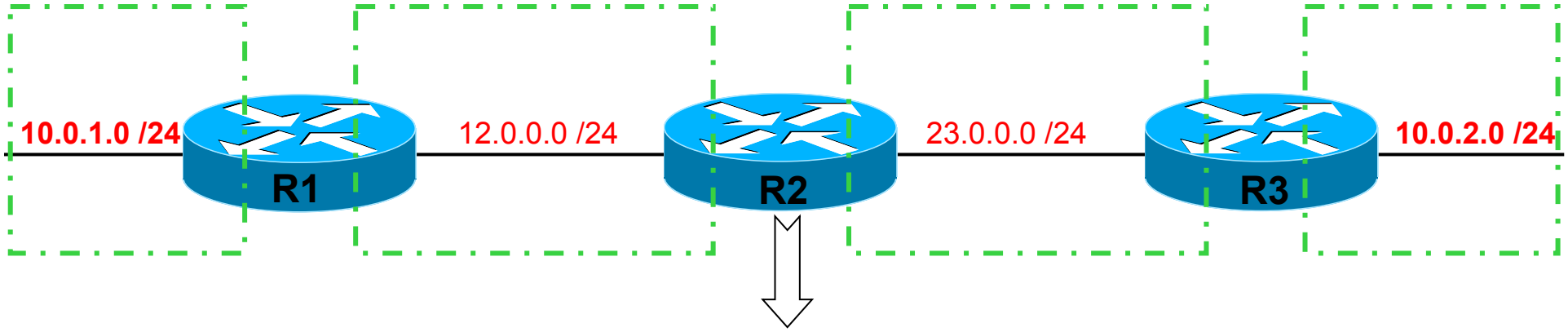


	Réseau	Masque
C	10.0.1.0	/24
C	10.0.2.0	/24
X	23.0.0.0	/24

	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24

	Réseau	Masque
X	10.0.1.0	/24
X	10.0.2.0	/24
C	23.0.0.0	/24

Problème avec réseaux disjoints



	Réseau	Masque	Next-hop
X	10.0.0.0	/8	via 12.0.0.1 via 23.0.0.3
C	12.0.0.0	/24	
C	23.0.0.0	/24	

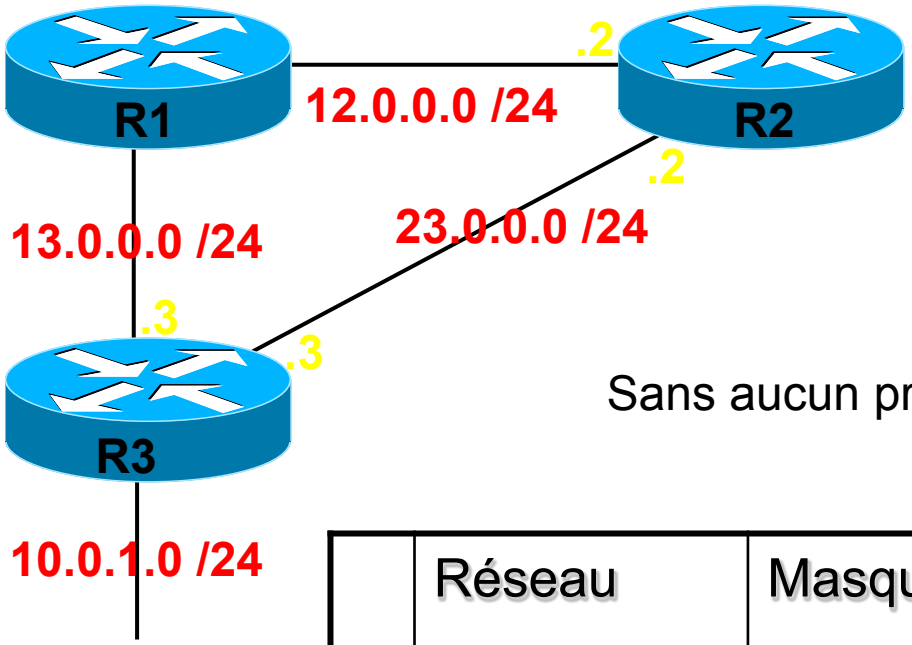
R2 croit qu'il peut joindre le réseau 10.0.0.0/8 indifféremment via R1 ou R3.
Il enverra un paquet à R1, le suivant à R3.

Il faut désactiver auto-summary !

Routage dynamique

Maîtriser la Table de routage

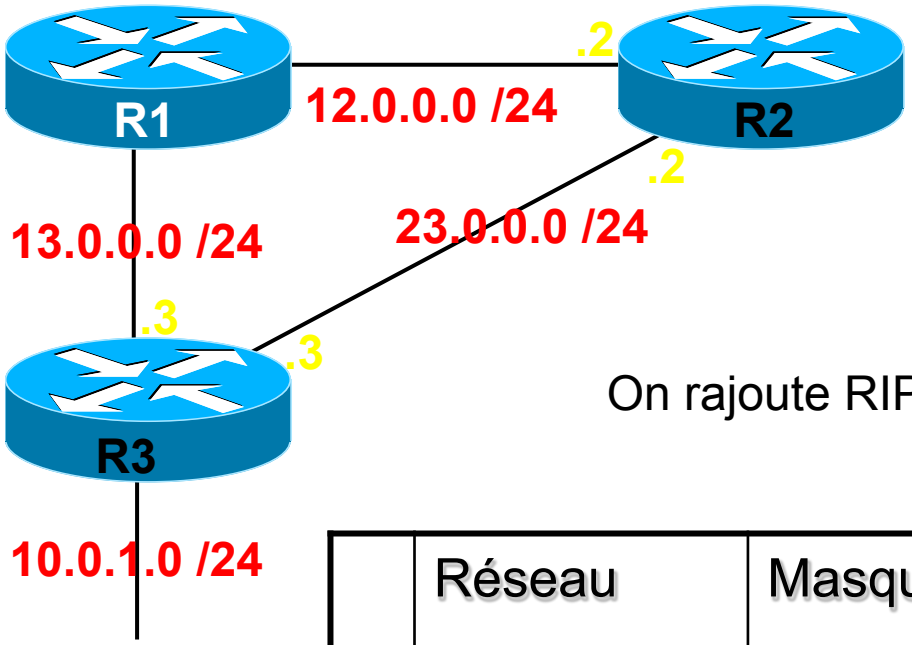
Exemple 1/3



Sans aucun protocole de routage sur R1 :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0

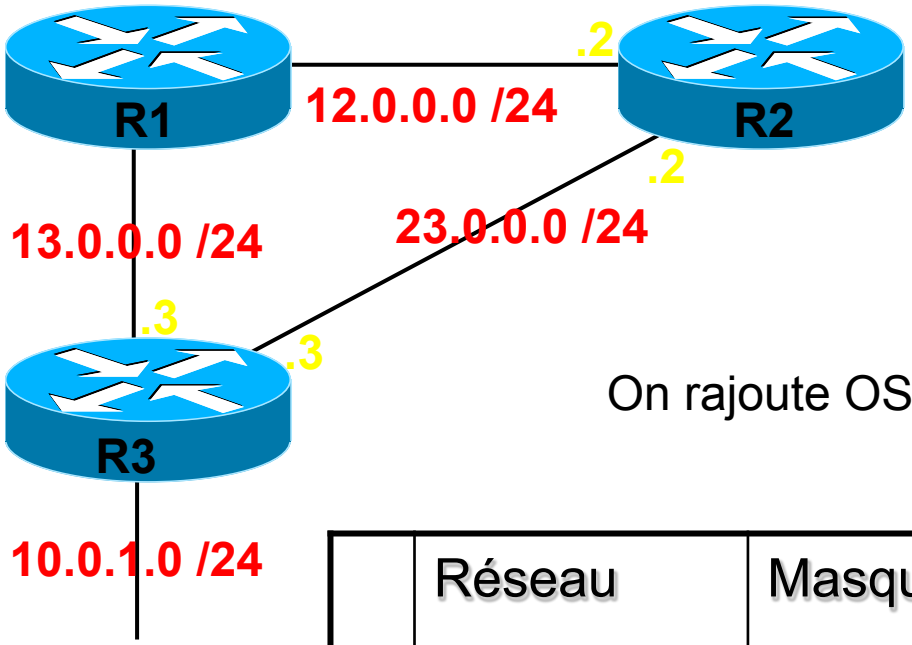
Exemple 2/3 sur R1



On rajoute RIP entre R1, R2 et R2 :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	10.0.0.0	/8	[120 / 1]	13.0.0.3	

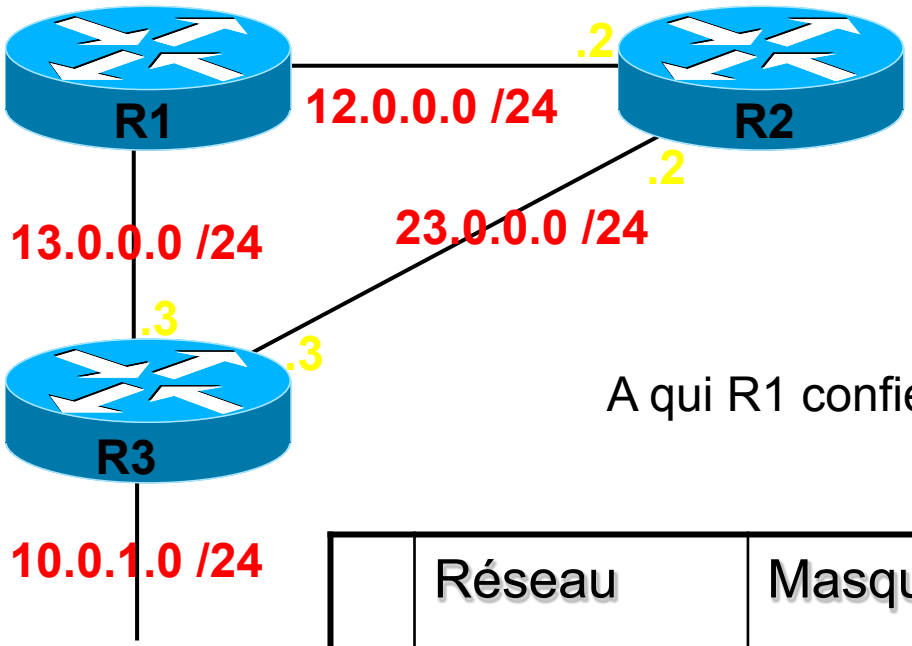
Exemple 3/3



On rajoute OSPF entre R1, R2 et R3 :

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	10.0.0.0	/8	[120 / 1]	13.0.0.3	
O	10.0.1.0	/24	[110 / 20]	12.0.0.2	
O	23.0.0.0	/24	[110 / 10]	12.0.0.2	

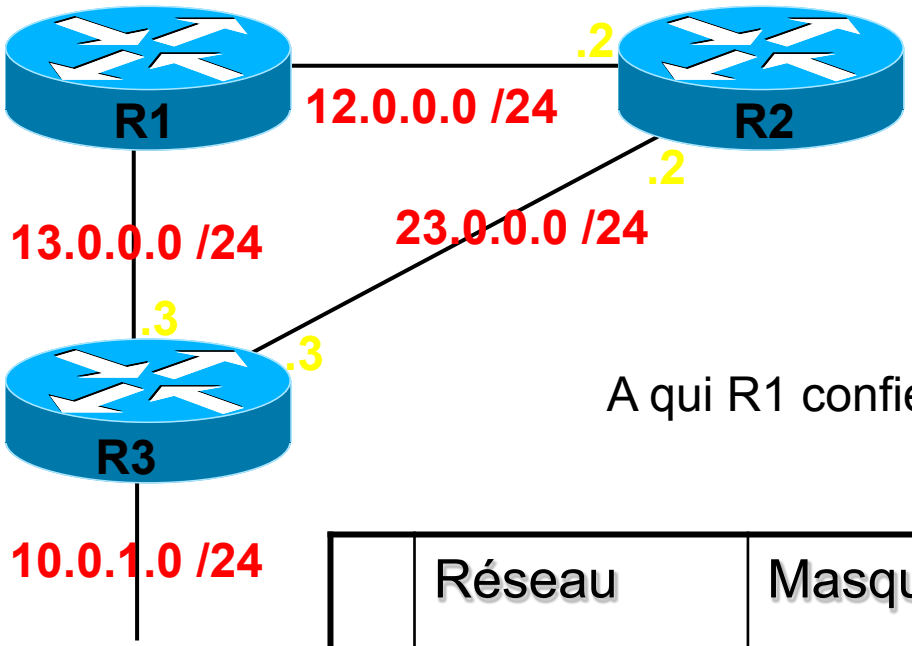
Exploitation de la table - Cas 1



A qui R1 confie un paquet pour 10.0.1.99 ?

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	10.0.0.0	/8	[120 / 1]	13.0.0.3	
O	10.0.1.0	/24	[110 / 20]	**12.0.0.2**	
O	23.0.0.0	/24	[110 / 10]	12.0.0.2	

Exploitation de la table - Cas 2



A qui R1 confie un paquet pour 10.0.2.99 ?

	Réseau	Masque	AD / Métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	10.0.0.0	/8	[120 / 1]	**13.0.0.3**	
O	10.0.1.0	/24	[110 / 20]	12.0.0.2	
O	23.0.0.0	/24	[110 / 10]	12.0.0.2	

Règle de sélection du meilleur chemin.

1. Route la plus précise,
   i.e. avec le masque le plus long.
2. Chemin dont AD est le plus petit.
3. Chemin dont la métrique est la plus petite

- Cette règle est maintenant complète.

RIP

Routing Information Protocol

Carte d'identité de RIP

- Standard ou Propriétaire ?
- standard
- IGP / EGP ?
- IGP
- DV ou LS ?
- DV : Vecteur de distance
- Distance administrative : AD ?
- 120
- Métrique ?
- Σ hops
- Lettre qui identifie ce protocole dans `sh ip route` ?
- R

Les annonces

- « Updates »
- Envoyées toutes les 30 secondes.
- Version 1 = envoyées en broadcast.
  - adresse IP destination = 255.255.255.255
- Version 2 = envoyées en multicast.
  - adresse IP destination = 224.0.0.9
- Envoyées sur toutes les interfaces où RIP est activé.

Activer RIP sur une interface

- `configure terminal`
- `router rip`
- `network 10.0.0.0`

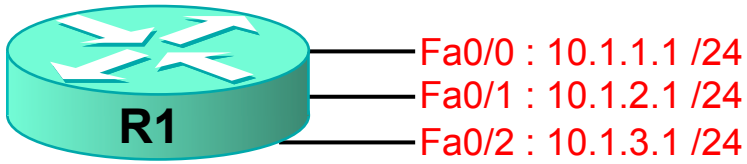
signifie :

« active RIP dès
qu'une de tes propres interfaces
est dans le pool 10.0.0.0 /8 »

Exemples

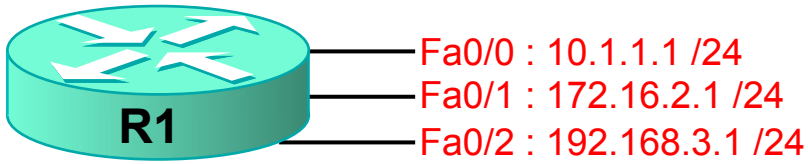
- `network 11.0.0.0`
- activer RIP sur toutes les interfaces en 11.0.0.0 /8
- `network 111.0.0.0`
- activer RIP sur toutes les interfaces en 111.0.0.0 /8
- `network 131.0.0.0`
- activer RIP sur toutes les interfaces en 131.0.0.0 /16
- `network 211.0.0.0`
- activer RIP sur toutes les interfaces en 211.0.0.0 /24

Exercice 1



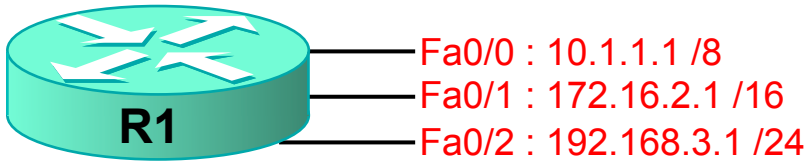
- Activer RIP sur toutes les interfaces
- `router rip`
- `network 10.0.0.0`

Exercice 2



- Activer RIP sur toutes les interfaces
- `router rip`
- `network 10.0.0.0`
- `network 172.16.0.0`
- `network 192.168.3.0`

Exercice 3



- Activer RIP sur Fa0/0 et Fa0/2 seulement :
- `router rip`
- `network 10.0.0.0`
- `network 192.168.3.0`

Partage de charge

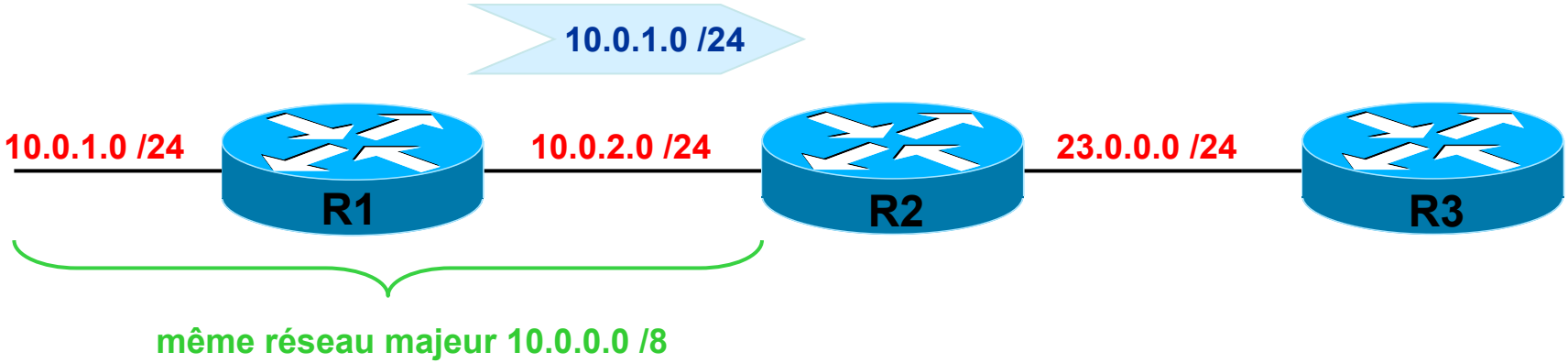
- A métriques égales, RIP est capable de faire du partage de charge via 4 chemins différents.
- Configurable jusqu'à 16 :

```
router rip

maximum-path 1     pas de partage de charge

maximum-path 4     valeur par défaut

maximum-path 16    valeur maximale
```

Summarization automatique

- Pour réduire la taille des tables de routage, certains protocoles effectuent de manière automatique une summarization à la frontière des réseaux majeurs.
- Ce sont les protocoles RIP et EIGRP.

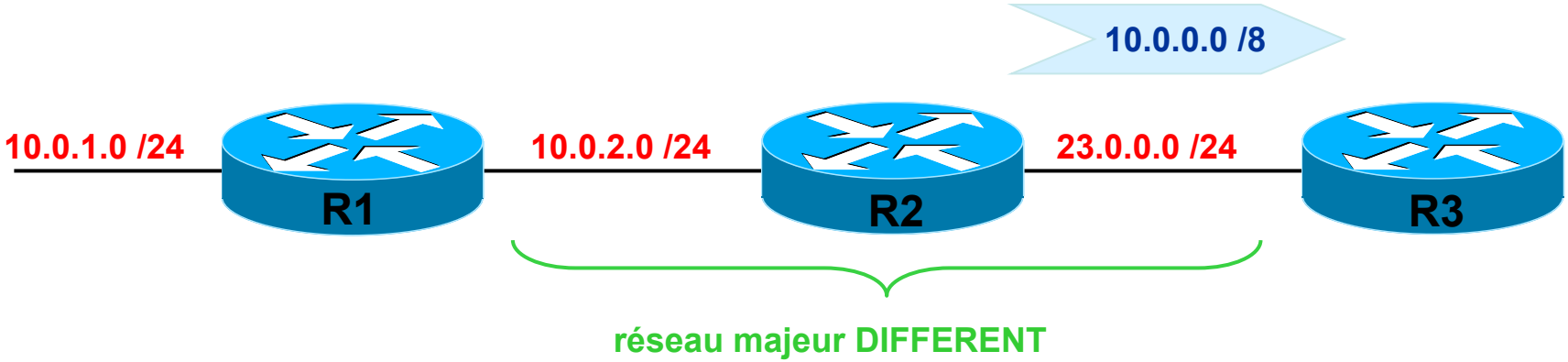
Exemple



Annonce du réseau 10.0.1.0/24 de R1 à R2 :

- R1 envoie cette annonce à R2.
- Le sous-réseau entre R1 et R2 est 10.0.2.0 /24.
- 10.0.1.0/24 et 10.0.2.0 /24 appartiennent au même réseau majeur.
- R1 n'applique pas de summarization automatique.
- R1 annonce donc 10.0.1.0 /24 à R2

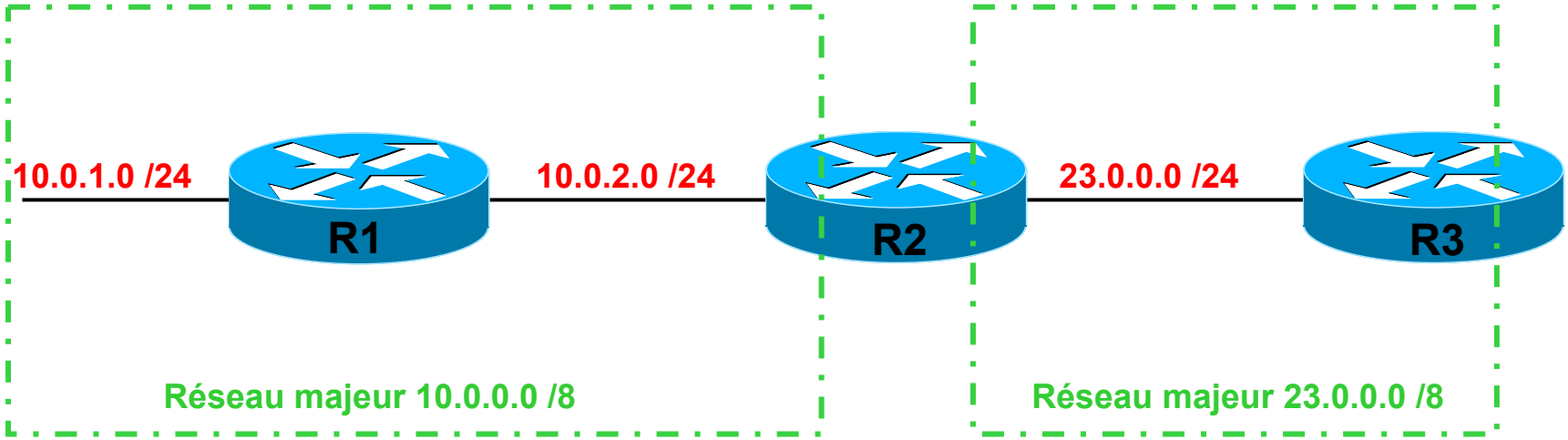
Exemple, suite



Annonce du réseau 10.0.1.0/24 de R2 à R3 :

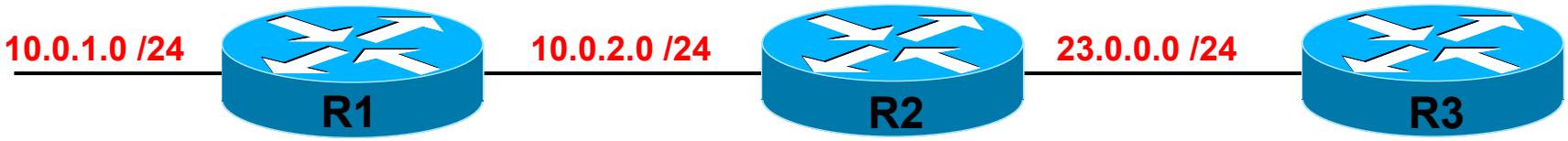
- R2 envoie cette annonce à R3.
- Le sous-réseau entre R2 et R3 est 23.0.0.0 /24.
- 10.0.1.0/24 et 23.0.0.0 /24 n'appartiennent pas au même réseau majeur.
- R2 applique DONC la summarization automatique.
- R2 annonce donc 10.0.0.0 /8 à R2

Frontière des réseaux majeurs



La summarization automatique ne concerne que les annonces qui traversent les frontières de réseaux majeurs.

show ip route



	Réseau	Masque
C	10.0.1.0	/24
C	10.0.2.0	/24
X	23.0.0.0	/24

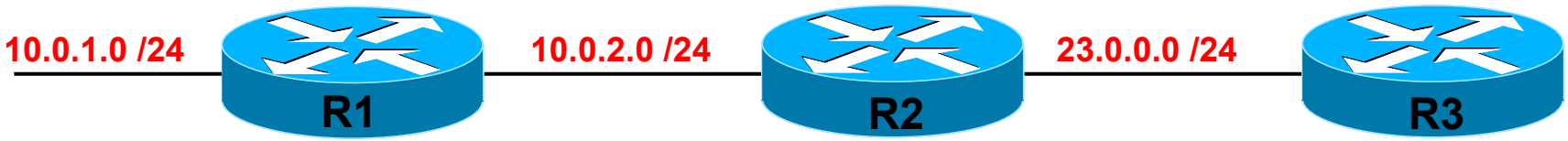
	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24

	Réseau	Masque
R	10.0.0.0	/8
C	23.0.0.0	/24

Désactiver

- Par défaut, RIP et EIGRP effectuent la summarization automatique.
- Elle peut être désactivée avec la commande suivnate :
  - `no auto-summary`
- et re-activée par :
  - `auto-summary`

Avec no auto-summary

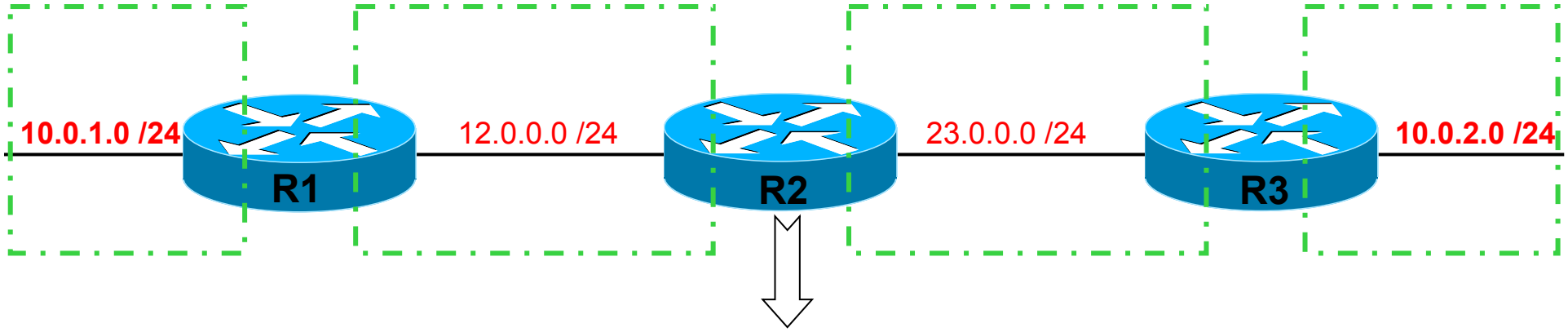


	Réseau	Masque
C	10.0.1.0	/24
C	10.0.2.0	/24
X	23.0.0.0	/24

	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24

	Réseau	Masque
X	10.0.1.0	/24
X	10.0.2.0	/24
C	23.0.0.0	/24

Problème avec réseaux disjoints



	Réseau	Masque	Next-hop
X	10.0.0.0	/8	via 12.0.0.1 via 23.0.0.3
C	12.0.0.0	/24	
C	23.0.0.0	/24	

R2 croit qu'il peut joindre le réseau 10.0.0.0/8 indifféremment via R1 ou R3.
Il enverra un paquet à R1, le suivant à R3.

Il faut désactiver auto-summary !

Passer en RIP version 2

- `configure terminal`
- `router rip`
- `version 2`

RIP sait maintenant indiquer
le masque des réseaux qu'il annonce.

Va-t-il toujours annoncer le vrai masque ?

NON !

Annoncer le vrai masque

- `configure terminal`
- `router rip`
- `version 2`
- `no auto-summary`

Routage OSPF

OSPF

Open Shortest Path First

Carte d'identité de OSPF

- Standard ou Propriétaire ?
- standard
- IGP / EGP ?
- IGP, capable de gérer VLSM
- DV ou LS ?
- LS : Link-State
- Distance administrative : AD ?
- 110
- Métrique ?
- Σ coûts
- Lettre qui identifie ce protocole dans `sh ip route` ?
- O

RIP ou OSPF ?

- Si un routeur reçoit 2 annonces pour exactement le même sous-réseau et le même masque :
  - l'une de RIP, métrique 5
  - l'autre de OSPF, métrique 10

- Laquelle sera préférée ?
  - OSPF
  - car on compare les Distances Administratives :
    - la plus petite AD est préférée
    - 110 < 120
    - OSPF est préférable à RIP

La métrique d'OSPF 1/2

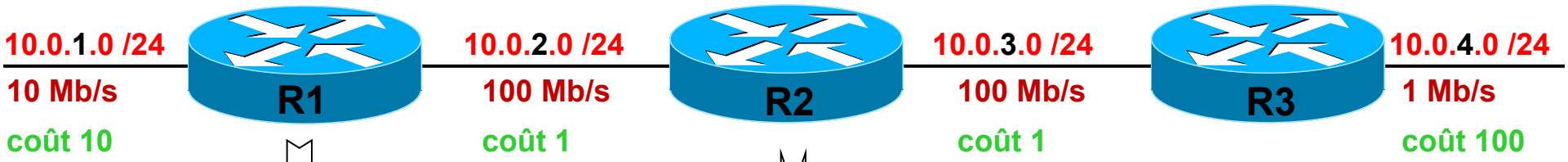
- Chaque interface a un coût :
  - BW = bande passante
  - Exprimée en **bits/s**

$$\frac{10^8}{BW}$$

- Exemples :
  - FastEthernet 100 Mb/s coût = 1
  - Ethernet 10 Mb/s coût = 10
  - 1 Mb/s coût = 100
  - Serial 1,544 Mb/s coût ≈ 65

La métrique d'OSPF 2/2

- La métrique est la somme des coûts : celui de l'interface ajouté à ceux des interfaces traversés



	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
0	10.0.3.0 /24	[110 / 2]	1+1
0	10.0.4.0 /24	[110 / 102]	1+1+100

	Réseau	[AD / m]	somme des coûts
O	10.0.1.0 /24	[110 / 11]	1+10
C	10.0.2.0 /24		
C	10.0.3.0 /24		
O	10.0.4.0 /24	[110 / 101]	1+100

Exercice 1

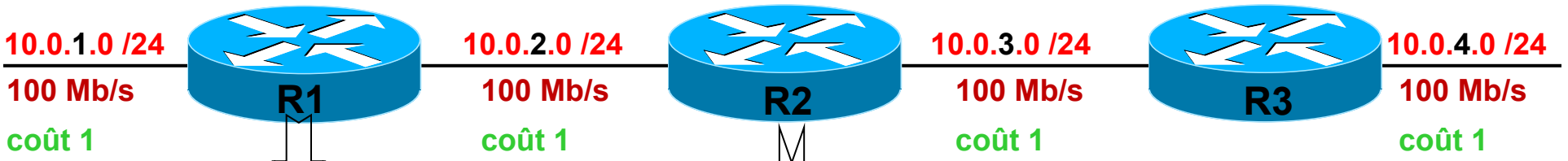
- La métrique est la somme des coûts.

	Réseau	[AD / m]
C	10.0.1.0 /24	
C	10.0.2.0 /24	
0	10.0.3.0 /24	[110 / ?]
0	10.0.4.0 /24	[110 / ?]

	Réseau	[AD / m]
O	10.0.1.0 /24	[110 / ?]
C	10.0.2.0 /24	
C	10.0.3.0 /24	
O	10.0.4.0 /24	[110 / ?]

Solution 1

- La métrique est la somme des coûts.



	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
0	10.0.3.0 /24	[110 / 2]	1+1
0	10.0.4.0 /24	[110 / 3]	1+1+1

	Réseau	[AD / m]	somme des coûts
O	10.0.1.0 /24	[110 / 2]	1+1
C	10.0.2.0 /24		
C	10.0.3.0 /24		
O	10.0.4.0 /24	[110 / 2]	1+1

Formule inadaptée

- Le coût doit être un entier.
  - Ceci pose problème pour toutes les bandes passantes supérieures à 100 Mb/s
- Exemples :
  - 100 Mb/s coût = 1
  - 1 Gb/s coût = 0,1 ramené à 1
  - 10 Gb/s coût = 0,01 ramené à 1
- Conséquence :
  - Par défaut, OSPF ne sait pas faire de distinction entre 100 Mb/s et 1 Gb/s

Adapter la formule 1/2

- On peut configurer OSPF pour qu'il adapte la formule de calcul du coût.
- Exemples :

	Formule de calcul du coût :	Le coût de 1 est attribué à :	soit :	« Reference bandwidth » =
Valeur par défaut :	$\frac{10^8}{BW}$	100 Mb/s	100 Mb/s	100
	$\frac{10^9}{BW}$	1 Gb/s	1000 Mb/s	1000
	$\frac{10^{10}}{BW}$	10 Gb/s	10,000 Mb/s	10,000

Adapter la formule 2/2

- `configure terminal`
- `router ospf 1`
  - `auto-cost reference-bandwidth` **`100`**
    - valeur par défaut
  - `auto-cost reference-bandwidth` **`1000`**
    - pour tenir compte de bandes passantes jusqu'à 1000 Mb/s, soit 1 Gb/s

Saisir cette commande sur tous les routeurs !

Exercice 2

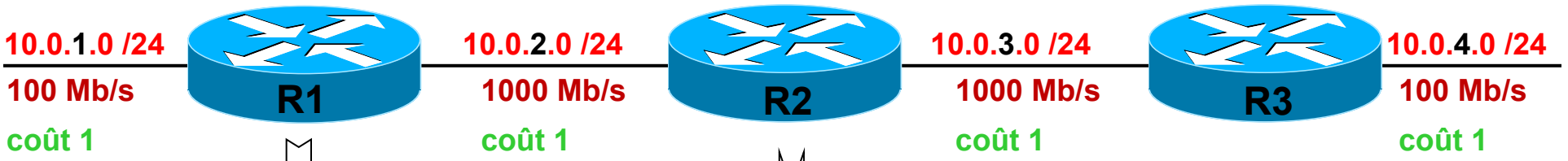
```
auto-cost reference-bandwidth 100
```

	Réseau	[AD / m]
C	10.0.1.0 /24	
C	10.0.2.0 /24	
0	10.0.3.0 /24	[110 / ?]
0	10.0.4.0 /24	[110 / ?]

	Réseau	[AD / m]
O	10.0.1.0 /24	[110 / ?]
C	10.0.2.0 /24	
C	10.0.3.0 /24	
O	10.0.4.0 /24	[110 / ?]

Solution 2

```
auto-cost reference-bandwidth 100
```



	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
0	10.0.3.0 /24	[110 / 2]	1+1
0	10.0.4.0 /24	[110 / 3]	1+1+1

	Réseau	[AD / m]	somme des coûts
O	10.0.1.0 /24	[110 / 2]	1+1
C	10.0.2.0 /24		
C	10.0.3.0 /24		
O	10.0.4.0 /24	[110 / 2]	1+1

Exercice 3

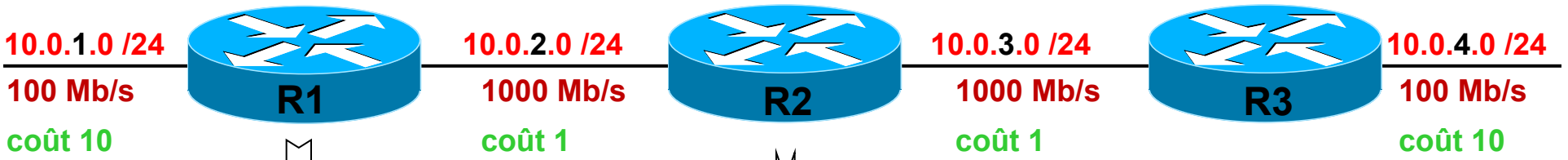
```
auto-cost reference-bandwidth 1000
```

	Réseau	[AD / m]
C	10.0.1.0 /24	
C	10.0.2.0 /24	
0	10.0.3.0 /24	[110 / ?]
0	10.0.4.0 /24	[110 / ?]

	Réseau	[AD / m]
O	10.0.1.0 /24	[110 / ?]
C	10.0.2.0 /24	
C	10.0.3.0 /24	
O	10.0.4.0 /24	[110 / ?]

Solution 3

```
auto-cost reference-bandwidth 1000
```



	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
O	10.0.3.0 /24	[110 / 2]	1+1
O	10.0.4.0 /24	[110 / 12]	1+1+10

	Réseau	[AD / m]	somme des coûts
O	10.0.1.0 /24	[110 / 11]	1+10
C	10.0.2.0 /24		
C	10.0.3.0 /24		
O	10.0.4.0 /24	[110 / 11]	1+10

Modifier le coût OSPF

- Le coût associé à une interface peut être modifié de 2 manières :
  - soit en configurant directement ce coût
  - soit en modifiant la bande passante de l'interface

Configurer le coût

```
configure terminal

interface gi0/0

ip ospf cost 10
```

Le routeur ne tiendra plus compte
de la bande passante de l'interface
pour calculer le coût de l'interface

Modifier la bande passante

```
configure terminal

interface Gi0/0

bandwidth 10 000
```

en kbit/s

Attention : d'autres protocoles seront impactés par cette modification.

Exemple : STP, EIGRP

OSPF

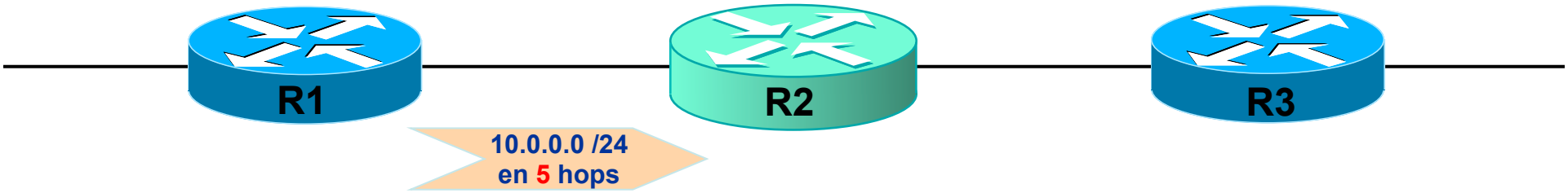
Un protocole à ETATS de LIENS : LS

« Link State »

DV et LS

- Les protocoles à Vecteur de distance envoient à leurs voisins une partie de leur table de routage.
  - cette information sera-t-elle transférée par le voisin à un tiers ?
- Les protocoles à Etat de Lien envoient à leurs voisins des données sur les réseaux auxquels ils sont connectés.
  - cette information sera-t-elle transférée par le voisin à un tiers ?

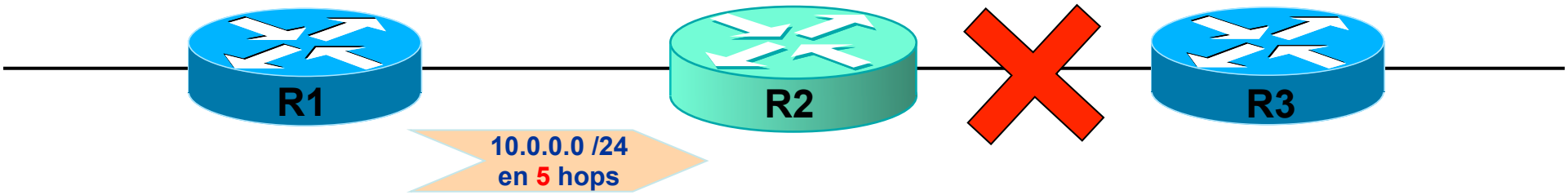
DV : Le transfert d'une annonce



1. R1 me dit que je peux atteindre le sous-réseau 10.0.0.0 /24 en 5 hops, AD 120.

2. Ai-je une meilleure route vers 10.0.0.0 /24 ?

DV : Le transfert d'une annonce



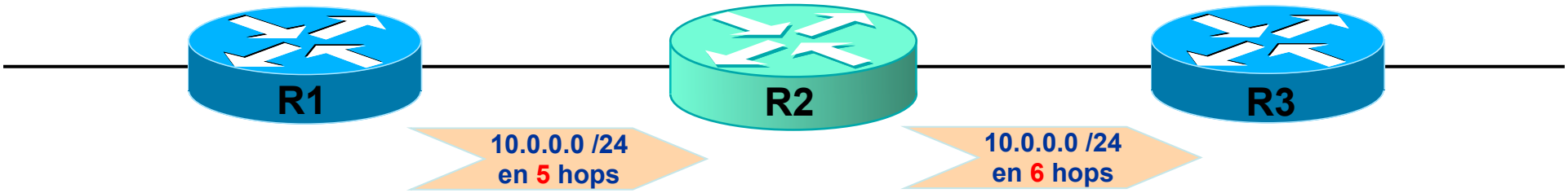
OUI : j'ai une meilleure route vers 10.0.0.0 /24 !

Je ne tiens pas compte de l'annonce reçue,

i.e. je ne modifie pas ma table de routage.

Je ne transfère pas cette annonce à R3

DV : Le transfert d'une annonce



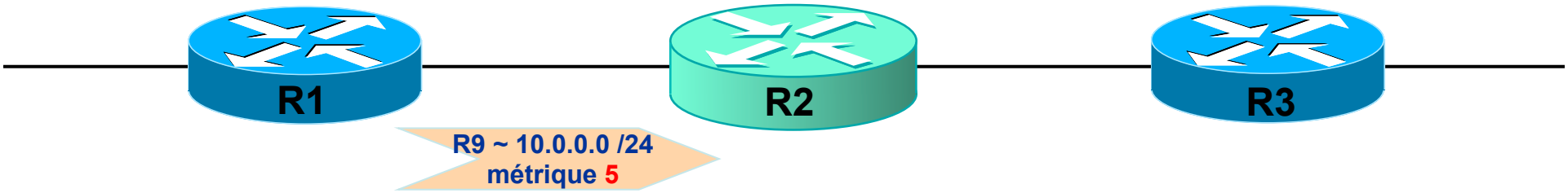
NON : je n'ai pas de meilleure route
vers 10.0.0.0 /24 !

Je tiens compte de l'annonce reçue,

i.e. j'injecte cette route dans ma table de routage.

Je transfère à R3 une annonce modifiée :
j'ai mis à jour la métrique.

LS : Le transfert d'une annonce

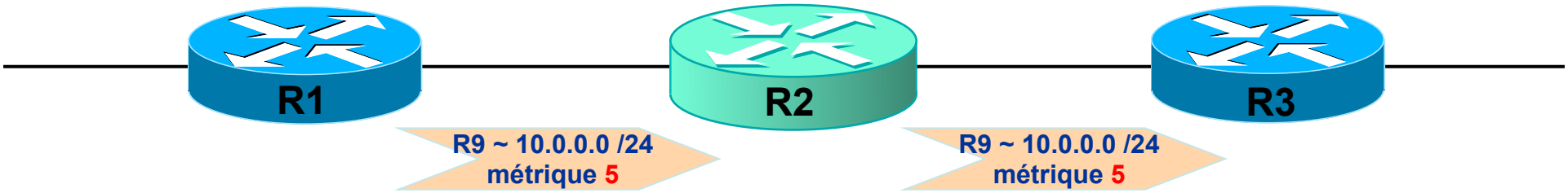


1. R1 m'envoie une annonce avec les informations suivantes :

> « le routeur R9 est connecté au sous-réseau 10.0.0.0 /24, coût du lien 5, AD 110. »

2. Je ne me pose pas la question de savoir si j'ai une meilleure route vers 10.0.0.0 /24 !

LS : Le transfert d'une annonce



J'envoie systématiquement cette information à mes voisins, sans la modifier (*) :

« le routeur R9 est connecté au sous-réseau 10.0.0.0 /24, coût du lien 5, AD 110. »

(*) des exceptions sont étudiées niveau CCNP

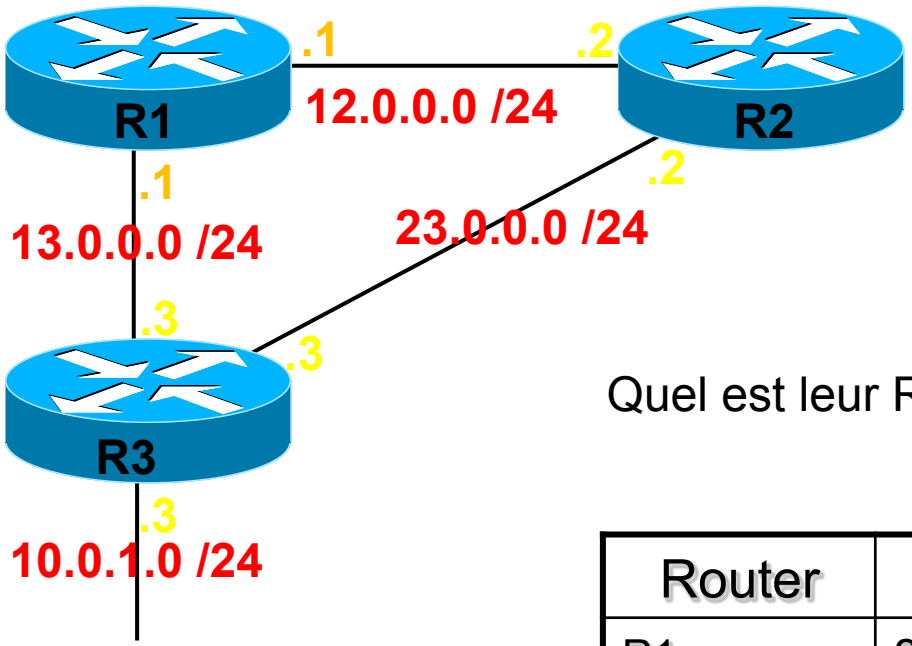
LS : les annonces

- Ces annonces s'appellent des LSA :
  - Link State Advertisement
- Elles contiennent :
  - l'identité du routeur qui a généré l'annonce
    - le ROUTER-ID
  - le sous-réseau annoncé
  - le masque de sous-réseau
  - la distance administrative
  - le coût du lien
  - etc….

Router-ID

- C'est une adresse IP.
- Le Router-ID peut être configuré manuellement :
  - `conf t`
  - `router ospf 1`
    - `router-ID 1.1.1.1`
- Sinon, il sera calculé automatiquement :
  - Existe-t-il une interface LOOPBACK ?
  - Si OUI, alors
    - le Router-ID = la plus grande adresse IP des interfaces Loopback.
  - Si NON, alors
    - le Router-ID = la plus grande adresse IP des interfaces UP

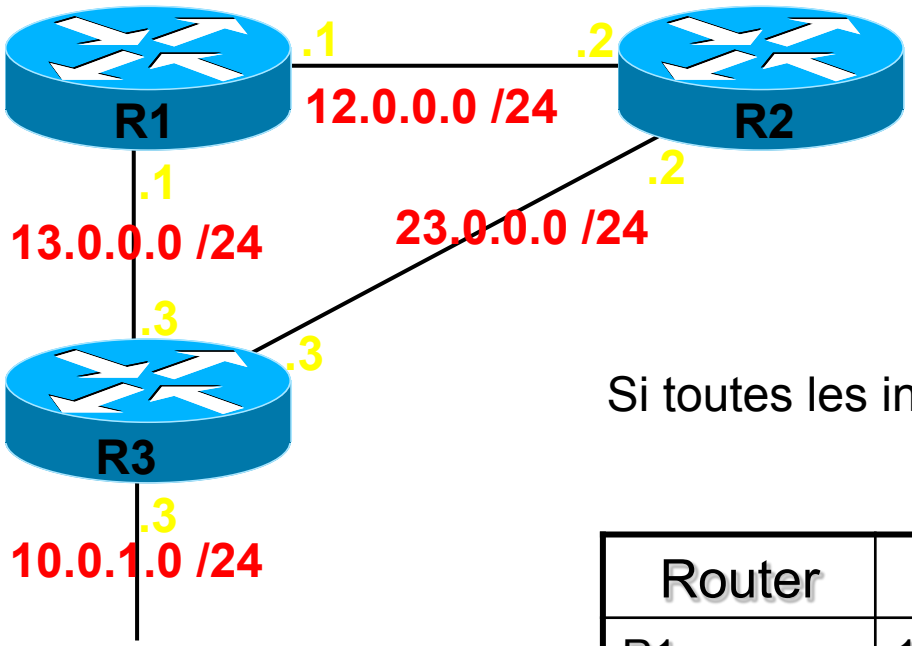
Exercice 1



Quel est leur Router-ID ?

Router	Router-ID
R1	?
R2	?
R3	?

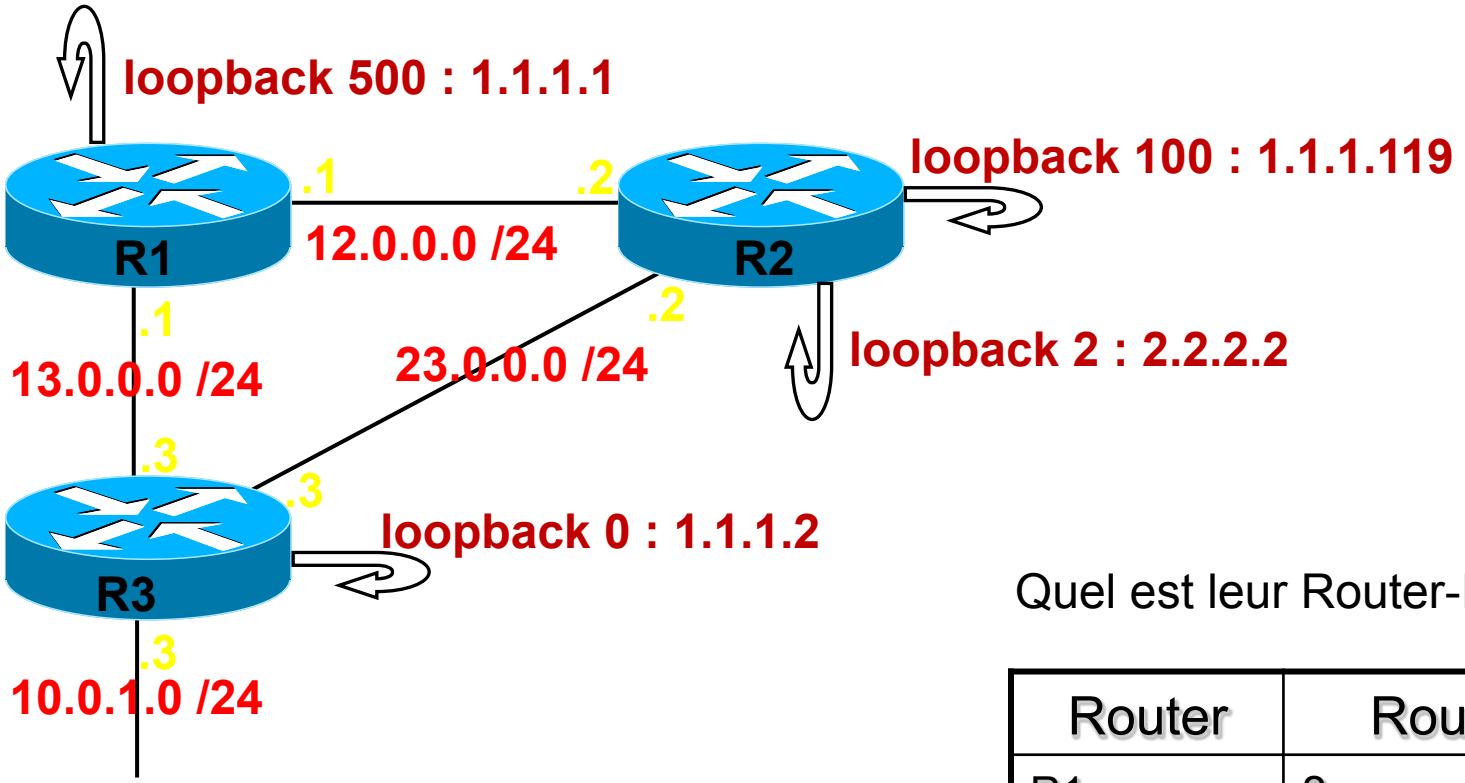
Solution 1



Si toutes les interfaces sont UP :

Router	Router-ID
R1	13.0.0.1
R2	23.0.0.2
R3	23.0.0.3

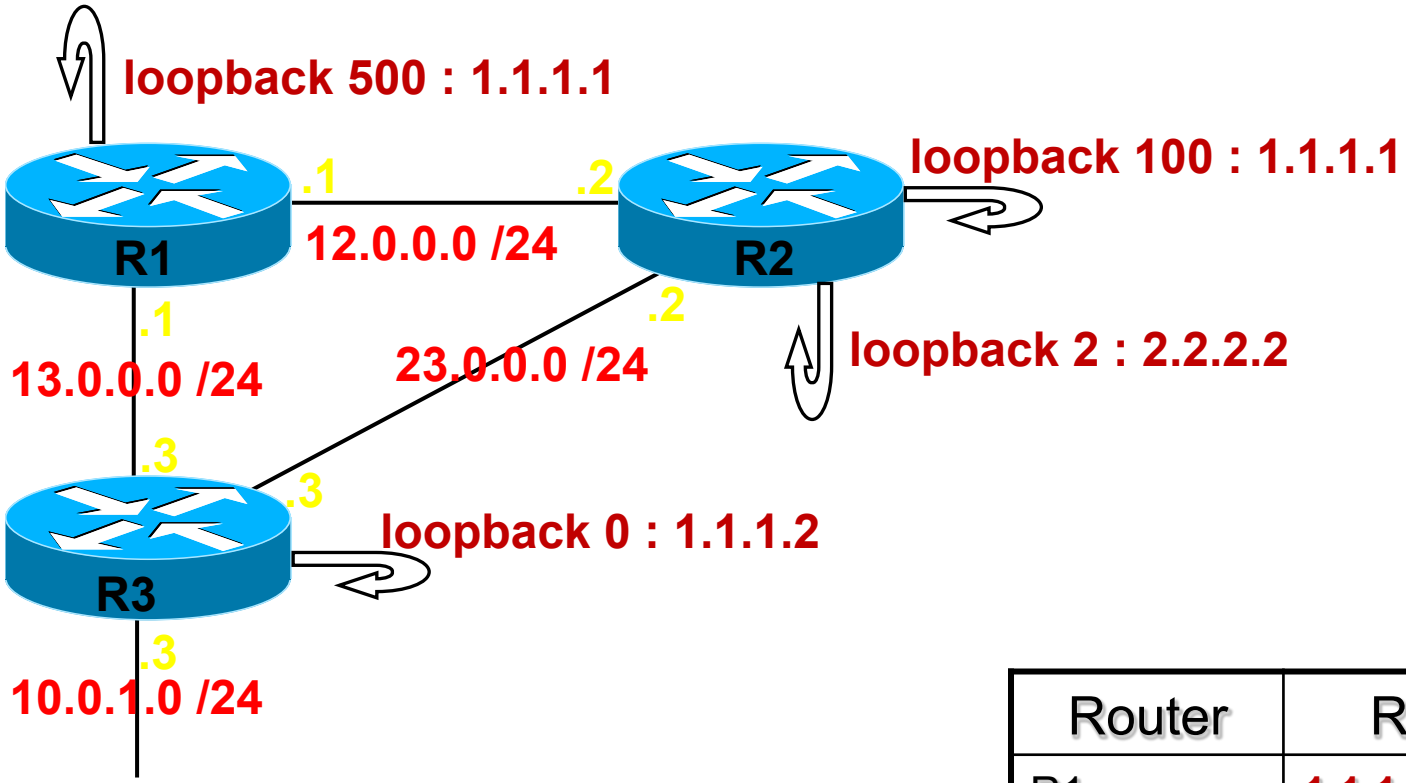
Exercice 2



Quel est leur Router-ID ?

Router	Router-ID
R1	?
R2	?
R3	?

Solution 2



Router	Router-ID
R1	1.1.1.1
R2	2.2.2.2
R3	1.1.1.2

Quelque soit l'état des interfaces physiques !

LSA

- Pourquoi les LSA sont-ils systématiquement envoyés à tous les voisins ?
- Pour que chaque routeur puisse construire la topologie globale du réseau.
- Les protocoles à états de liens ne se basent pas sur des rumeurs :

1. Chacun identifie ses voisins (routeur directement connecté)
2. Chacun construit la cartographie du réseau.
3. Chacun applique ensuite un algorithme pour décider du chemin qu'il prendra pour atteindre les sous-réseaux annoncés.

Ressources

- Mémoriser la cartographie :
  - nécessite de la RAM
- Appliquer un algorithme :
  - nécessite du CPU

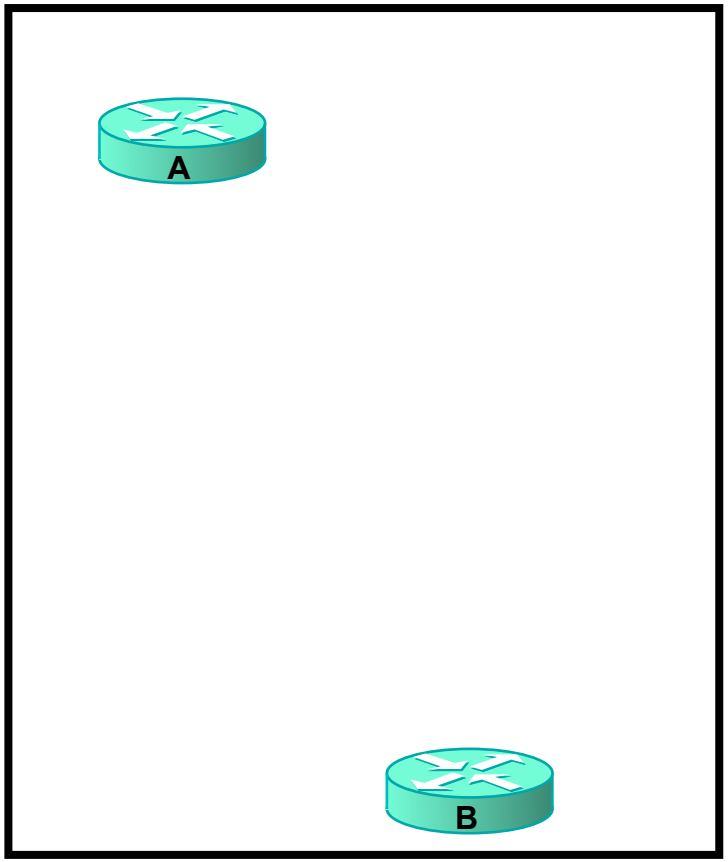
Problèmes pour « grands » réseaux.

Solution :
découper la réseau en plusieurs AIRES

OSPF

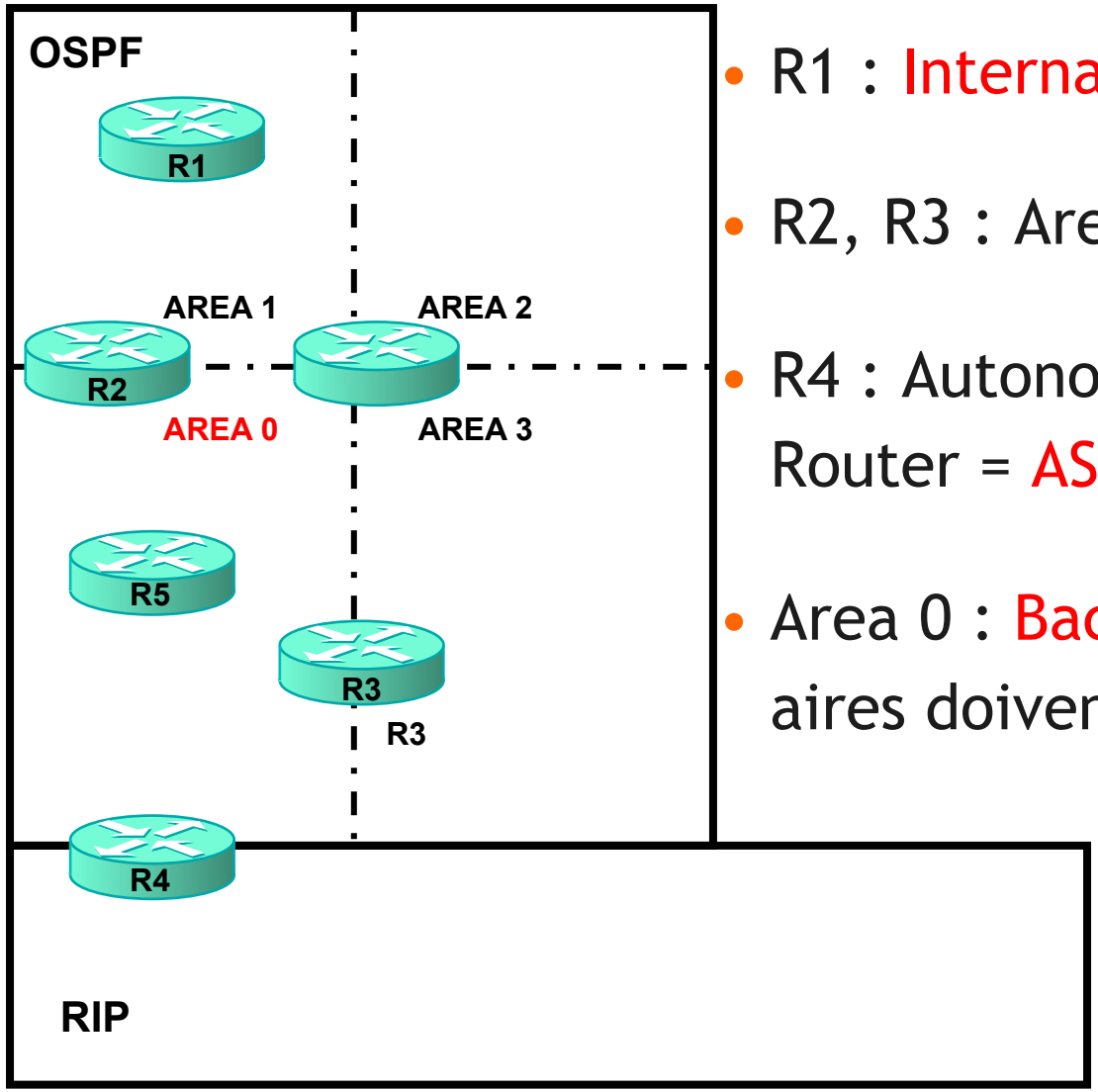
Optimiser les ressources

Sans aires



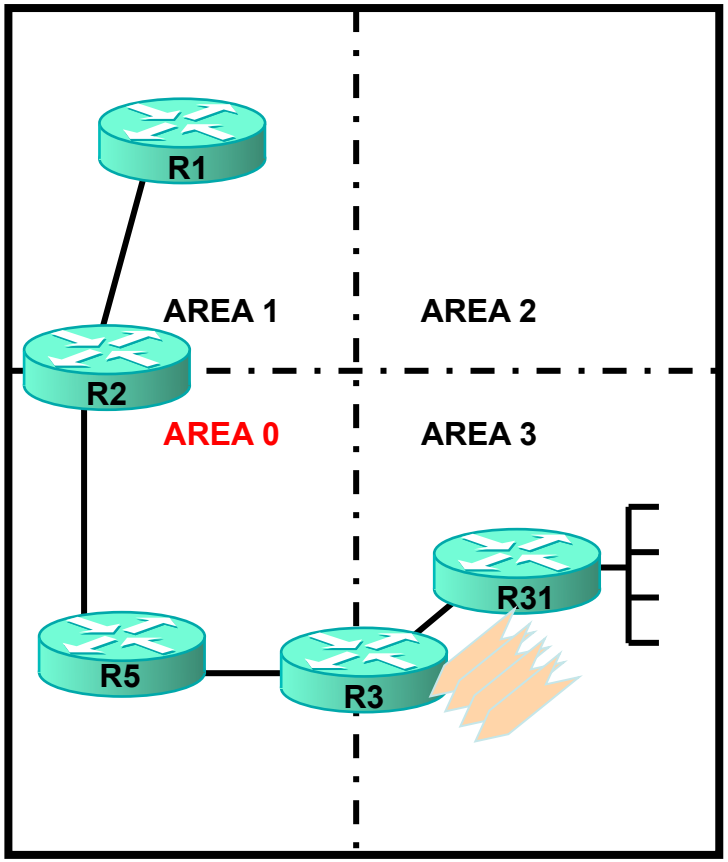
- A et B auront en mémoire la même cartographie, i.e. TOUT le réseau.
- A et B devront appliquer l'algorithme à toute la cartographie, i.e. TOUS les sous-réseaux.

Rôles



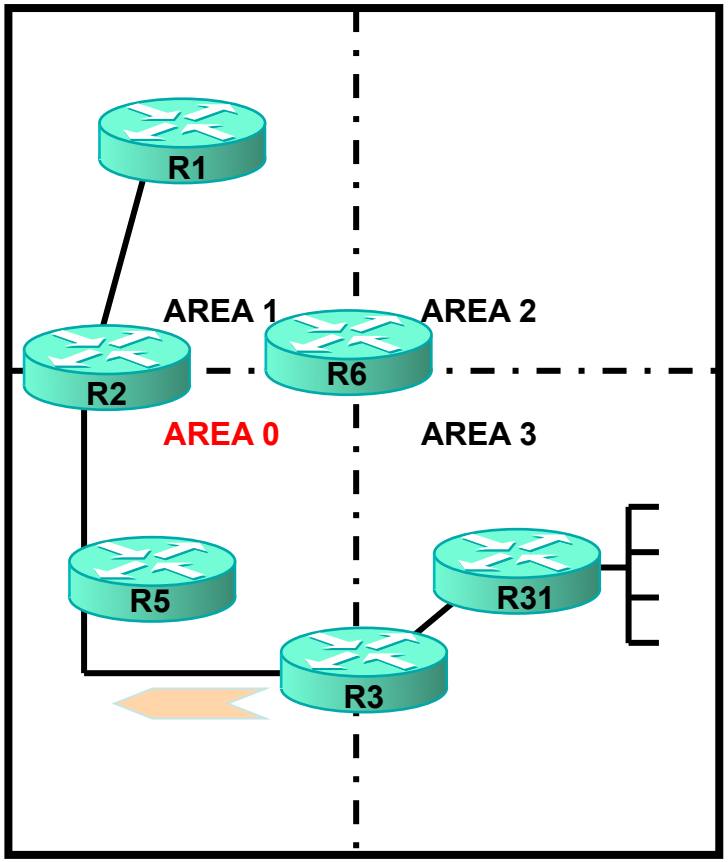
- R1 : Internal Router.
- R2, R3 : Area Border Router = ABR.
- R4 : Autonomous Sytem Border Router = ASBR.
- Area 0 : Backbone = toutes les autres aires doivent lui être rattachées.

Intérêts des Aires 1/3



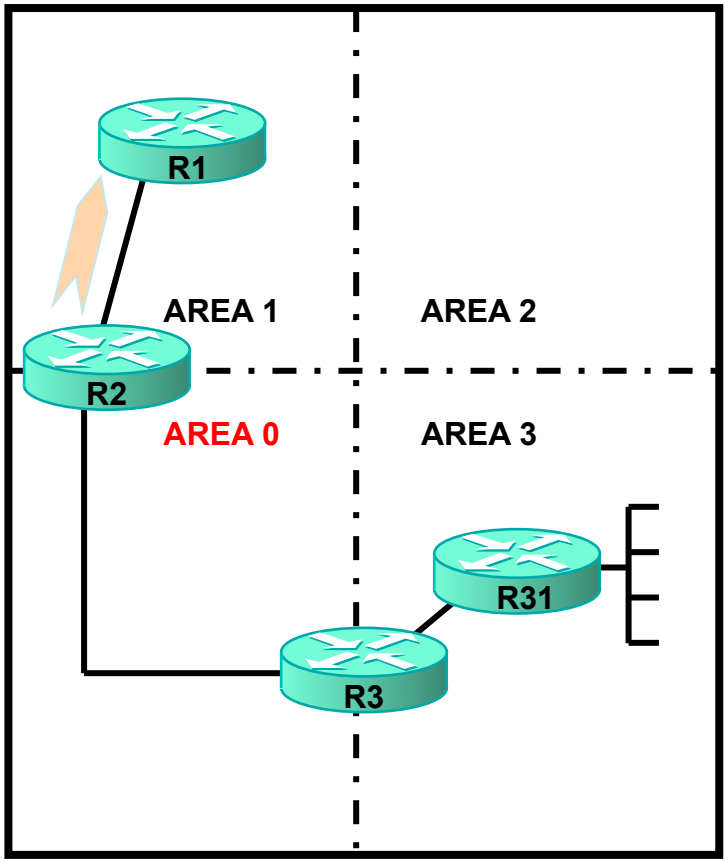
- R31 (internal) va générer au moins 4 LSA, une pour chacun de ses 4 sous-réseaux.

Intérêts des Aires 2/3



- R3 (ABR) va résumer les 4 sous-réseaux en un seul sous-réseau.

Intérêts des Aires 3/3



- R1 (internal) n'aura donc qu'une seule LSA pour ces 4 sous-réseaux.
  - Moins de RAM nécessaire pour conserver en mémoire la cartographie du réseau
  - Moins de CPU nécessaire pour exécuter l'algorithme
    - si bagotage d'un des 4 sous-réseaux, aucun impact sur la summary.
    - l' instabilité est donc confinée à une seule aire
  - Pas de perte de connectivité
  - Convergence plus rapide

Le Masque Inversé

Le masque inversé (1 octet)

- Chaque **bit** est inversé, un par un.

- Exemple sur 1 octet :

Masque normal	1	1	1	1	1	0	0	0
Masque inversé	0	0	0	0	0	1	1	1

Exercice

- Inverser :

255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Solution

- Réponse :

0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	1
3	0	0	0	0	0	0	1	1
7	0	0	0	0	0	1	1	1
15	0	0	0	0	1	1	1	1
31	0	0	0	1	1	1	1	1
63	0	0	1	1	1	1	1	1
127	0	1	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1

Formule d'inversion sur 1 octet

Masque normal	Masque inversé
255	0
254	1
252	3
248	7
240	15
224	31
192	63
128	127
0	255

Masque normal

+

Masque inversé

=

255

Le masque inversé (4 octets)

- Chaque **octet** est inversé, un par un.
- Exemple sur 4 octets:

Masque normal	255	255	255	128
Masque inversé	0	0	0	127

OSPF

Configuration

Lancer OSPF

- `configure terminal`
- `router ospf` **1**

signifie :

« lancer sur ce routeur un process OSPF
et attribuer le numéro de process **1** »

- on peut lancer plusieurs process OSPF sur un même routeur
- le numéro de process a une portée **LOCALE**
  - il n'est PAS nécessaire que deux routeurs voisins utilisent le même numéro de process.
  - Il est compris entre 1 et 65 535

Activer OSPF sur une interface

- `configure terminal`
- `interface fa0/0`
- `ip ospf 1 area 0`

signifie :

« activer le process OSPF 1 sur cette interface
et la positionner dans l'aire 0 »

Activer OSPF sur une interface

Autre commande :

- `configure terminal`
- `router ospf 1`
- `network 10.0.0.0 0.0.0.255 area 0`

masque inversé

signifie :

« activer OSPF sur toute interface dont l'adresse IP est 10.0.0.X et positionner cette interface dans l'aire 0»

Masques « extrêmes »

- Activer sur TOUTES les interfaces en une seule commande :
  - `network 0.0.0.0 255.255.255.255 area 0`

- Activer sur UNE SEULE interface :
  - `network 1.1.1.1 0.0.0.0 area 0` activer sur 1.1.1.1
  - `network 2.2.2.2 0.0.0.0 area 0` activer sur 2.2.2.2

Vérifier les interfaces OSPF

Vérifier sur quelles interfaces OSPF est activé :

```
R1(config)#router ospf 1

R1(config-router)#network 0.0.0.0 255.255.255.255 area 0

(ou network 0.0.0.0 0.0.0.0 area 0)

R1#show ip ospf interface brief

Interface    PID   Area    IP Address/Mask    Cost  State Nbrs
  F/C

Fa1/0        1     0       13.0.0.1/24        1     BDR   1/1

Fa0/0        1     0       12.0.0.1/24        1     BDR   1/1
```

Process ID

Bande passante = 100 Mb/s
(si 'reference-bandwidth' par défaut)

Que signifie « Activer » ?

« Activer OSPF sur une interface »

signifie :

le routeur va chercher des voisins OSPF
sur cette interface.

Il échangera ensuite des LSA
avec tous ces voisins.

OSPF

Recherche de voisins

TROIS étapes

ETAPE 1	ETAPE 2	ETAPE 3
Objectif : Découvrir tous mes voisins directs.	*Objectif :* Construire la cartographie du réseau.	*Objectif :* Décider du chemin le plus court pour atteindre chaque sous-réseau annoncé.

Deux méthodes

Est-ce que les multicast sont autorisés sur cette interface ?

- Si OUI :
  - recherche automatique des voisins
  - utiliser l'adresse IP multicast 224.0.0.5.

- Si NON :
  - recherche manuelle des voisins

Recherche automatique

- Le routeur envoie des paquets HELLO sur l'interface :
  - envoyés à fréquence fixe :
    - selon la valeur du **timer 'HELLO'**
      - configurable
    - par défaut :
      - HELLO = 10 sec. sur un réseau 'broadcast' (Exemple : Ethernet)
      - HELLO = 30 sec. sur un réseau 'NBMA' (Exemple : Frame Relay)
  - ont une durée de vie limitée :
    - selon la valeur du **timer 'DEAD'**
      - configurable
    - par défaut :
      - DEAD = HELLO x 4
      - 40 secondes sur un réseau 'broadcast'
      - 120 secondes sur un réseau 'NBMA'

Configurer un timer

- `configure terminal`
- `interface fa0/0`
- `ip ospf hello-interval 5`
  - » entre 1 et 65535 sec.
    - Si vous changez la valeur de Hello, l'IOS adapte automatiquement celle du Dead :
      - » Dead = Hello x 4
- `ip ospf dead-interval 30`
  - » entre 1 et 65535 sec.

Vérifier le timer

```
sh ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 12.0.0.1/24, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
    Wait time before Designated router selection 00:00:29
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Le paquet HELLO

- Il est envoyé à l'adresse IP destination : 224.0.0.5
- Il contient les infos suivantes :
  - mon Router-ID
  - l'AREA de mon interface
  - la valeur de mon timer HELLO
  - la valeur de mon timer DEAD
  - les Router-ID de tous les voisins que j'ai déjà identifiés
  - etc…

La relation de voisinage

- Si je reçois un paquet HELLO avec :
  - la même valeur de AREA que la mienne
  - la même valeur du timer HELLO que le mien
  - la même valeur du timer DEAD que le mien
- Alors je reconnais cet individu comme un voisin :
  - je rajoute son Router-ID dans ma liste des voisins

La relation ’TWO-WAY’

- Si je reçois un paquet HELLO dans lequel je vois mon propre Router-ID :
  - ce voisin m’a reconnu comme voisin.

- Deux équipements qui se reconnaissent mutuellement comme voisins ont une relation dite ’TWO-WAY’

Réseaux NBMA

- Certains réseaux n'autorisent pas le multicast.
- Il faut alors configurer manuellement chaque voisin :

```
configure terminal
router ospf 1
neighbor 3.3.3.3
```

Adresse IP du voisin

Cinq types de paquets OSPF

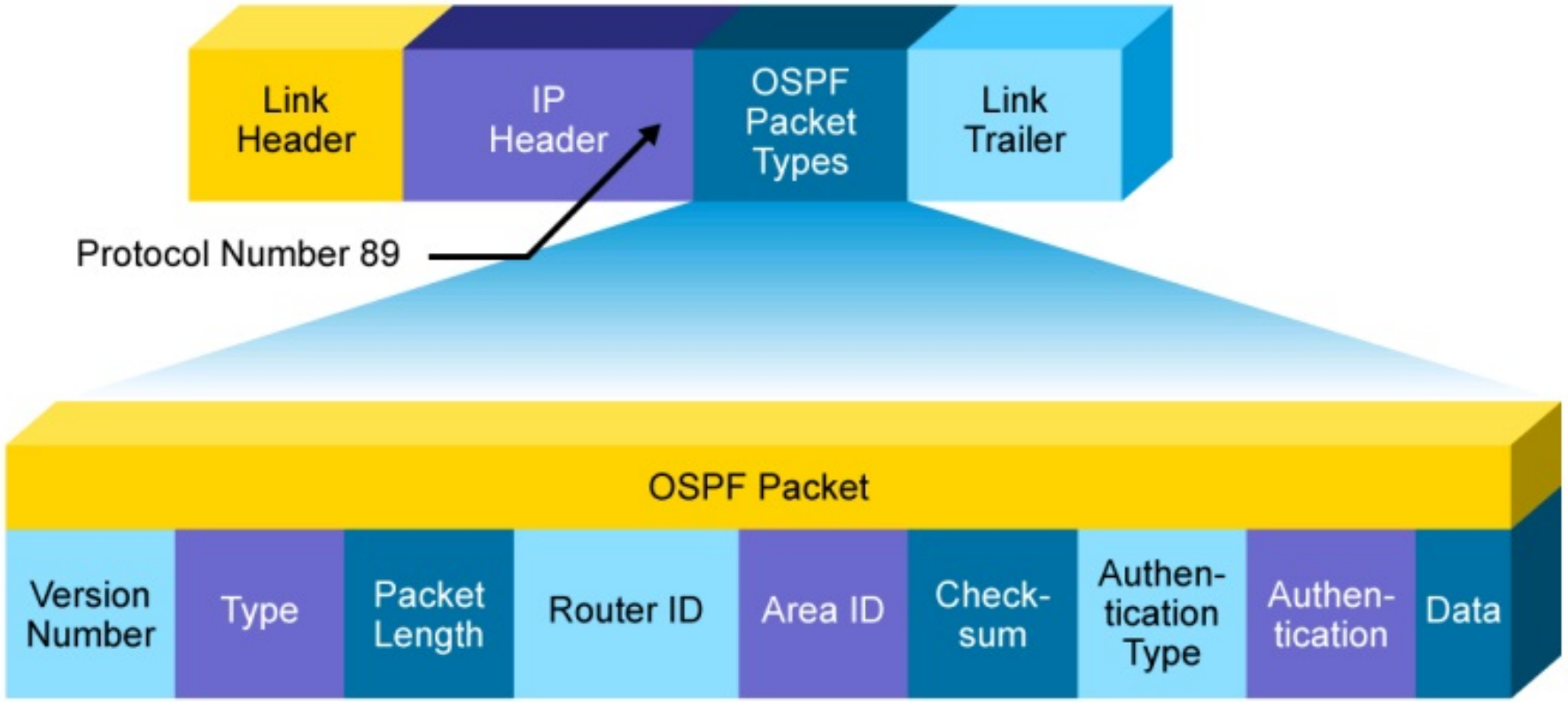
1. HELLO
2. DBD
   - Database Description
3. LSR
   - Link State Request
4. LSU
   - Link State Update
     - Contient les LSA = Link state advertisement
5. LSAck
   - Link State Acknowledgment

Format du paquet OSPF

- Encapsulé dans un paquet IP
  - Protocole n°89

- Contient les champs suivants :
  - N° de version = 2
  - Type de paquet = entre 1 et 5
  - Longueur du paquet
  - Router ID du routeur ayant généré ce paquet
  - Area ID dans lequel ce paquet a été généré
  - Checksum
  - Type authentification (none, clear, MD5)
  - Authentification (le mot de passe ou le hash)
  - Data

OSPF Packet Header Format



Le paquet HELLO

- Router-ID
- Hello timer
- Dead timer
- Liste des routers ID des voisins découverts
- Area ID
- Router priority
- Adresse IP du DR
- Adresse IP du BDR
- Authentification
- Stub area

OSPF

La cartographie

TROIS étapes

ETAPE 1	ETAPE 2	ETAPE 3
Objectif : Découvrir tous mes voisins directs.	*Objectif :* Construire la cartographie du réseau.	*Objectif :* Décider du chemin le plus court pour atteindre chaque sous-réseau annoncé.

Echanges des LSA

- Dès que deux voisins sont 'TWO-WAY', ils commencent à s'envoyer tous leurs LSA.

- Lorsque l'échange est terminé, ils deviennent 'FULL' :

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
34.0.0.3          1   FULL            00:00:39    13.0.0.3        FastEthernet1/0
24.0.0.2          1   FULL            00:00:39    12.0.0.2        FastEthernet0/0
```

Le statut 'FULL'

- Ce statut indique que les 2 voisins ont maintenant la même vision du réseau, i.e. la même cartographie.
- La commande `show ip ospf database` permet de voir la cartographie du réseau.
- Cette commande donnera donc le même résultat sur les 2 voisins, pour l'aire dans laquelle sont configurées leurs interfaces.

Timers

- Tant qu'il n'y a pas de modification de topologie, je n'envoie que des paquets HELLO toutes les 10 sec.

- Chaque LSA est également renvoyé toutes les 30 minutes, pour une meilleure synchronisation des bases de données.

OSPF

L’algorithme

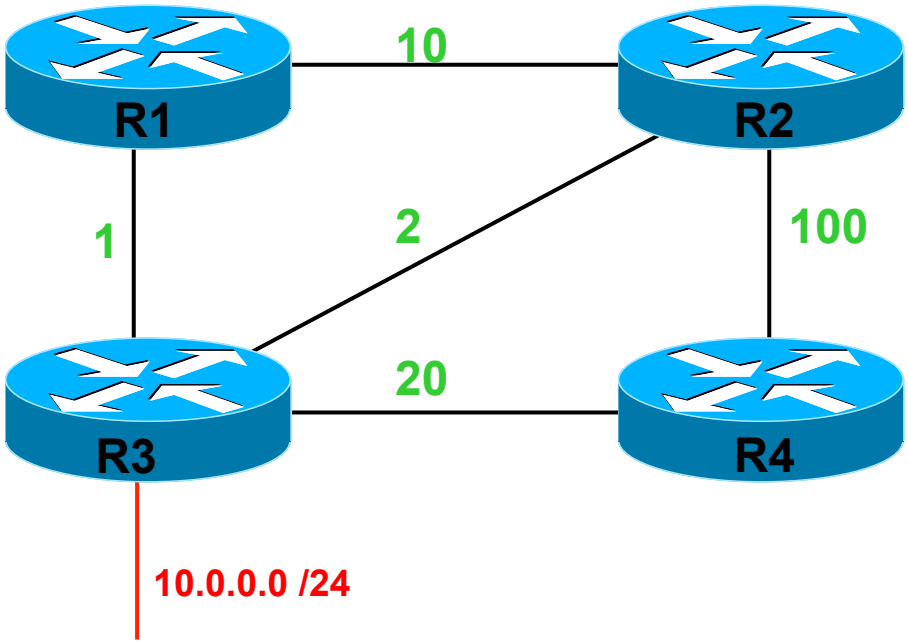
TROIS étapes

ETAPE 1	ETAPE 2	ETAPE 3
Objectif : Découvrir tous mes voisins directs.	*Objectif :* Construire la cartographie du réseau.	*Objectif :* Décider du chemin le plus court pour atteindre chaque sous-réseau annoncé.

Dijkstra

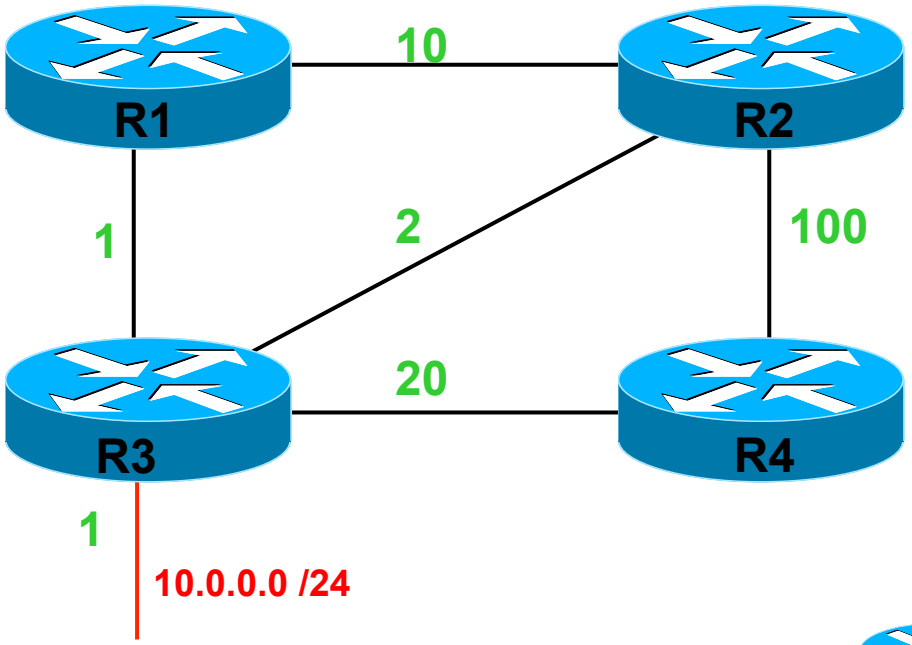
- Egalement appelé algorithme SPF : Shortest Path First
- Déterminer le chemin le plus court pour atteindre chaque réseau annoncé.
- Injecter ce chemin dans la table de routage, si pas de meilleur chemin déjà présent.

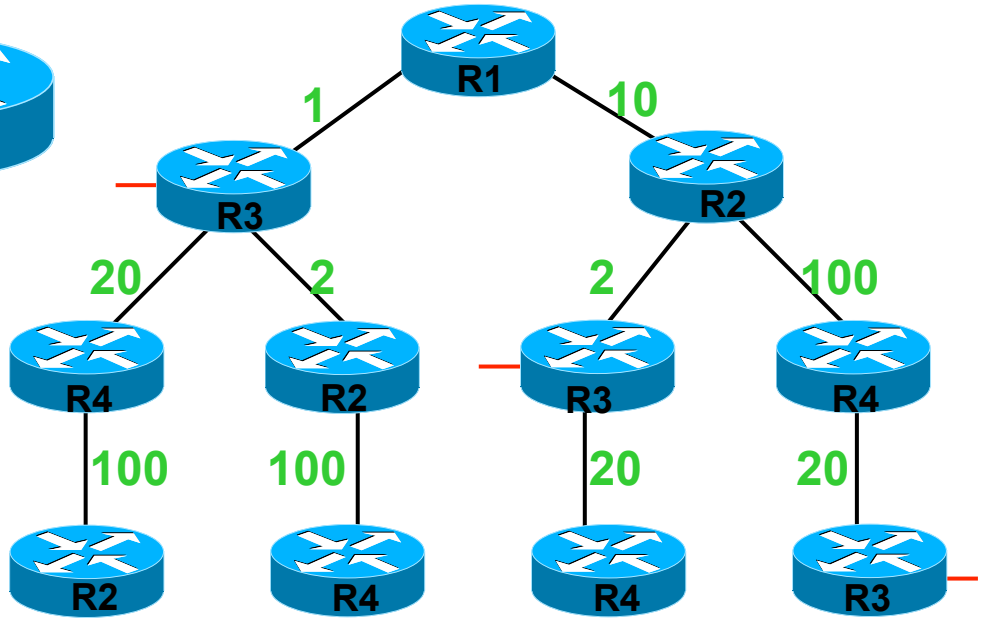
Exemple de topologie



Pour R1, quel est le chemin le plus court pour aller vers 10.0.0.0 /24 ?

Exemple d'application de l'algorithme Dijkstra



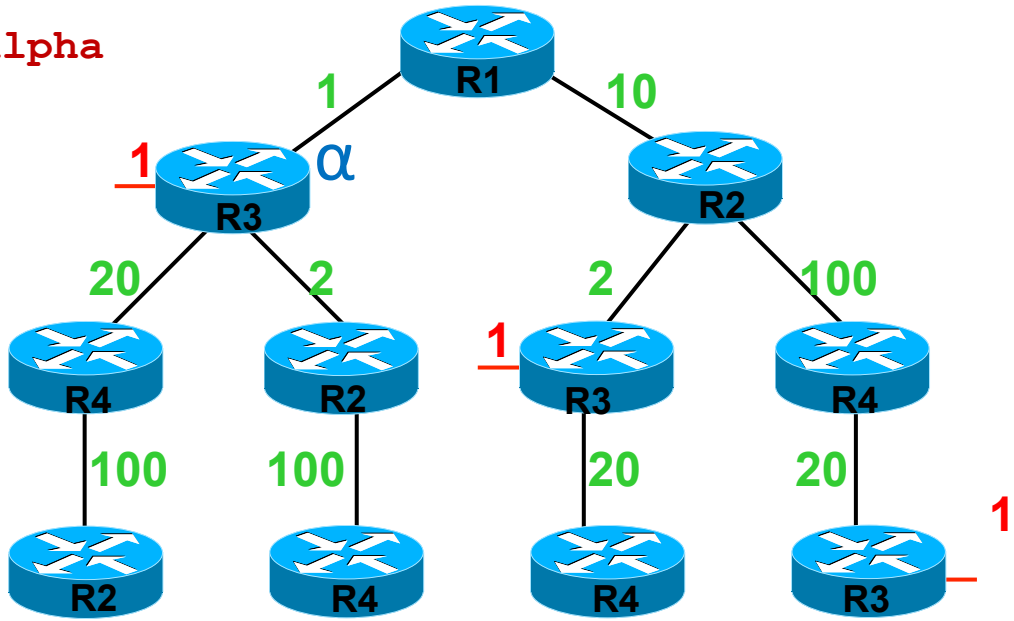


Métrique = somme des coûts

Le coût est égal à celui de l'interface ajouté de ceux des interfaces traversés.

Le chemin le plus court est injecté dans la table de routage, si elle ne contenait pas de meilleur chemin :

```
show ip route
O       10.0.0.0/24 [110/2] alpha
```



Vérifier les 3 étapes

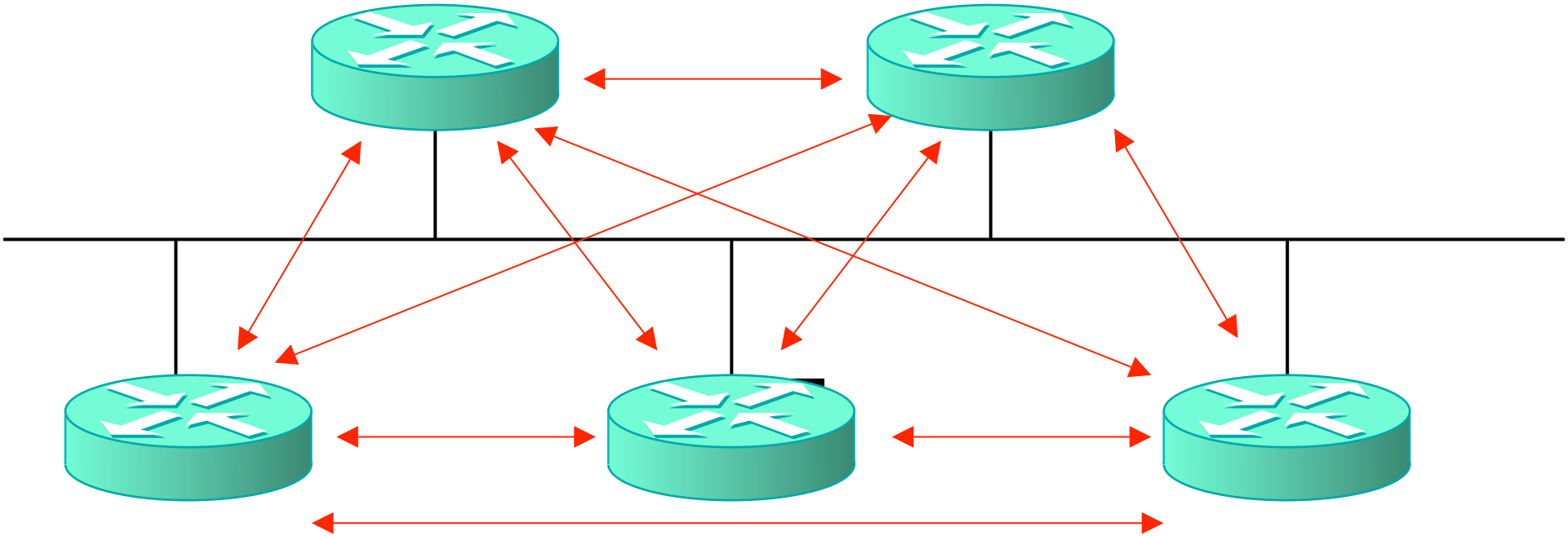
ETAPE 1	ETAPE 2	ETAPE 3
`show ip ospf neighbor`	`show ip ospf database`	`show ip route ospf`

OSPF

Optimisation

DR et BDR

10 relations 'FULL'

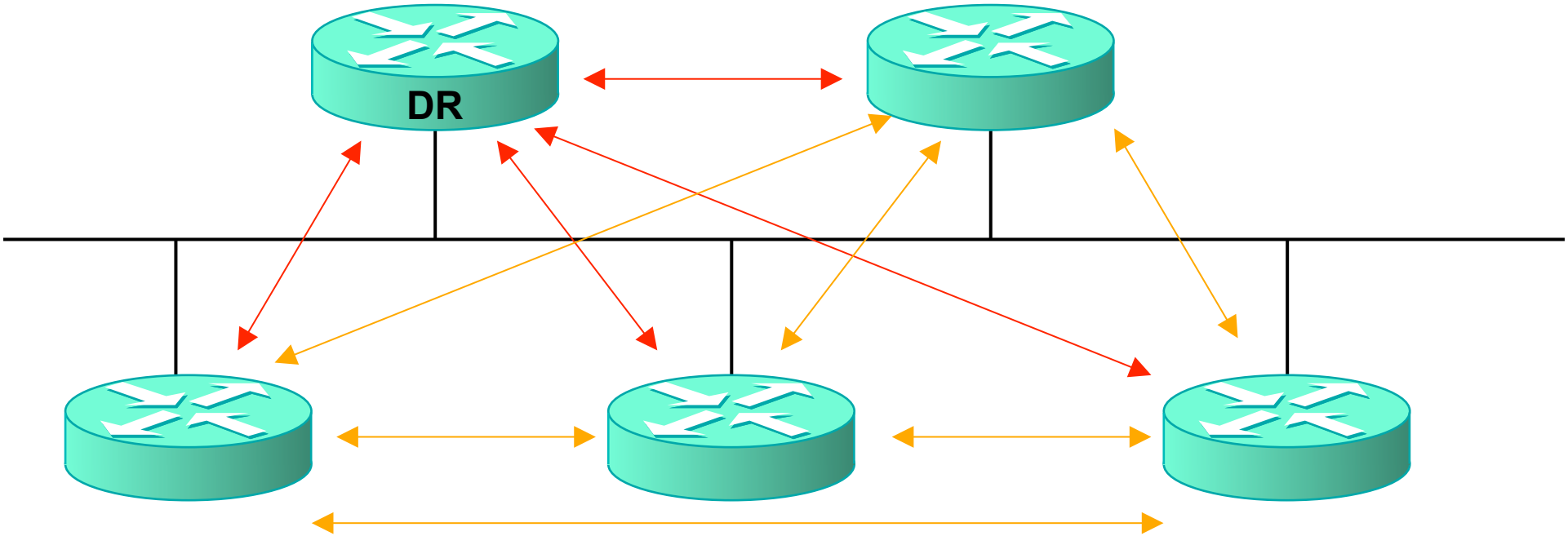


Avec 5 routeurs sur un même segment :

- Chaque routeur a 4 voisins.
- Il est 'FULL' avec chacun des 4 voisins.

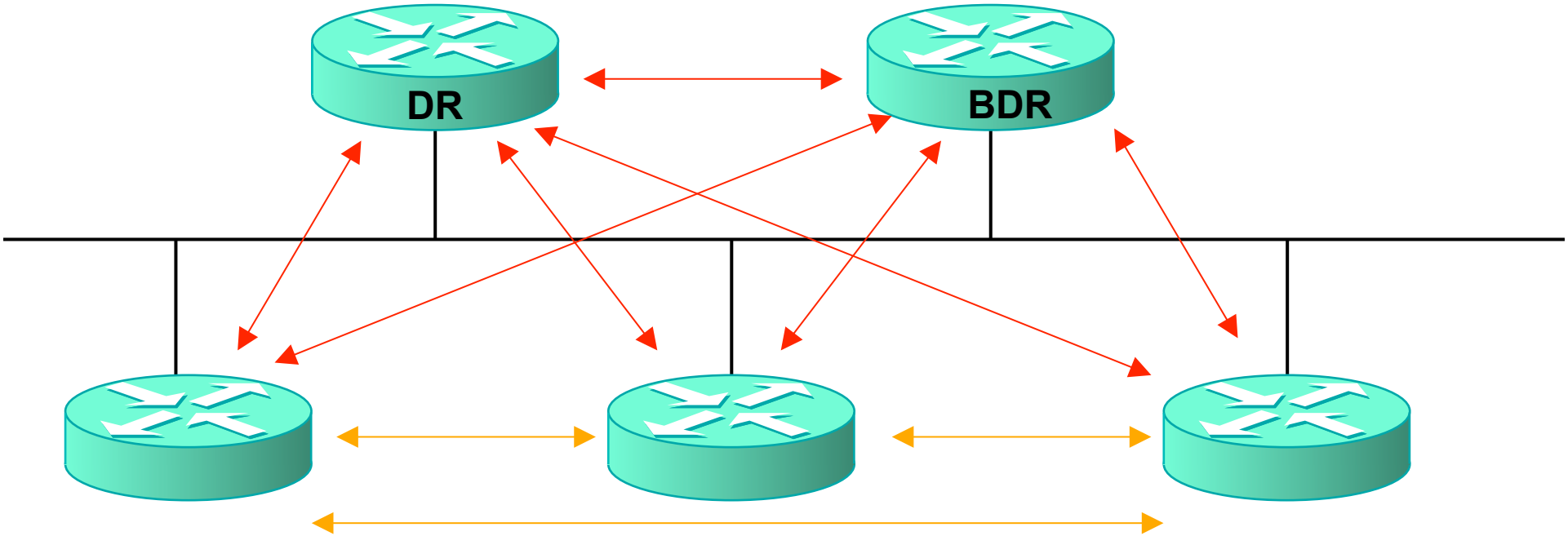
Avec N routeurs :

4 relations 'FULL'



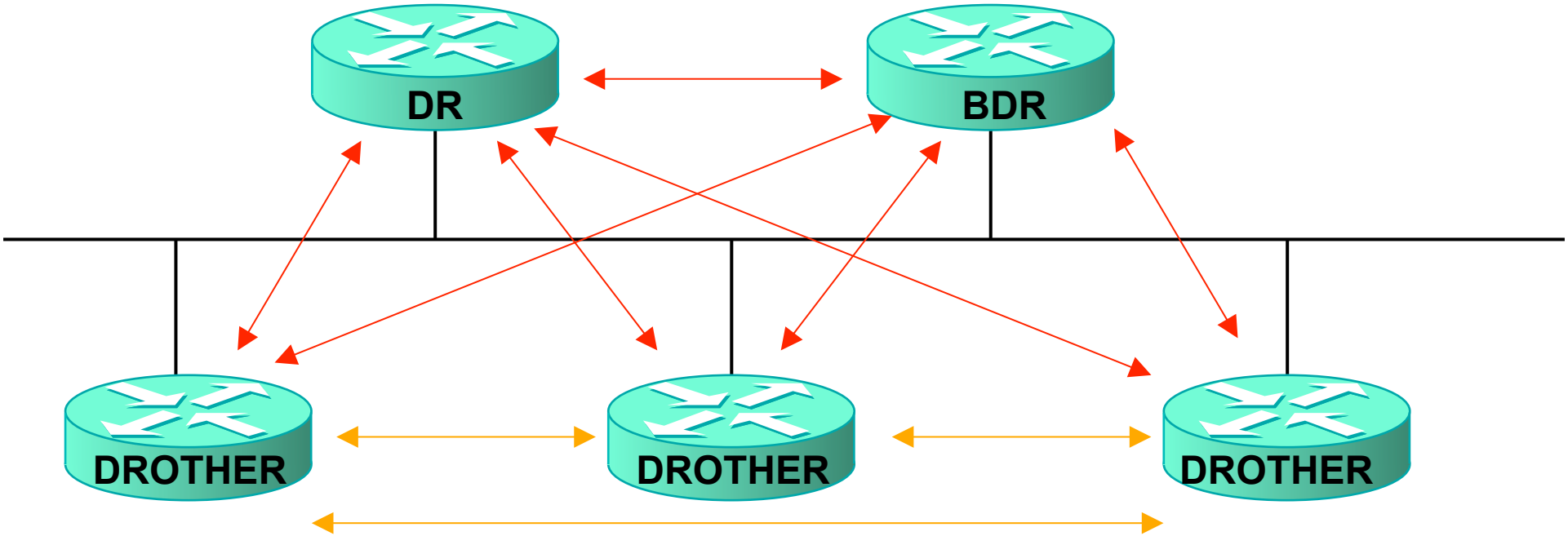
- Un routeur joue le rôle de compilateur :
  - DR = Designated Router.
- Tous les routeurs sont 'FULL' avec les DR.
- Les autres relations de voisinage sont 'TWO-WAY'.

7 relations 'FULL'



- Et si le DR tombe en panne ?
  - Un autre routeur joue le rôle de back-up du DR : BDR
  - Tous les routeurs sont 'FULL' avec les BDR.
  - Les autres relations de voisinage sont 'TWO-WAY'.

Configuration finale



- 1 DR
- 1 BDR
- Les autres sont 'DROTHER'.

Priorité OSPF

- Chaque interface a une priorité.
- Par défaut, la priorité est égale à 1.
- Configurable entre 0 et 255 :
  - `configure terminal`
  - `interface fa0/0`
  - `ip ospf priority 2`

Le choix du DR

- Le DR est celui …

  dont la priorité est la plus grande.

une priorité de 0 signifie que
ce routeur n'est pas éligible en tant que DR ni BDR

- En cas d'égalité, le DR est celui …

  dont le Router-ID est le plus grand.

le Router-ID est unique

Le choix du DR n'est pas préemptif !

Deux adresses multicast

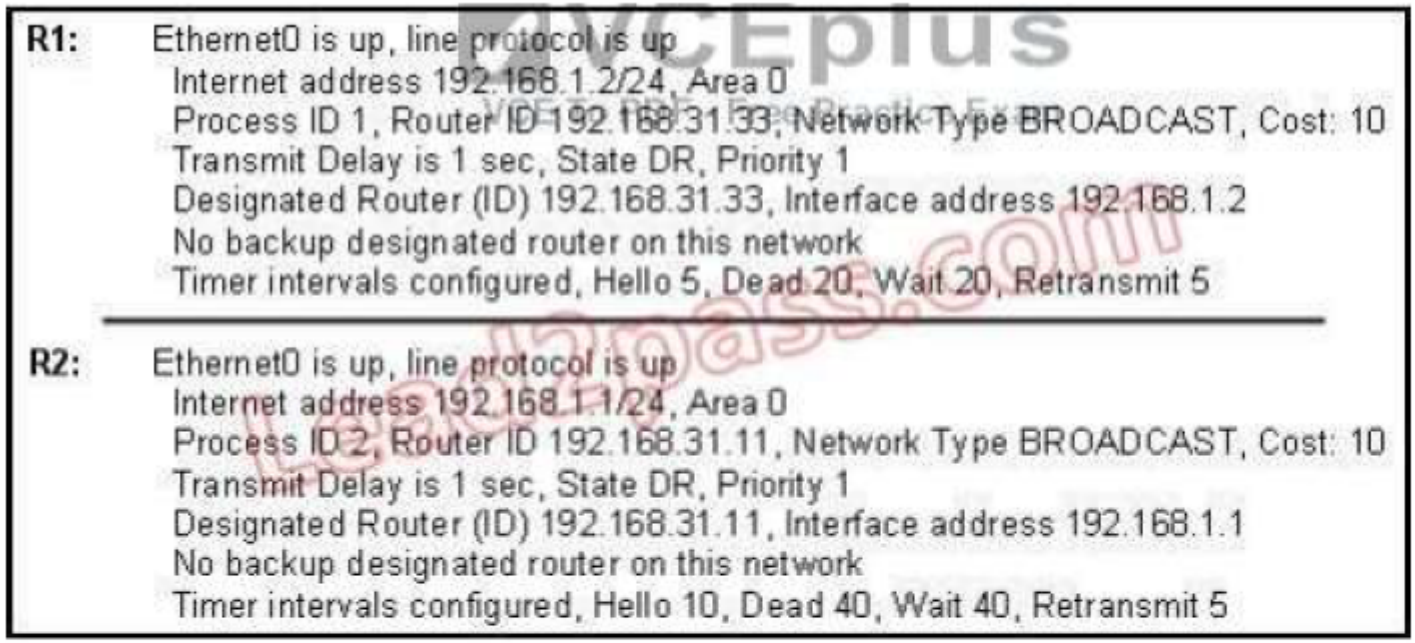
- Les DR et BDR écoutent sur 224.0.0.6
- Tous les routeurs OSPF écoutent sur 224.0.0.5

- Pour communiquer avec le DR ou BDR, j'utilise 224.0.0.6
- Pour communiquer avec tout voisin OSPF, j'utilise 224.0.0.5

La route par défaut

- Aucune route par défaut n'est injectée par défaut.
- Un routeur peut annoncer une route par défaut :
  - `default-information originate`
    - uniquement si le routeur a lui-même une route par défaut
  - `default-information originate always`
    - même si le routeur n'a pas de route par défaut
  - `default-information originate metric 10`
    - pour préférer une route par défaut par rapport à une autre
- Le routeur anonçant la route par défaut devient alors un ASBR.

A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link.



The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

A. The OSPF area is not configured properly.
B. The priority on R1 should be set higher.
C. The cost on R1 should be set higher.
D. The hello and dead timers are not configured properly.
E. A backup designated router needs to be added to the network.
F. The OSPF process ID numbers must match.

Correct Answer: D

Which three statements about link-state routing are true? (Choose three.)

A. OSPF is a link-state protocol.
B. Updates are sent to a broadcast address.
C. It uses split horizon.
D. Routes are updated when a change in topology occurs.
E. RIP is a link-state protocol.
F. Updates are sent to a multicast address by default.

Correct Answer: ADF

Routage EIGRP

EIGRP

Enhanced Interior Gateway Routing Protocol

Carte d'identité d'EIGRP

- Standard ou Propriétaire ?
  - Propriétaire CISCO
- IGP / EGP ?
  - IGP
- DV ou LS ?
  - Advanced DV - Hybrid
- AD ?
  - 90
- Lettre qui identifie ce protocole dans `sh ip route` ?
  - D
- Envois en broadcast ou multicast ?
  - 224.0.0.10

Métrique d'EIGRP

- Par défaut, calculée selon 2 critères
  - La Bande Passante
  - Le Délai
- Métrique = 256 * (10^7 / BW + Σ DLY)
  - BW = la plus mauvaise des BW
  - Exprimée en kb/s
  - DLY exprimé en dizaines de µsec.

Métrique théorique

- Initialement, EIGRP, capable d'utiliser 5 critères:
  - BW K1 1
  - Charge K2 0
  - DLY K3 1
  - Fiabilité K4 0
  - MTU K5 0
- Métrique = [K1 * 256*10^7 / BW + K2 * (BW / 256 –charge) + K3 * 256 Σ DLY] * (K5 / (K4 + fiabilité))

Configuration d'EIGRP

- `# conf t`
- `# router eigrp 100`
  - 100 représente le numéro de AS (système autonome privé)
- `# network 192.168.10.0  0.0.0.255`
  - activer EIGRP sur toute interface dont l'adresse IP appartient à 192.168.10.0/24

MASQUE INVERSE !

Timers EIGRP

- Selon le type de réseau
- ETHERNET :
  - HELLO = 5 sec
  - DEAD = 15 sec
- NBMA :
  - HELLO = 60 sec
  - DEAD = 180 sec
- Si vous changez la valeur de Hello, l'IOS ne modifie pas automatiquement celle du HOLD
  - c'est l'inverse d'OSPF

Relations de voisinage

- OSPF exigeait….
- Même Area
- Même HELLO
- Même DEAD
- EIGRP exige….
- Même AS
- Même K1, K2, K3, K4, K5

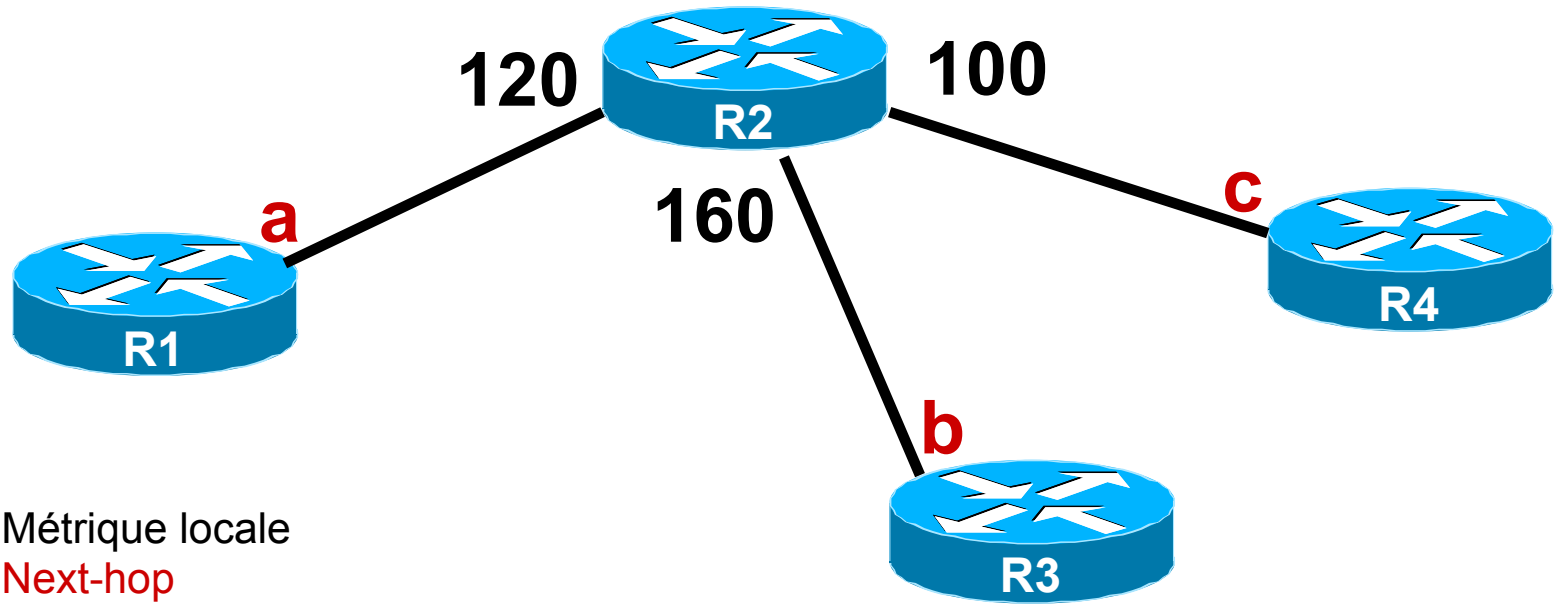
Masque annoncé

- EIGRP, par défaut, annonce le masque naturel de la classe.
- i.e. par défaut, on a :
  - `router EIGRP 100`
    - `auto-summary`
- pour annoncer le vrai masque:
  - **router EIGRP 100**
    - **`no`** `auto-summary`

EIGRP

L’ algorithme DUAL

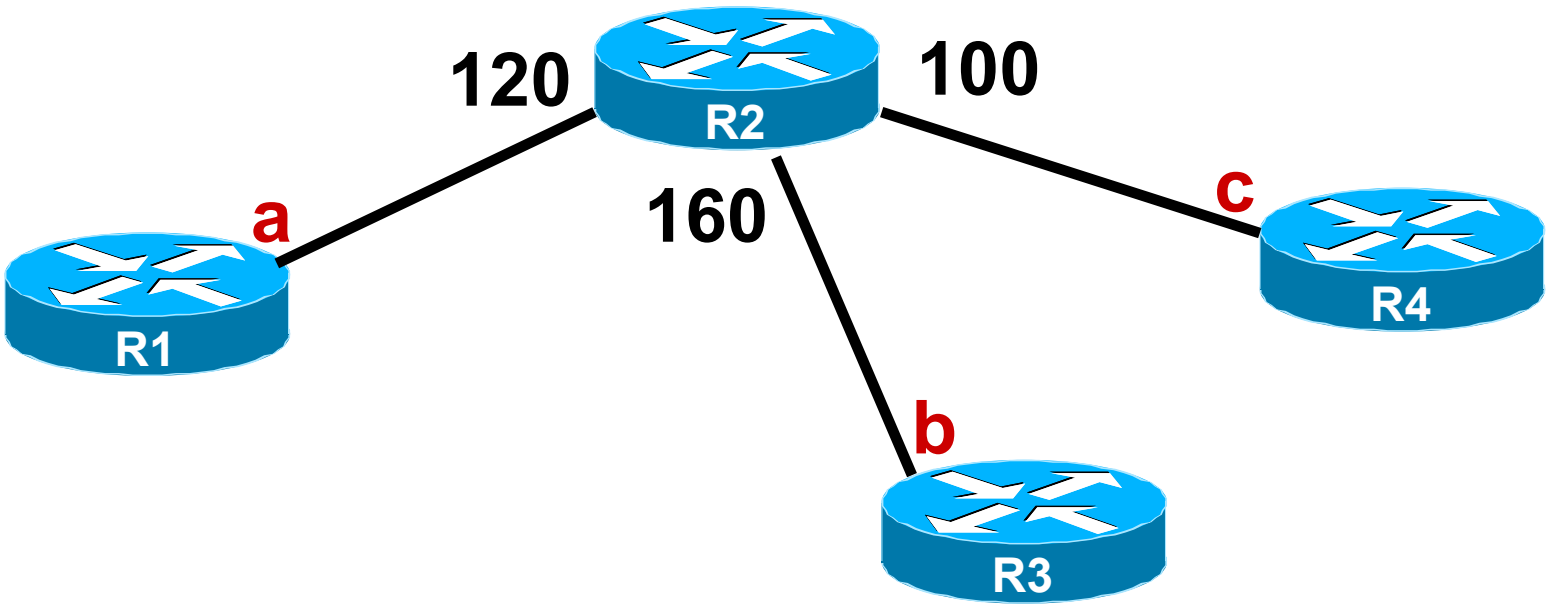
La terminologie DUAL



Métrique locale
Next-hop

Quel est le meilleur chemin depuis R2 vers le sous-réseau 10.0.0.0/24 ?

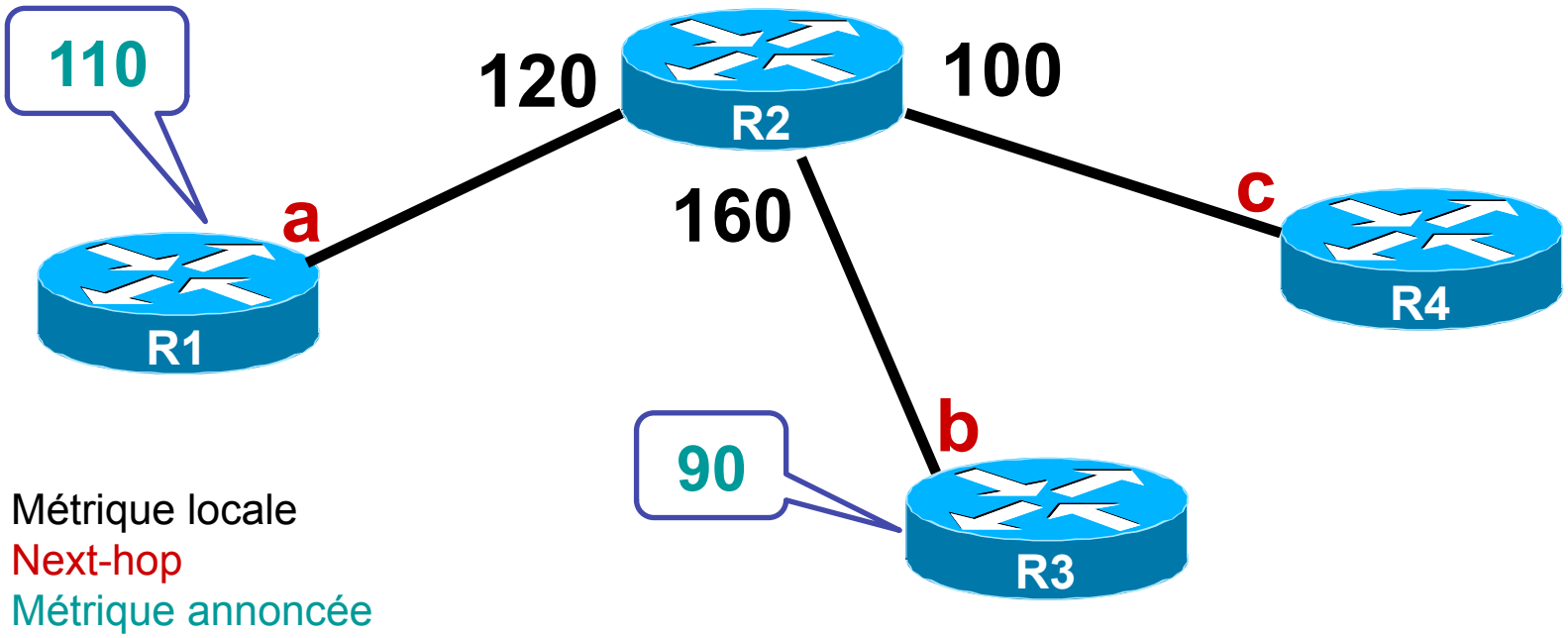
FD & S



feasible Distance = 100

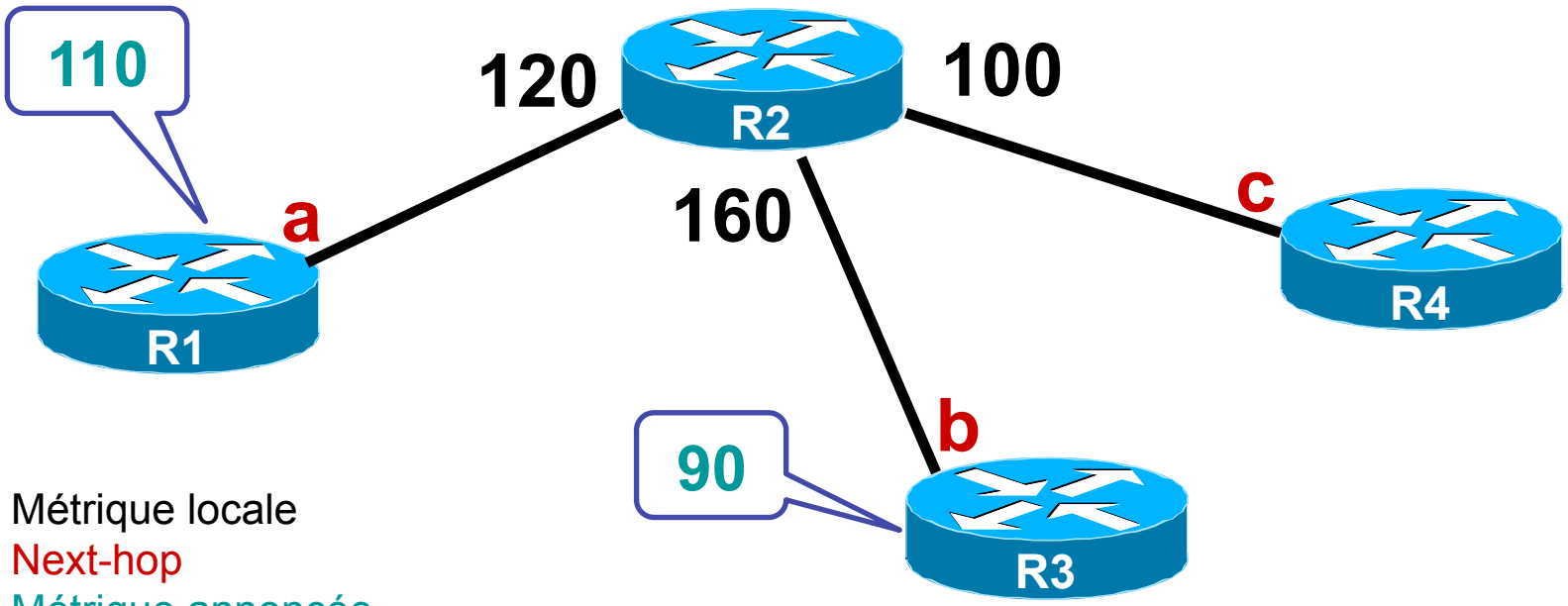
Successor = c

Attention aux boucles !



R1 annonce à R2 une métrique de 110.
R3 annonce à R2 une métrique de 90

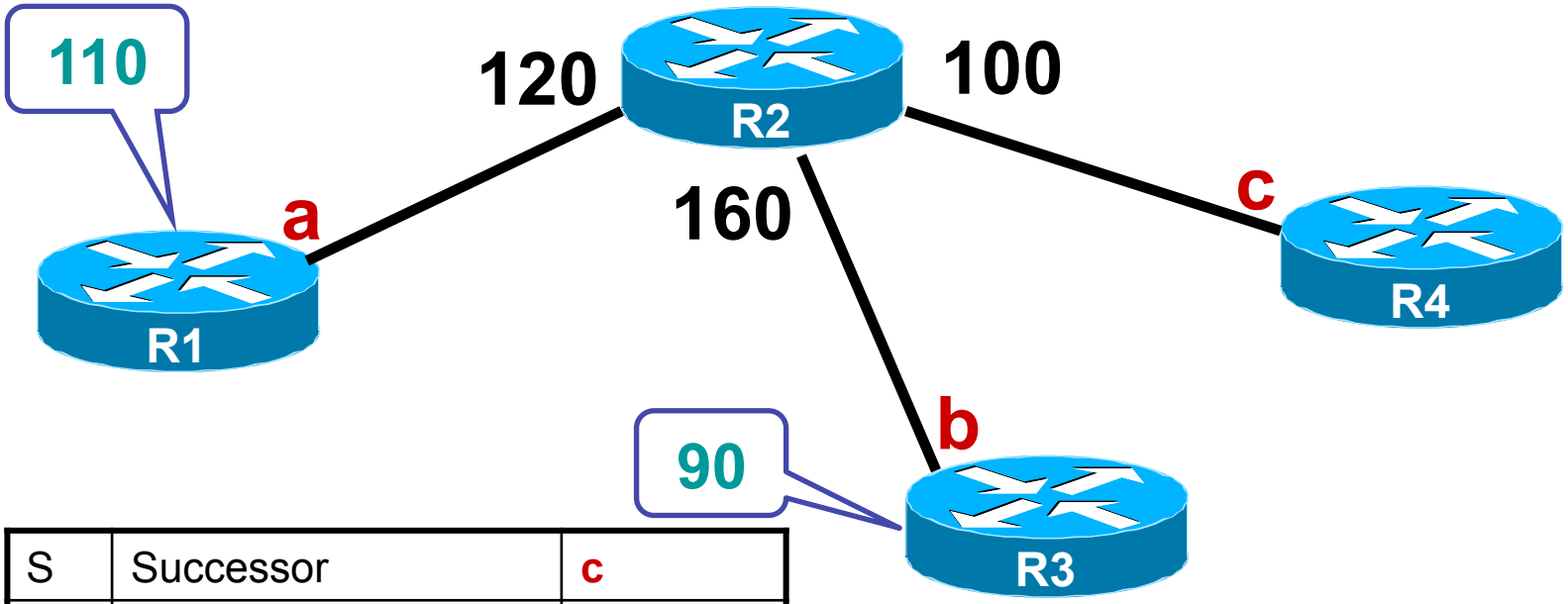
RD & FS



Métrique locale
Next-hop
Métrique annoncée

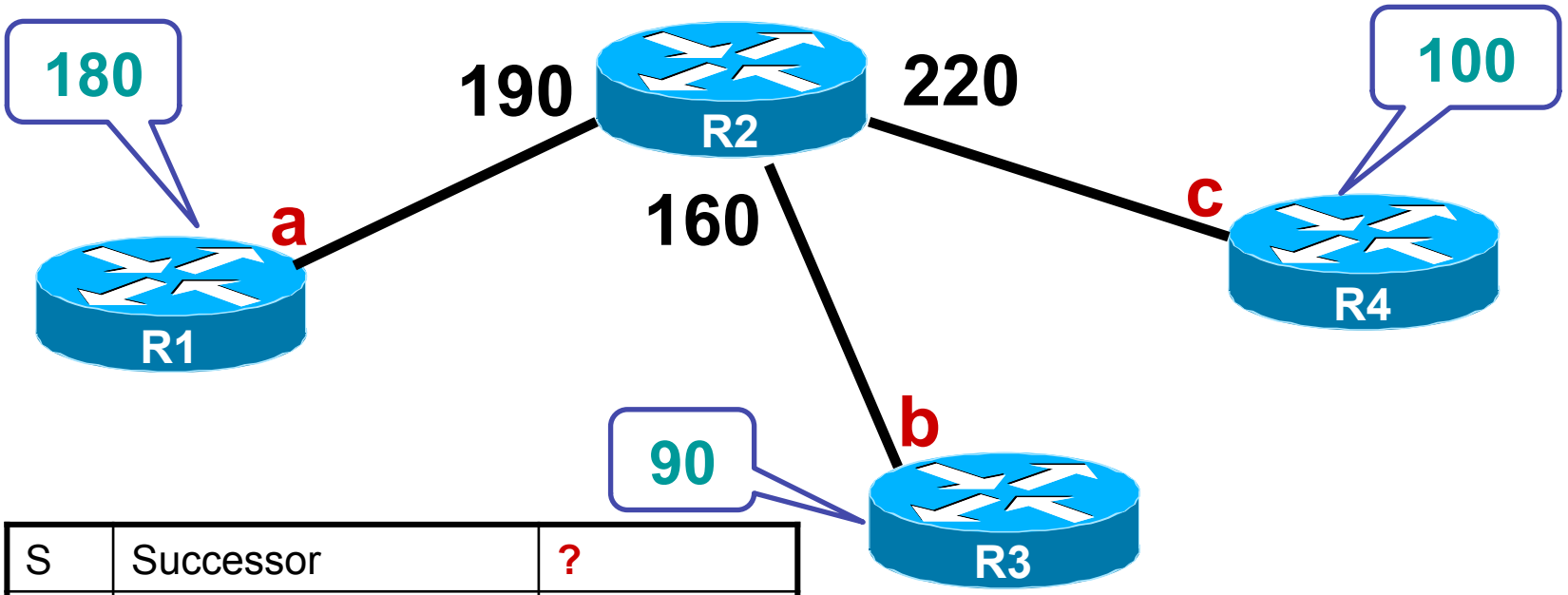
Reported Distance = 90
feasible Successor = b

La terminologie DUAL



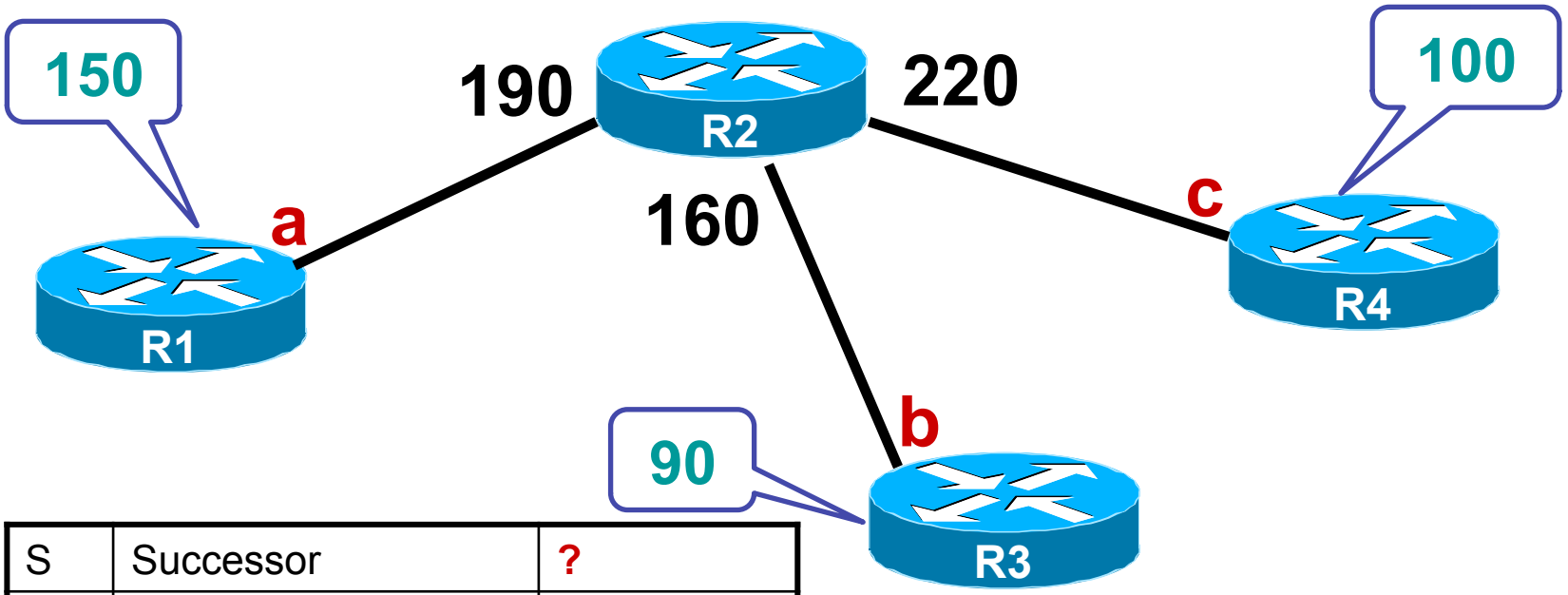
S	Successor	c
FS	feasible successor	b
FD	feasible distance	**100**
RD	Reported distance	90
FC	Feasible condition	90 **< 100**

Exercice 1



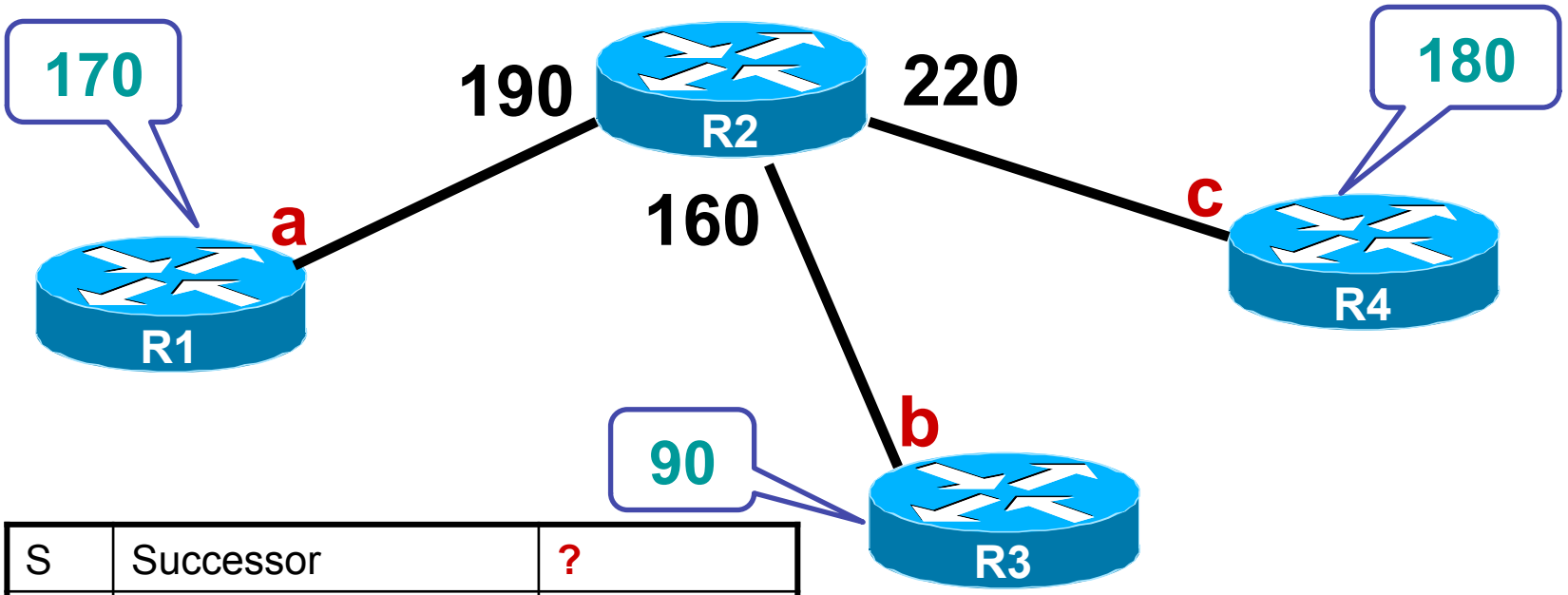
S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

Exercice 2



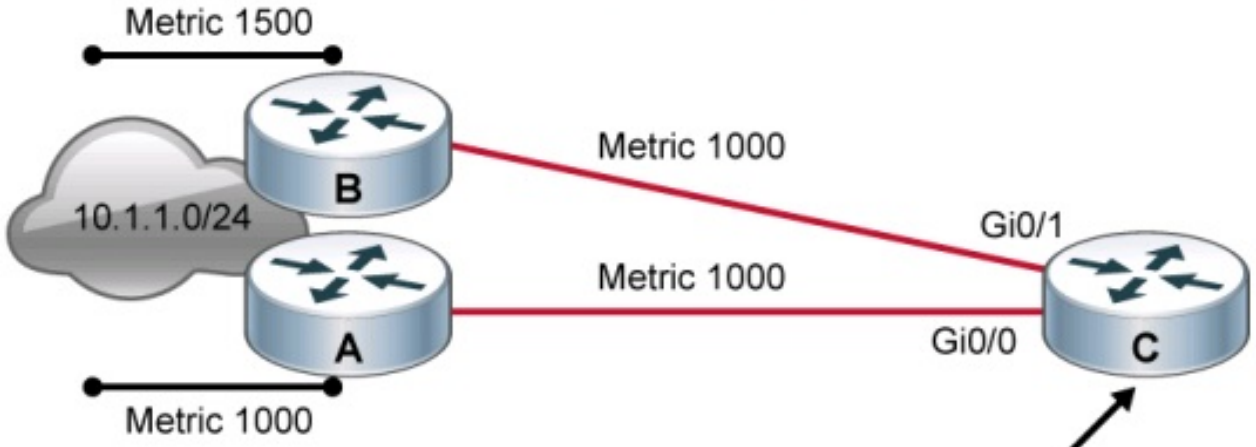
S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

Exercice 3



S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

EIGRP Path Selection (Cont.)



EIGRP Neighbor Table

Next-Hop Router	Interface
Router A	Gi0/0
Router B	Gi0/1

EIGRP Topology Table

Network	Feasible Distance	Advertised Distance	EIGRP Neighbor
10.1.1.0/24	**2000**	**1000**	**Router A**
10.1.1.0/24	2500	1500	Router B

Successor

Feasible Successor

Routing Table

Network	Metric	Outbound Interface	Next-Hop
10.1.1.0/24	2000	Gi0/0	Router A

Successeurs non retenus

```
R4# show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(1)/ID(4.4.4.4)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.12.0/24, 1 successors, FD is 6400, serno 95
        via 10.0.34.3 (6400/3840), Serial1/0
        via 10.0.45.5 (7680/6400), Serial1/1
P 10.0.13.0/24, 1 successors, FD is 5120, serno 91
        via 10.0.34.3 (5120/2560), Serial1/0
        via 10.0.45.5 (6400/5120), Serial1/1
P 10.0.23.0/24, 1 successors, FD is 5120, serno 94
        via 10.0.34.3 (5120/2560), Serial1/0
        via 10.0.45.5 (6400/5120), Serial1/1
P 10.0.45.0/24, 1 successors, FD is 1280, serno 90
        via Connected, Serial1/1
P 10.0.34.0/24, 1 successors, FD is 2560, serno 89
        via Connected, Serial1/0
P 10.0.35.0/24, 1 successors, FD is 3840, serno 96
        via 10.0.45.5 (3840/2560), Serial1/1
        via 10.0.34.3 (5120/2560), Serial1/0
P 192.168.5.0/24, 1 successors, FD is 1792, serno 97
        via 10.0.45.5 (1792/512), Serial1/1
        via 10.0.34.3 (5632/3072), Serial1/0
```

Deux types de partage de charge

- Partage de charge à métrique égale :
  - activé par défaut
  - sur 4 chemins différents par défaut
  - configurable jusqu'à 16 chemins différents :
    - `router eigrp 100`
      - `maximum-path 16`
- Partage de charge à métrique inégale :
  - désactivé par défaut

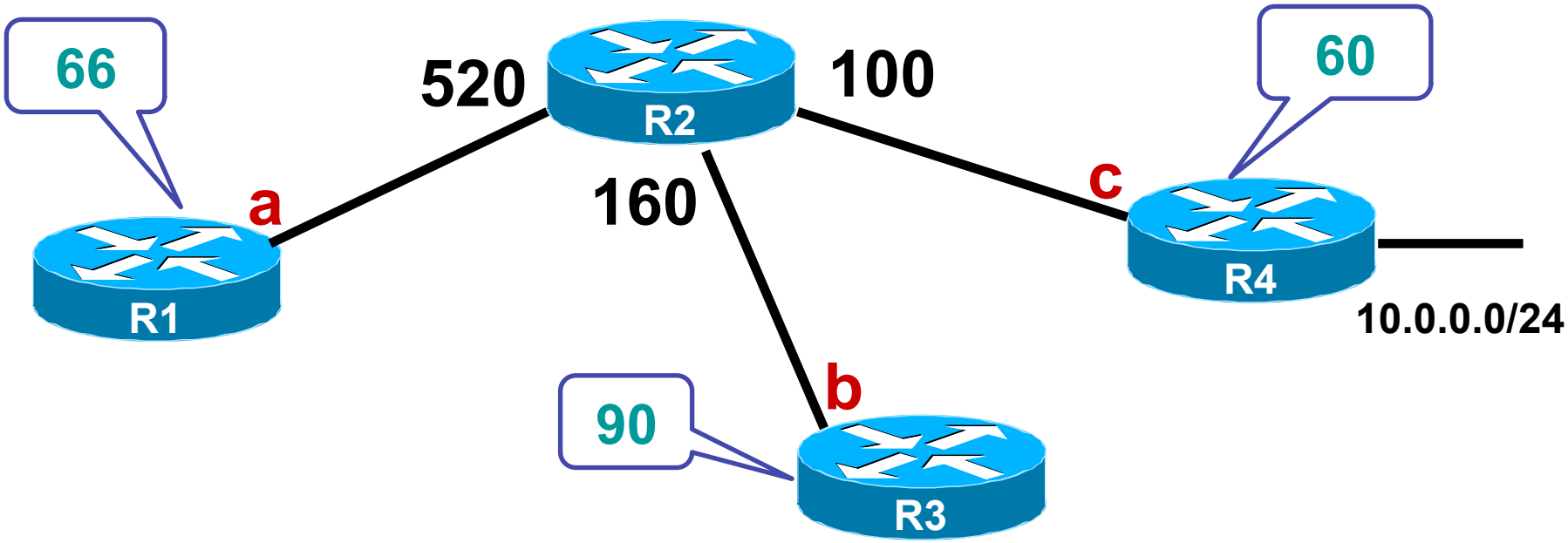
Variance

Par défaut EIGRP ne fait pas de partage de charge à métriques inégales : variance = 1.

Pour faire du partage de charge à métriques inégales :

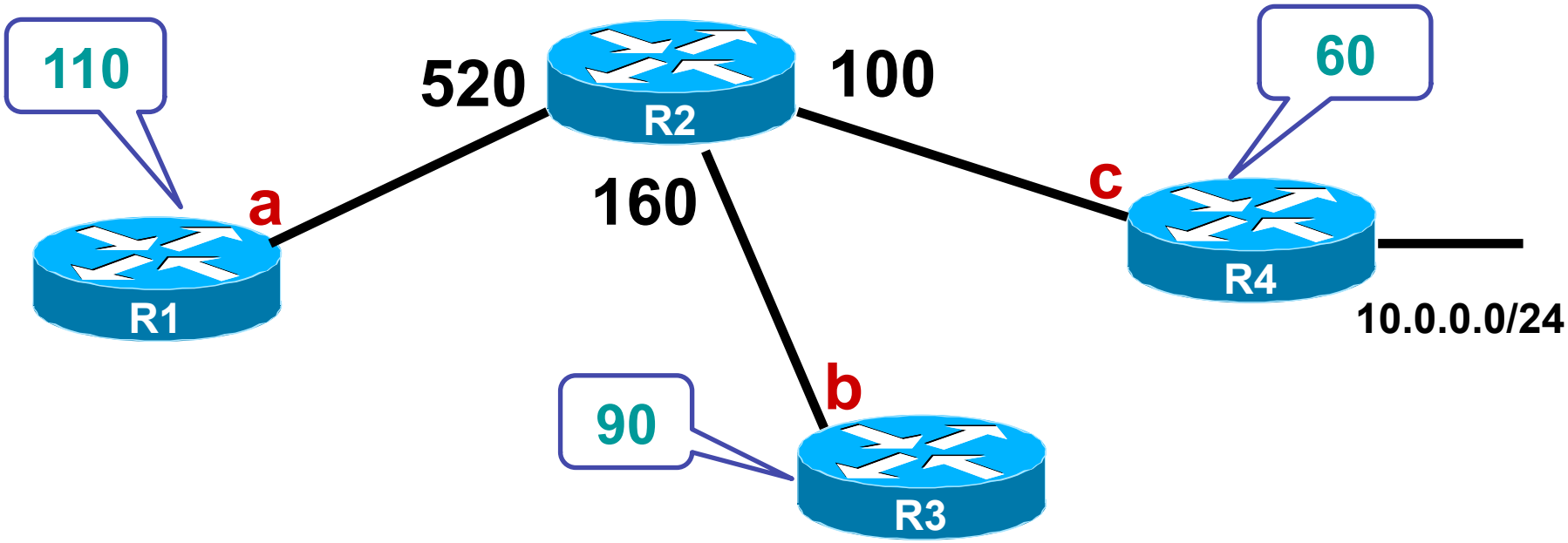
- configurer la variance à V > 1
- permet d'utiliser tout chemin qui est V fois moins bon que mon meilleur chemin
- la commande `maximum-path` contrôle le nombre maximum de chemins injectés dans la table de routage

Variance



- Variance = 1 ➔ NEXT-HOP c
- Variance = 2 ➔ NEXT-HOP c, b
- Variance = ? ➔ NEXT-HOP c, b, a

Exercice



- Variance = 1 ➔ NEXT-HOP ?
- Variance = 2 ➔ NEXT-HOP ?
- Variance = 6 ➔ NEXT-HOP ?

Configurer la variance

- `conf t`
- `router eigrp 100`
  - `variance 2`
  - avec 1 < V < 128
- Pour voir comment se fait le partage de charge :
  - `Show ip route 10.0.0.0 /24`

    `« traffic share count X »`

A router has learned three possible routes that could be used to reach a destination network. One route is from EIGRP and has a composite metric of 20514560. Another route is from OSPF with a metric of 782. The last is from RIPv2 and has a metric of 4. Which route or routes will the router install in the routing table?

A. the OSPF route
B. the EIGRP route
C. the RIPv2 route
D. all three routes
E. the OSPF and RIPv2 routes

Correct Answer: B

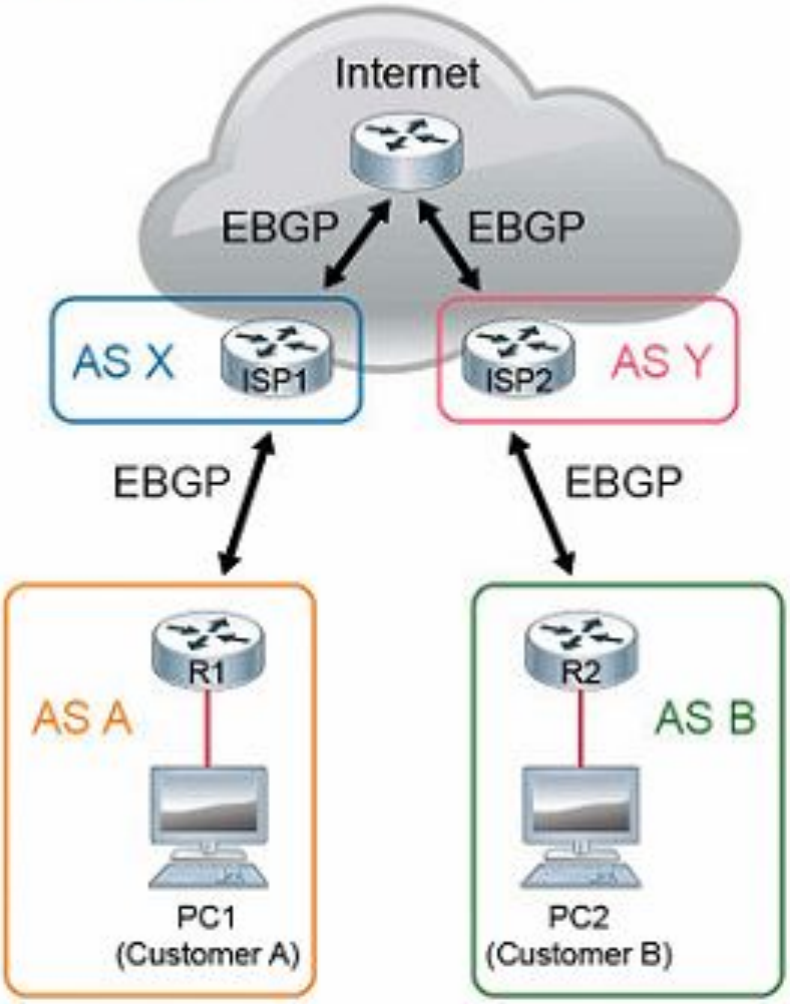
A network administrator is troubleshooting an EIGRP problem on a router and needs to confirm the IP addresses of the devices with which the router has established adjacency. The retransmit interval and the queue counts for the adjacent routers also need to be checked. What command will display the required information ?

A. Router# show ip eigrp neighbors
B. Router# show ip eigrp interfaces
C. Router# show ip eigrp adjacency
D. Router# show ip eigrp topology

Correct Answer: A

eBGP

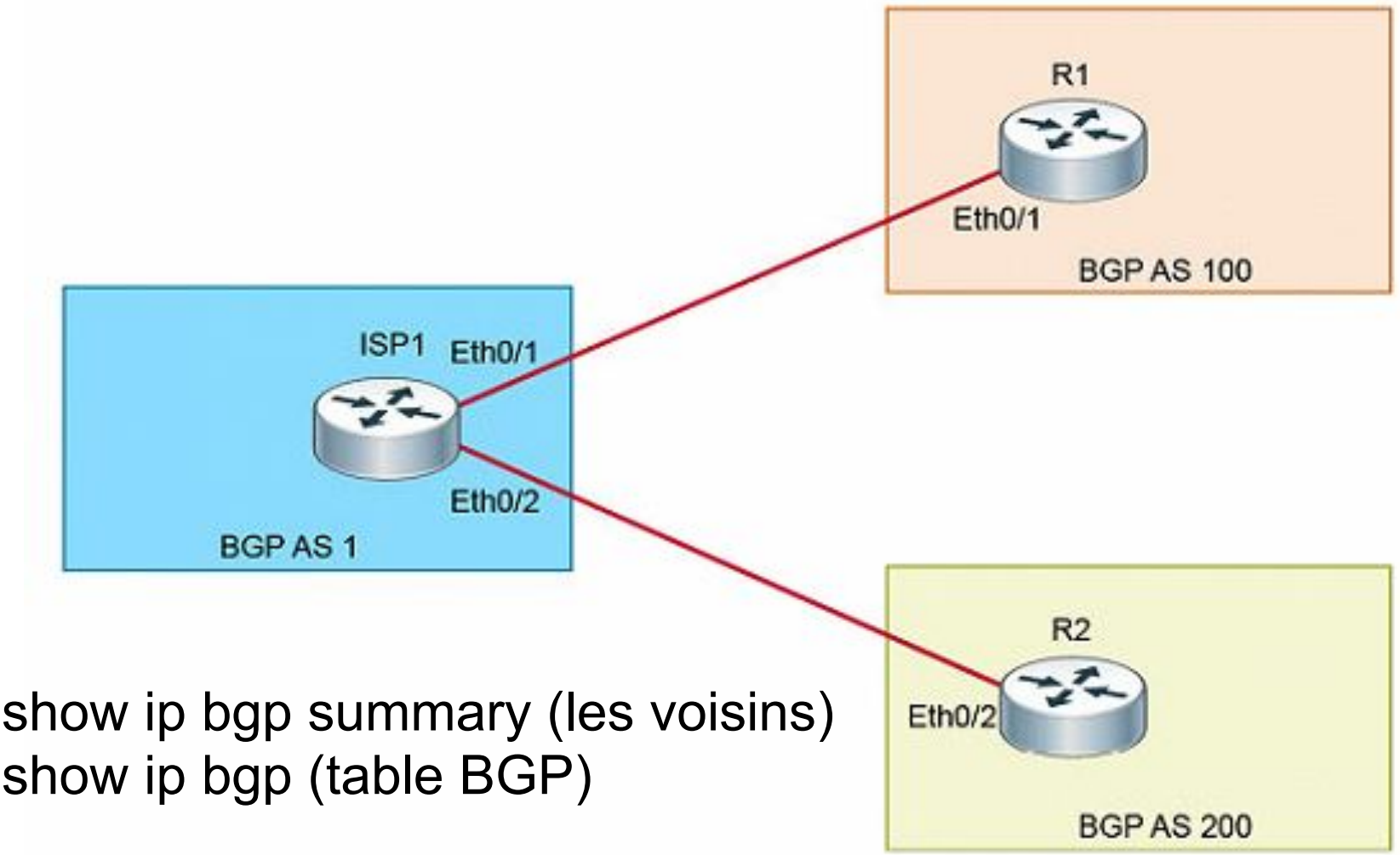
Introduction to EBGP



EBGP characteristics:

- Reliable updates: TCP port 179
- Interdomain routing—EGP
- Customer exchanges routes with the ISP
- ISPs exchange routes with other ISPs
- Scalable
- Secure
- Supports routing policies

Topology



show ip bgp summary (les voisins)
show ip bgp (table BGP)

Commande de vérification

Which command can you enter to verify that a BGP connection to a remote device is established?

A. show ip bgp summary
B. show ip community-list
C. show ip bgp paths
D. show ip route

- Réponse : A

ROUTAGE
IP v6

Routage statique

- Configuration:
  - `ipv6 unicast-routing`
  - `ipv6 route ::/0 NEXT-HOP [AD]`
  - `ipv6 route 2001:1::/64 NEXT-HOP [AD]`

Protocoles de routage

Rappel sur IPv4:

- RIP
- OSPF
- EIGRP

IPv6 :

- RIPng
- OSPFv3
- EIGRP for IPv6

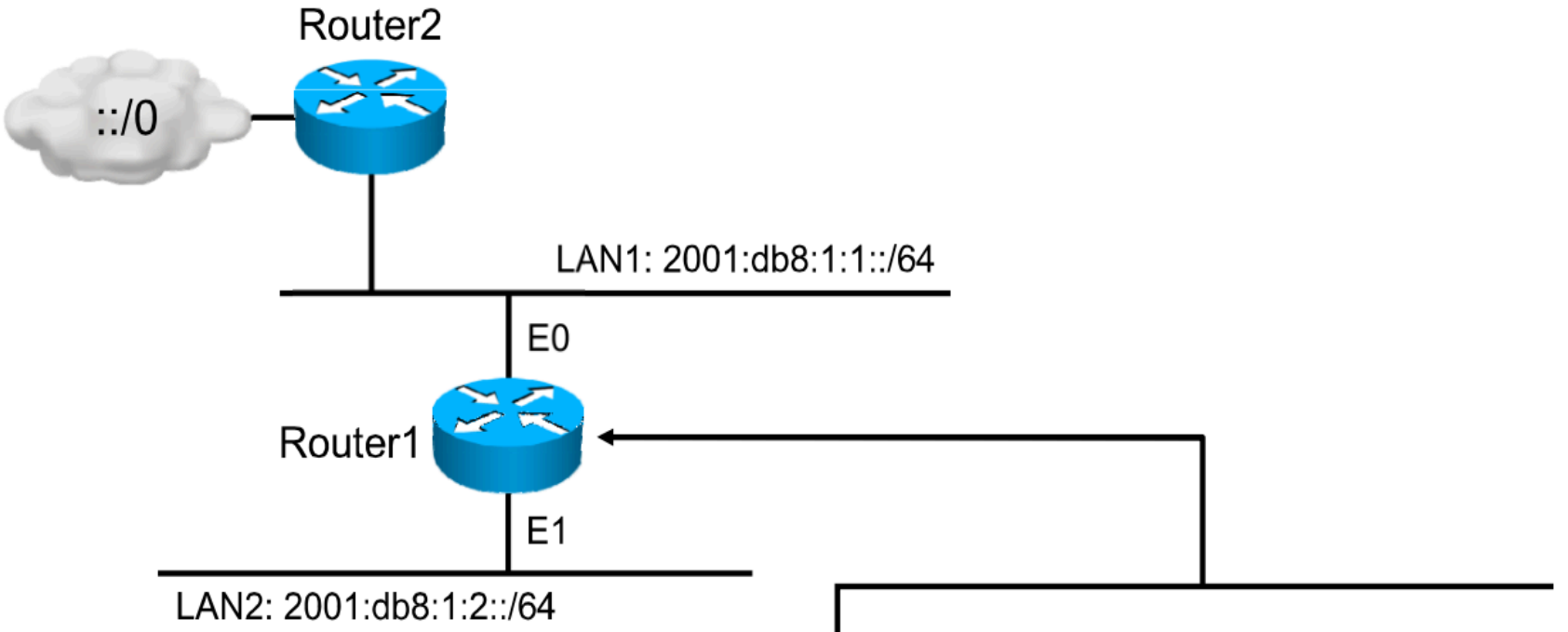
RIPng

- RFC 2080
- Similaire à RIP v2:
  - vecteur de distance
  - AD 120
  - métrique = somme des sauts
  - multicast FF02::9
- Différences avec RIPv2:
  - UDP port 521 (port 520 sur IPv4)
  - utilise adresses link-local

Configurer RIPng

- `ipv6 unicast-routing` (pas activé par défaut)
- `ipv6 router rip` **TAG** (identique entre voisins)
- `interface fa0/0`
  - **`ipv6 rip TAG enable`**
- `debug ipv6 rip`

Exemple RIPng



OSPFv3

- Similaire à OSPFv2:
  - état de lien
  - découverte des voisins
  - AD 110
  - métrique = somme des couts
  - multicast FF02::5 & 6

- Différence avec OSPFv2:
  - utilise les adresses link-local pour les adjacences

Configurer OSPFv3

- ipv6 unicast-routing
- ipv6 router ospf **PROCESS**
  - router-id 0.0.0.1
- interface fa0/0
  - **ipv6 ospf PROCESS area X**
  - ipv6 ospf cost 2
  - ipv6 ospf hello-interval 10

EIGRP for IPv6

- Similaire à EIGRP:
  - DV avancé ou hybride
  - AD 90
  - métrique = 256 * (10^7/BW + somme (délais))
  - multicast FF02::A

- Différences avec EIGRP:
  - utilise les adresses link-local pour les adjacences

Configurer EIGRP for IPv6

- `ipv6 unicast-routing`
- `ipv6 router eigrp` **`AS`**
  - `no shutdown`
- `interface fa0/0`
  - **`ipv6 eigrp AS`**

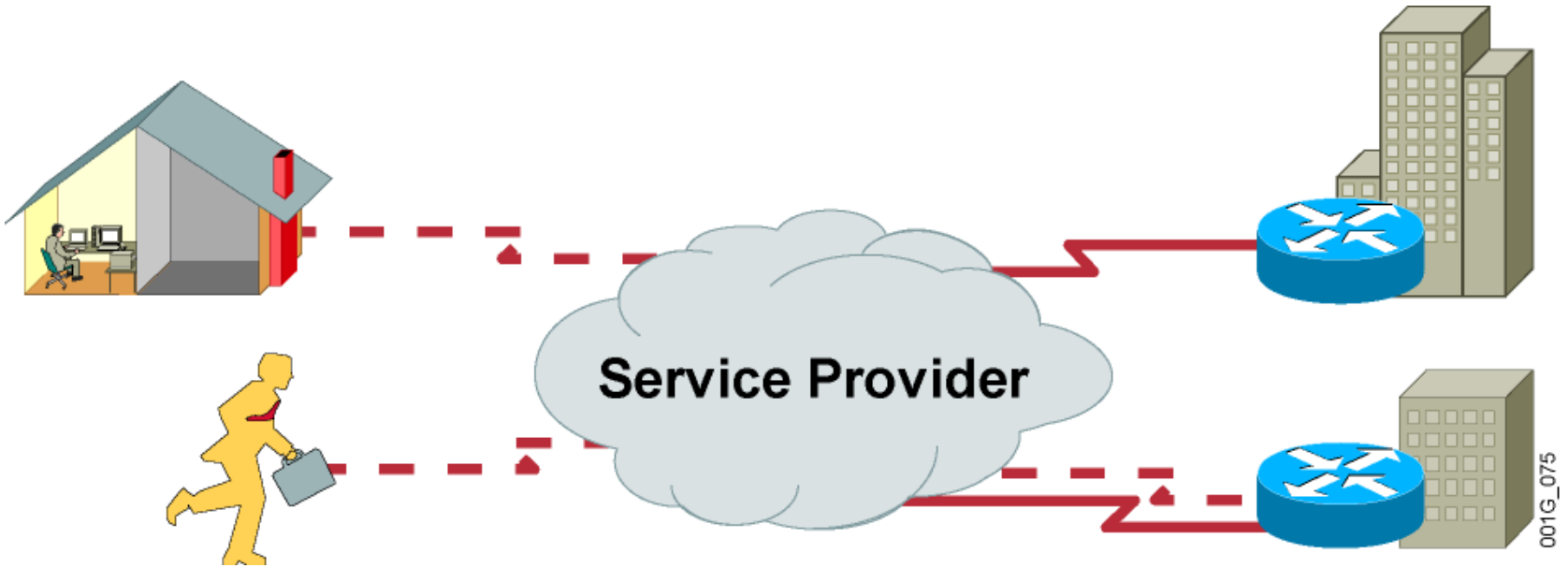
Vérifications

- `show ipv6 interface brief`
- `show ipv6 route`
- `show ipv6 protocols`
- `show ipv6 rip`
- `show ipv6 ospf interface`
- `show ipv6 ospf neighbor`
- `show ipv6 ospf database`
- `show ipv6 eigrp interface`
- `show ipv6 eigrp neighbor`
- `show ipv6 eigrp topology`

WAN

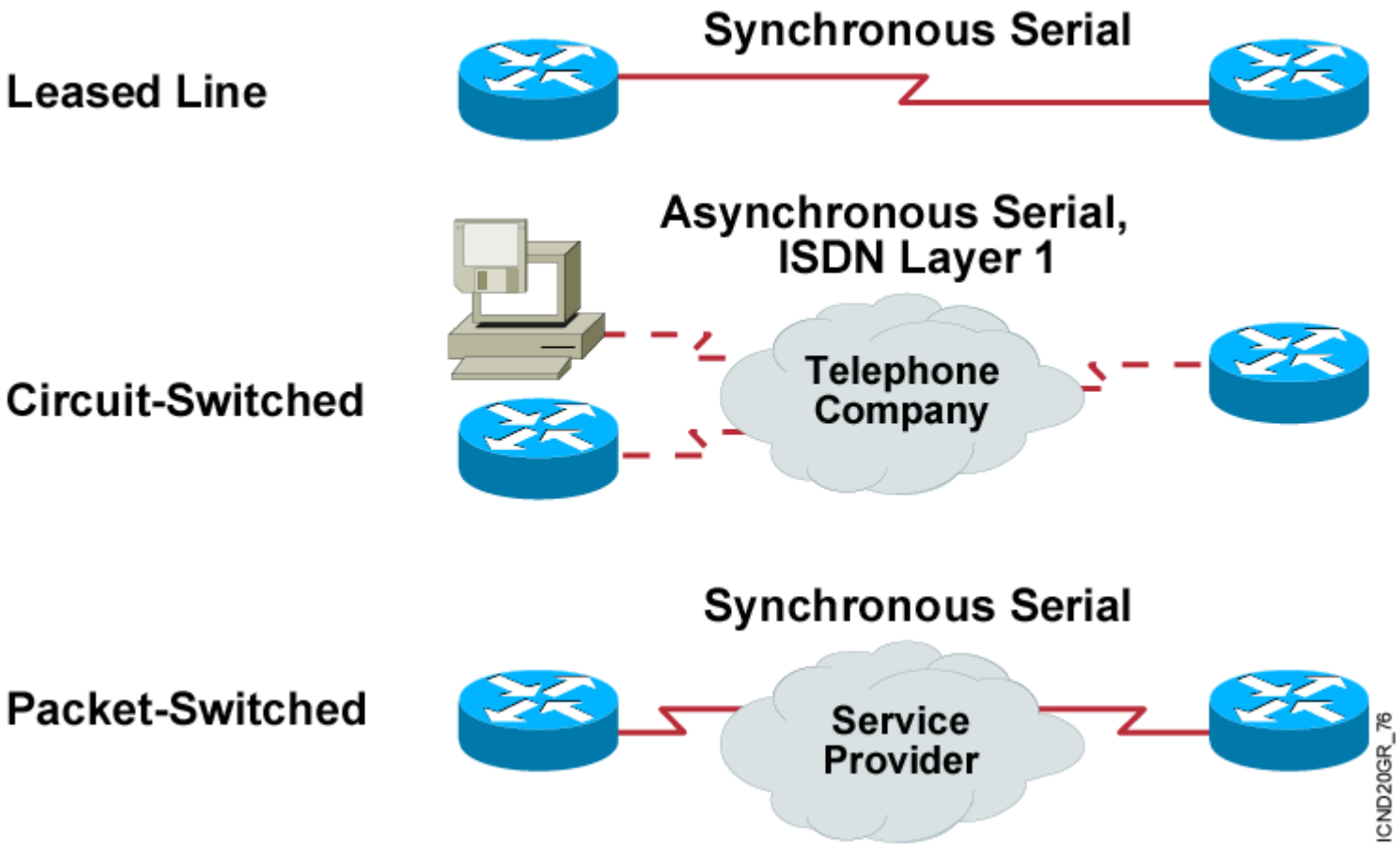
Couche Physique du WAN

Le WAN

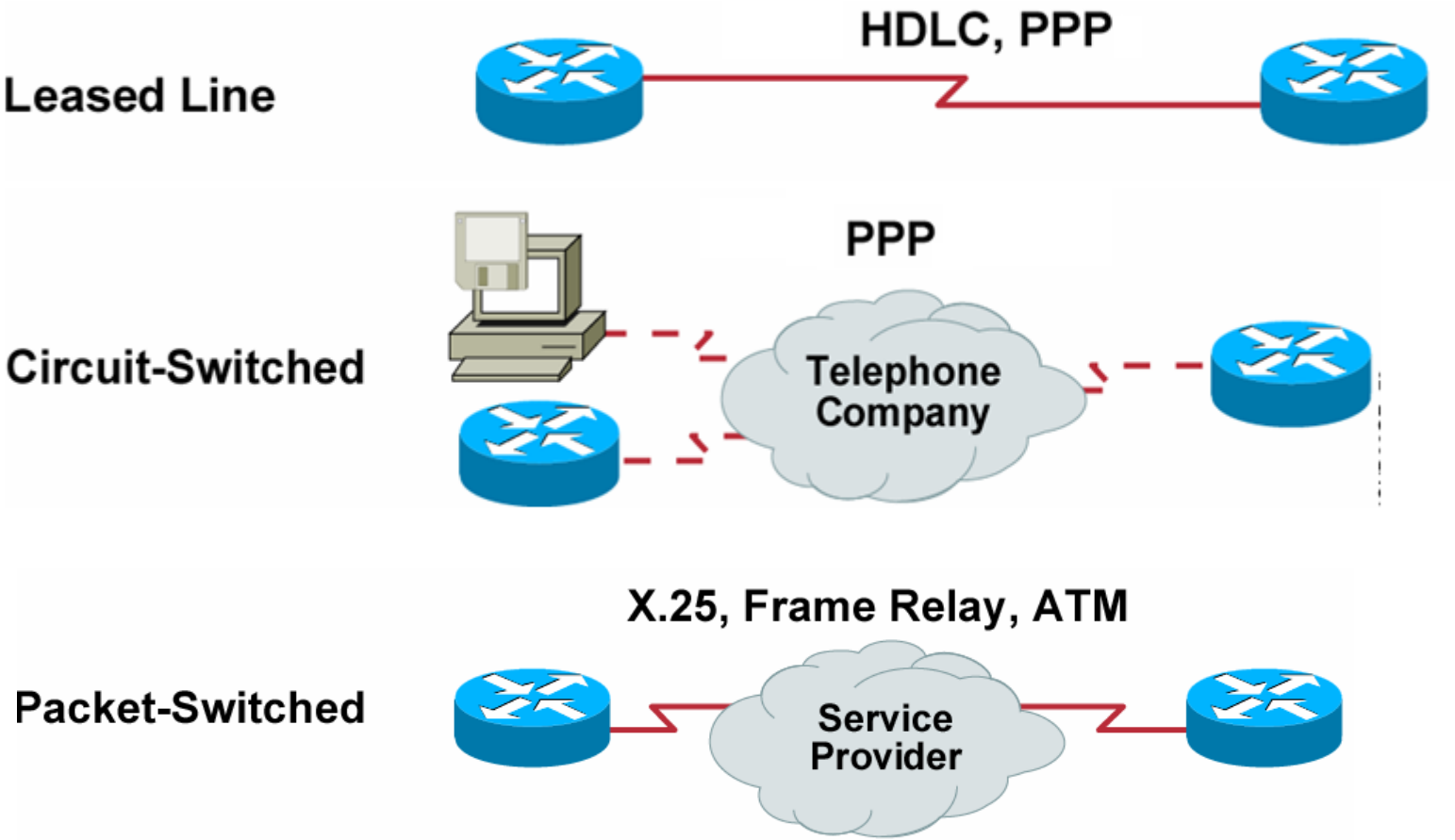


- Le WAN interconnecte les sites distants
- Le type de connection dépend du besoin et des coûts

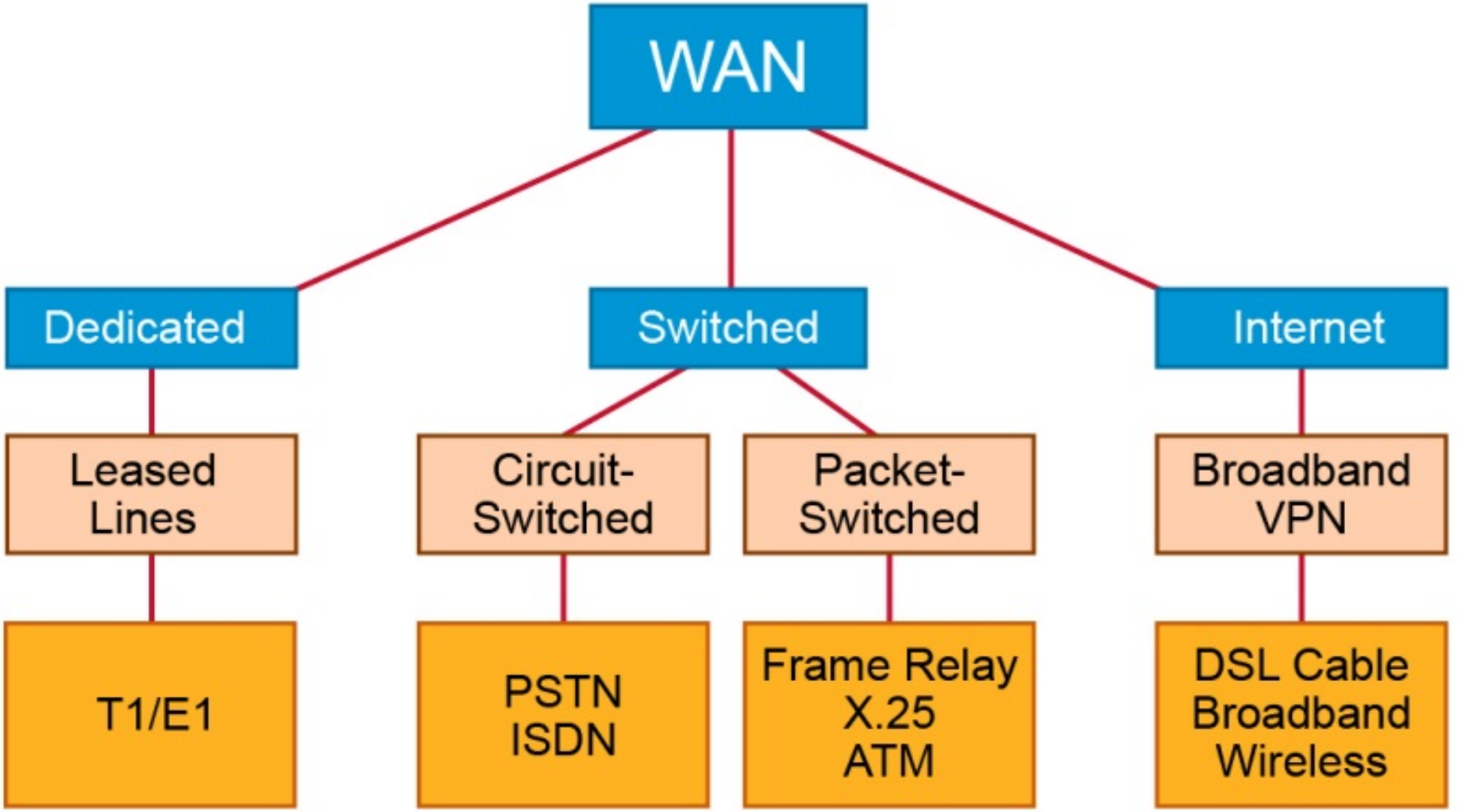
Les types de connections



Les encapsulations sur le WAN

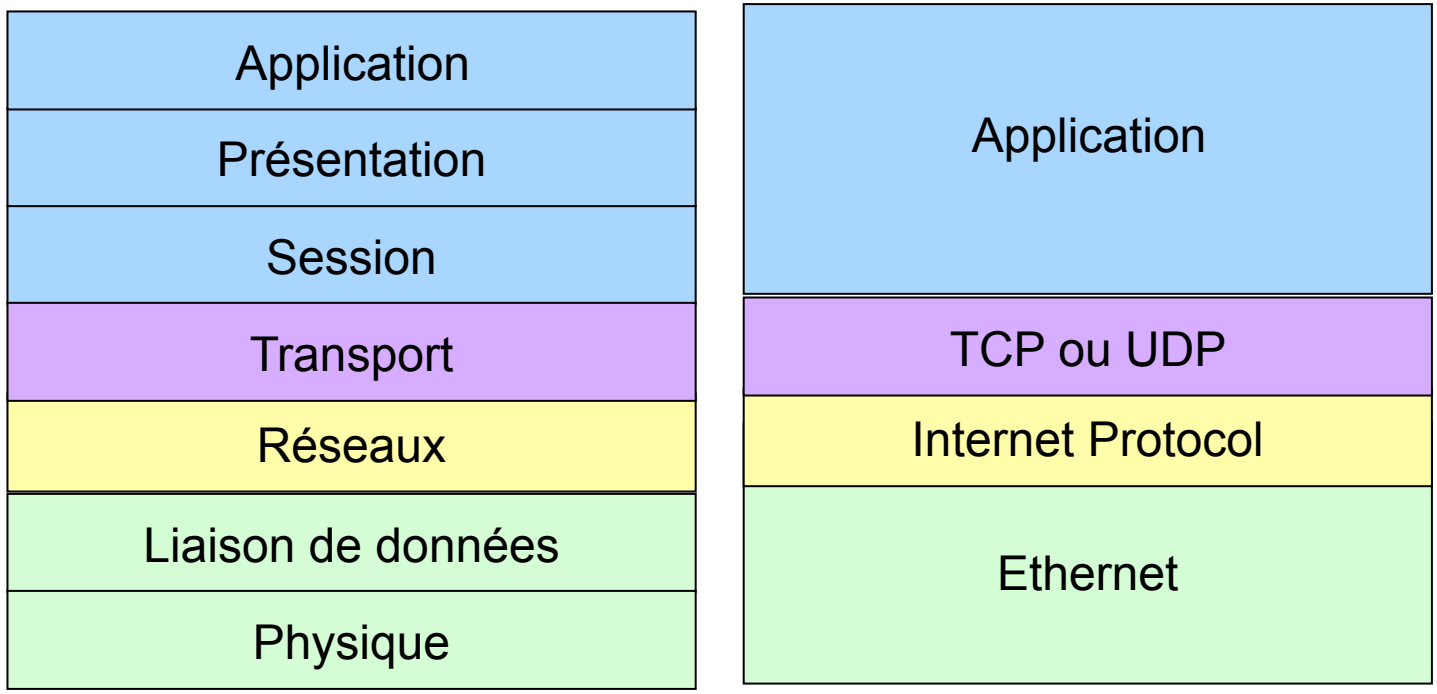


WAN Connectivity Options



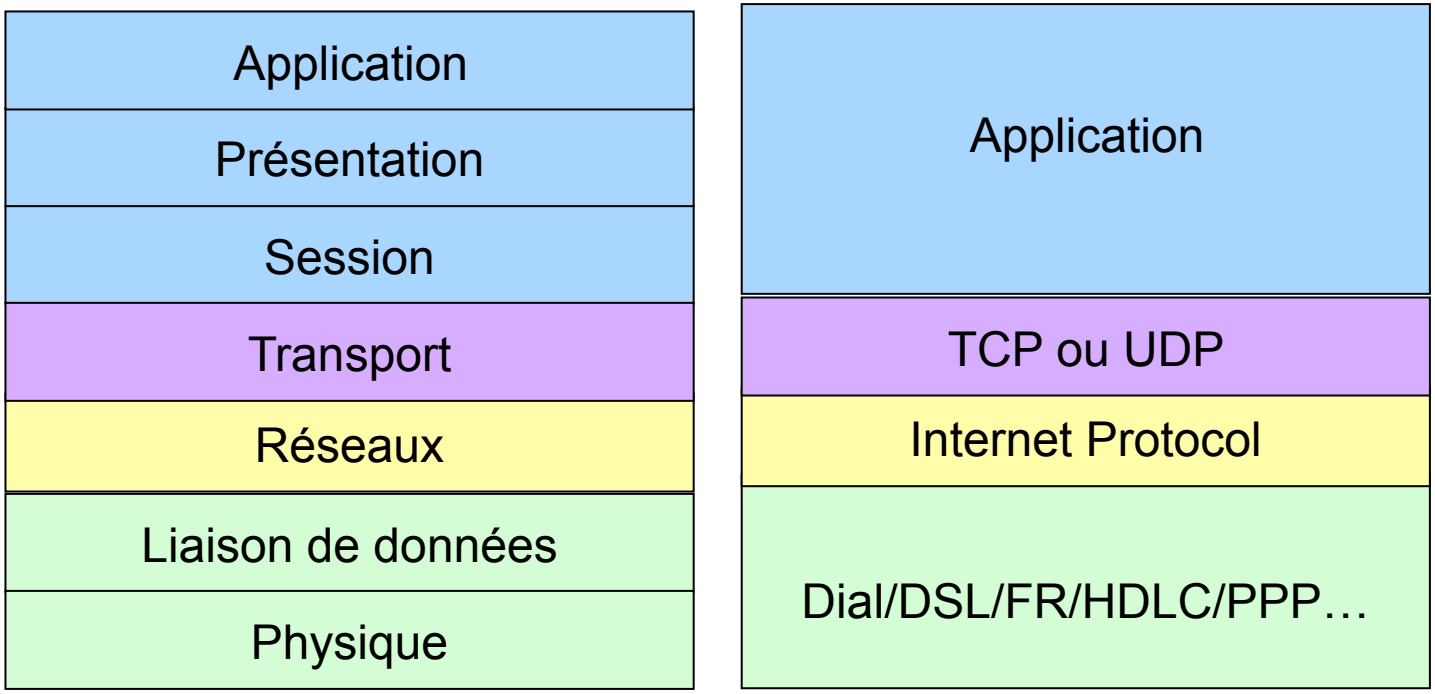
Comparaison de OSI et TCP/IP dans le LAN

TCP/IP sur Ethernet est le modèle qui s'est imposé dans les réseaux locaux

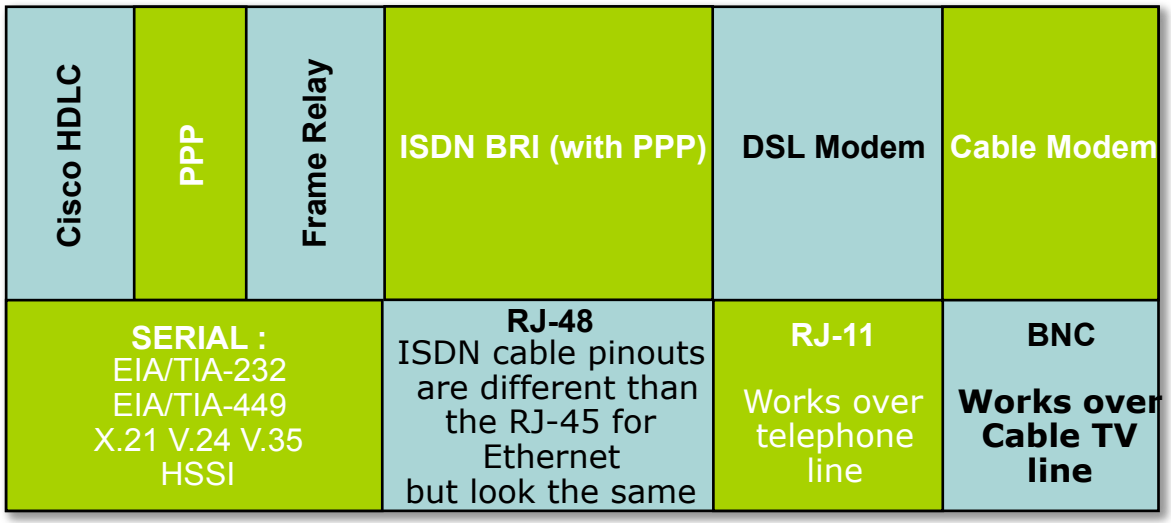


Comparaison de OSI et TCP/IP dans le WAN

Le réseau étendu est caractérisé par les deux premières couches

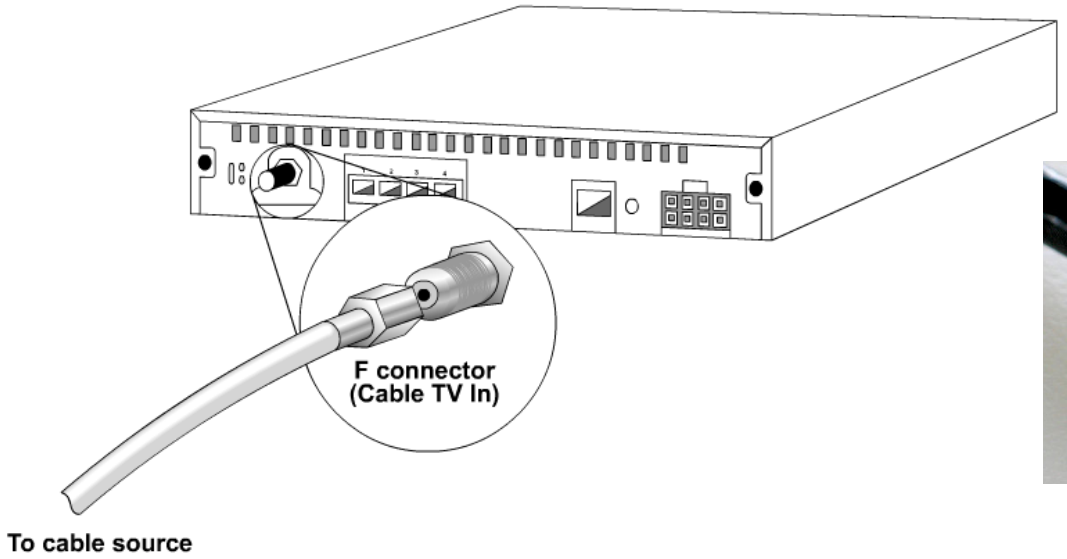


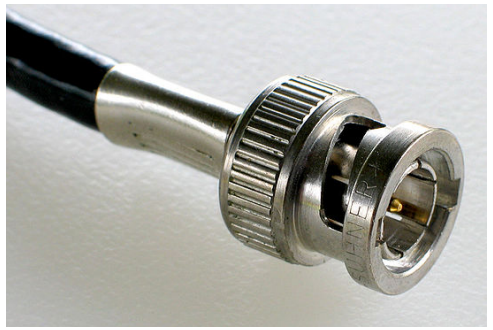
Couches physiques sur le WAN



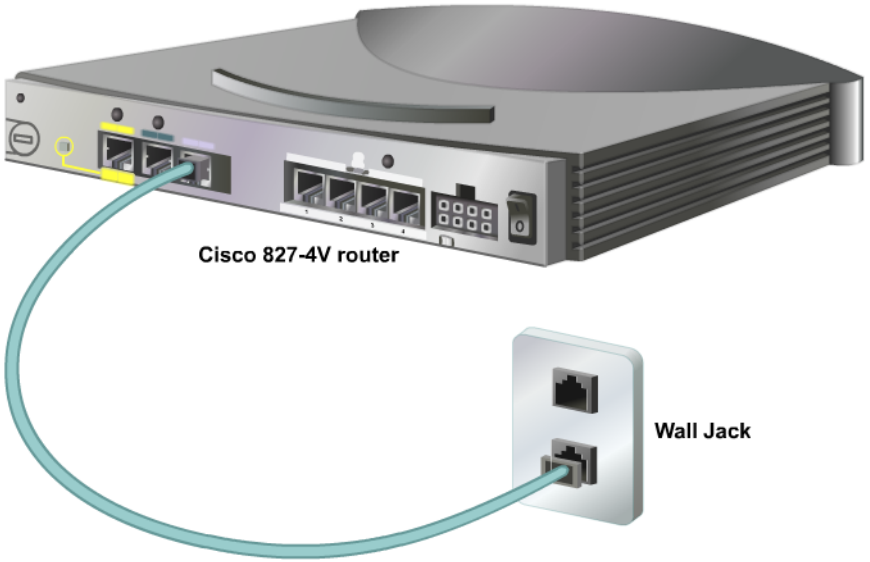
- **Les liens WAN sont vus par IP comme des couches 2**
- **Le type de lien détermine la bande passante**

Routeur Cable Modem



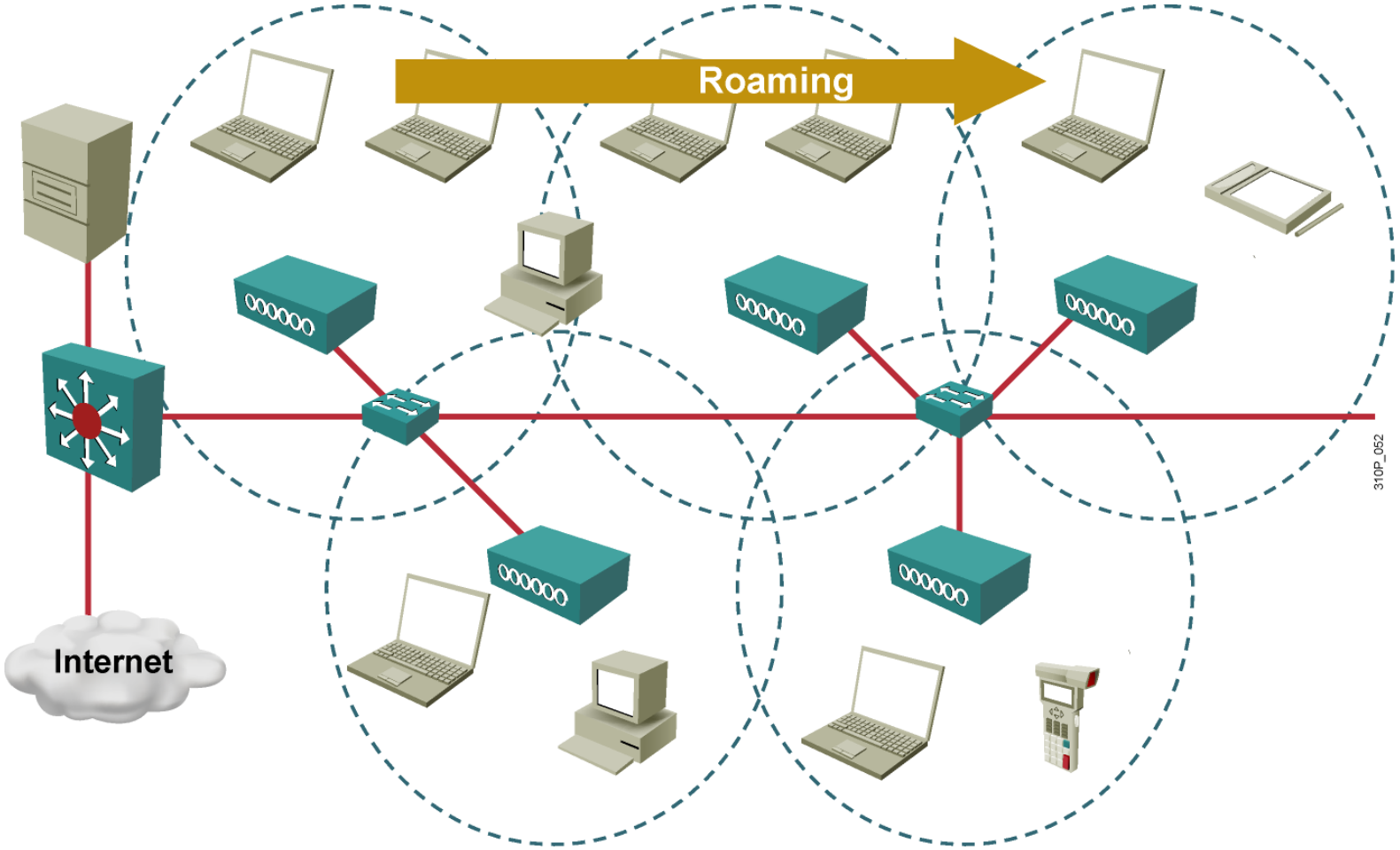


Routeurs DSL (RJ11)

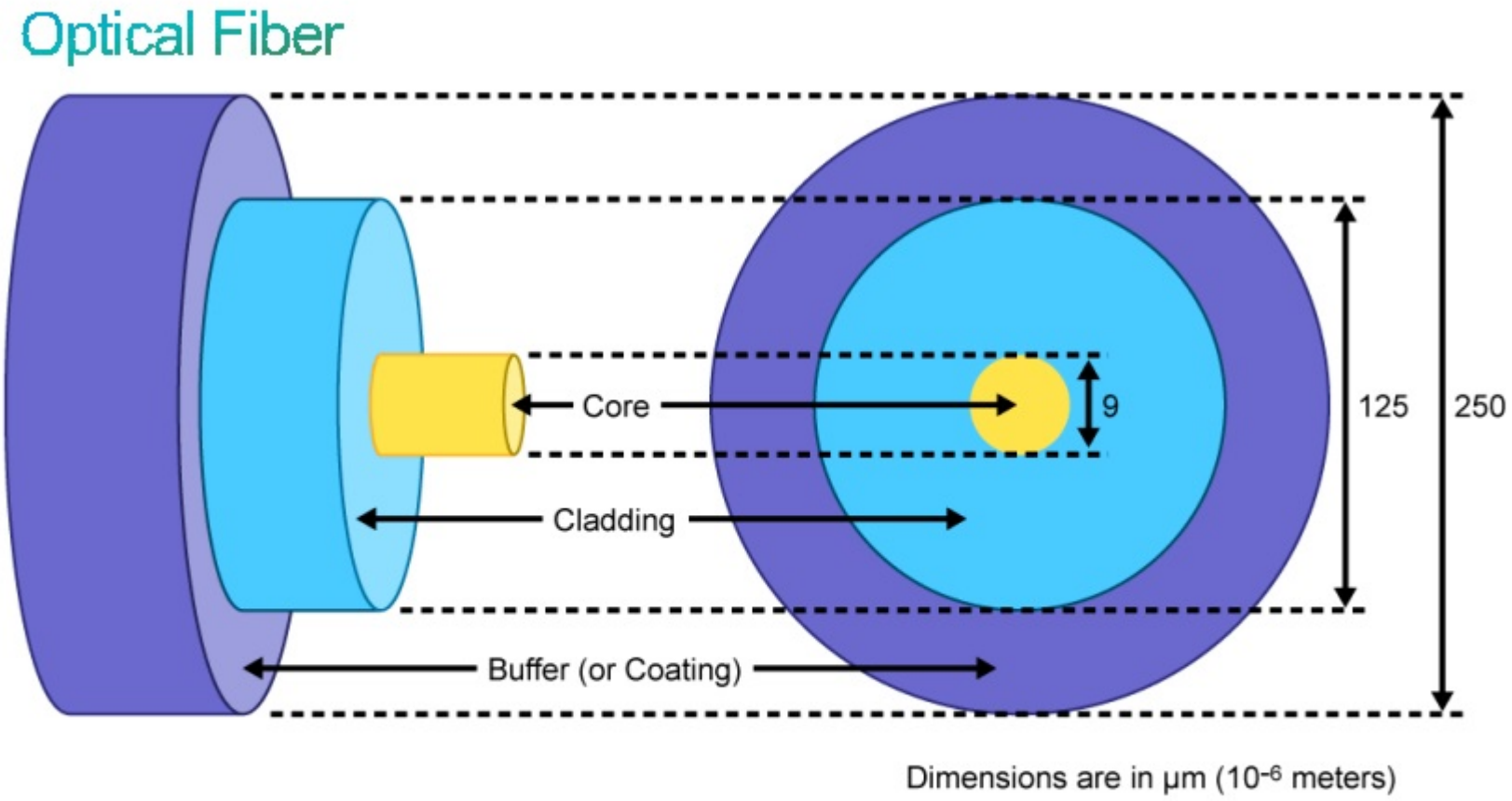


- Le modem est branché sur la prise téléphonique

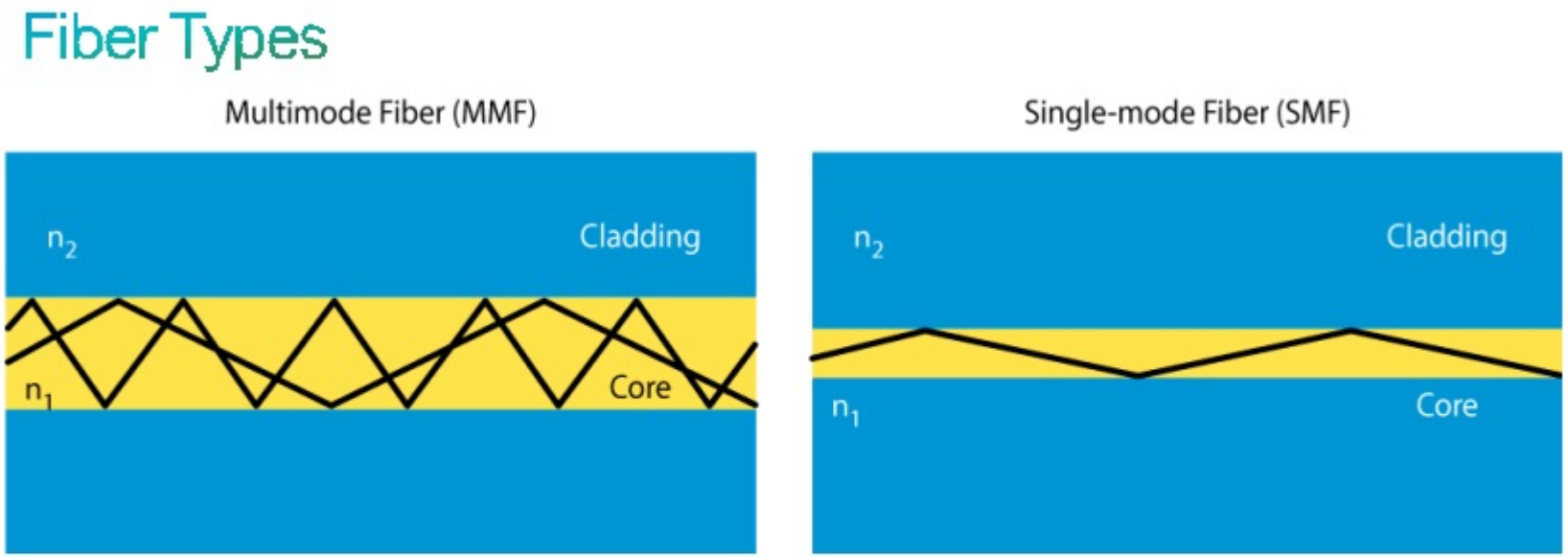
Réseau sans fil avec un controlleur



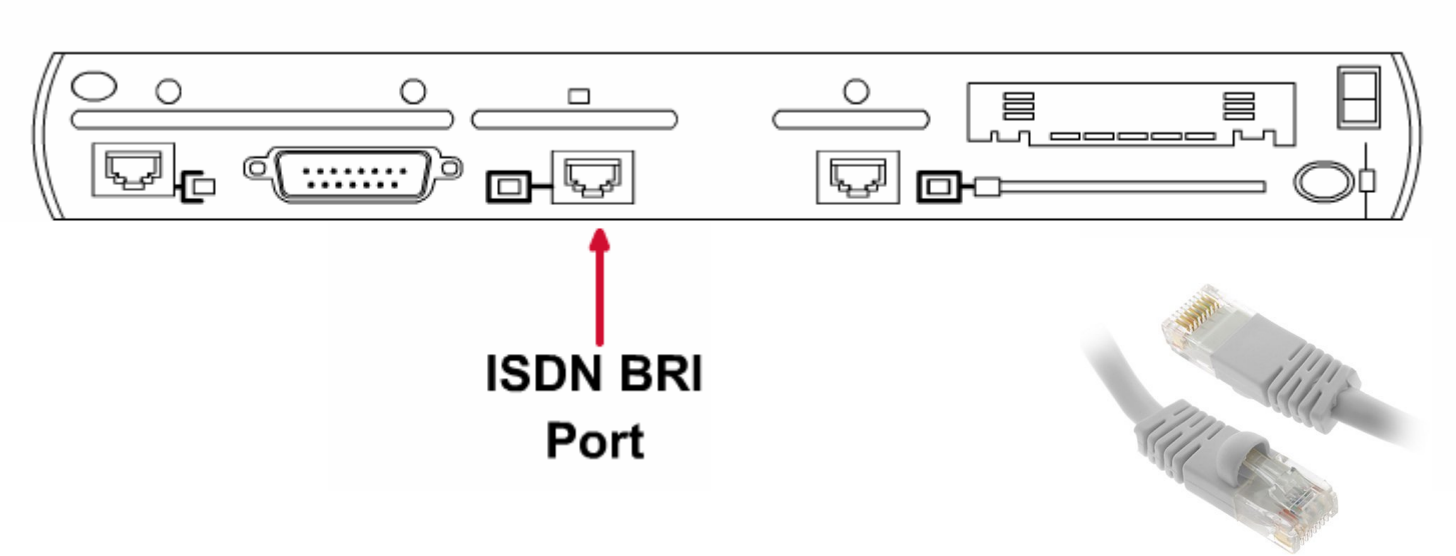
Fibre optique mono et bi directionel (DWDM)



Cœur entouré de la gaine

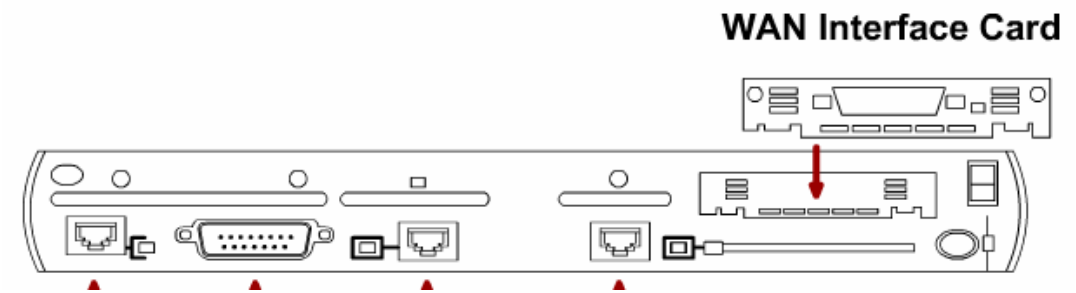


Connections RNIS (RJ 48)

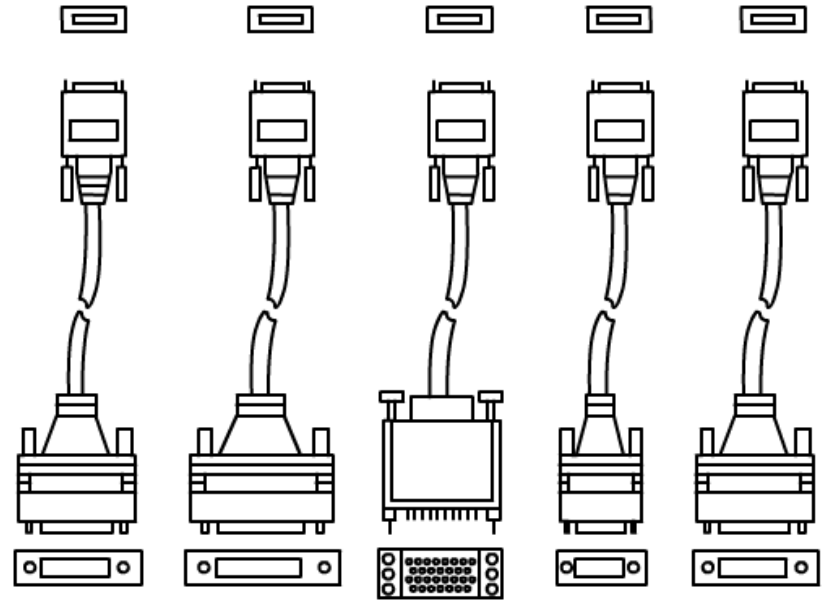


- Le connecteur RJ48 est très semblable au RJ45 (un détrompeur en plus)
- L'accès de base (T0 en France) est utilisé pour tranporter de la voix numérisée ou des données

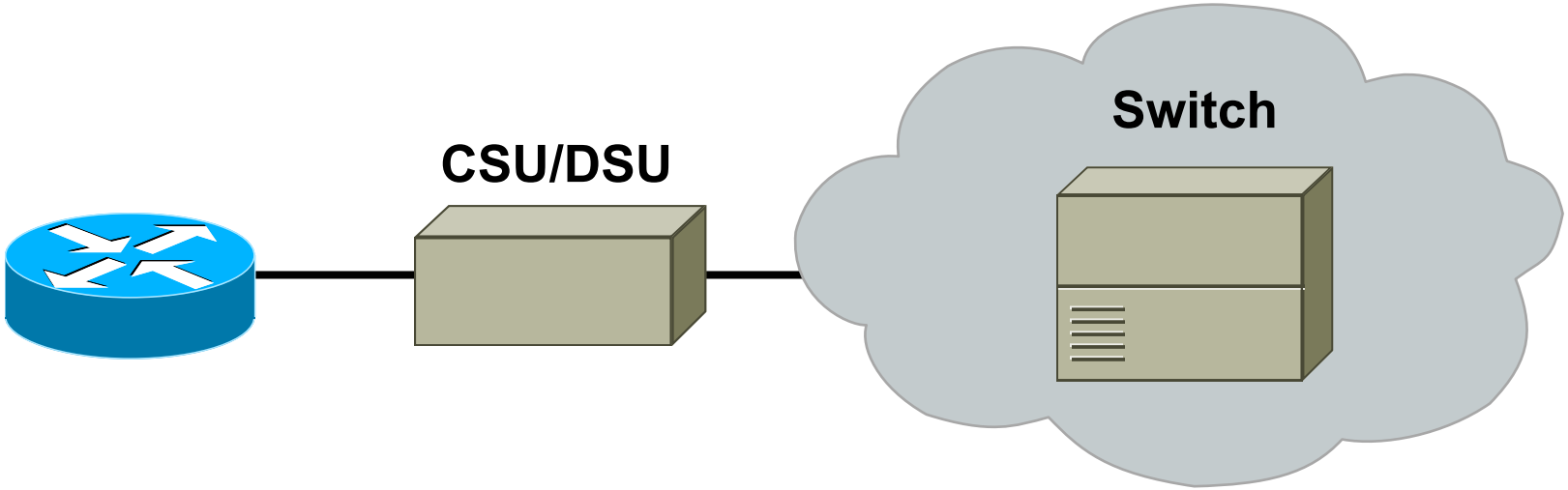
Connection Série



CSU/DSU

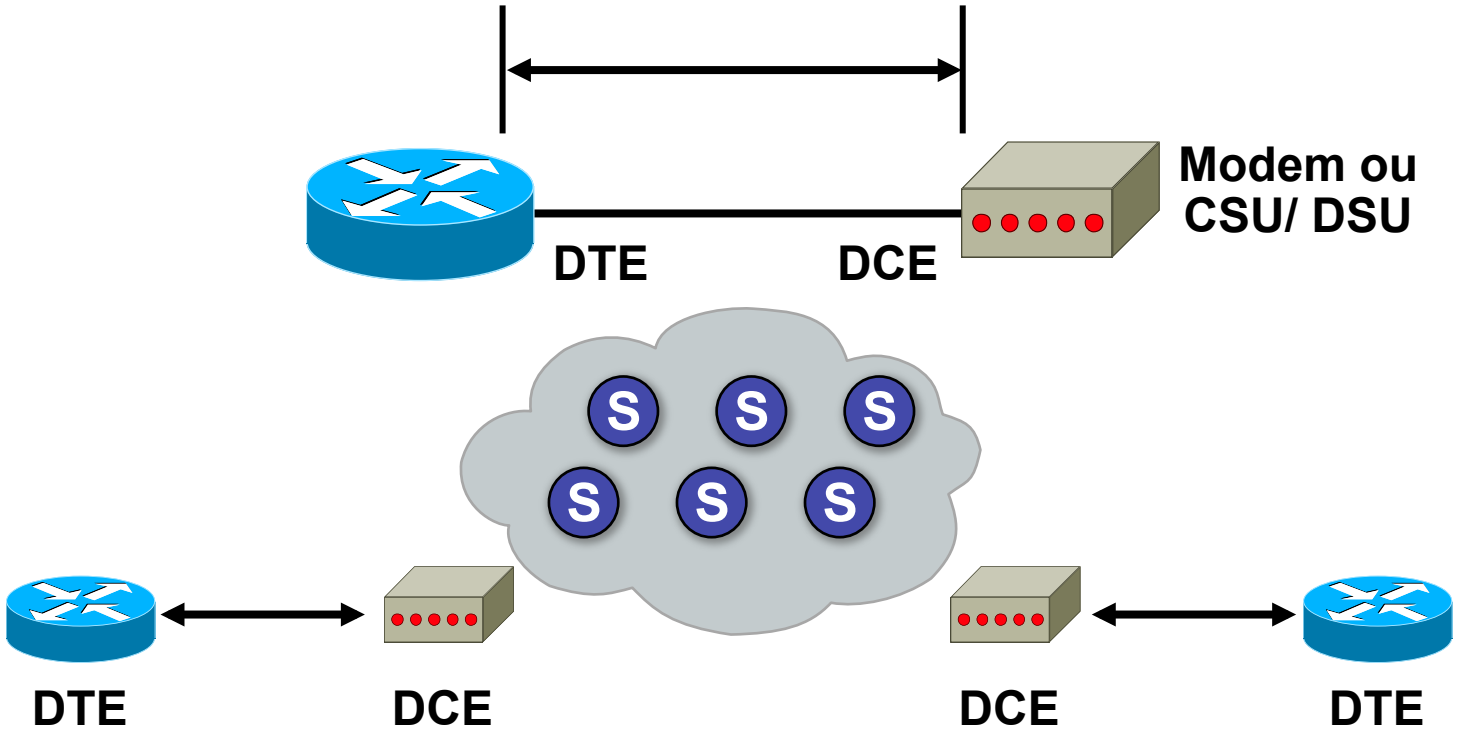


CSU/DSU



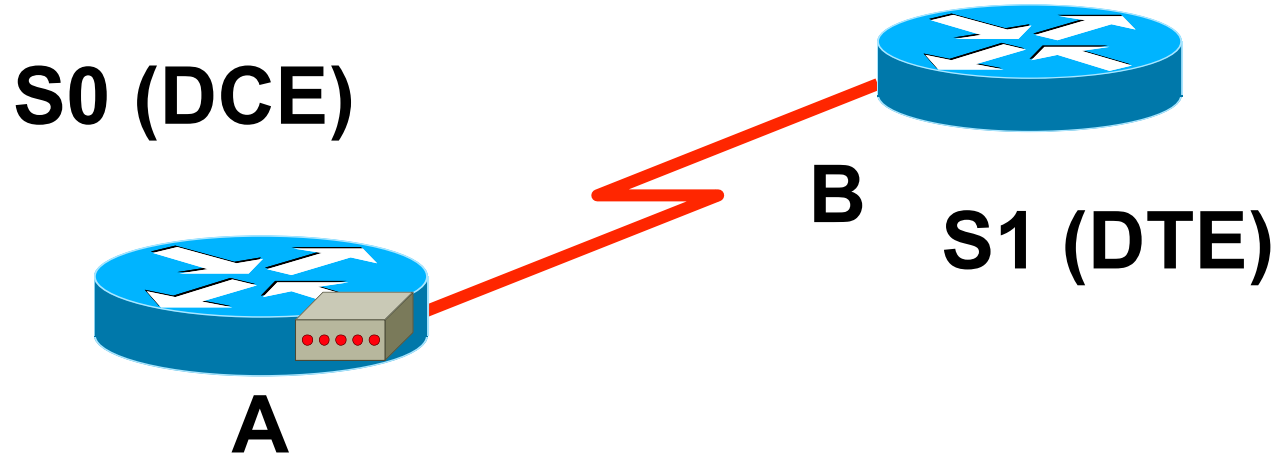
- **Le CSU/DSU est un modem numérique**
- **Il est utilisé pour les liaisons spécialisées**

DTE/DCE



- **C'est le réseau opérateur qui est en charge de l'horloge**

Connection Back-to-Back



- L'un des routeurs doit simuler le modem et envoyer l'horloge
- La fréquence d'horloge indique la vitesse :

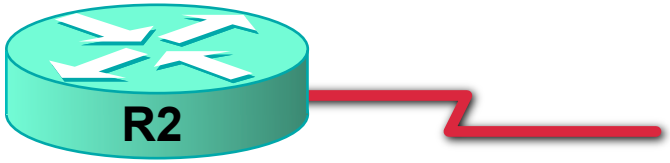
Exemple : clock rate 64 000 pour 64 Kbits

WAN

Wide Area Network

Protocoles d'encapsulation

- Protocoles de Niveau 2 :
  - HDLC
    - High Data Link Control Protocol
  - PPP
    - point-to-point Protocol
  - Frame-Relay



- Sur interface serial
- Pour les commandes show, utiliser show interface (niveau 2) et non show ip interface (niveau 3)

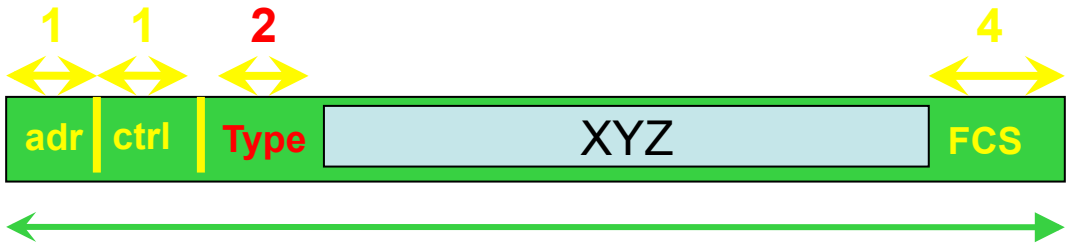
HDLC

- C'est le protocole par défaut sur interface serial d'un équipement Cisco

```
Router#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
```

Entêtes HDLC CISCO

- CISCO n'utilise pas le standard HDLC de l'OSI conçu à la base pour X25.
  - Il rajoute un champ TYPE propriétaire pour indiquer le type de protocol encapsulé, c'est-à-dire IP.
    - 2 octets
- On ne pourra faire du HDLC qu'entre équipements Cisco
- Entre routeurs de marque différente, il faudra passer en encapsulation ppp



la trame HDLC **cisco**

Configuration

- `configure terminal`
- `interface serial 0/0`
- `encapsulation hdlc`

- C'est déjà l'encapsulation par défaut.
- Cette commande permet donc de revenir à HDLC si un autre protocole d'encapsulation avait été configuré.

Test

Which command can you enter to determine whether serial interface 0/2/0 has been configured using HDLC encapsulation?

A. router#show platform
B. router#show interfaces Serial 0/2/0
C. router#show ip interface s0/2/0
D. router#show ip interface brief

- Réponse : B

Test

Which two statements about using leased lines for your WAN infrastructure are true? (Choose two.)

A. Leased lines provide inexpensive WAN access.
B. Leased lines with sufficient bandwidth can avoid latency between endpoints.
C. Leased lines require little installation and maintenance expertise.
D. Leased lines provide highly flexible bandwidth scaling.
E. Multiple leased lines can share a router interface.
F. Leased lines support up to T1 link speeds.

- Réponse : CD

Test

Which two statements about wireless LAN controllers are true? (Choose two.)

A. They can simplify the management and deployment of wireless LANs.
B. They rely on external firewalls for WLAN security.
C. They are best suited to smaller wireless networks.
D. They must be configured through a GUI over HTTP or HTTPS.
E. They can manage mobility policies at a systemwide level.

- Réponse : AE

PPP

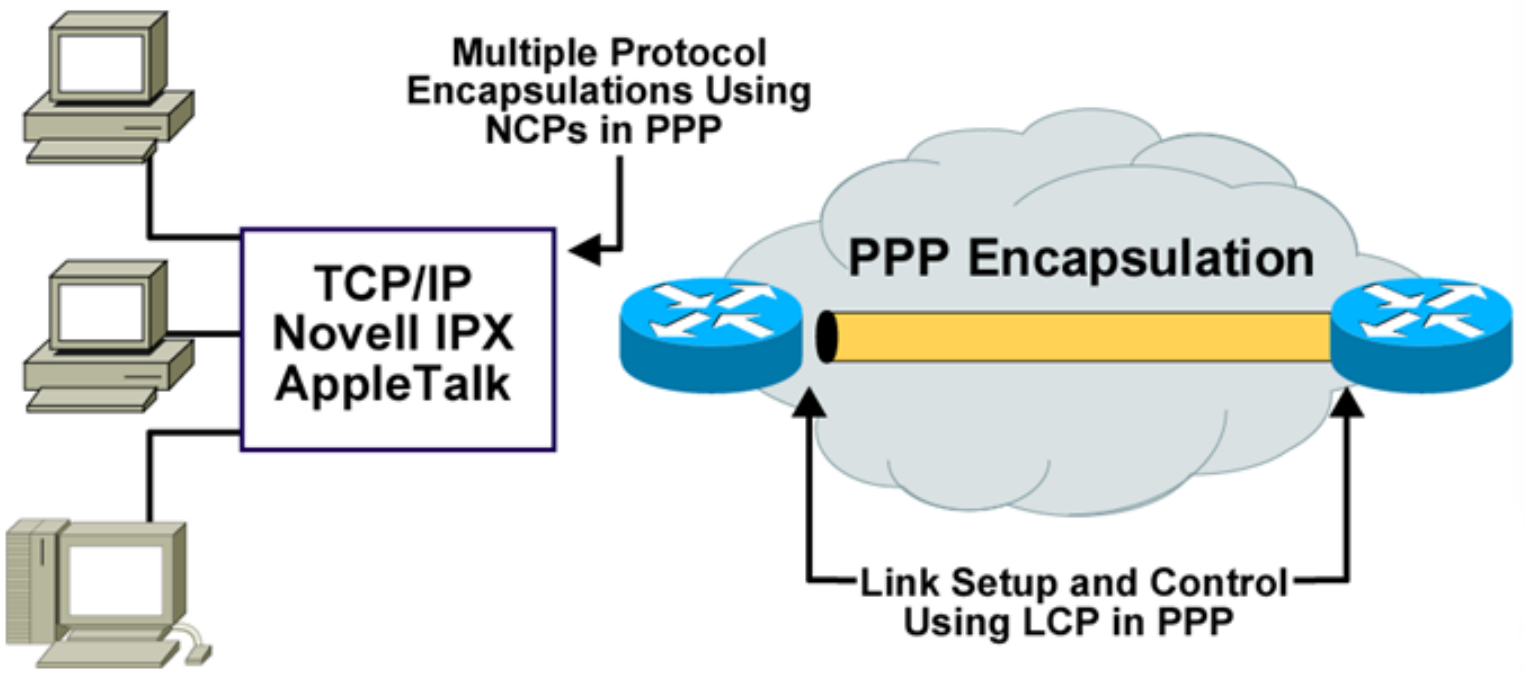
Point to Point Protocol

Avantages de PPP

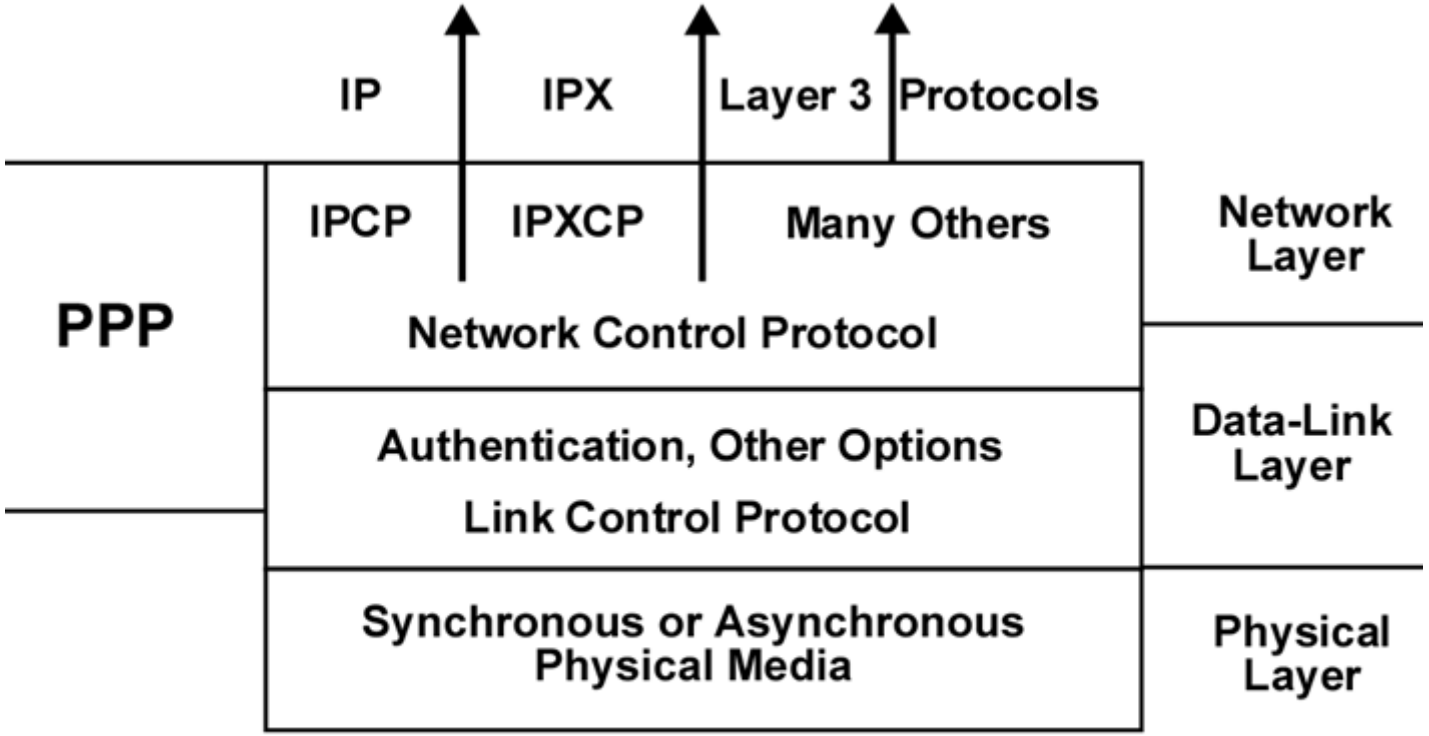
- N’est pas propriétaire CISCO
  - standard
- Gère l’autentification
- Gère le multi-link
- Surveille la qualité de la liaison
- Sait faire la compression

Deux familles de protocoles

- LCP
  - Link Control Protocol
  - Permet détablir la liaison avant d'envoyer des trames.
  - Gère les négotiations à effectuer avant de monter la liaison PPP session phase
  - Dans `show interface`, « LCP open » signifie les phases de négociation sont terminées et le trafic peut être envoyé.
- NCP
  - Network Control Protocol
  - Permet d'envoyer les trames du trafic.
  - Gère l'encapsulation des paquets :
    - IPCP pour les paquets IP : IP Control Protocol
    - CDPCP pour les paquets CDP : CDP Control Protocol



- PPP can carry packets from several protocol suites using NCP.
- PPP controls the setup of several link options using LCP.



- PPP = Data link with network layer services

Configuration

- `configure terminal`
- `interface serial 0/0`
- `encapsulation ppp`

- `show interface serial 0/0`

L'authentification

- Objectif :
  - garantir l'identitié de l'équipement distant.

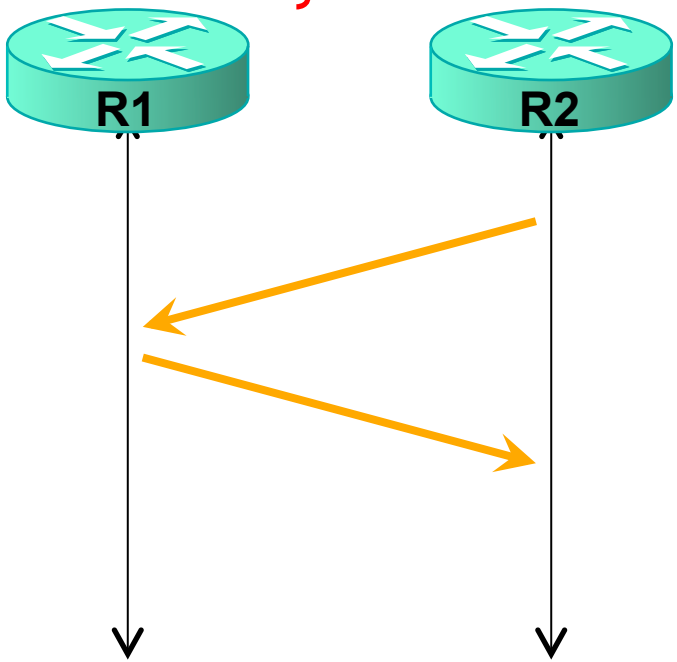
- Deux protocoles disponibles :
  - PAP :
    - Point-to-point Authentication Protocol
    - Le mot des passe est envoyé en clair
  - CHAP :
    - Challenge Handshake Authentication Protocol
    - Le mot de passe n'est pas envoyé

Handshake

Combien d'échanges sont nécessaires pour que R1 puisse authentifier R2 ?

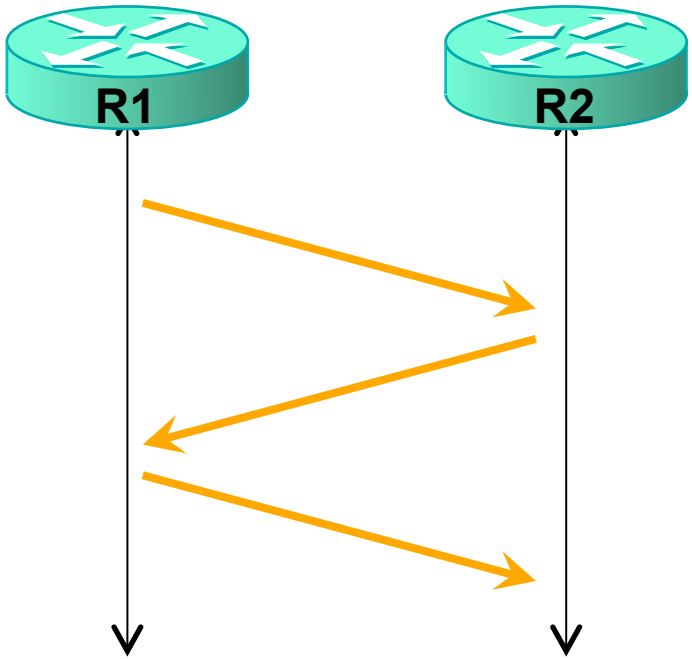
PAP

Two-way handsake



CHAP

Three-way handsake

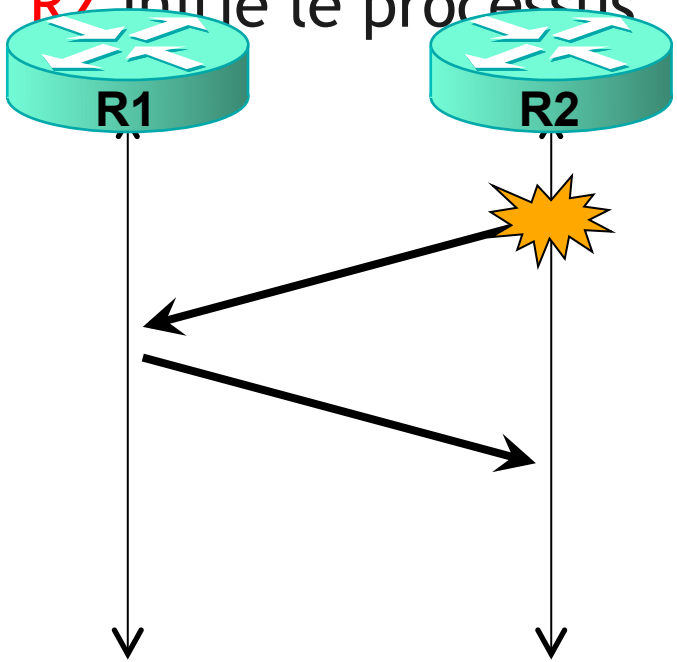


Initiation de l'authentification

Lorsque R1 veut authentifier R2, qui initie le processus d'authentification ?

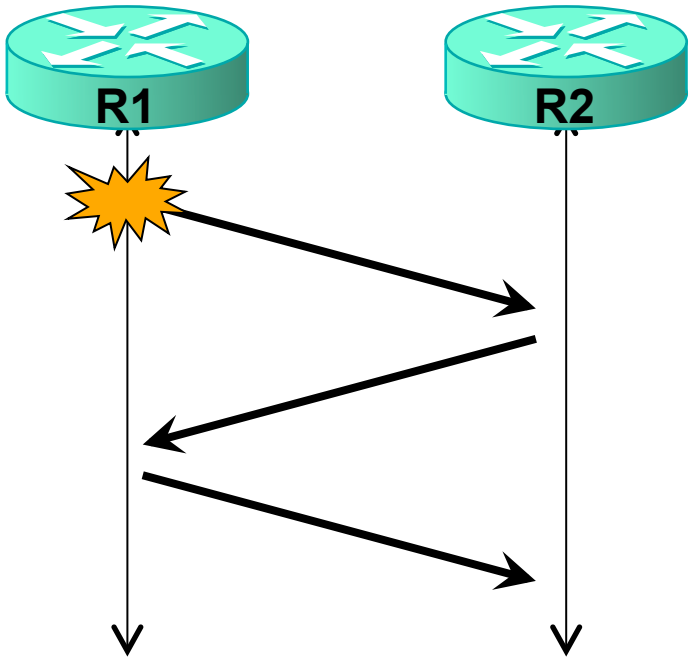
PAP

R2 initie le processus



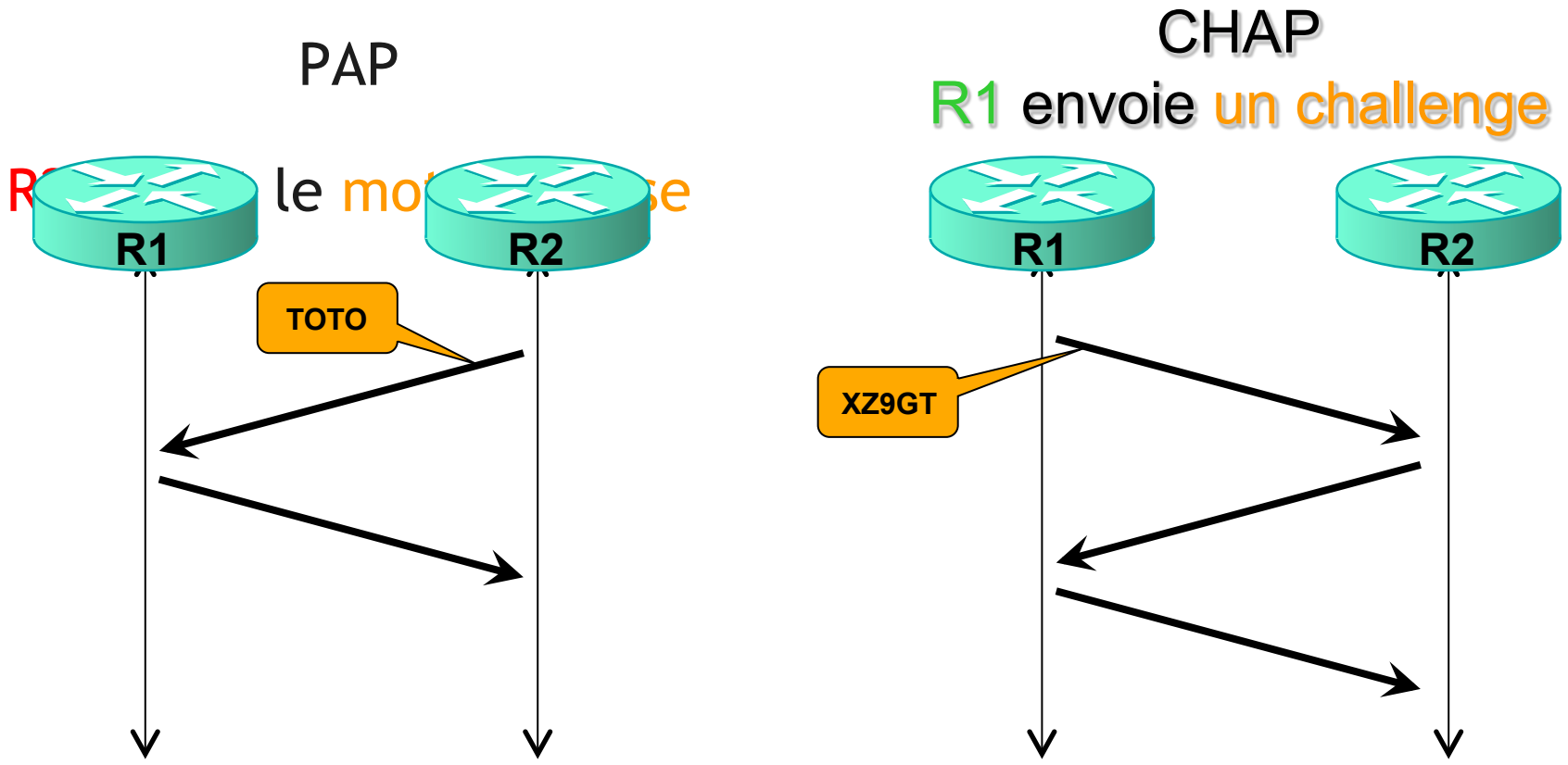
CHAP

R1 initie le processus



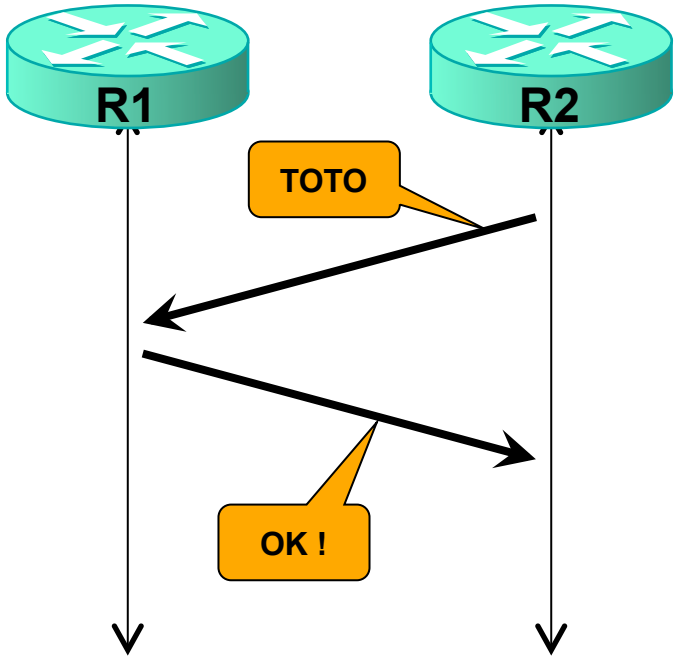
Le Mot de passe TOTO

Un individu qui écoute la communication pourra-t-il facilement découvrir le mot de passe ?



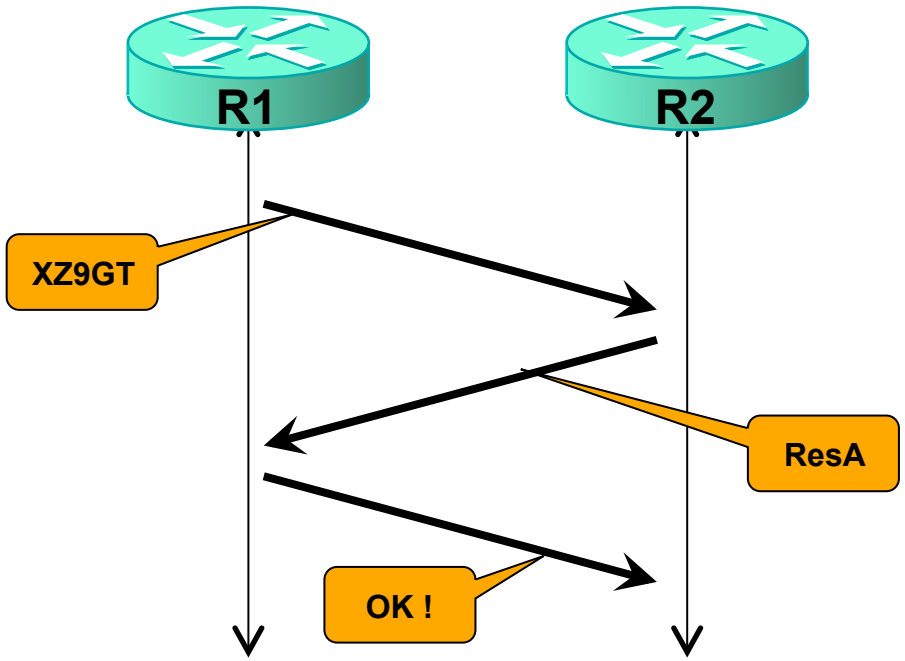
Fonctionnement de PAP

- Deux étapes :
  - R2 envoie le mot de passe TOTO
  - R1 vérifie le mot de passe reçu et répond



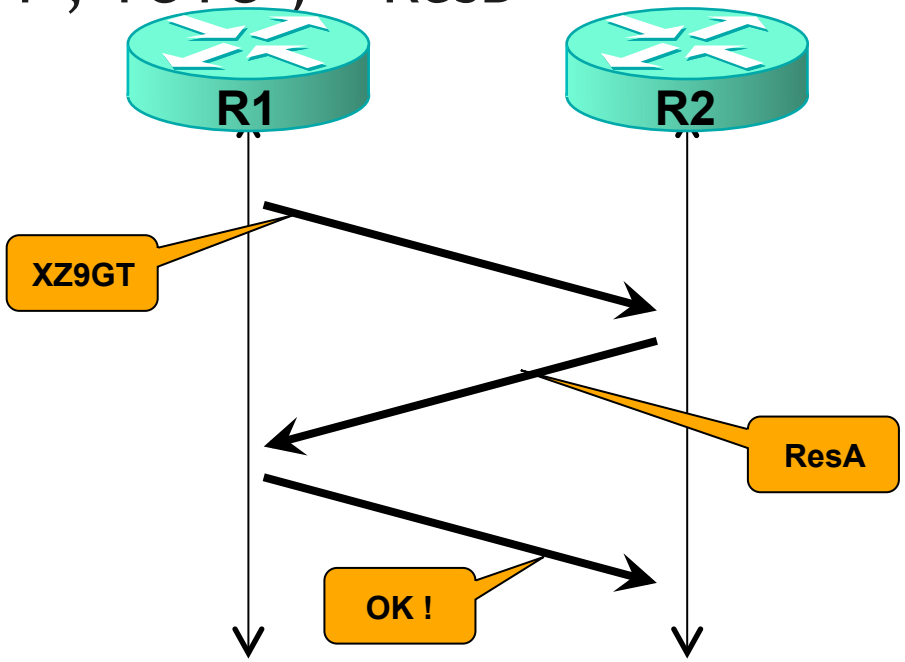
Fonctionnement de CHAP

- Trois étapes :
  - R1 envoie un challenge
    - différent à chaque fois
  - R2 calcule le MD5 et envoie le résultat à R1
    - fonction mathématique
    - dont le résultat dépend
      - du challenge
      - du mot de passe TOTO
  - R1 calcule le même MD5 et compare son résultat avec celui envoyé par R2

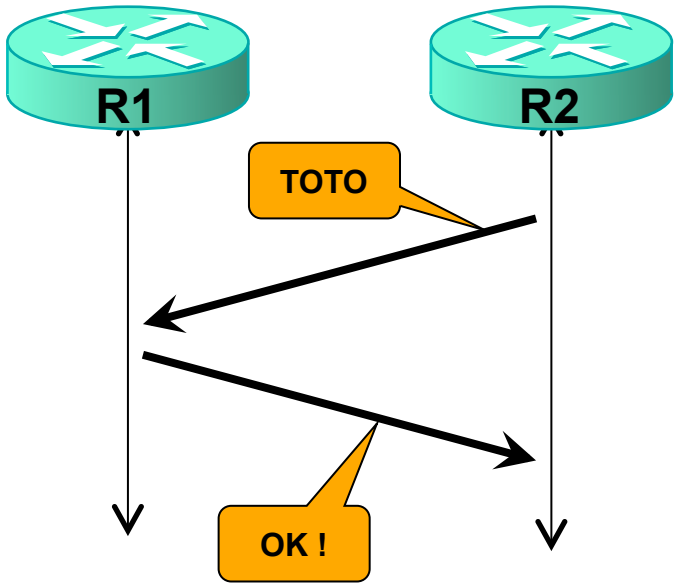


Exemple CHAP

- Trois étapes :
  - R1 envoie le XZ9GT
  - R2 calcule le MD5 (XZ9GT , TOTO) = ResA
  - R1 calcule le MD5 (XZ9GT , TOTO) = ResB
    - si ResA = ResB
    - alors R1 répond OK



Configuration de PAP

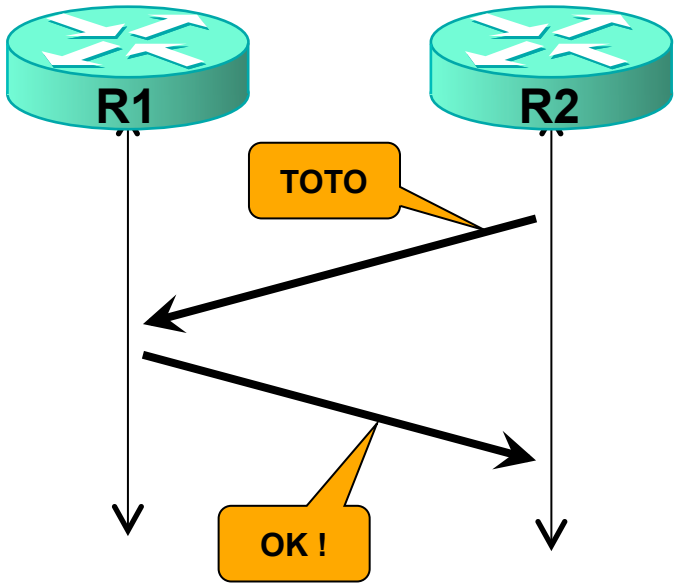



```
hostname R1

username R2 password TOTO

interface s0/0

encapsulation ppp

ppp authentication pap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
```

QUI authentifie QUI ?

Configuration de PAP

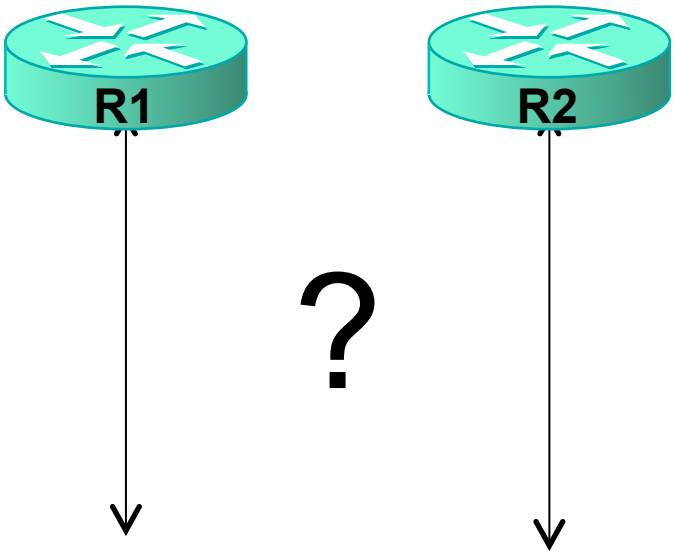



```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication pap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
```

Seul R1 authentifie R2

Configuration de PAP

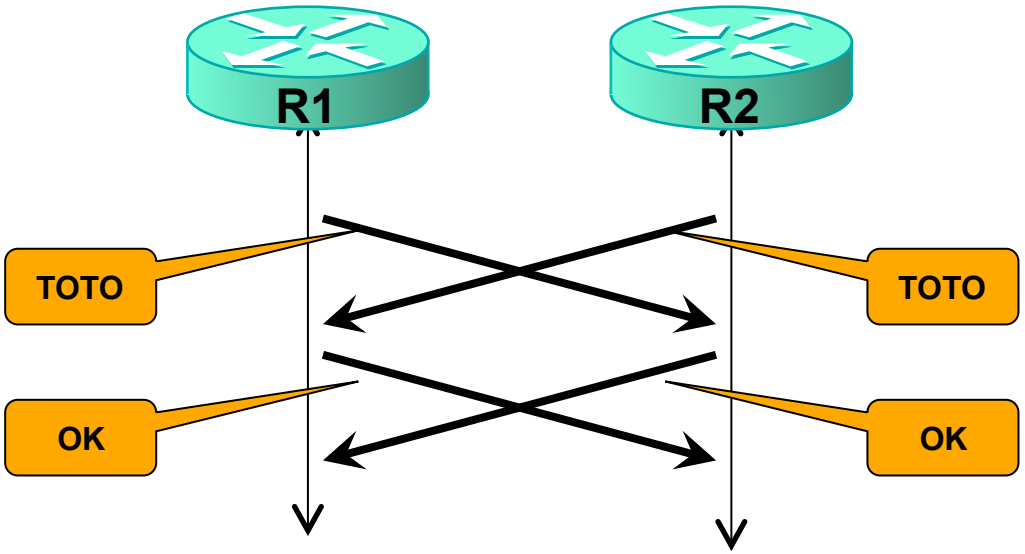



```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication pap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
ppp authentication pap
```

QUI authentifie QUI ?

Configuration de PAP

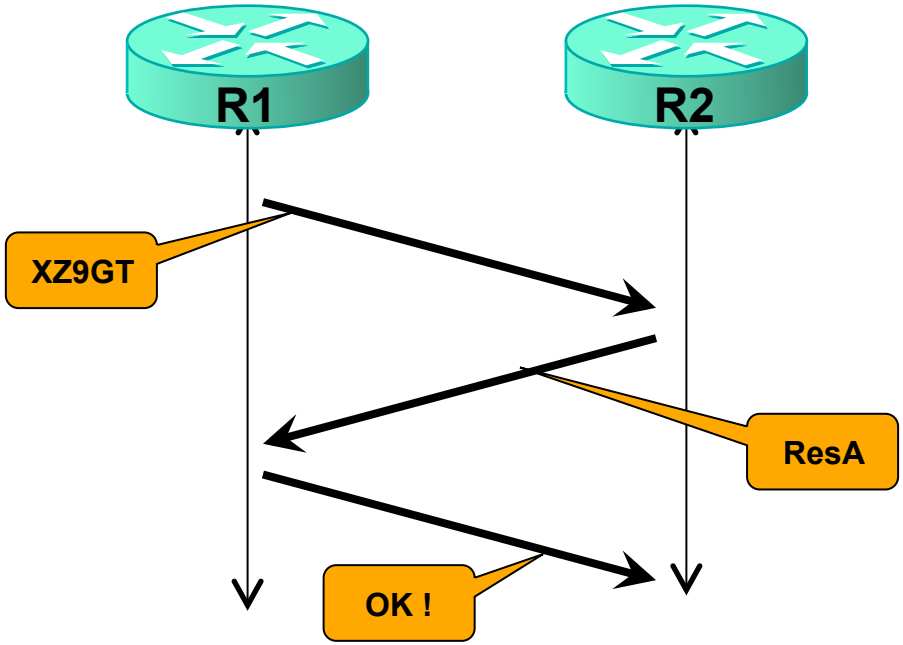



```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication pap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
ppp authentication pap
```

R1 et R2 s'authentifient mutuellement

Configuration de CHAP

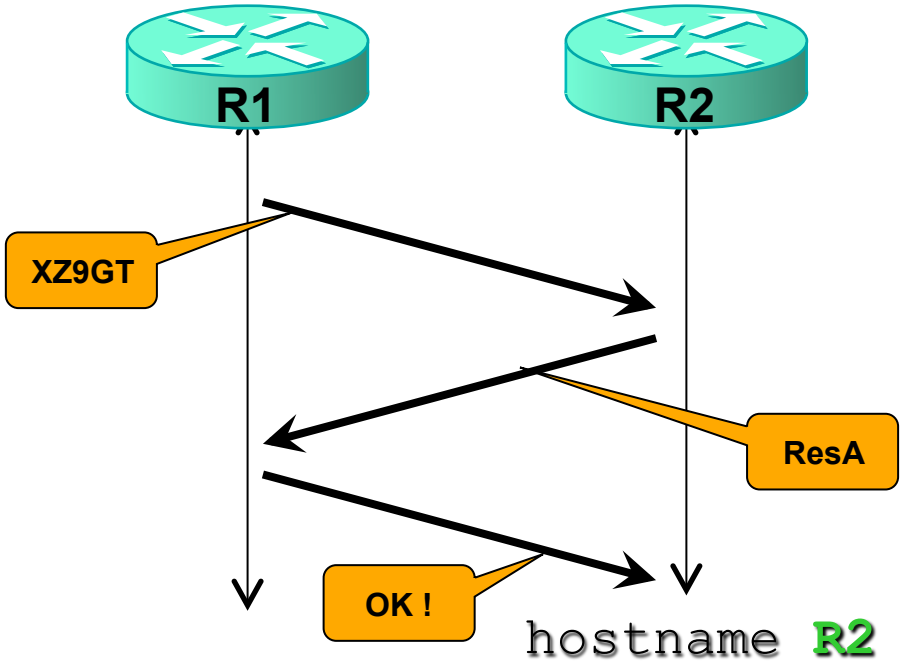



```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication chap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
```

QUI authentifie QUI ?

Configuration de CHAP




```
hostname R1

username R2 password TOTO

interface s0/0

encapsulation ppp
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
```

ppp authentication chap Seul R1 authentifie R2

Configuration de CHAP

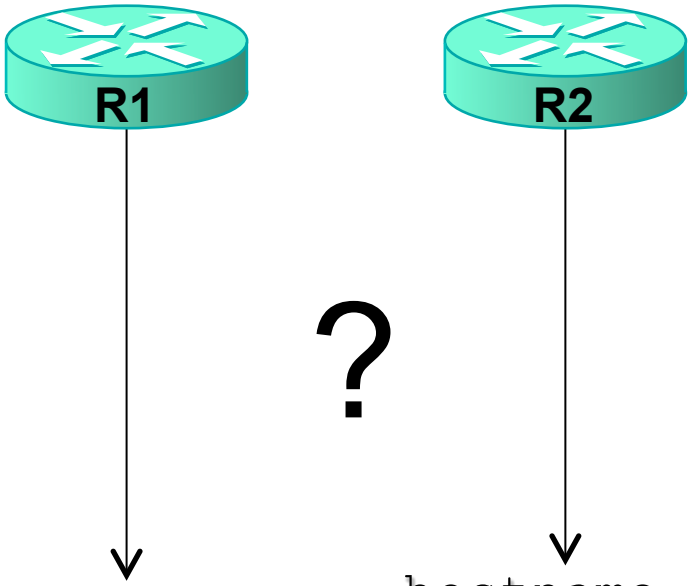
?

```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication chap
```

```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
ppp authentication chap
```

QUI authentifie

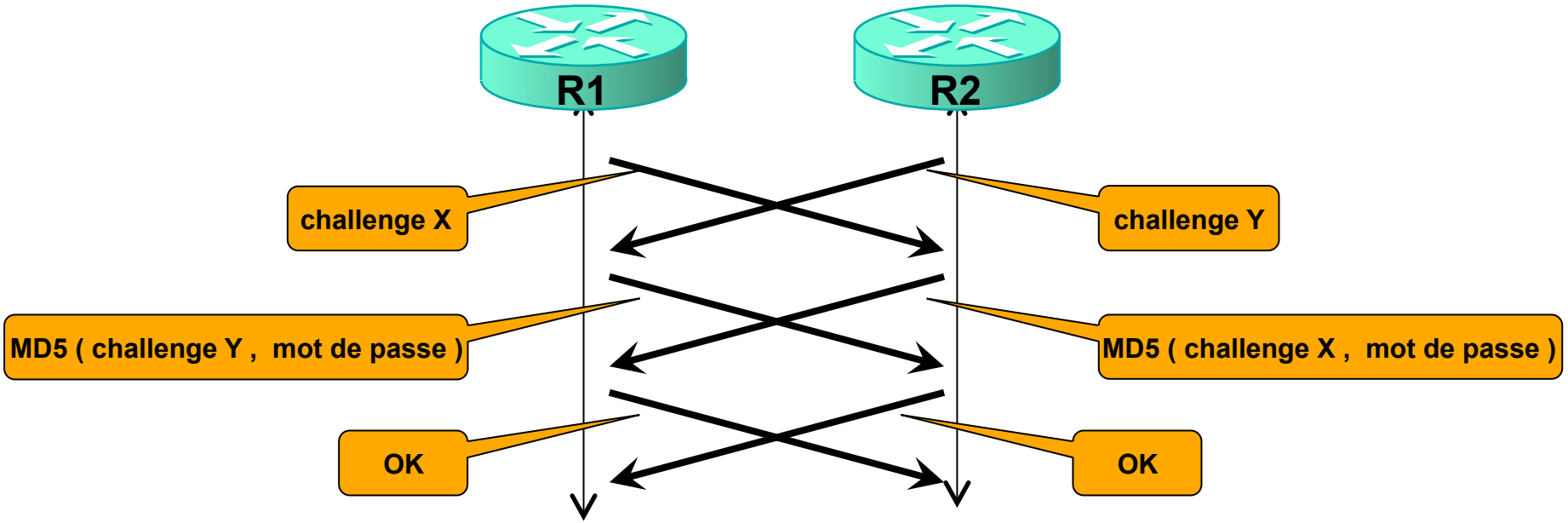
Configuration sur interface




```
hostname R1

username R2 password TOTO

  interface s0/0
  encapsulation ppp
  ppp authentication chap
```

```
hostname R2
username R1 password TOTO

interface s0/0
encapsulation ppp
ppp chap hostname R2
ppp chap password TOTO
ppp authentication chap
```

Configuration de CHAP

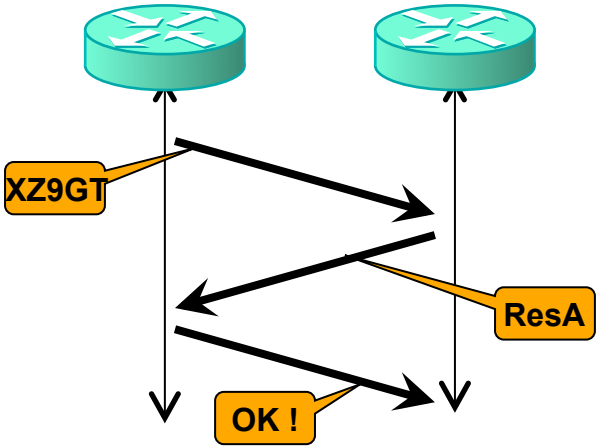



```
hostname R1
username R2 password TOTO
interface s0/0
encapsulation ppp
ppp authentication chap
```

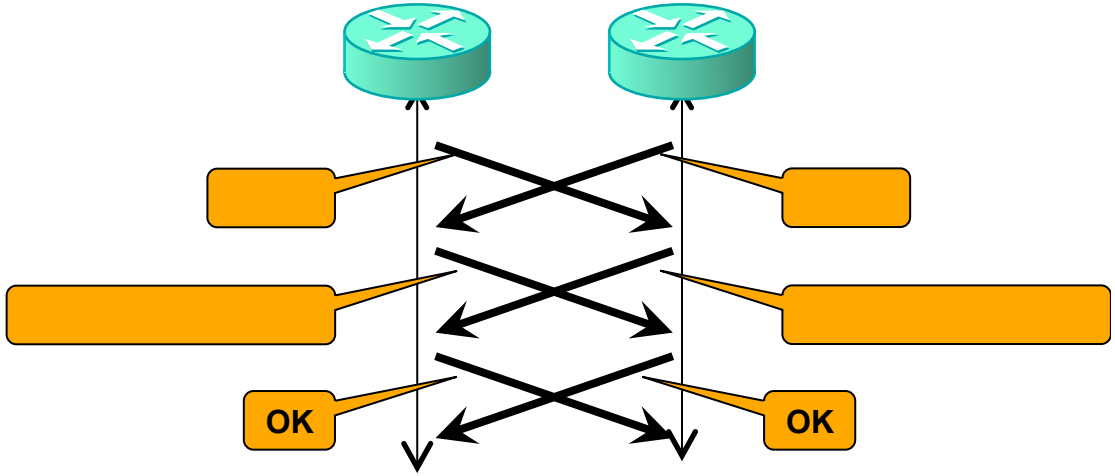
```
hostname R2
username R1 password TOTO
interface s0/0
encapsulation ppp
ppp authentication chap
```

R1 et R2 s'authentifient mutuellement

Nomenclature

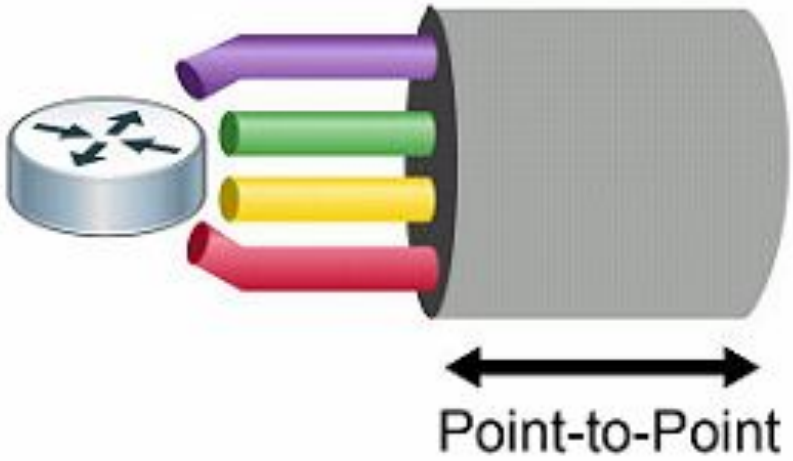


ONE-WAY
CHALLENGE



TWO-WAY
CHALLENGE

Multilink PPP



MLP overview:

- MLP combines multiple physical links into a logical bundle called a Multilink PPP bundle.
- The MLP over Serial Interfaces feature provides the following functionalities:
  - Load balancing
  - Increased redundancy
  - Link fragmentation and interleaving (LFI)

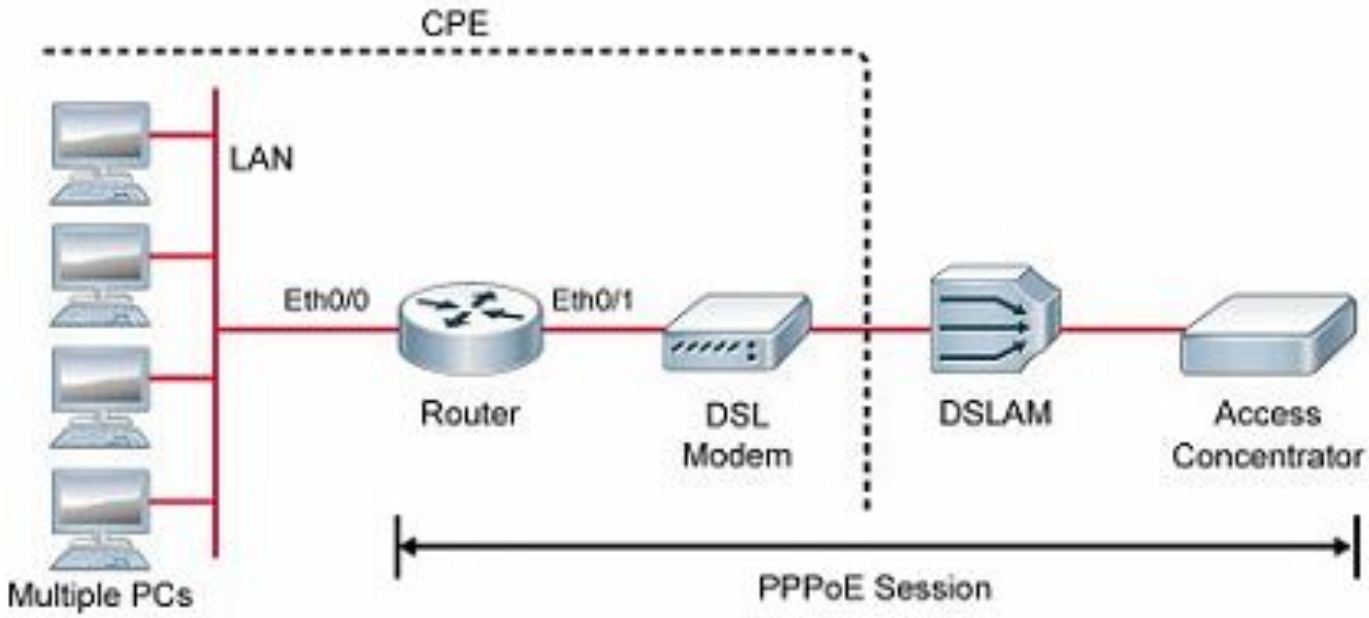
Configuration PPP multilink

```
interface multilink1
   ppp multilink
   ppp multilink group 1
   ip address ….

Interface serial 0/0
   encap ppp
   ppp multilink
   ppp multilink group 1

Interface serial 0/1
   encap ppp
   ppp multilink
   ppp multilink group 1

   show ppp multilink
   show interfaces multilink1
```

PPPoE Client

PPPoE client overview:

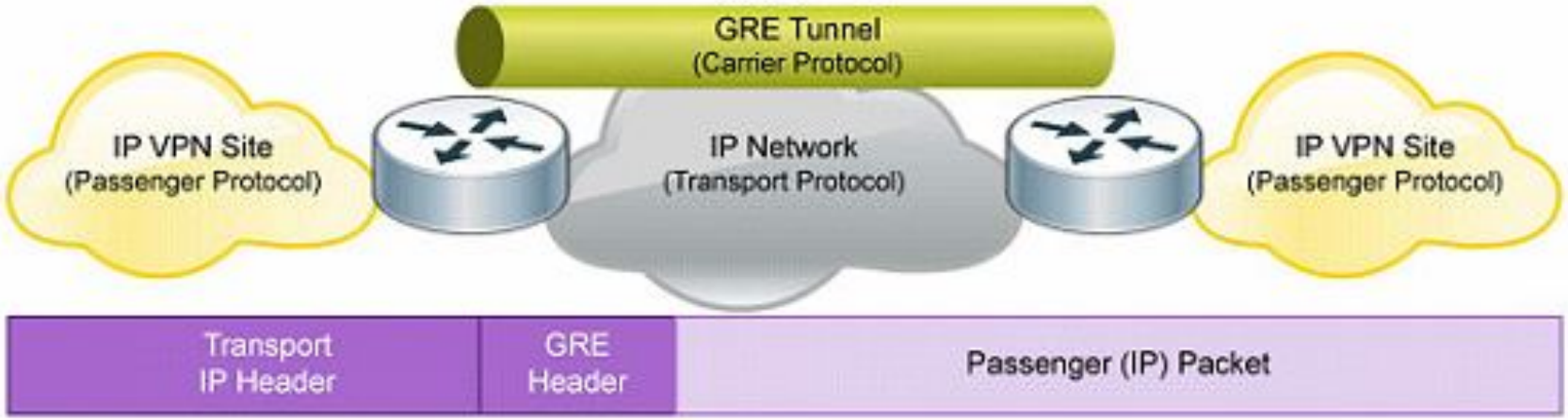
- PPPoE is a commonly used application in the deployment of DSL.
- A Cisco router can act as a PPPoE client.
- You can connect multiple PCs on the Ethernet segment that is connected to the Cisco IOS router acting as a PPPoE client.



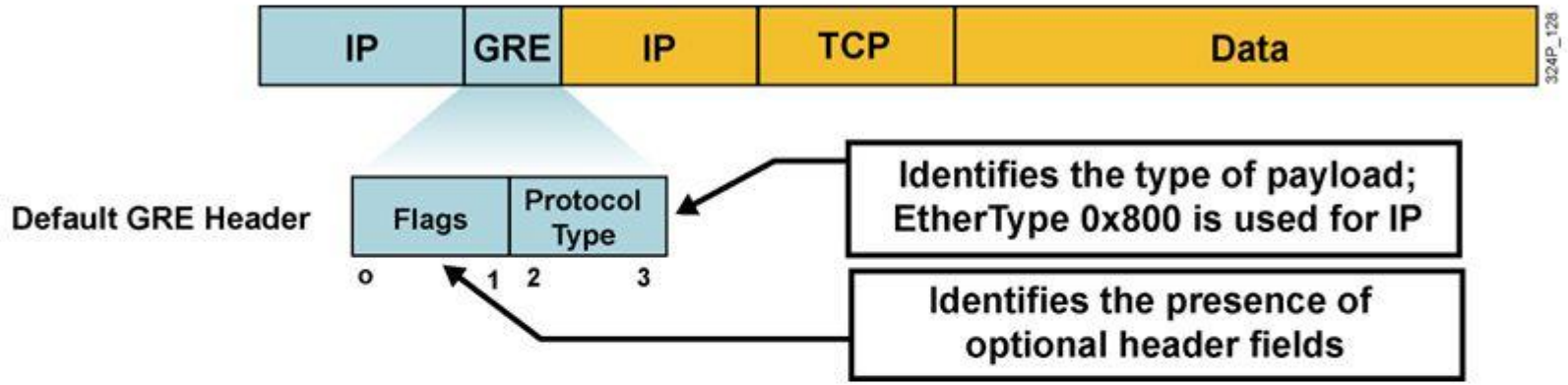
GRE Tunnel Overview

The following are the main GRE—Generic Routing Encapsulation characteristics:

- GRE is one of many tunneling protocols
- IP protocol 47 defines GRE packets
- Allows routing information to be passed between connected networks
- No encryption



Default GRE Characteristics



- Tunneling of arbitrary OSI Layer 3 payload is the primary goal of GRE
- Stateless (no flow control mechanisms)
- No security (no confidentiality, data authentication, or integrity assurance)
- 24-byte overhead by default (20-byte IP header and 4-byte GRE header)

Configuration d'un GRE

- R1 :
  - interface tunnel 10
    - tunnel source 1.1.1.1
    - tunnel destination 2.2.2.2
    - ip address 10.0.0.1 255.255.255.0
- R2 :
  - interface tunnel 10
    - tunnel source 2.2.2.2
    - tunnel destination 1.1.1.1
    - ip address 10.0.0.2 255.255.255.0

Configuring GRE Tunnel

To implement a GRE tunnel, perform the following actions:

Create a tunnel interface.

```
Router(config)# interface tunnel tunnel-id
```

Configure GRE tunnel mode. This is a default tunnel mode so it is not necessary to configure it.

```
Router(config-if)# tunnel mode gre ip
```

Configure an IP address for the tunnel interface.

```
Router(config-if)# ip address ip-address mask
```

Specify the tunnel source IP address.

```
Router(config-if)# tunnel source ip-address
```

Specify the tunnel destination IP address.

```
Router(config-if)# tunnel destination ip-address
```

Verifying GRE Tunnel

To verify a GRE tunnel, perform the following actions:

Determine whether the tunnel interface is up or down.

```
Router# show ip interface brief Tunnel tunnel-id
```

Verify the state of the GRE tunnel.

```
Router# show interface tunnel tunnel-id
```

Verify that the tunnel network is seen as directly connected in the routing table.

```
Router# show ip route
```

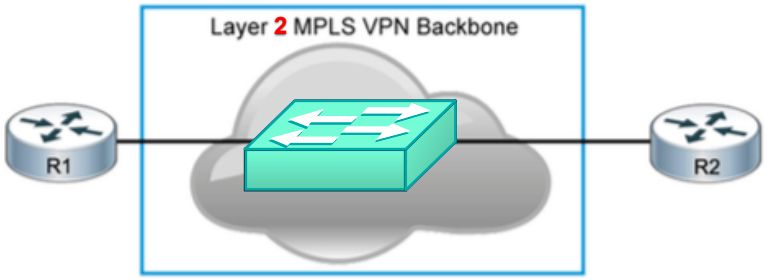
VPN

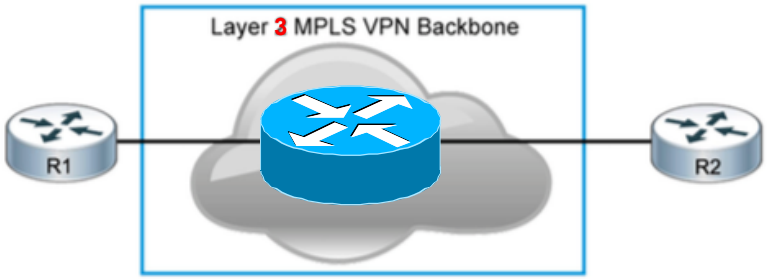
Connexions entre le siège et les branches

- Connections traditionnelles :
  - Liaison LS, Frame-Relay, …
  - Désavantages :
    - Cout
    - Bande passante
    - Scalabilité
- Nouveaux modes de connection :
  - VPN MPLS
  - VPN tunnelé (GRE, IPSec, DMVPN)
  - Avantages :
    - Full-mesh
    - Sécurité
    - Scalabilité

Routage via VPN MPLS

- VPN couche 2 :
  - R1 et R2 sont connectés sur le même réseau IP.
  - La relation de voisinage sera établie directement entre R1 et R2
  - Le client souhaite gérer lui-même son infrastructure de routage

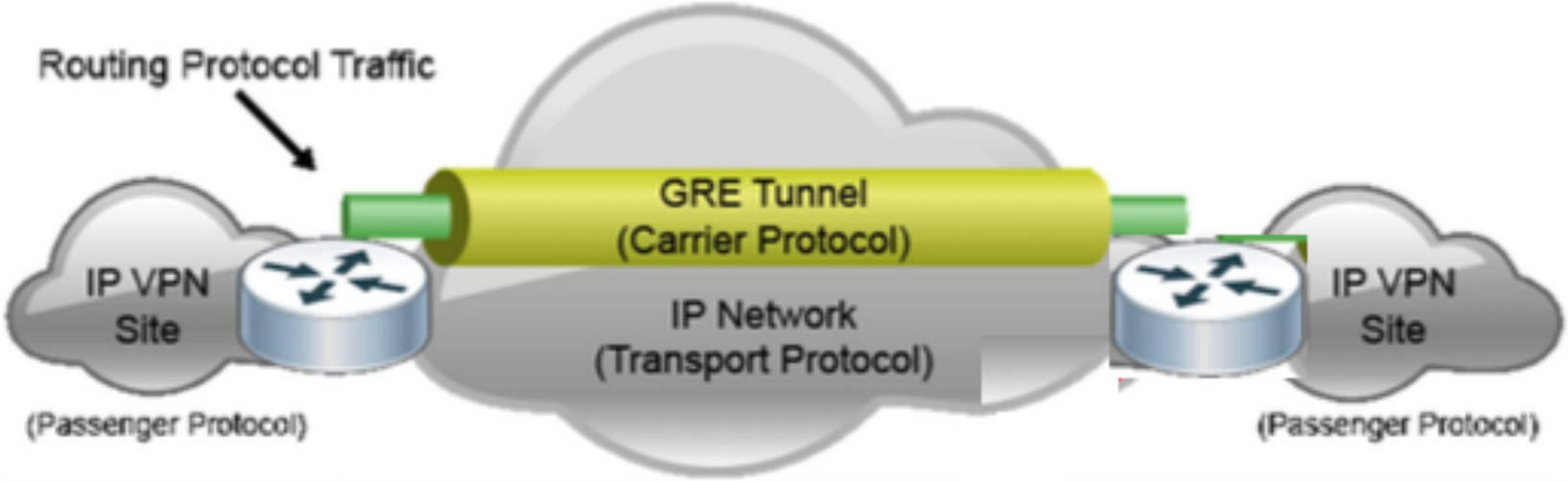




- VPN couche 3 :
  - R1 et R2 sont chacun sur un réseau IP différent.
  - Le FAI doit participer au routage entre vos sites.
  - Le client laisse le FAI gérer le routage entre ses sites

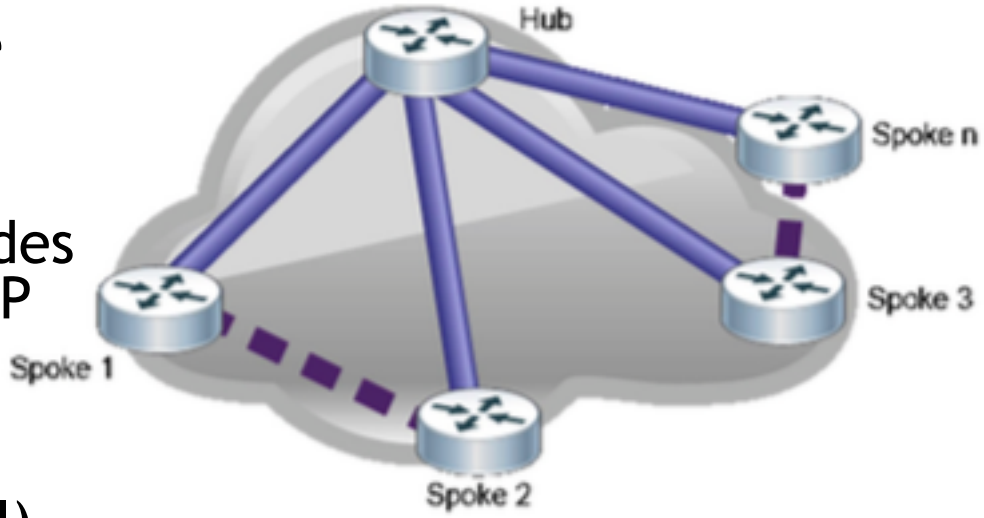
Routage via Tunnel GRE

- Le Tunnel GRE :
  - Crée un tunnel virtuel point à point entre 2 routeurs
  - Utilise l'identifiant IP protocol 47
  - Pas de cryptage, pas de mécanisme de contrôle de flux
  - Rajoute l'entête GRE (24 octets)
  - Peut encapsuler une grande variété de protocoles
    - Peut encapsuler le multicast
      - Approprié pour les protocoles de routage



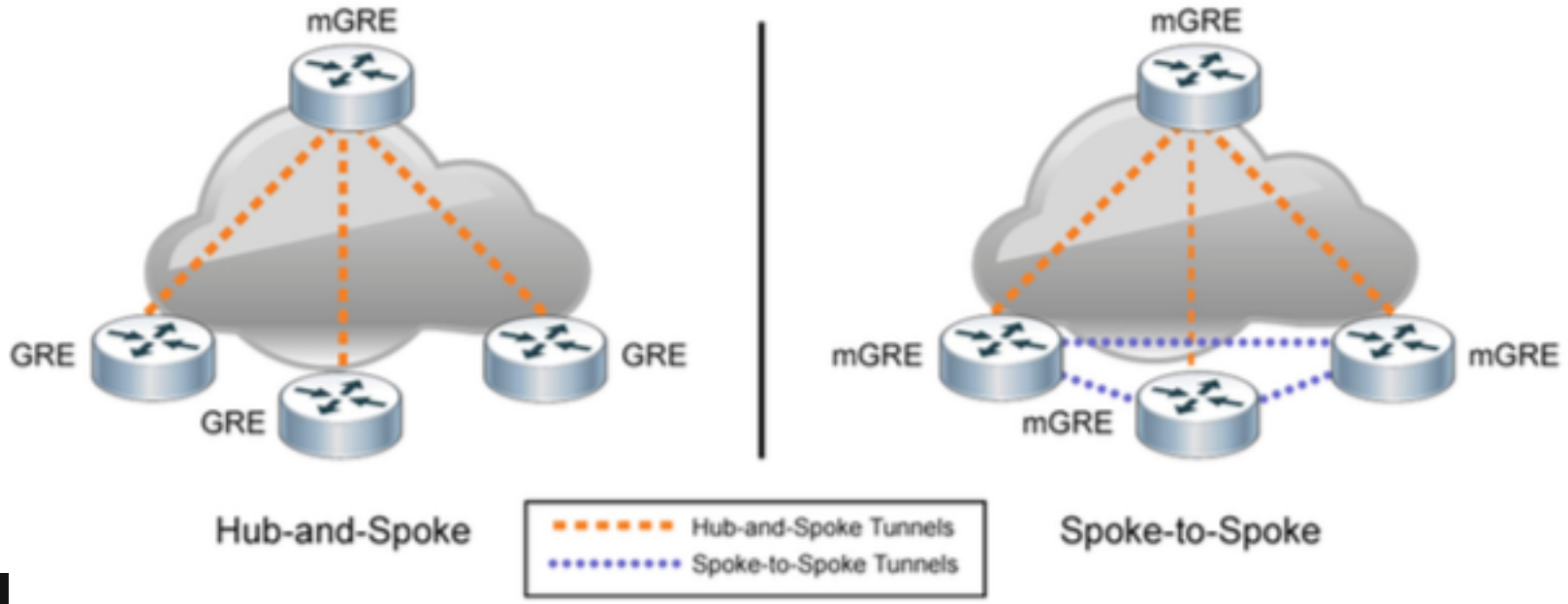
Routage via DMVPN

- Désavantages du tunnel GRE :
  - Le rajout d'un nouveau spoke entraîne une reconfiguration du hub
  - Le trafic entre les spokes doit traverser le hub
- DMVPN :
  - Scalable avec configuration minimale sur hub
  - Utilise mGRE et NHRP.
  - Fonctionne aussi avec des spokes dont l'adresse IP est attribuée dynamiquement (nécessite authentification via PKI)



mGRE

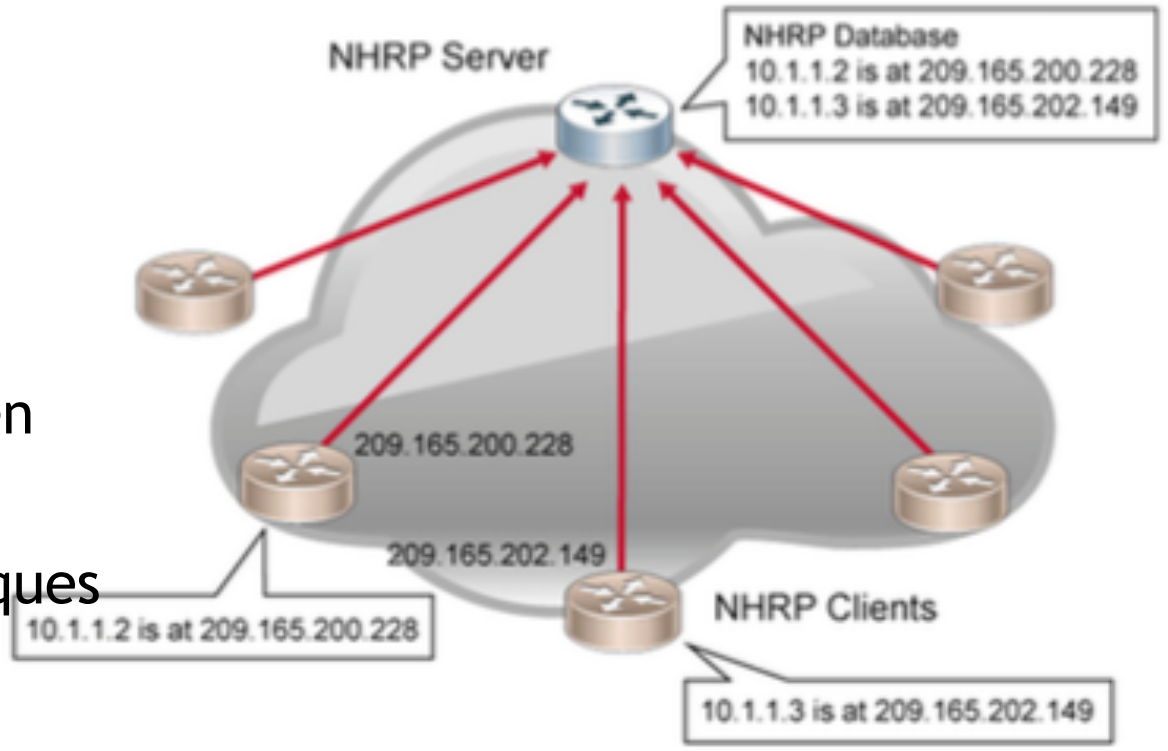
- Plusieurs spokes peuvent se connecter à une seule interface tunnel mGRE
- Autorise le multicast :
  - Permet la diffusion des annonces de routage



NHRP

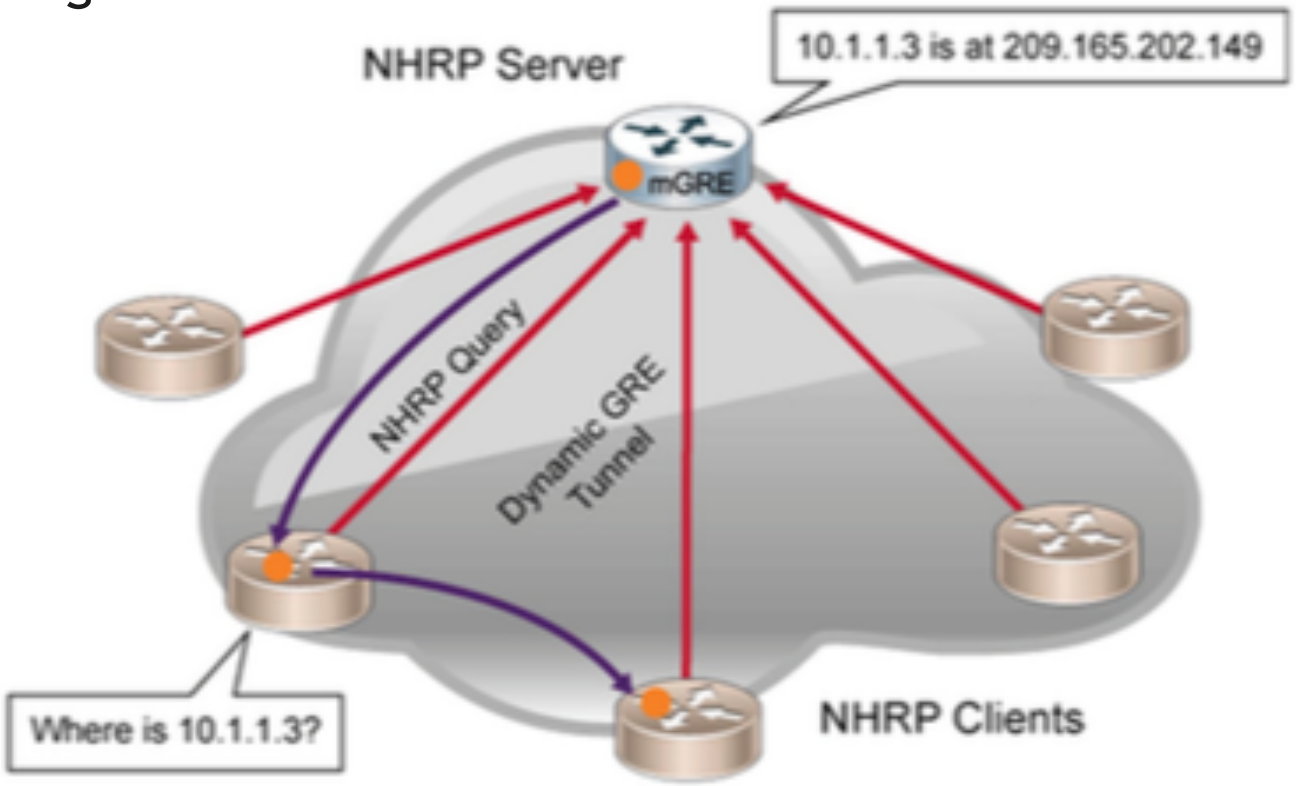
- Next Hop Resolution Protocol
  - Permet au hub de découvrir dynamiquement l'adresse IP distante des spokes
  - Permet aux spokes découvrir l'adresse IP des autres spokes

- Hub = server, Spokes = clients
  - Chaque spoke s'enregistre auprès du hub.
  - Le hub maintien une base de données des adresses physiques et virtuelles (tunnel) des spokes.



Requête NHRP

- Lorsqu'un spoke souhaite envoyer du trafic à un autre spoke, il interroge la base de données du hub, puis monte un tunnel direct :



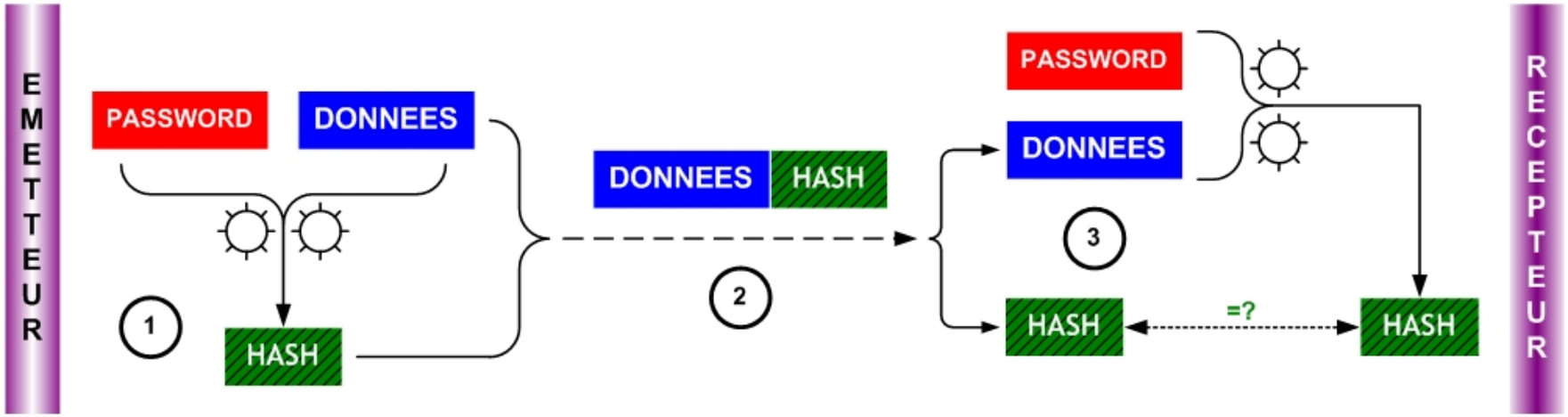
Introduction aux algorithmes

- Clefs symétriques :
  - DES
    - 64 bits
  - 3DES
  - AES
    - 128, 192 ou 256 bits
  - MD5
    - 128 bits
  - SHA1
    - 160 bits
- Clefs asymétriques :
  - RSA
    - 512 bits … 2048 bits …
- Diffie-Hellman :
  - group 1 : 768 bits
  - group 2 : 1024 bits
  - group 5 : 1536 bits

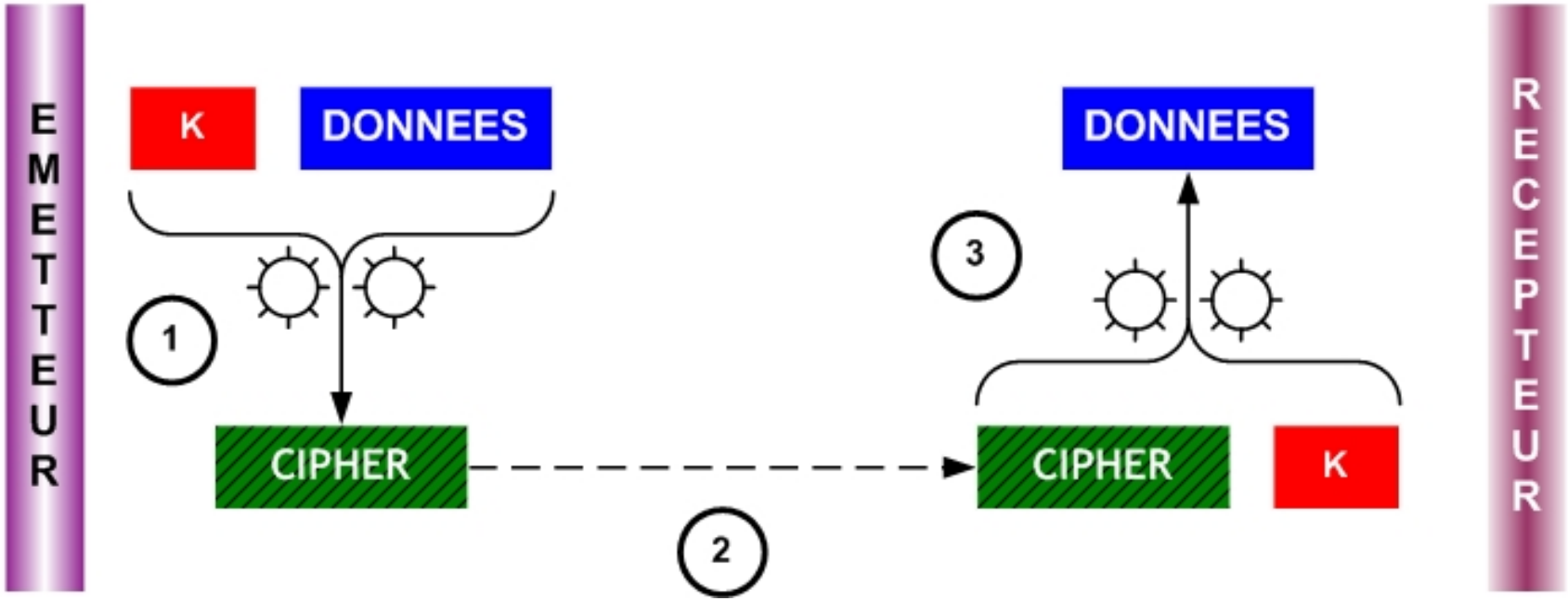
Fonctions d'un VPN

- Confidentialité
  - cryptage DES, 3DES, AES
- Intégrité
  - Hash MD5, SHA1
- Authentification
  - PSK
    - pre shared key
  - RSA signatures
    - certificat
- Avantages d'un VPN sur une solution point à point WAN :
  - Réduction des coûts
  - Sécurité
  - Extensibilité

Authentification & intégrité



Confidentialité

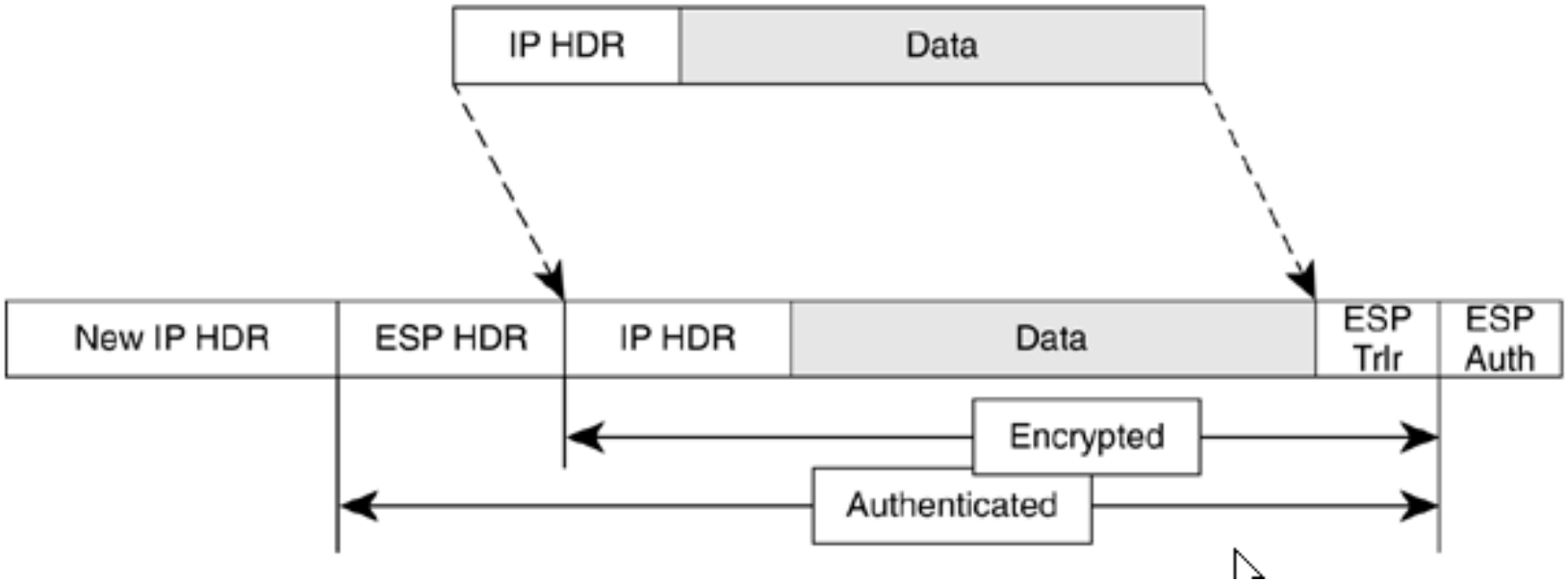


VPN IPSec

- Couche 3 OSI
- Equipements à chaque extrémité :
  - 2 routeurs
  - 2 pare-feu ASA (‘Adaptative Security Appliance’)
  - 1 routeur et 1 pare-feu ASA
- Ils sont classifiés de 3 types :
  - Remote access VPN
  - Site to site VPN
  - Host to host VPN

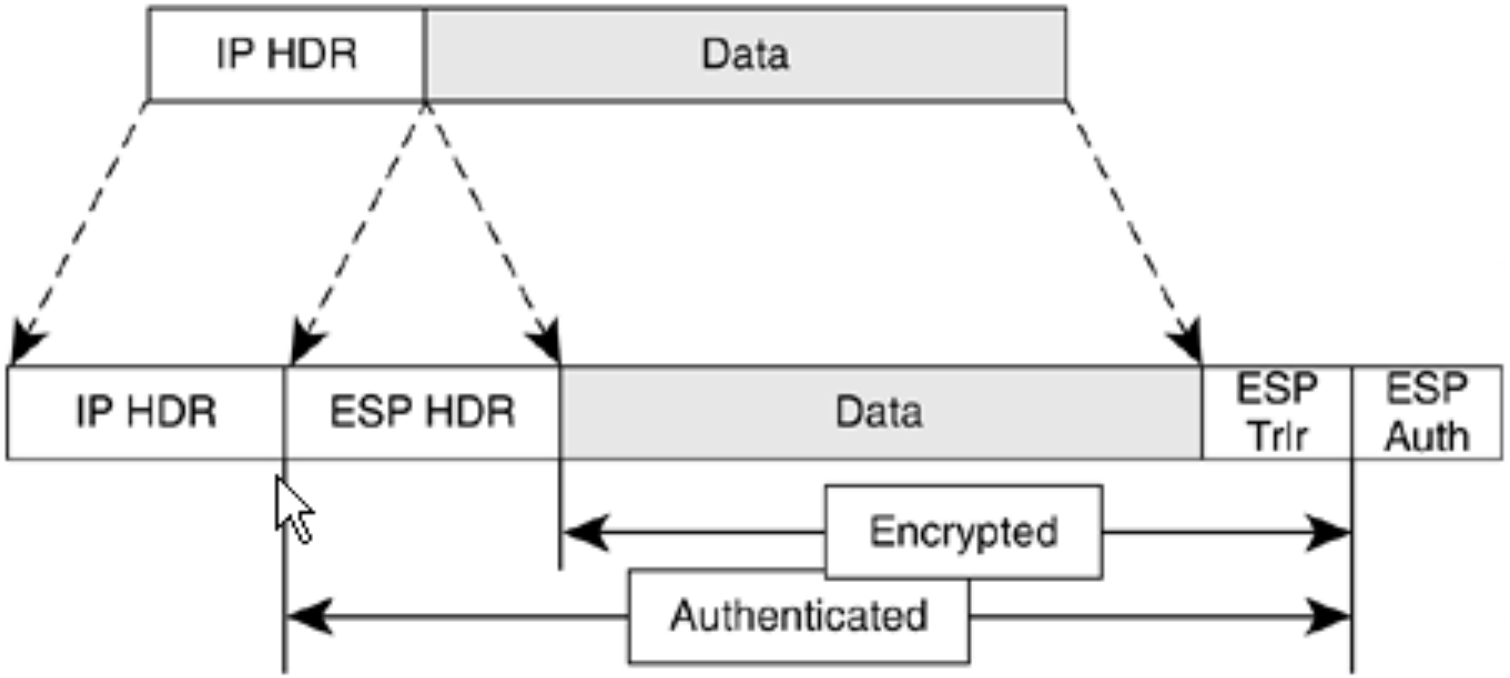
IP Sec Mode Tunnel

- Le paquet original n'est pas modifié.
- Il est encapsulé dans un header IPSec.



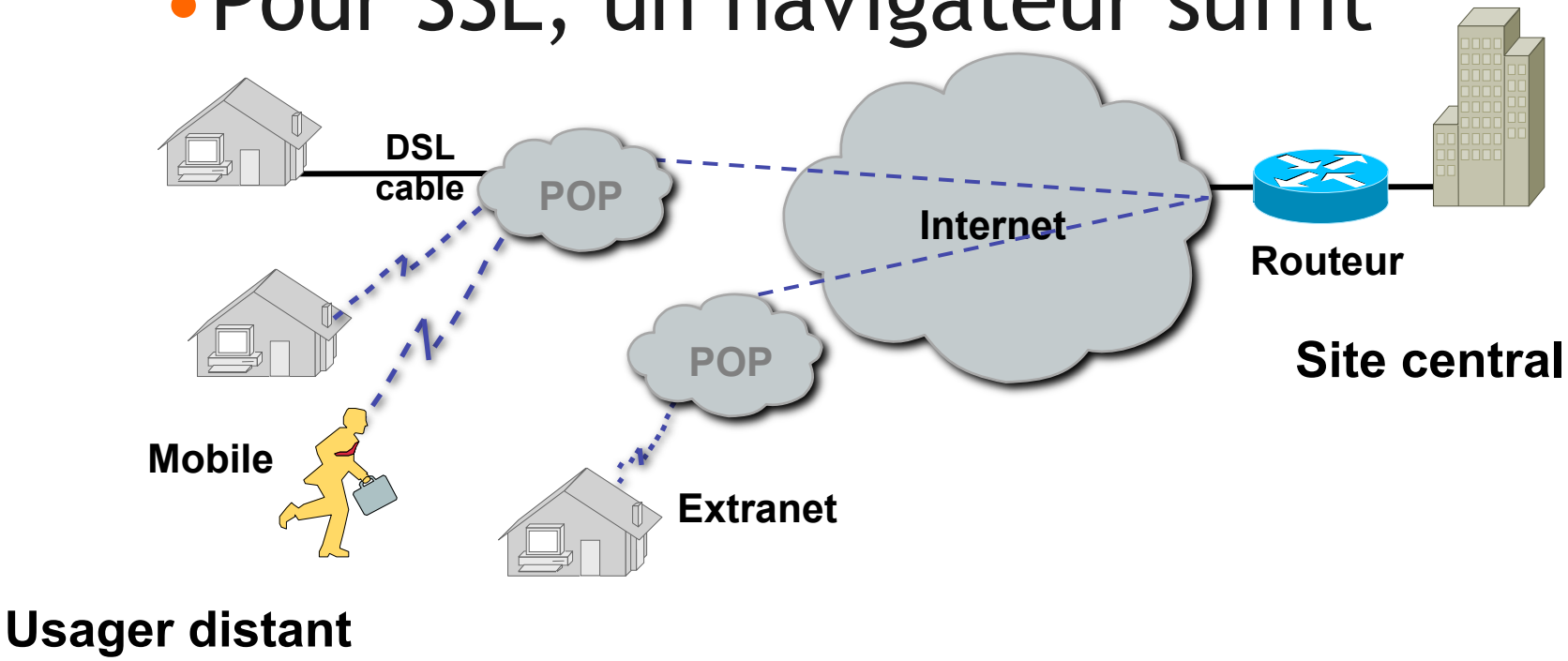
IP Sec Mode Transport

- Protège les données du paquet IP (couche 4) mais pas les entêtes IP



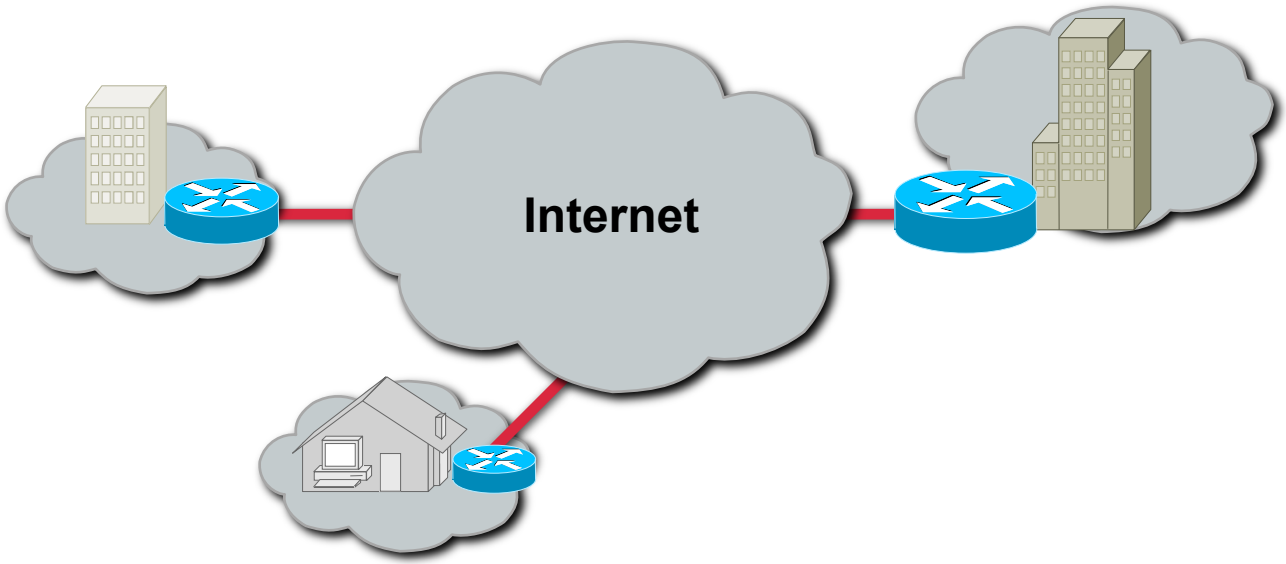
Remote access VPN

- Easy VPN nécessite un logiciel client
- Pour SSL, un navigateur suffit



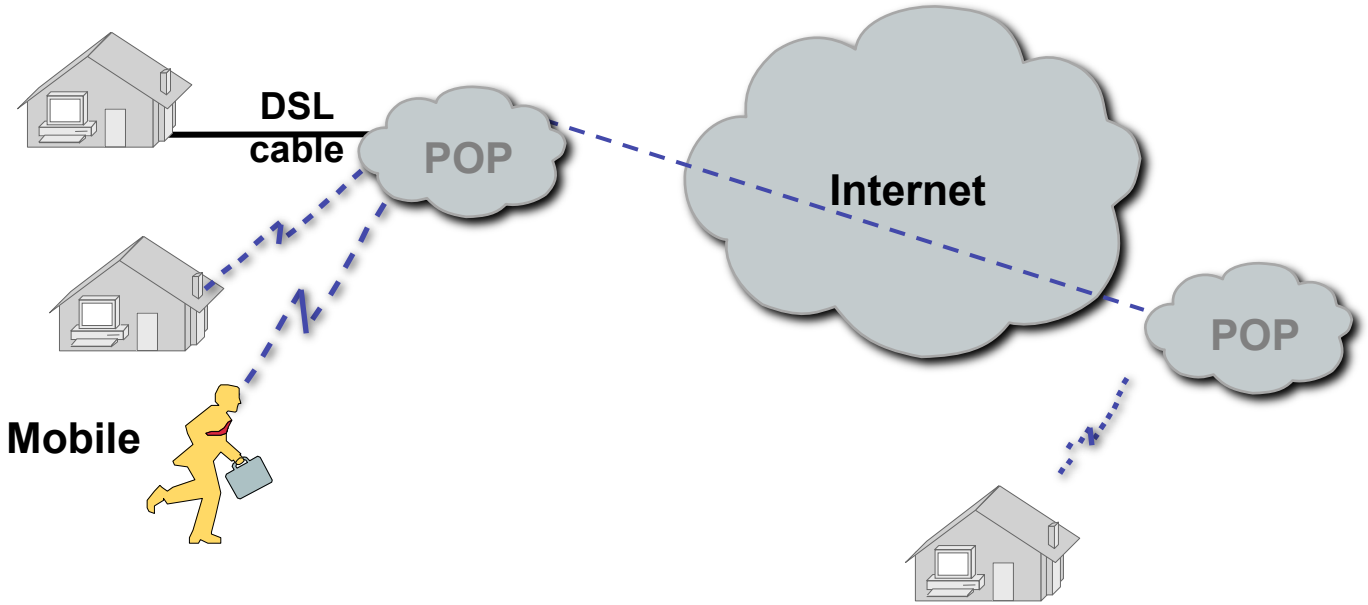
Site to site VPN

- Extension du LAN sur le WAN



Host to host VPN

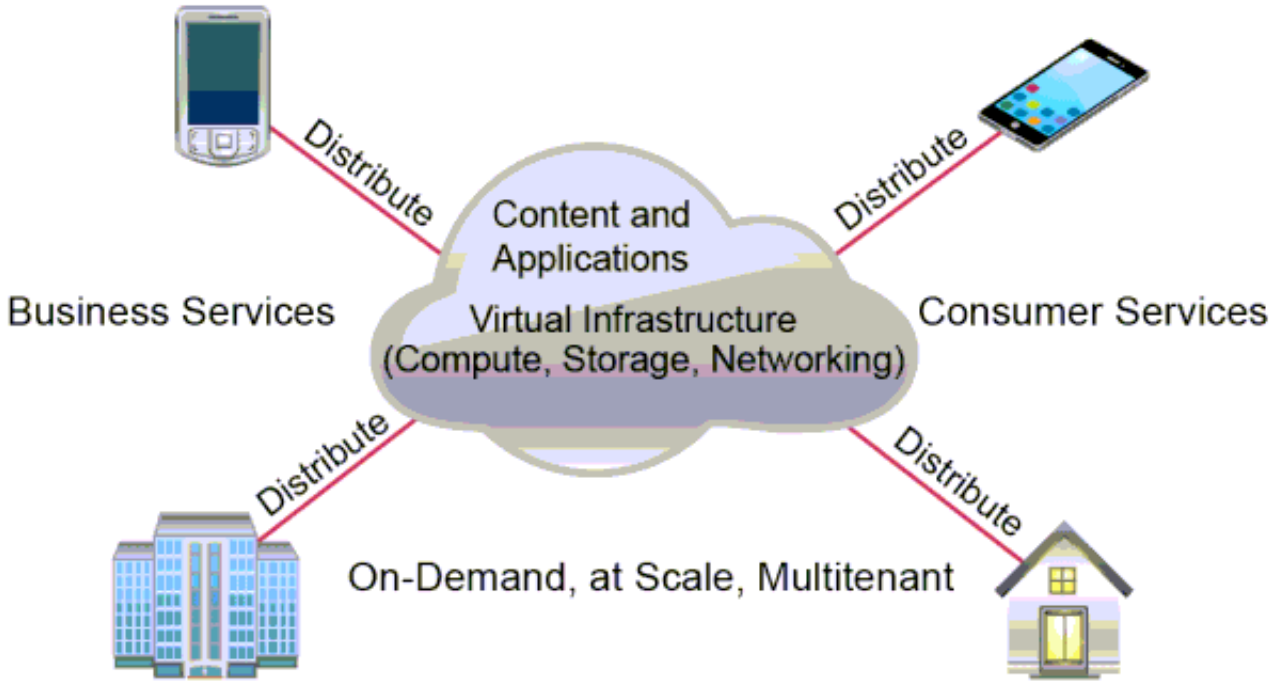
- VPN de hôte à hôte



Cloud Computing

Cloud Computing and Its Effect on Enterprise Network

- IT resources and services are abstracted from the underlying infrastructure.
- Computing is delivered as a service rather than a product.
- A cloud can be an off-premise hosted model, either application hosting or storage hosting.



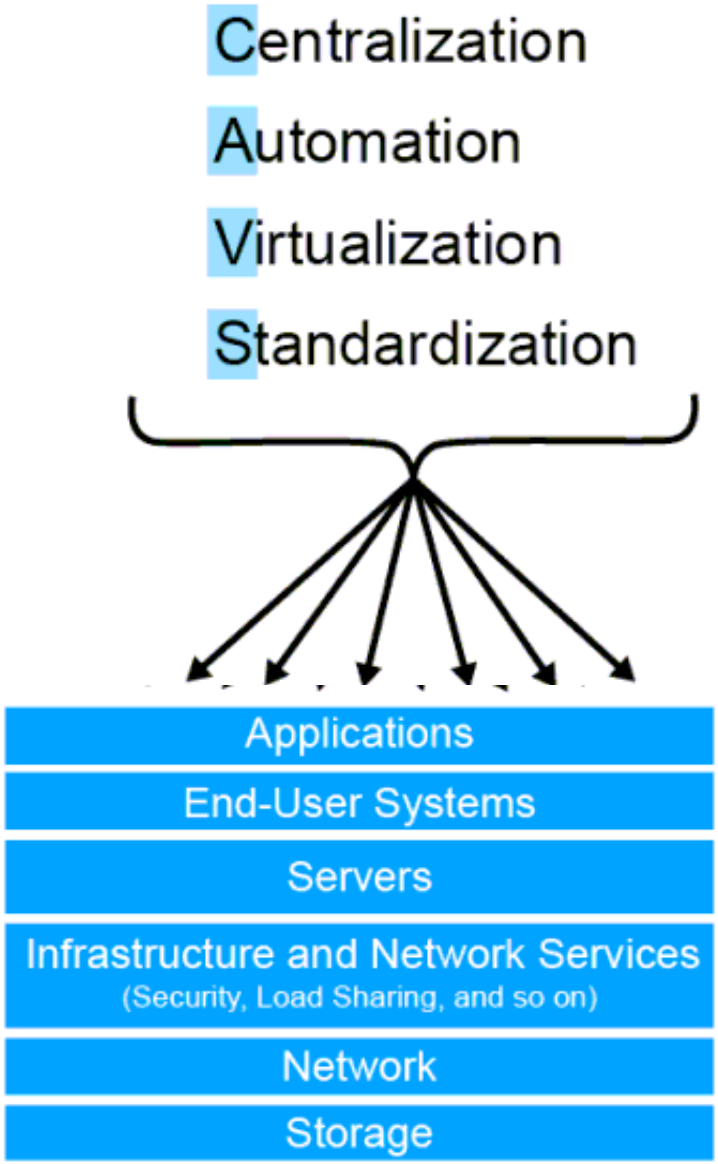
Cloud Computing and Its Effect on Enterprise Network (Cont.)

Advantages to the cloud service builder or provider:

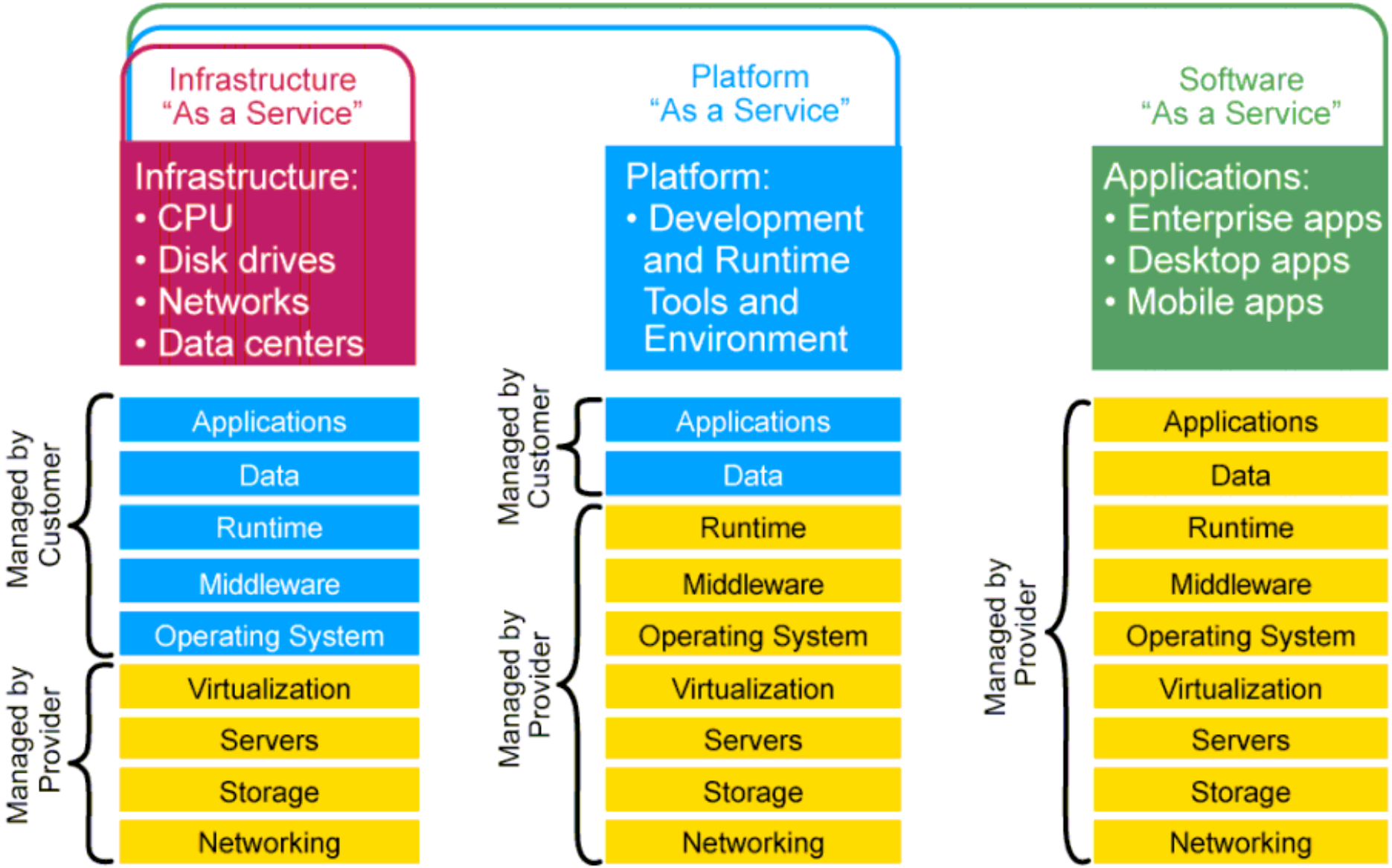
- Cost reduction from standardization and automation
- High utilization through virtualized, shared resources
- Easier administration
- Fail-in-place operations model

Advantages to cloud users:

- On-demand, self-service resource provisioning
- Centralized appearance of resources
- Highly available, horizontally scaled application architectures
- No local backups



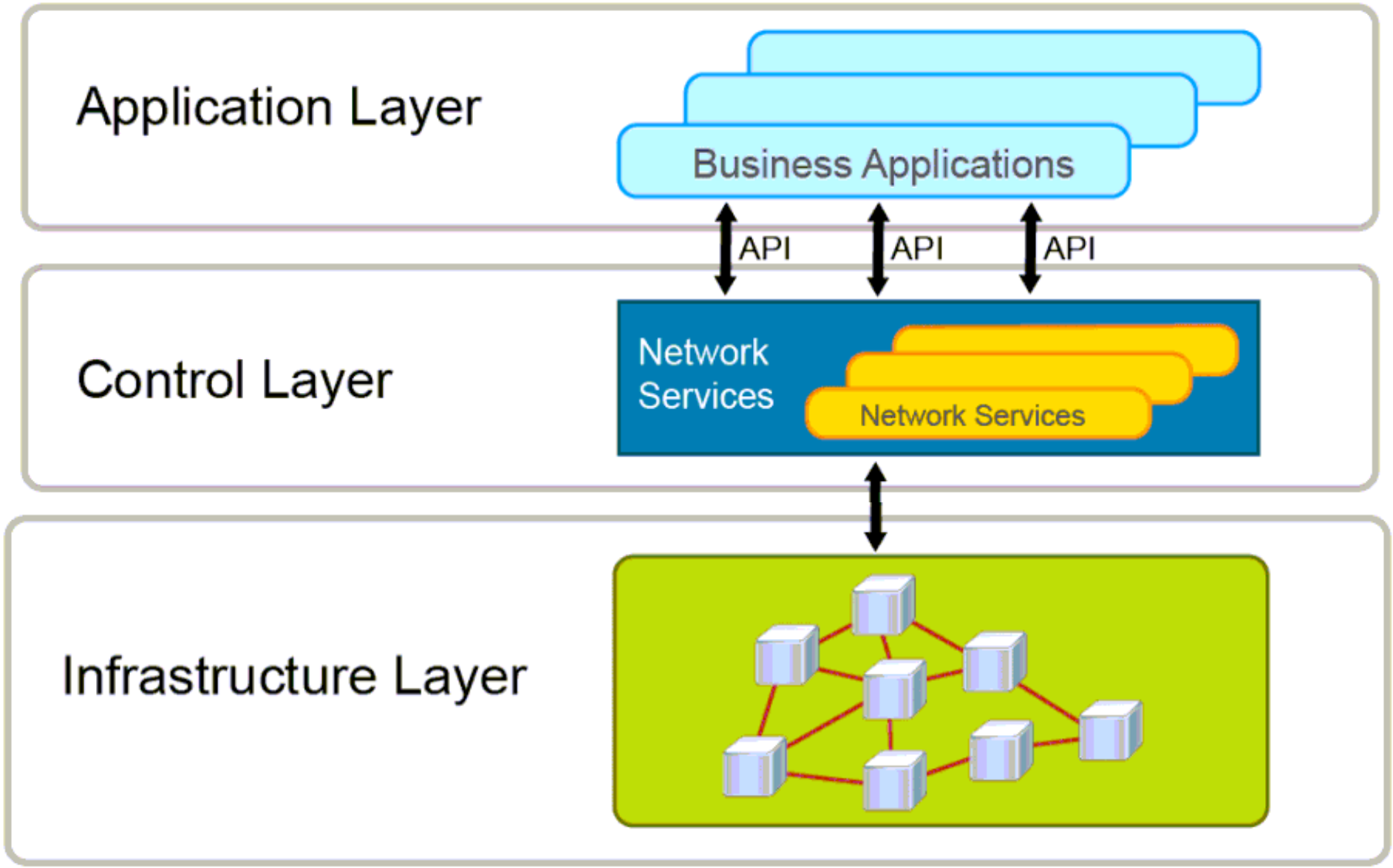
Cloud Computing Services



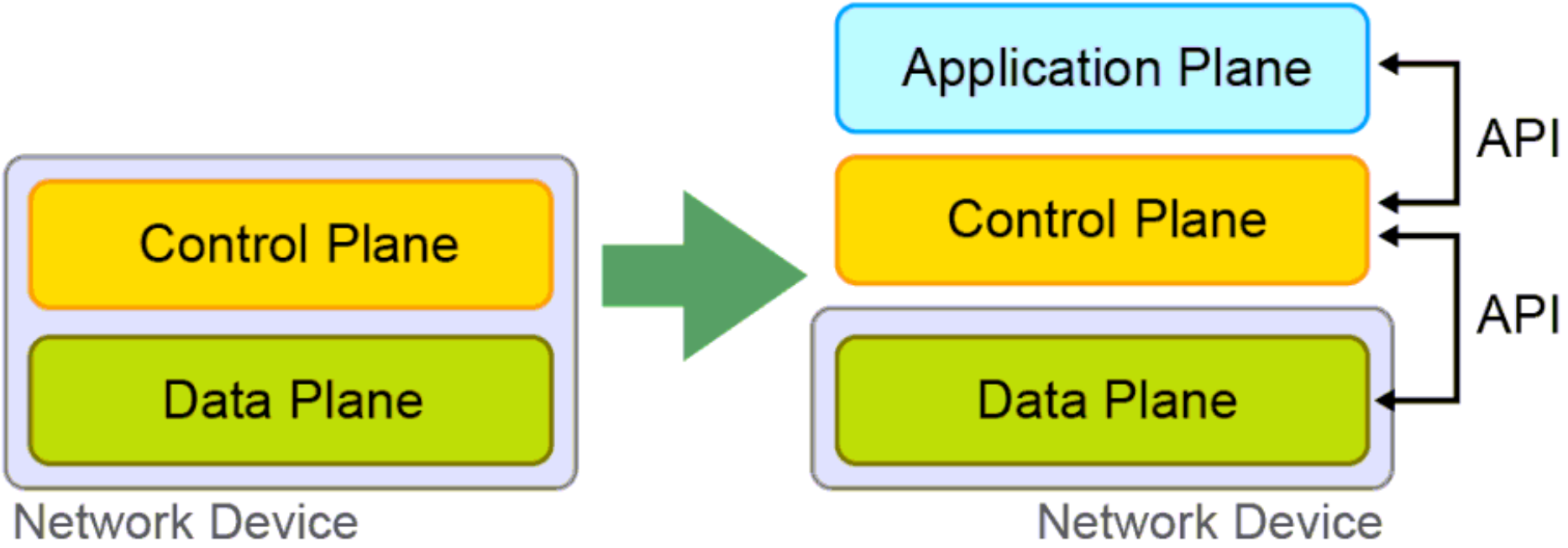
Sofware Defined Network

SDN

Overview of Network Programmability in Enterprise Network



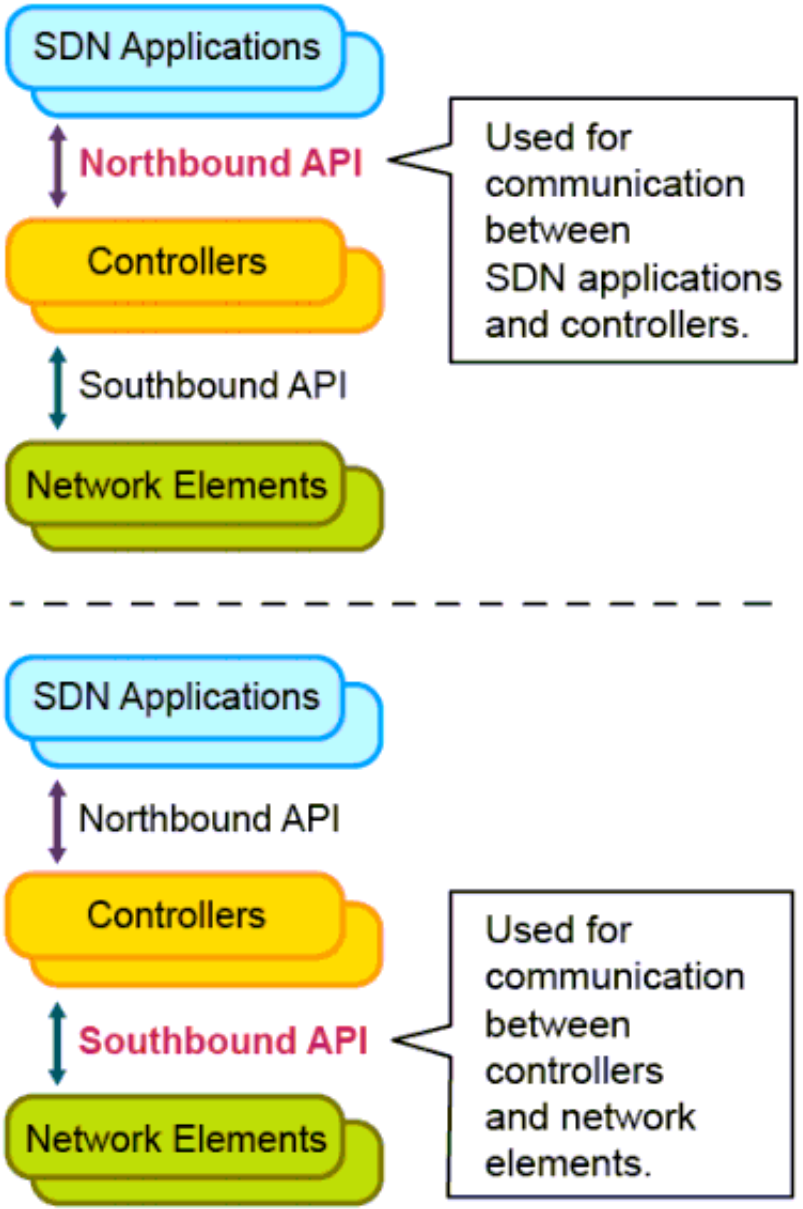
Application Programming Interfaces



Traditional Network Architecture

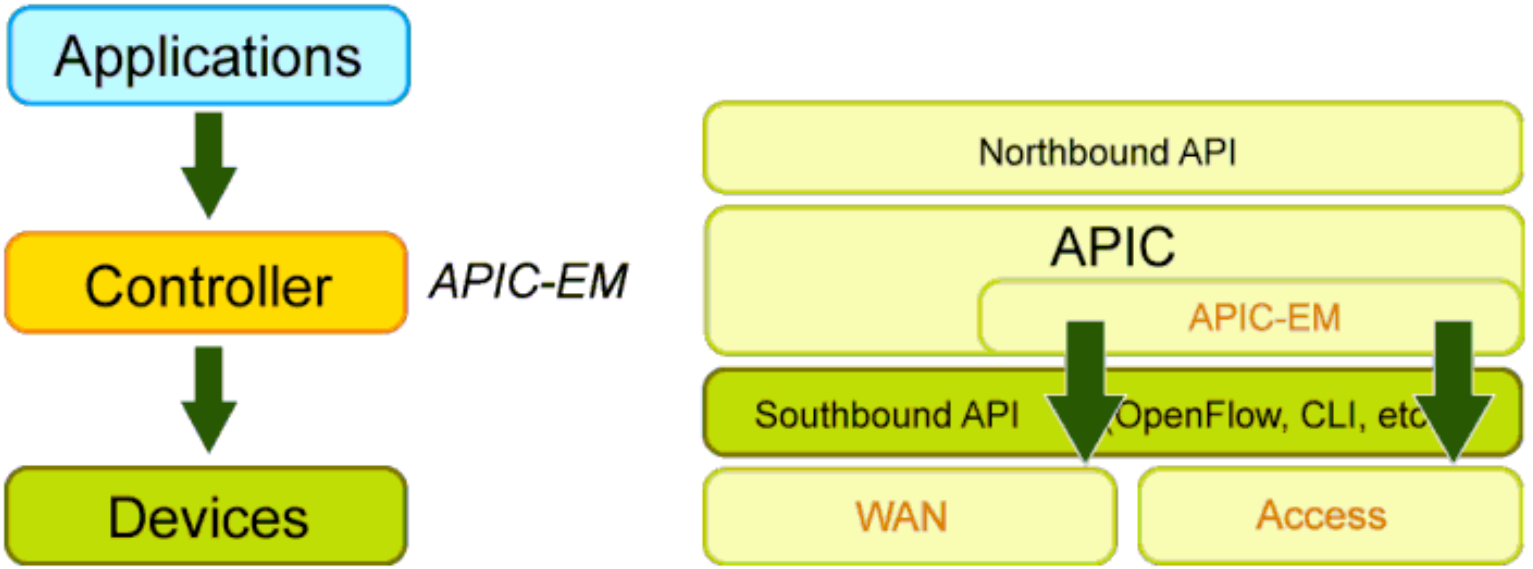
SDN Architecture

Application Programming Interfaces (Cont.)



- Northbound API:
  - Currently, very little has been done for unification; different applications use different APIs.
- Southbound API:
  - **OpenFlow:** Configure the flow tables in switches.
  - **NETCONF: C**onfigure devices with XML, transactional.
  - **OpFlex**

Cisco APIC-EM



APIC-EM is a centralized automation of policy-based application profiles with the following benefits:

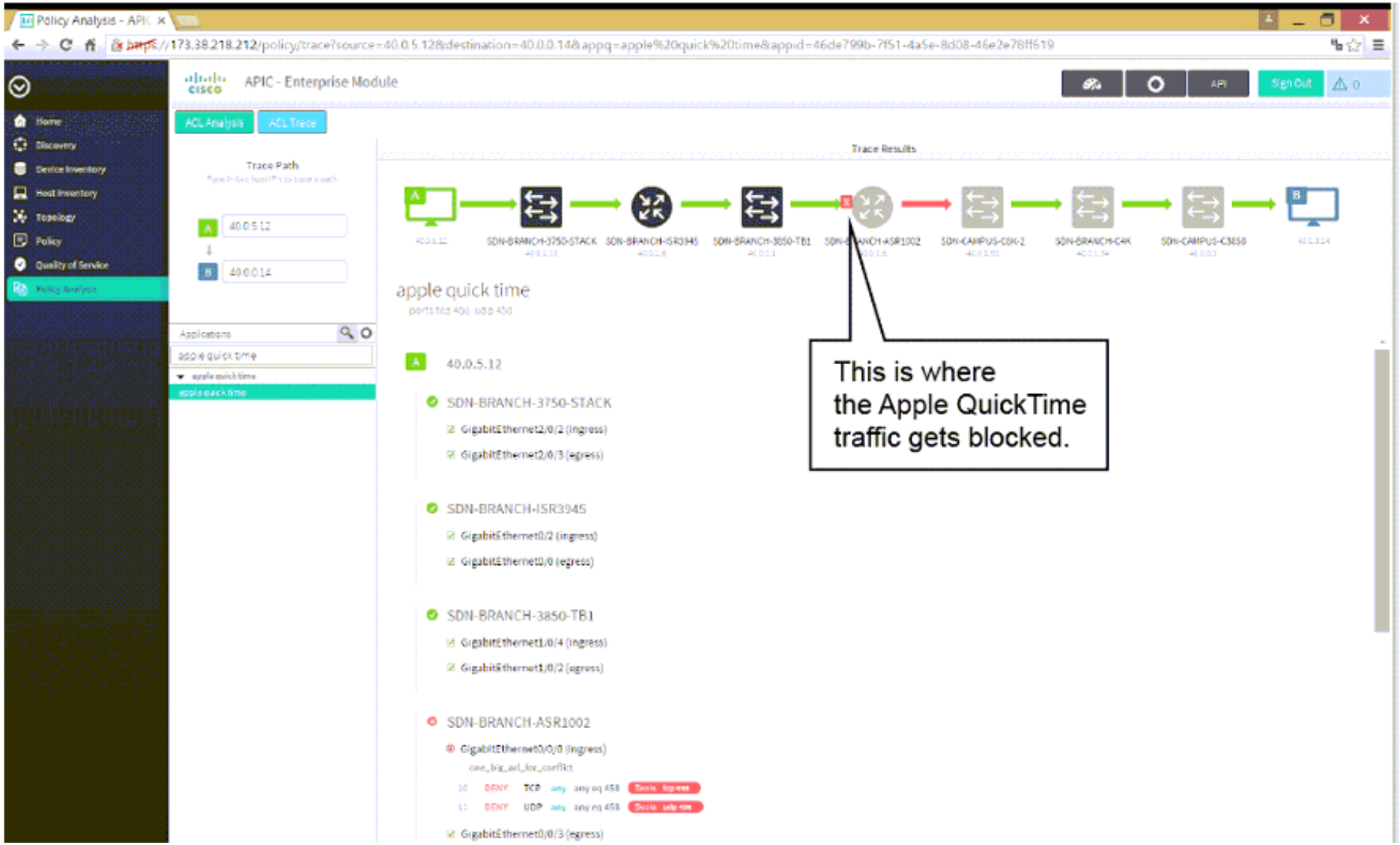
- Single point for network automation for consistency
- Automation, which saves time and costs.
- Open and programmable network devices, using APIs
- Support for greenfield and brownfield deployments

Cisco APIC-EM Features

Cisco APIC-EM has these features:

- Optimize and automate Enterprise WAN and access operations:
  - ACL
  - IWAN
  - QoS
  - User policy
  - Zero-touch provisioning of new devices (images and configuration)
- Improve visibility into the network:
  - Discovery
  - Topology

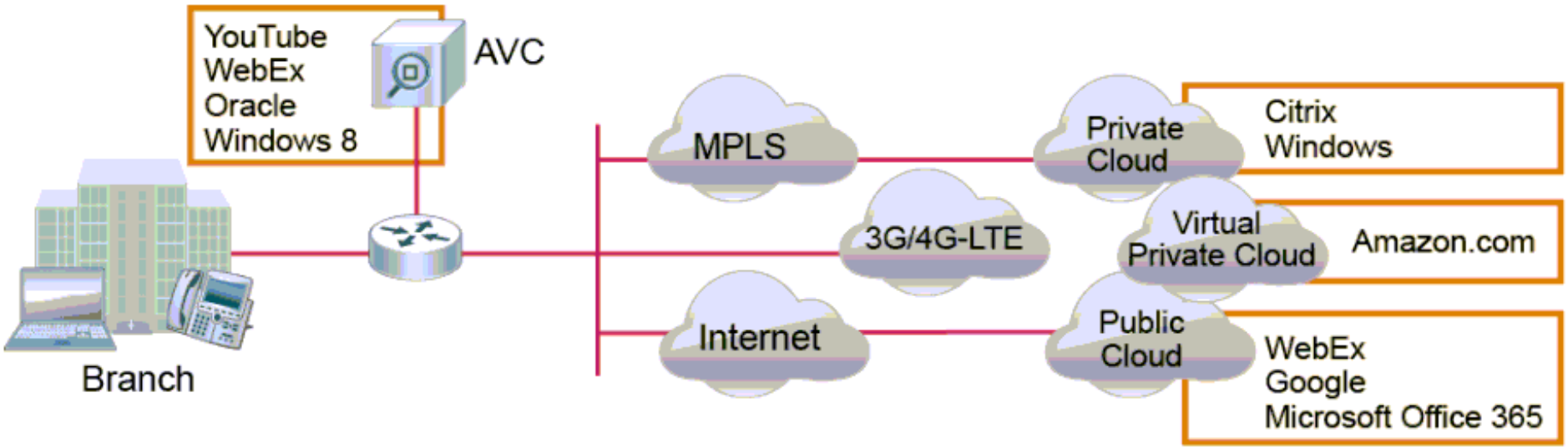
Using APIC-EM for Path Tracing



Introducing Cisco Intelligent WAN

The following are the four components of IWAN:

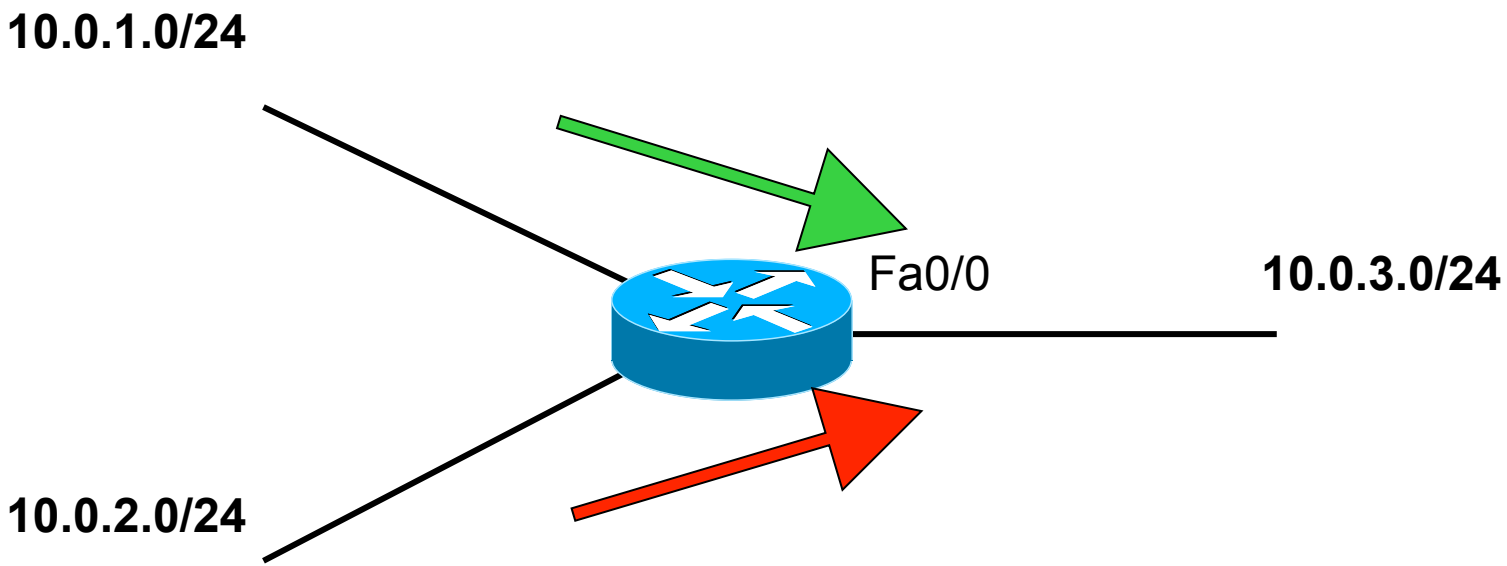
- Transport Independent Connectivity
- Intelligent Path Control
- Application Optimization
- Highly Secure Connectivity



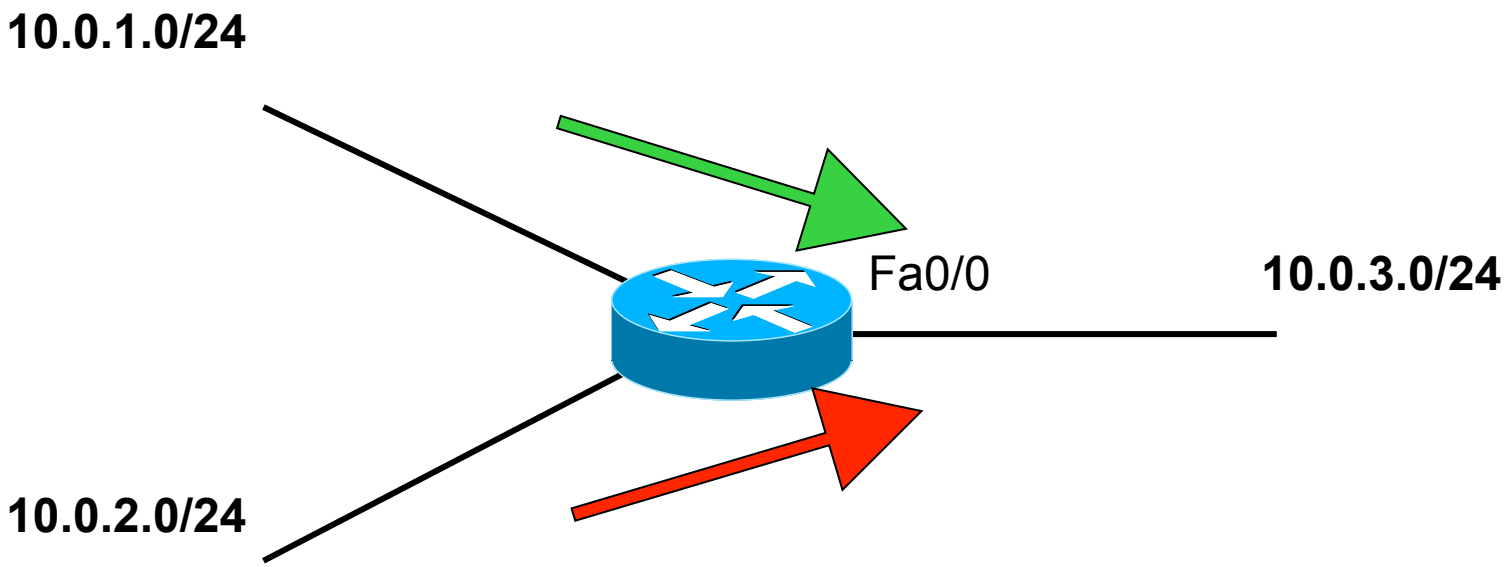
ACL

Access-List

Objectif



Objectif



- 1. CRÉER le filtre :
  - access-list 1 permit 10.0.1.0 0.0.0.255
  - access-list 1 deny 10.0.2.0 0.0.0.255
- 2. APPLIQUER le filtre sur une interface :
  - interface fa0/0
    - ip access-group 1 **out**

ACL standard

- Filtrer selon l'@ IP **source**
- Son **identifiant global** est un numéro
  - entre 1 et 99
- Chaque ligne de l'ACL se voit attribuer automatiquement un **numéro de ligne** qui incrémente de 10 en 10

Numéros de ligne

- show ip access-list
  - access-list 1
    - **10** permit 10.0.1.0 0.0.0.255
    - **20** deny 10.0.2.0 0.0.0.255
- Chaque ligne sera testée une par une, **dans l'ordre**.
  - **Si** l'@ IP source appartient à la population de la ligne, la commande *deny/permit* est exécutée
  - **Sinon**, la ligne suivante est testée.

Raccourcis

Pour filtrer selon une seule addresse :

- access-list 1 permit 10.1.1.1 **0.0.0.0**
- access-list 1 permit **host** 10.1.1.1

Pour filtrer quelque soit l'addresse :

- Exemple : autoriser toute address
- access-list 1 permit 0.0.0.0 **255.255.255.255**
- access-list 1 permit **any**

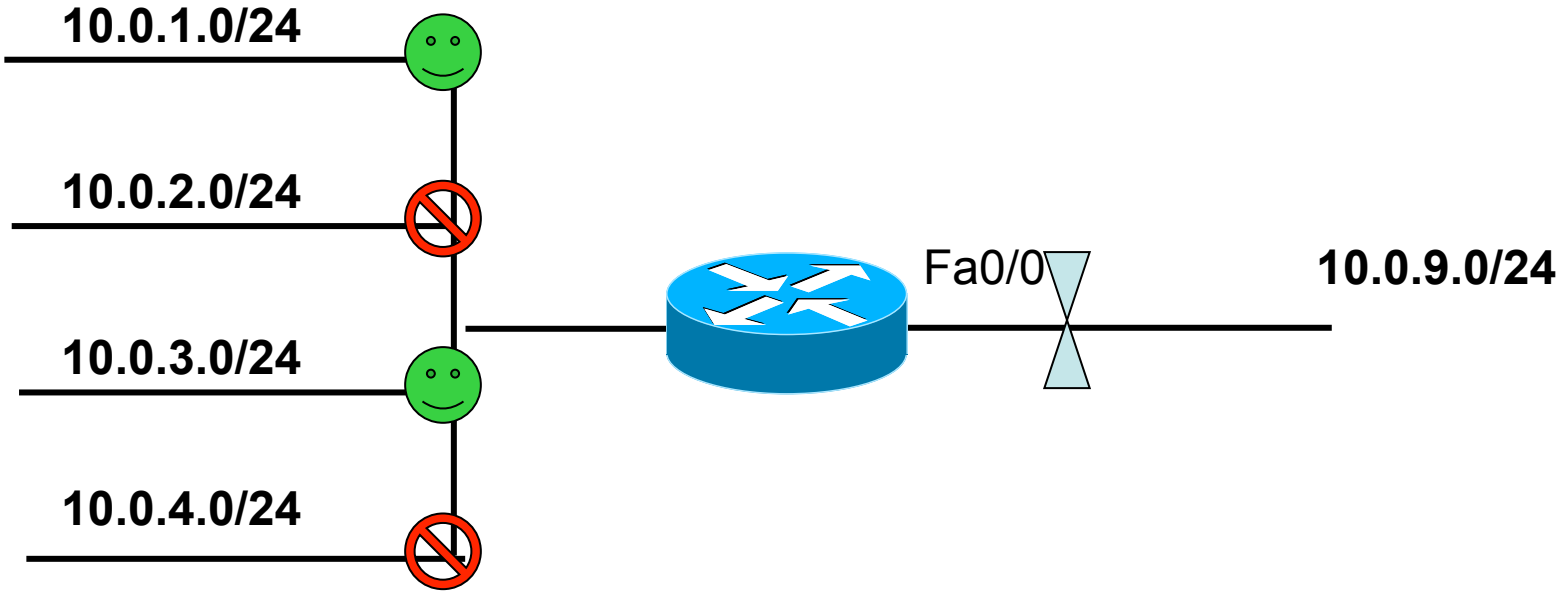
Dernière ligne implicite

- Pour toute ACL, l'IOS rajoute une dernière ligne avec **deny any.**
- Cette ligne n'apparait pas dans le **show ip access-list**
  - Comment optimiser notre ACL 1 ?

  access-list 1 permit 10.0.1.0 0.0.0.255

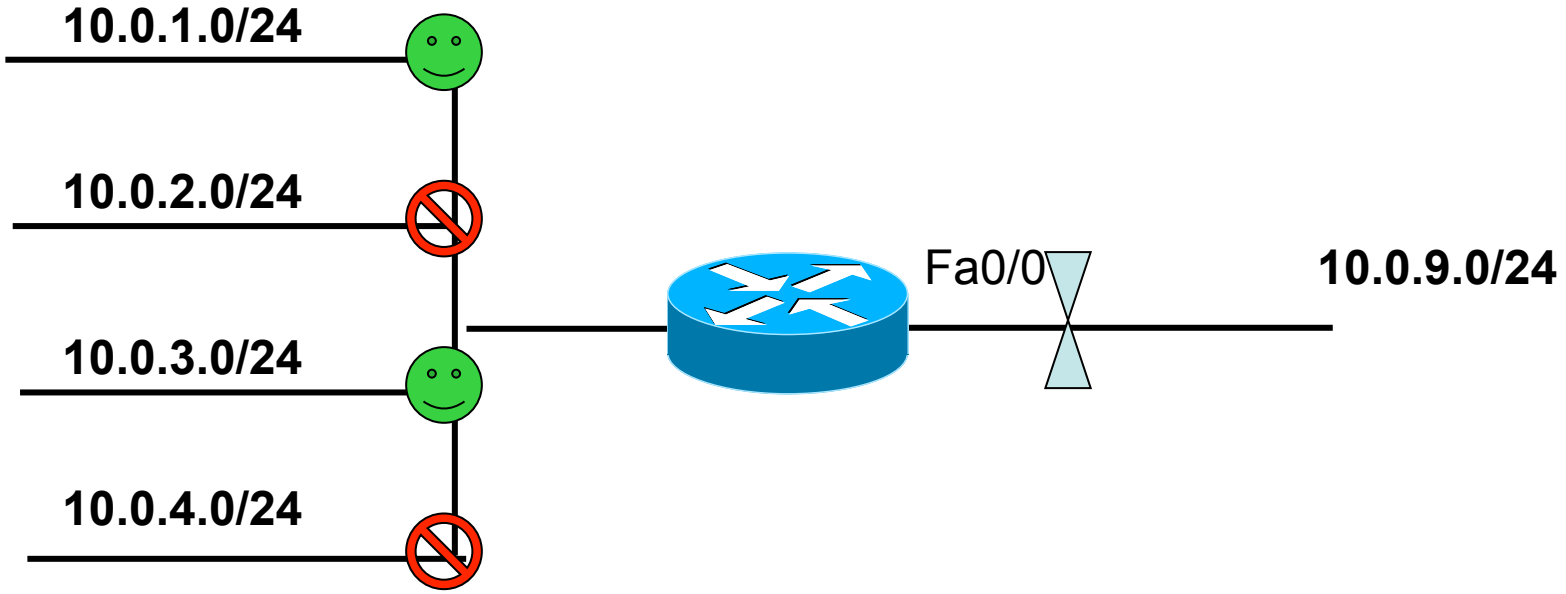
  deny any (implicite, non écrit)

Exemple 1



- access-list 1 permit 10.0.1.0 0.0.0.255
- access-list 1 deny 10.0.2.0 0.0.0.255
- access-list 1 permit 10.0.3.0 0.0.0.255
- access-list 1 deny 10.0.4.0 0.0.0.255

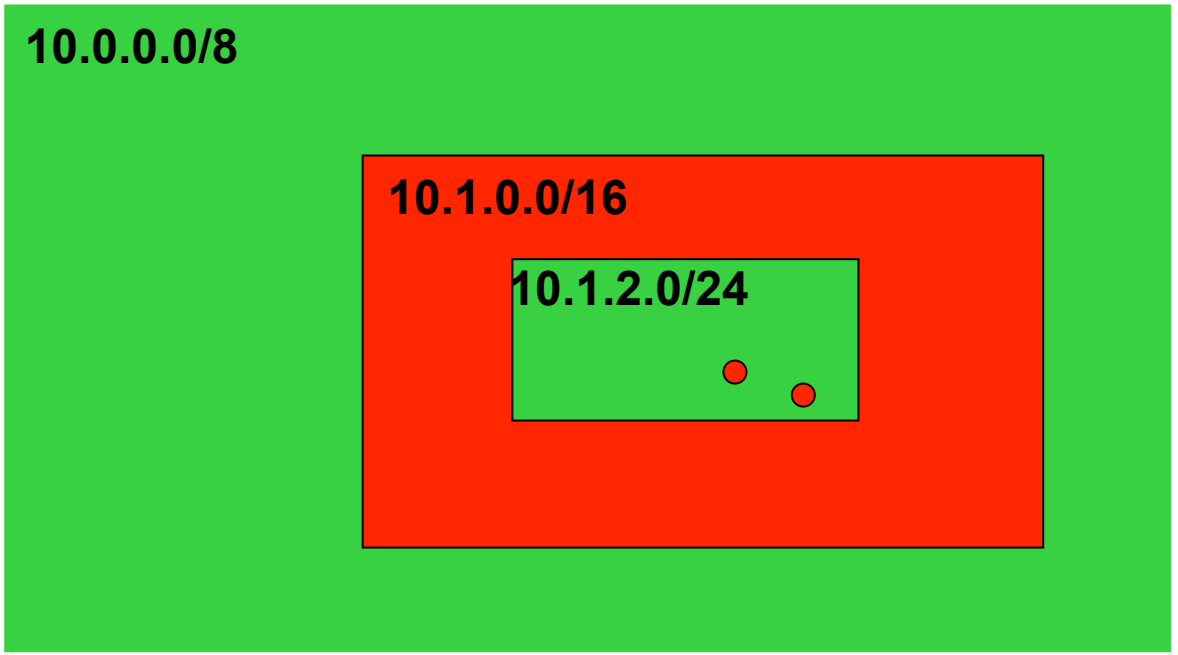
Exemple 1 Optimisation



- access-list 1 permit 10.0.1.0 0.0.0.255
- access-list 1 permit 10.0.3.0 0.0.0.255

Exemple 2 - schéma

- Autoriser tous les 10.0.0.0 /8
  - Sauf, les 10.1.0.0/16 qui sont interdits
    - Par contre, les 10.1.2.0/24 sont autorisés
      - Mais les 10.1.2.18 et 10.1.2.33 sont interdits



Exemple 2 - bonne réponse

- Autoriser tous les 10.0.0.0 /8
  - Sauf, les 10.1.0.0/16 qui sont interdits
    - Par contre, les 10.1.2.0/24 sont autorisés
      - Mais les 10.1.2.18 et 10.1.2.33 sont interdits

de PLUS précis au MOINS précis

- access-list 1 deny host 10.1.2.18
- access-list 1 deny host 10.1.2.33
- access-list 1 permit 10.1.2.0 0.0.0.255
- access-list 1 deny 10.1.0.0 0.0.255.255
- access-list 1 permit 10.0.0.0 0.255.255.255

Appliquer l'ACL sur une interface

- Deux possibilités :
  - filtrer le traffic entrant
  - filtrer le traffic sortant
- Deux commandes :
  - interface Fa0/0
    - ip access-group 1 **in**
    - ip access-group 2 **out**

Mais une seule ACL

par interface et par direction

pour le protocole (IP)

Vérification

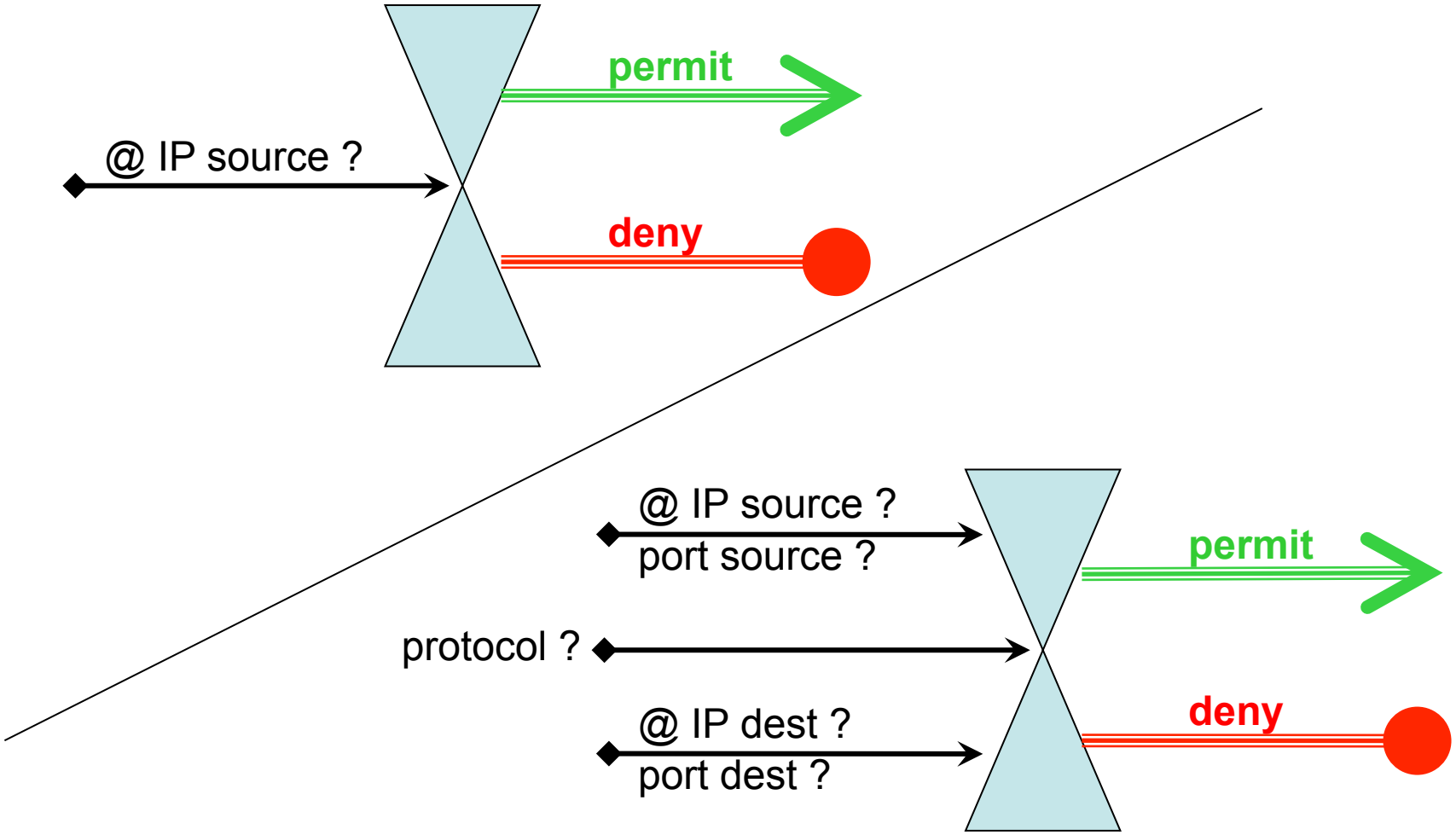
- Vérifier les ACL configurées :
  - `Show access-lists`

- Vérifier où sont appliquées les ACL :
  - `Show ip interface`

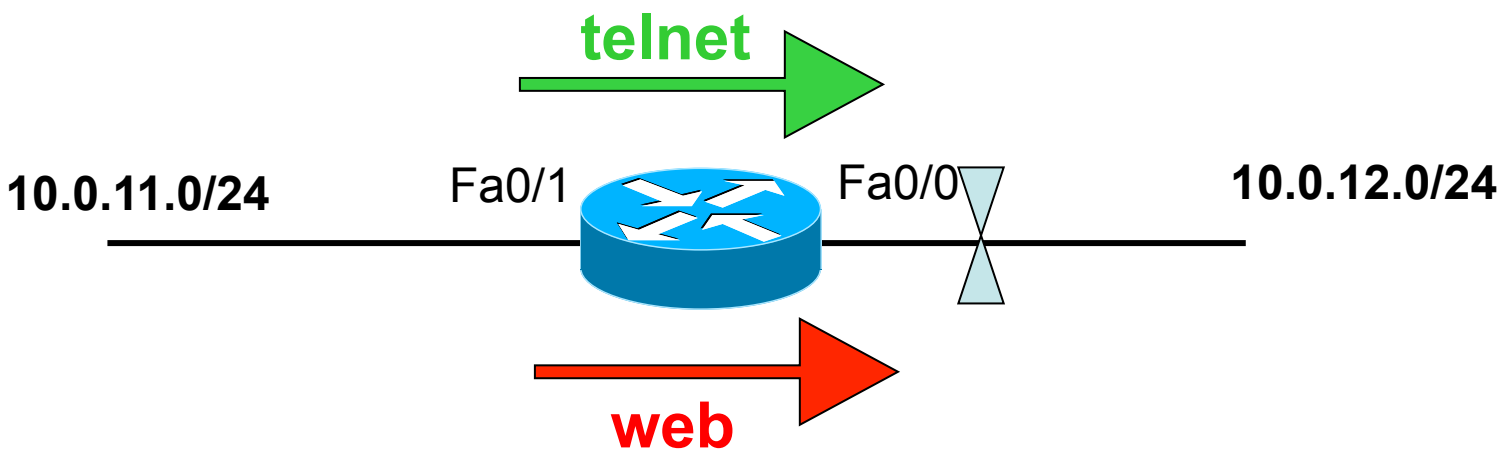
ACL étendues

- Capable de filtrer selon **5** critères
  - protocole
  - @ IP source
  - port source (optionnel)
  - @ IP destination
  - port destination (optionnel)
- Son **identifiant global** est un numéro
  - entre 100 et 199

Standard vs étendue

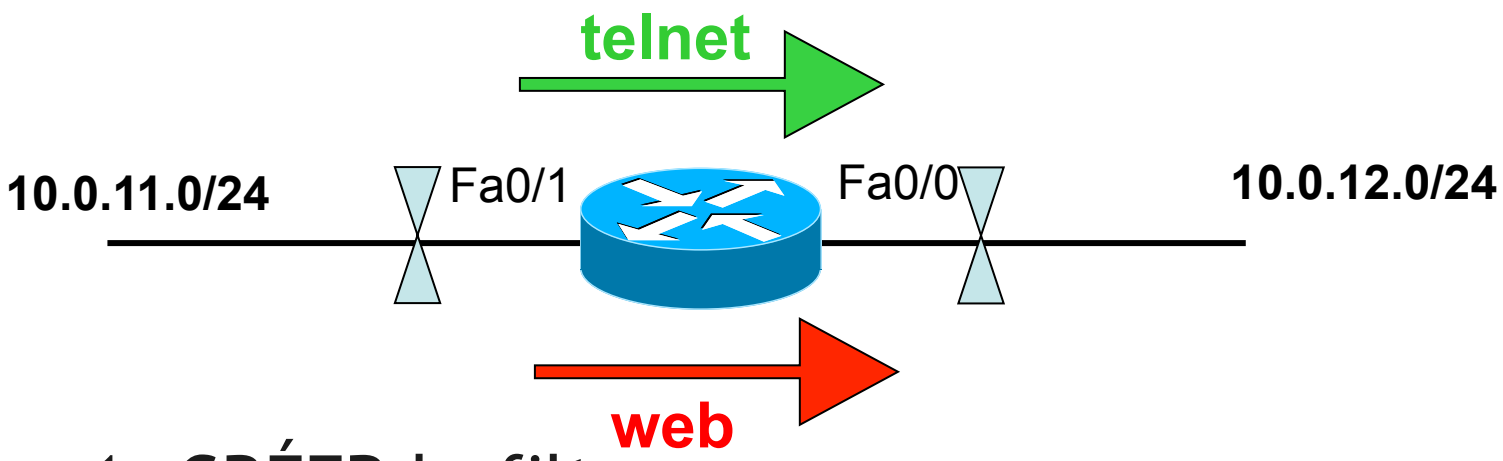


Utilité d'une ACL étendue



- Autoriser 10.0.11.0/24 à aller sur 10.0.12.0/24 en telnet, mais pas en http

Solutions



- 1. CRÉER le filtre :
  - access-list 100 **permit** tcp 10.0.11.0 0.0.0.255 10.0.12.0 0.0.0.255 eq **23**
  - access-list 100 **deny** tcp 10.0.11.0 0.0.0.255 10.0.12.0 0.0.0.255 eq **80**
- 2. APPLIQUER le filtre à l'interface :
  - int fa0/**0**
    - ip access-group 100 **?**

OU

  - int fa0/**1**
    - ip access-group 100 **?**

Détail de l'ACL

access-list	Iden-tifiant	permit ou deny	Proto cole	@ IP Source	Masque Source	Port Source	@ IP Dest	Masque Dest.	Port Dest.
access-list	100	permit	tcp	10.0.11.0	0.0.0.255		10.0.12.0	0.0.0.255	eq 23
access-list	100	deny	tcp	10.0.11.0	0.0.0.255		10.0.12.0	0.0.0.255	eq 80
			ip						**neq**
			udp						**lt**
			ospf						**gt**
			eigrp						**range**
			etc..						

Opérateurs

- Opérateurs disponibles pour filtrer le port :
  - **eq** **equal**
  - **neq** **not equal**
  - **lt** **less than**
  - **gt** **greater than**
  - **range** **plage**

ACL nommées

- ip access-list standard TOTO
  - permit ….
  - deny….
- ip access-list extended TATA
  - permit ….
  - deny….
- idem pour appliquer l'ACL sur une interface
  - int fa0/0
    - ip access-group TOTO in | out

Avantages des ACL nommées

- possibilité de supprimer une ligne :
  - ip access-list standard TOTO
  - **no 20**
    - supprime la ligne 20
- possibilité d'insérer une ligne :
  - ip access-list standard TOTO
  - **33 permit ….**
    - entre la ligne 30 et la ligne 40

Traffic filtré

- Les ACL ne filtrent que le traffic qui traverse le routeur.
- Elle ne filtrent pas le traffic généré par le routeur.
- Cette règles s'applique à toutes les ACL
  - nommées ou numérotées
  - standards ou étendues

Exemple

Sur R2:

- access-list 100 deny tcp any any eq 23
- access-list 100 permit ip any any
- implicit deny
- int fa0/0
  - ip access-group 100 out

Est-ce que R1 peut faire un telnet vers R3 ?

Est-ce que R2 peut faire un telnet vers R3 ?

ACL

Appliquée sur une ligne VTY

Cas particulier du TELNET

- Au lieu d'appliquer une ACL
  - sur une interface physique,
  - on peut l'appliquer sur les lignes vty.

- Objectif = filtrer les individus qui peuvent accéder au routeur / switch.

Exemple

- access-list 1 permit host 10.0.0.1
- line vty 0 4
  - access-class 1 in

- seul l'individu 10.0.0.1 pourra faire un telnet sur cet équipement

Exercice

- Seuls les administrateurs peuvent accéder aux routeurs en telnet.
- Les administrateurs sont tous sur le réseau 10.1.128.0/17.
- Un administrateur ne doit pas pouvoir accéder aux routeurs.

  Son adresse est 10.1.128.200

Solution

- conf t

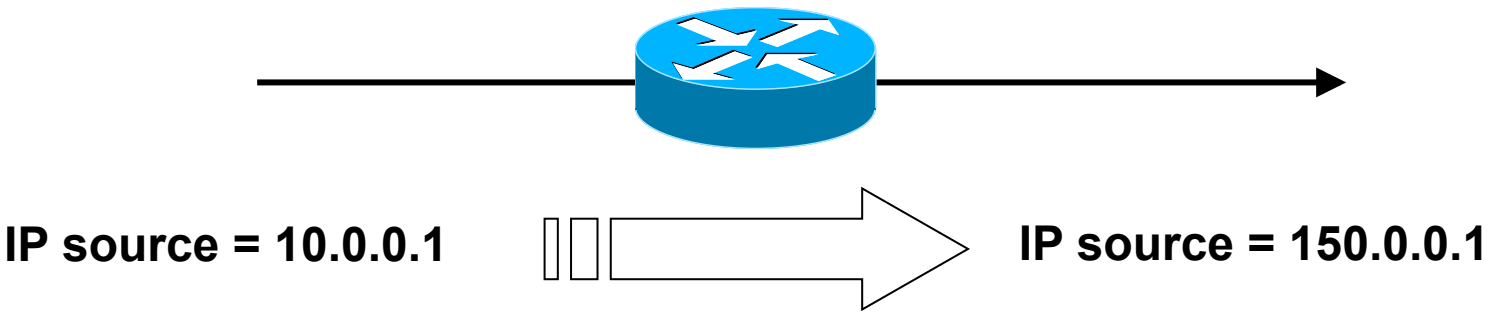
- access-list 1 deny host 10.1.128.200
- access-list 1 permit 10.1.128.0 0.0.127.255

- line vty 0 4
  - access-class 1 in

NAT

Network Address Translation

Principe du NAT



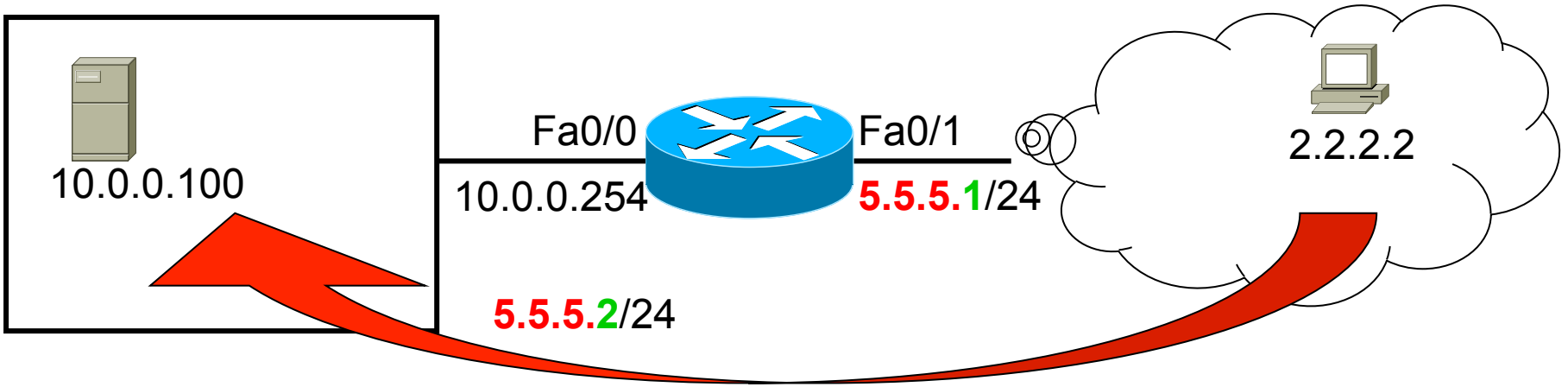
- Le routeur a modifié l'@ IP source du paquet avant de le transmettre.

Quel peut être l'intérêt ?

Quatre possibilités

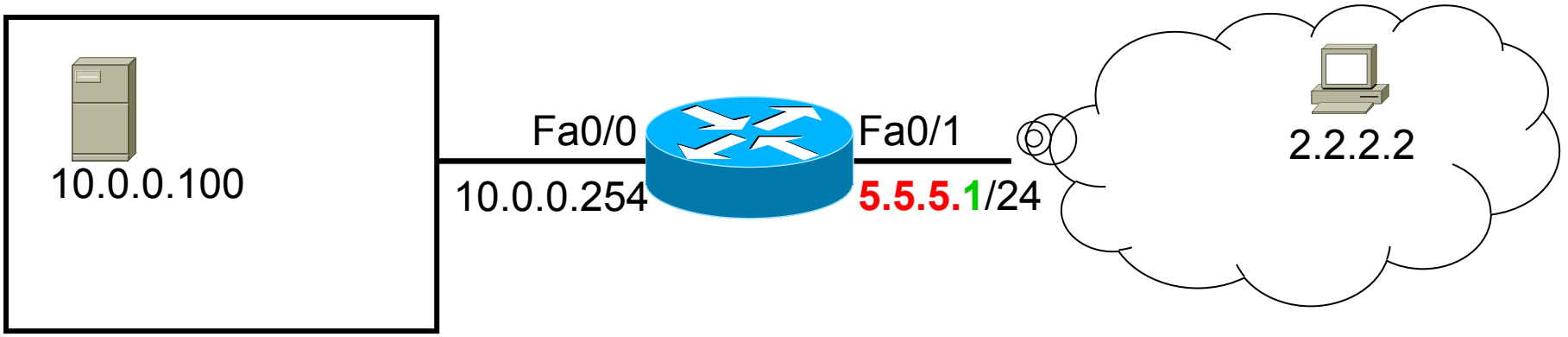
- NAT Statique
- PAT Statique
- NAT Dynamique
- PAT Dynamique

NAT Statique



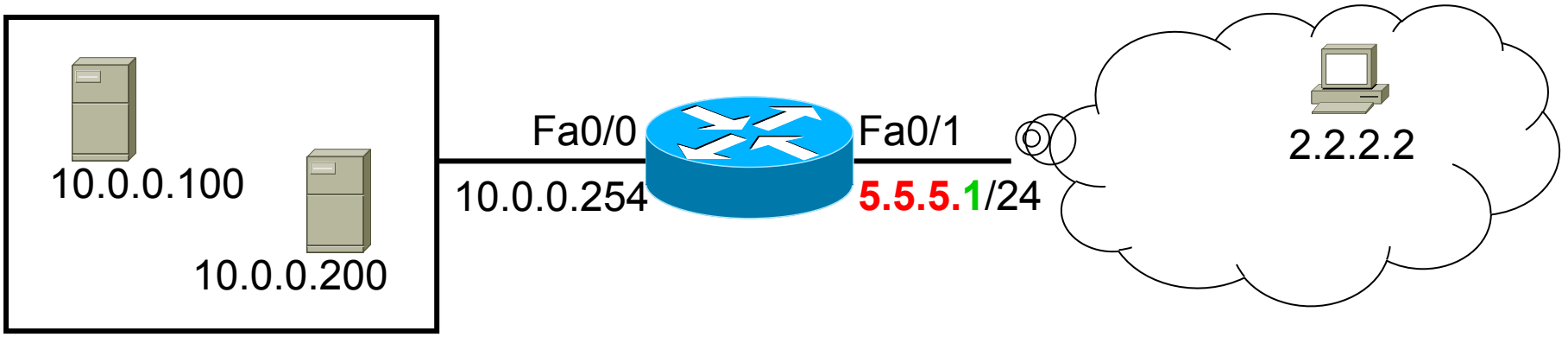
- Objectif :
  - permettre aux clients d'accéder à mon serveur web
- Problème :
  - 10.0.0.100 est interdit sur internet
- Solution :
  1. prétendre que mon serveur web est accessible sur **5.5.5.2**
  2. translater 5.5.5.2 en 10.0.0.100

NAT Statique



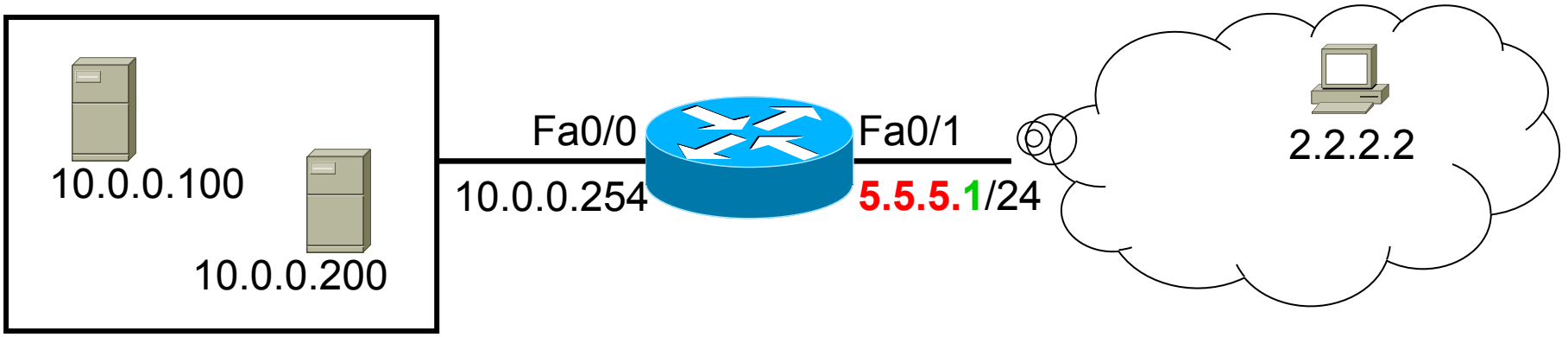
- conf t
- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- ip nat inside source static 10.0.0.100 5.5.5.2

NAT Statique



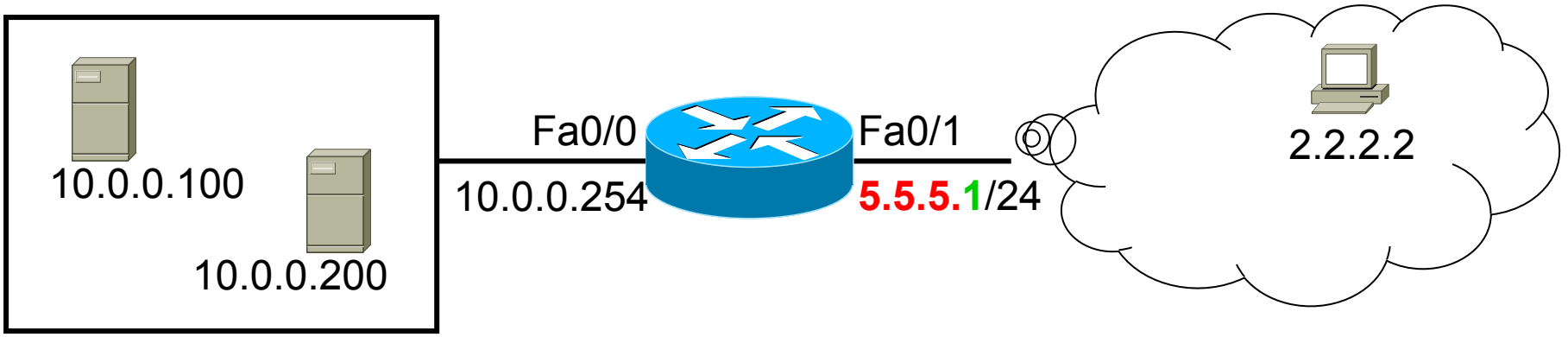
- Objectif :
  - permettre aux clients d'accéder à mes 2 serveurs (web, smtp)
- Solution n°1:
  - prétendre que mon serveur web est accessible sur **5.5.5.2** + translater 5.5.5.2 en 10.0.0.100
  - prétendre que mon serveur smtp est accessible sur **5.5.5.3** + translater 5.5.5.3 en 10.0.0.200

NAT Statique



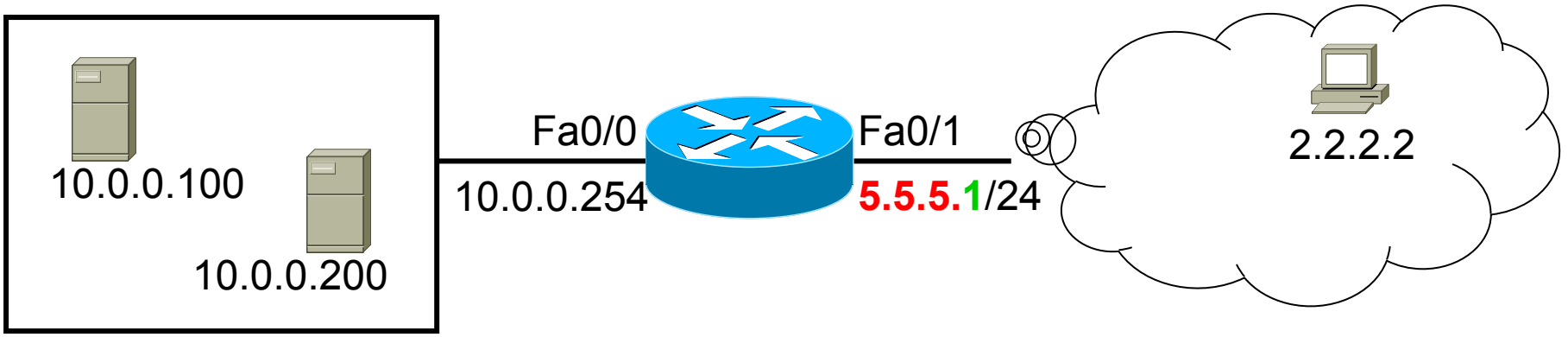
- conf t
- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- ip nat inside source static 10.0.0.100 5.5.5.2
- ip nat inside source static 10.0.0.200 5.5.5.3

PAT Statique



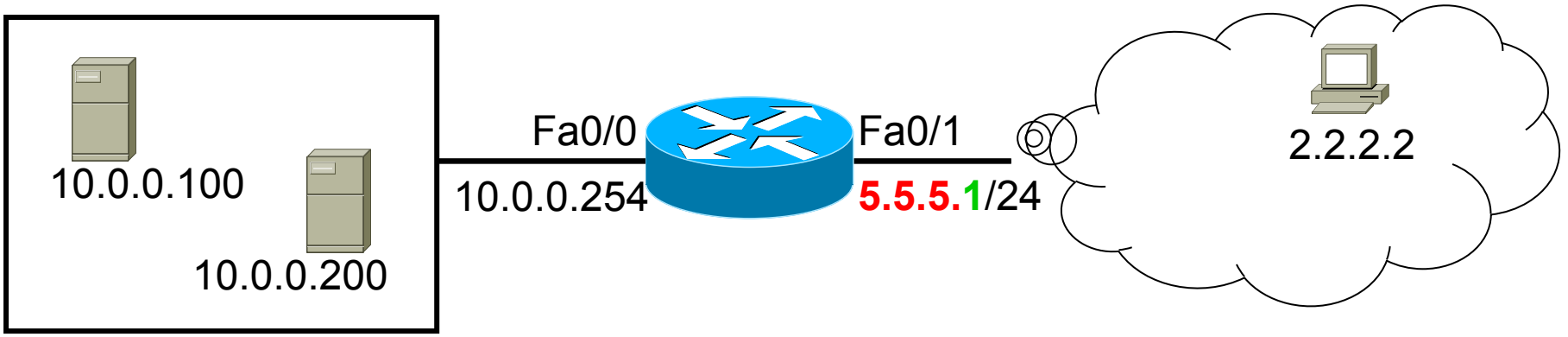
- Objectif :
  - permettre aux clients d'accéder à mes 2 serveurs web
  - utiliser une seule adresse publique pour accéder aux 2 serveurs
- Solution n°2:
  - prétendre que mon serveur web est accessible sur le port 80 de **5.5.5.2** + translater 5.5.5.2 en 10.0.0.100
  - prétendre que mon serveur smtp est accessible sur le port 8080 de **5.5.5.2** + translater 5.5.5.2 en 10.0.0.200

PAT Statique



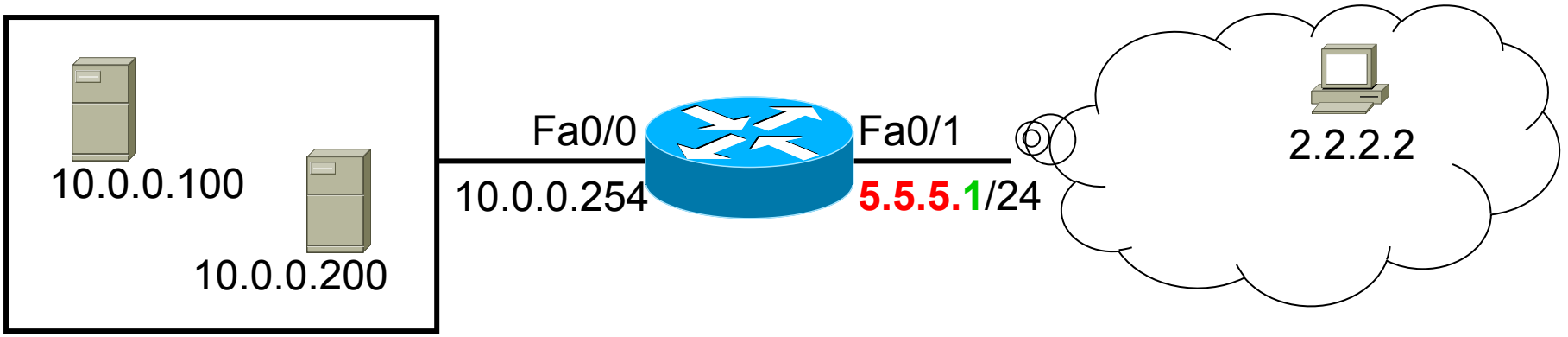
- Objectif WEB1 :
  - mon serveur web en 10.0.0.100 répond sur le port 80
  - les clients doivent attaquer mon serveur web en allant sur 5.5.5.2 port 80.
- Objectif WEB2:
  - mon serveur smtp 10.0.0.200 répond sur le port 80
  - les clients doivent attaquer mon serveur smtp en allant sur 5.5.5.2 port 8080.

PAT Statique



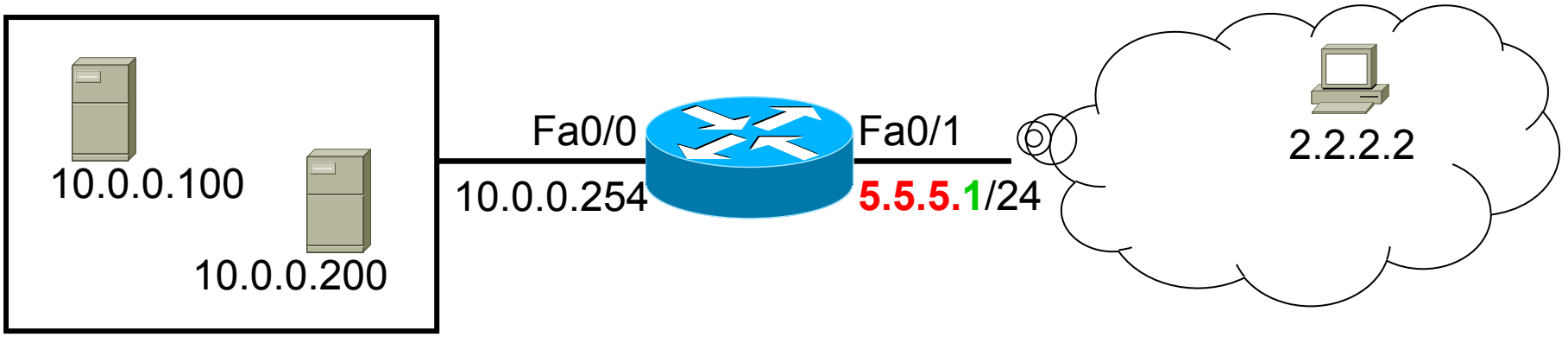
- conf t
- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- ip nat inside source static tcp 10.0.0.100 80 5.5.5.2 80
- ip nat inside source static tcp 10.0.0.200 80 5.5.5.2 8080

Exercice



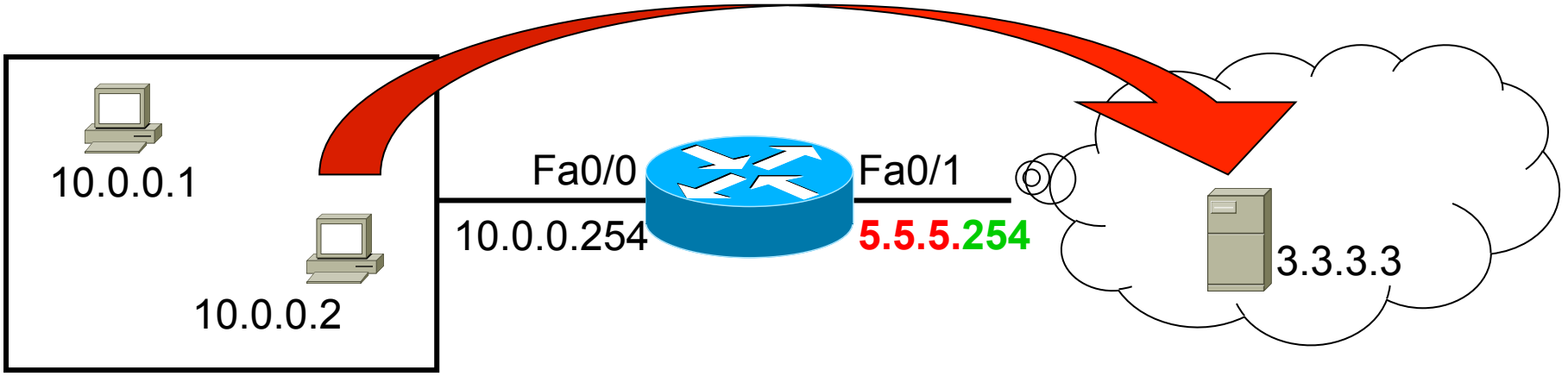
- Objectif WEB :
  - mon serveur web en 10.0.0.100 répond sur le port 80
  - les clients doivent attaquer mon serveur web en allant sur 5.5.5.2 port 8080.
- Objectif WEB2:
  - mon serveur telnet 10.0.0.200 répond sur le port 80
  - les clients doivent attaquer mon serveur telnet en allant sur 5.5.5.2 port 8081.

Solution



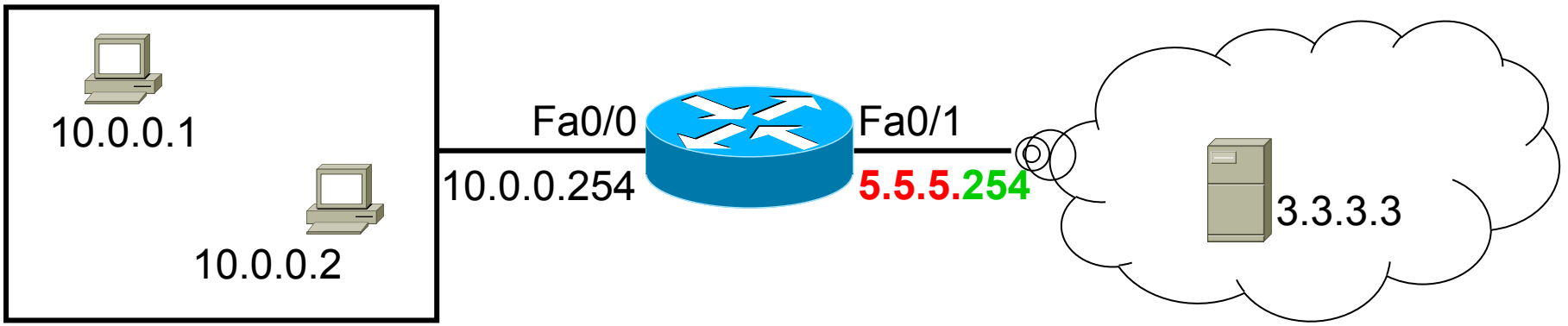
- conf t
- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- ip nat inside source static tcp 10.0.0.100 80 5.5.5.2 8080
- ip nat inside source static tcp 10.0.0.200 80 5.5.5.2 8081

NAT Dynamique



- Objectif :
  - permettre à mon réseau interne d'accéder à internet.
- Problème :
  - toutes mes adresses internes (10.0.0.1, 10.0.0.2 etc..) sont interdites sur internet.
- Solution :
  1. prétendre que mon réseau interne est en **5.5.5.X**
  2. translater 10.0.0.**1** en 5.5.5.**1**
  3. translater 10.0.0.**2** en 5.5.5.**2**
  4. etc…

NAT Dynamique



- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- ip nat pool TOTO 5.5.5.1 5.5.5.253 netmask 255.255.255.0
  - ce sont les adresses fictives qui seront attribuées aux adresses translatées
- access-list 1 permit 10.0.0.0 0.0.0.255
  - ce sont les adresses qui seront translatées
- ip nat inside source list 1 pool TOTO
  - pour activer le NAT

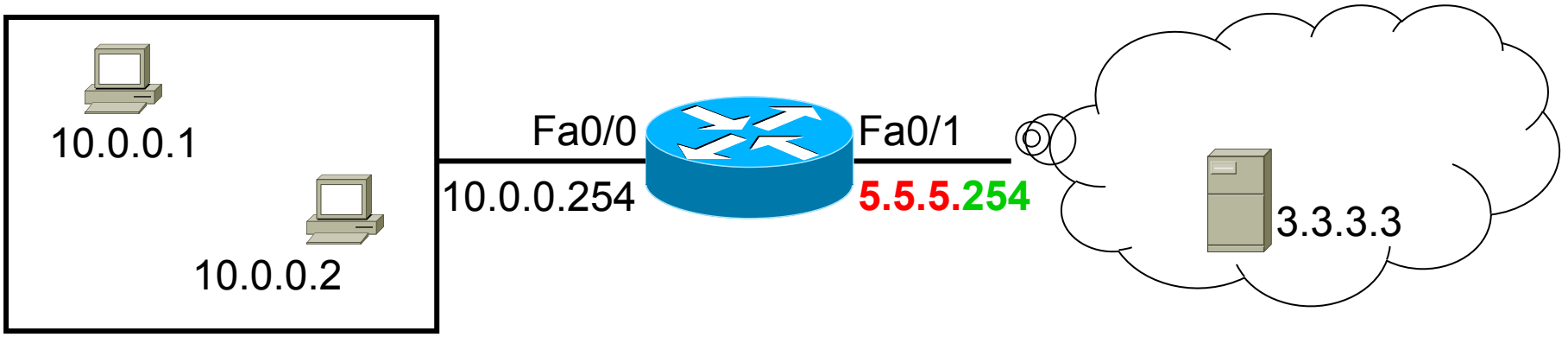
NAT dynamique

- ip nat pool TOTO 5.5.5.1 5.5.5.253 netmask 255.255.255.0
  - ce sont les adresses fictives en interne qui seront attribuées aux adresses translatées

Cette méthode nécessite

d'acquérir plusieurs adresses publiques !

PAT dynamique

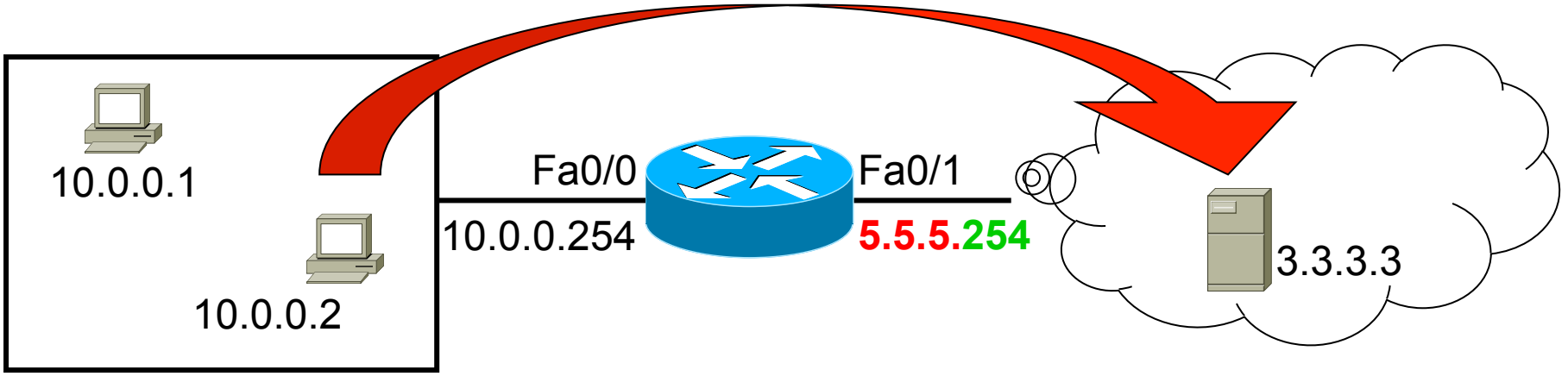


- int fa0/0
  - ip nat inside
- int fa0/1
  - ip nat outside
- access-list 1 permit 10.0.0.0 0.0.0.255
  - ce sont les adresses qui seront translatées
- ip nat inside source list 1 interface fa0/1 overload
  - toutes les adresses nattés se verront attribuées l'adresse IP de l'interface fa0/1 i.e. 5.5.5.254

Terminologie dans show ip nat translation

- Où est placé l'équipement :
  - Inside = équipement physiquement situé côté inside
  - Outside = équipement physiquement situé côté outside
- De quel point de vue je me place :
  - Local = point de vue d'un équipement situé inside
  - Global = point de vue d'un équipement situé outside
- Définitions :
  - Inside Local = @ IP d'un équipement situé dans inside du point de vue d'un équipement situé dans inside
  - Inside Global = @ IP d'un équipement situé dans inside du point de vue d'un équipement situé dans outside
  - Outside Local = @ IP d'un équipement situé dans outside du point de vue d'un équipement situé dans inside
  - Outside Global = @ IP d'un équipement situé dans outside du point de vue d'un équipement situé dans outside

Exemple 1 - NAT dynamique



- 10.0.0.1 est translaté en 5.5.5.1
- 10.0.0.2 est translaté en 5.5.5.2

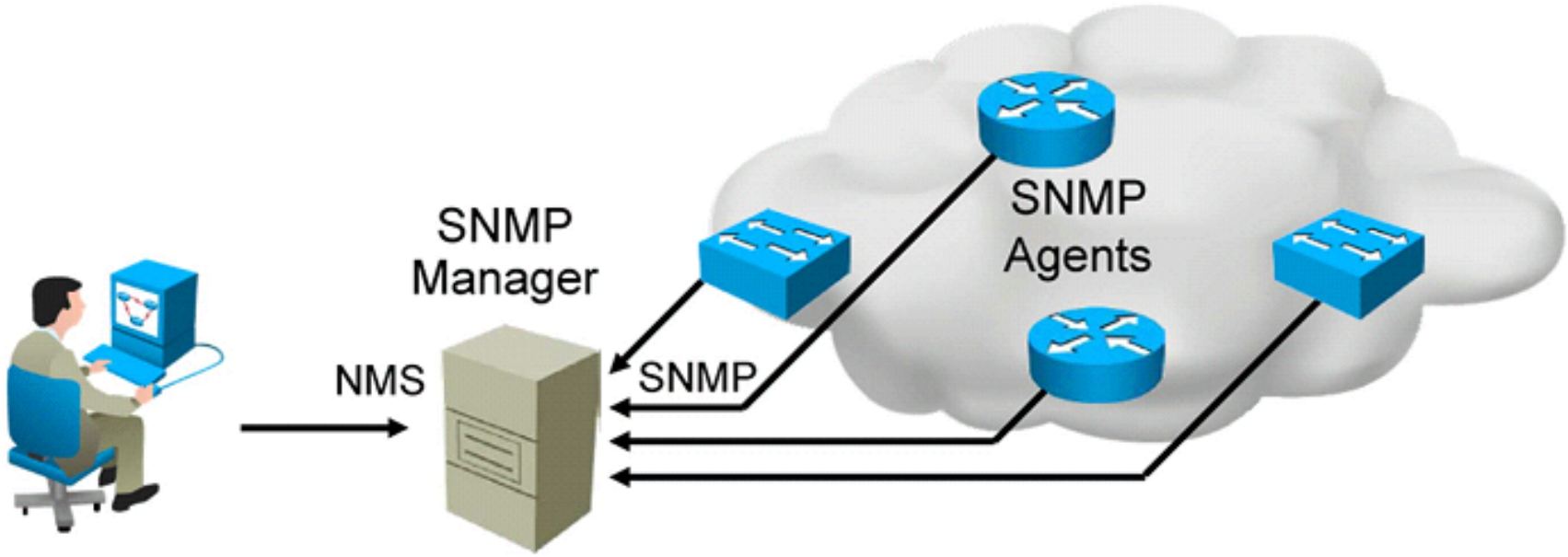
Inside Global	Inside Local	Outside Local	Outside Global
5.5.5.1	10.0.0.1	3.3.3.3	3.3.3.3
5.5.5.2	10.0.0.2	3.3.3.3	3.3.3.3

Administration des réseaux

SNMP : Simple Network Management Protocol

SNMP Overview

- NMS polls the SNMP agent on the network device to obtain statistics.
- Analyzing and representing the results:
  - Graphing
  - Reporting
- Thresholds can be set to trigger a notification process when exceeded.



SNMP

- Deux rôles:
  - SNMP managers
  - SNMP agents
- Utilise la MIB.
- Opérations disponibles:
  - Get + GetNext + GetBulk (si Version 2)
  - Set
  - Traps
  - Informs (= trap + ack) si Version 2

SNMP Versions

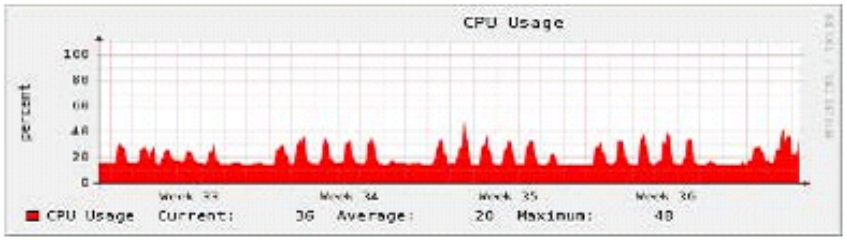
SNMP Version	Security	Bulk Retrieval Mechanism
SNMPv1	Plaintext authentication with community strings	No
SNMPv2c	Plaintext authentication with community strings	Yes
SNMPv3	Strong authentication, confidentiality, and integrity	Yes

Versions SNMP

- SNMPv1:
  - community
- SNMPv2c:
  - GetBulk
  - messages d'erreurs plus détaillés
- SNMPv3:
  - 3 niveaux de sécurité:
    - noAuthNoPriv
      - » authentification basée sur usernames
    - authNoPriv
      - » authentification basée sur algo MD5 / SHA
    - authPriv
      - » + cryptage basé sur algo DES, 3DES /AES

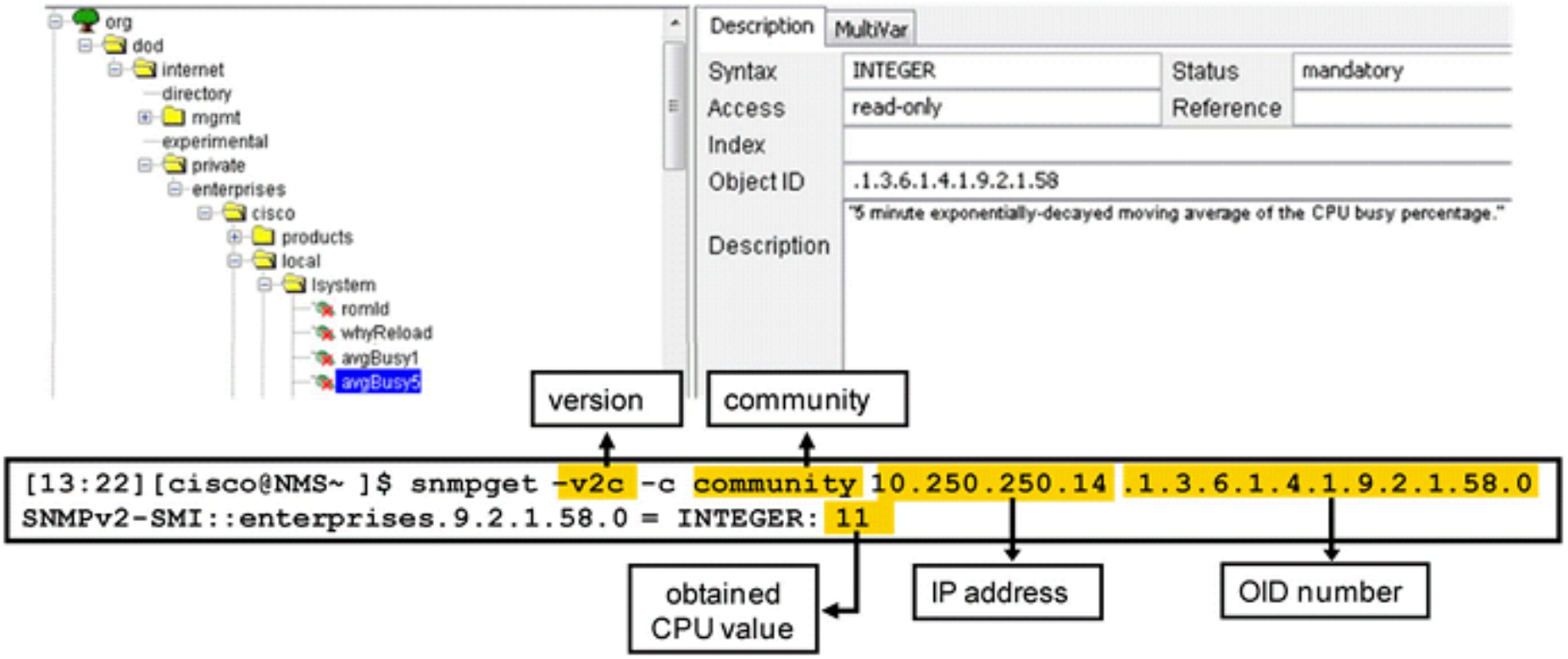
Obtaining Data from an SNMP Agent

An SNMP graphing tool periodically polls an SNMP agent (for example, a router) and graphs obtained values:



Obtaining Data from an SNMP Agent (Cont.)

- MIB is a collection of information that is organized hierarchically.
- OIDs uniquely identify managed objects in an MIB.
  - A 5-minute, exponentially moving average of the CPU busy percentage: 1.3.6.1.4.1.9.2.1.58.0



Configuration SNMP

- Exemple de configuration :

- **snmp-server community** *string* [**ro** | **rw**] [*acl*]
- **snmp-server enable traps** [*notification-type*]
- **snmp-server host** *host-id* [**traps** | **informs**] *community*

Gestion des messages

Syslog

Le Process de Logging

- Le PROCESS de Logging :
  - reçoit les messages de log et les debug
  - distribue ces messages à :
    - console, logging buffer, terminal lines (si ‘terminal monitor’
    - serveurs syslog , serveurs SNMP
- Format d'un message de log:
  - *seq no:timestamp: %facility-severity-MNEMONIC:description*
    - *seq no:* sequence number
    - *timestamp:* horodatage
    - *facility:* syslog facility
    - *severity:* entre 0 et 7
    - *MNEMONIC:* *identifiant alphanumérique unique*
    - *description:* détail textuel
  - *Jun 13 10:17:20.352: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up*

Niveaux de sévérité

Level	Keyword	Description	Definition
0	emergencies	System is unusable	LOG_EMERG
1	alerts	Immediate action is needed	LOG_ALERT
2	critical	Critical conditions exist	LOG_CRIT
3	errors	Error conditions exist	LOG_ERR
4	warnings	Warning conditions exist	LOG_WARNING
5	notification	Normal but significant condition	LOG_NOTICE
6	informational	Informational messages only	LOG_INFO
7	debugging	Debugging messages	LOG_DEBUG

Configuration du Logging

- Activer:
  - **`logging on`**

- Envoyer aux destinations internes:
  - **`logging buffered`** [*`buffer-size | severity-level`*]
  - **`logging console`** [*`severity-level`*]
  - **`terminal monitor`**
  - **`logging monitor`** *`severity-level`*

Configuration du Logging

- Envoyer à un server syslog :
  - **logging host** {{*ip-address* | *hostname*} | **ipv6** {*ipv6-address* | *hostname*}}
  - **logging trap** *severity-level*
- Envoyer à un server SNMP :
  - **snmp-server enable trap syslog**
  - **logging history** *[severity-level]*

Test

Which logging command can enable administrators to correlate syslog messages with millisecond precision?

A. no logging console
B. logging buffered 4
C. no logging monitor
D. service timestamps log datetime mscec
E. logging host 10.2.0.21

- Réponse : D

NetFlow

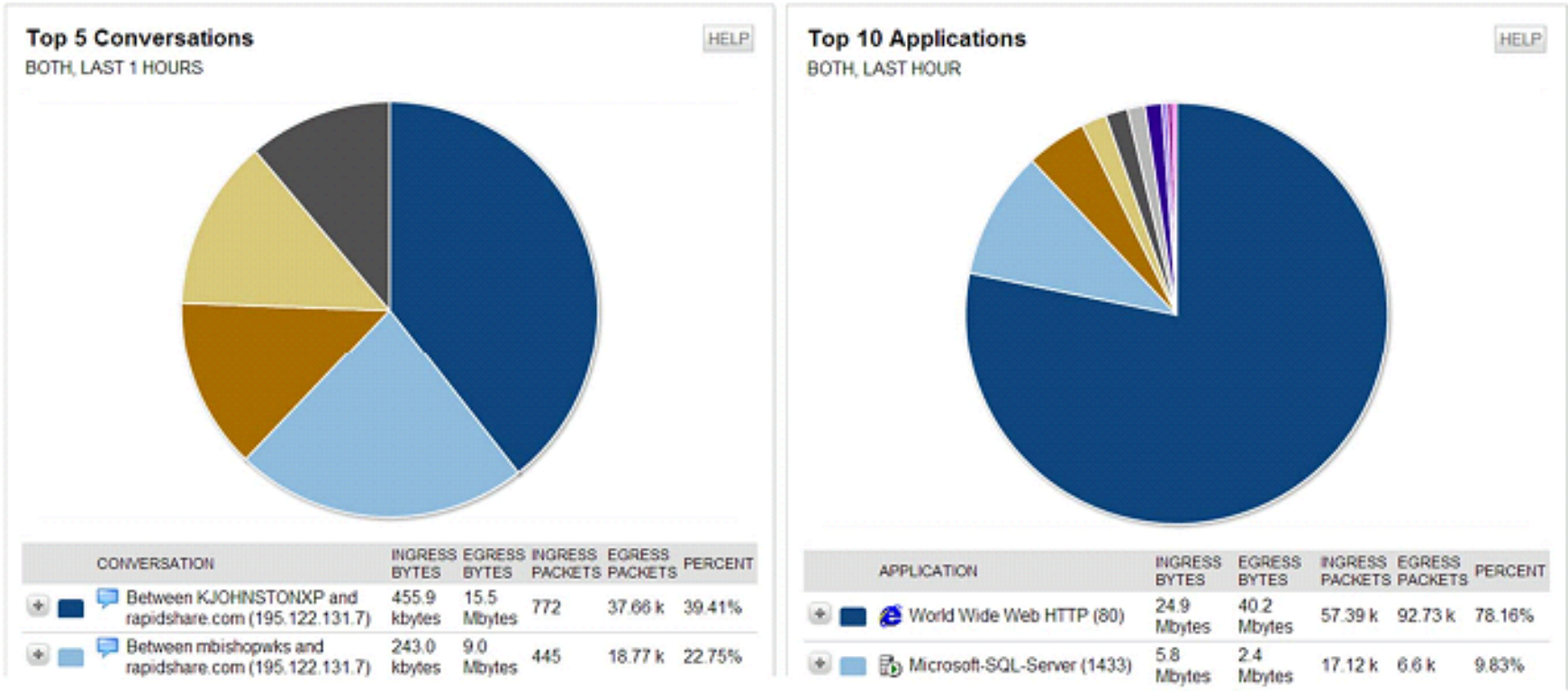
NetFlow Overview

- NetFlow is an application for collecting IP traffic information.
- Reports from NetFlow are like a phone bill.
- NetFlow enables the following:
  - Measuring who uses network resources
  - Accounting and charging for resource utilization
  - Using the measured information to do effective network planning
  - Using the measured information to customize applications and services

NetFlow Overview (Cont.)

Example of analysis on a NetFlow collector:

- Shows the top talkers, top listeners, top protocols, and more.



Top 5 Conversations
BOTH, LAST 1 HOURS
HELP

CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
Between KJOHNSTONXP and rapidshare.com (195.122.131.7)	455.9 kbytes	15.5 Mbytes	772	37.66 k	39.41%
Between mbishopwks and rapidshare.com (195.122.131.7)	243.0 kbytes	9.0 Mbytes	445	18.77 k	22.75%

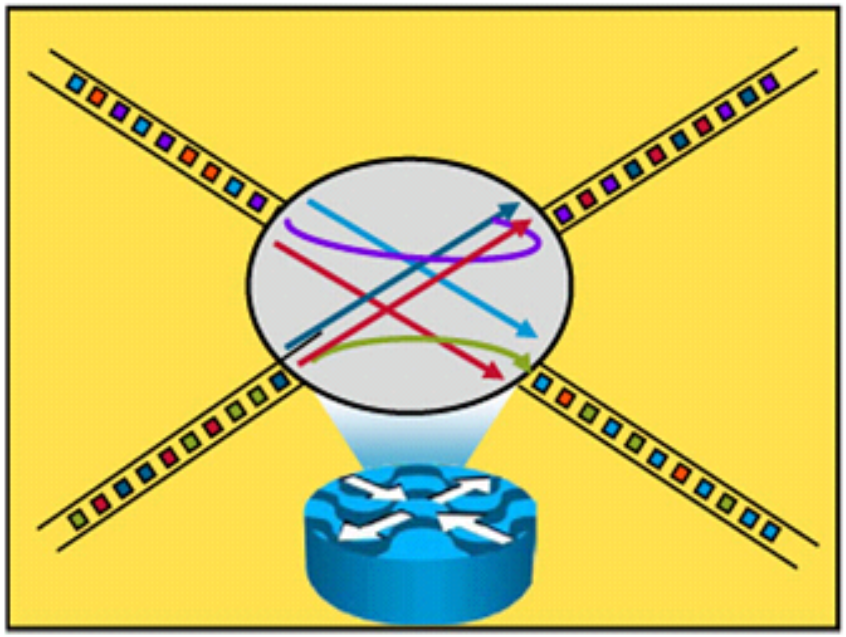
Top 10 Applications
BOTH, LAST HOUR
HELP

APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
World Wide Web HTTP (80)	24.9 Mbytes	40.2 Mbytes	57.39 k	92.73 k	78.16%
Microsoft-SQL-Server (1433)	5.8 Mbytes	2.4 Mbytes	17.12 k	6.6 k	9.83%

NetFlow Overview (Cont.)

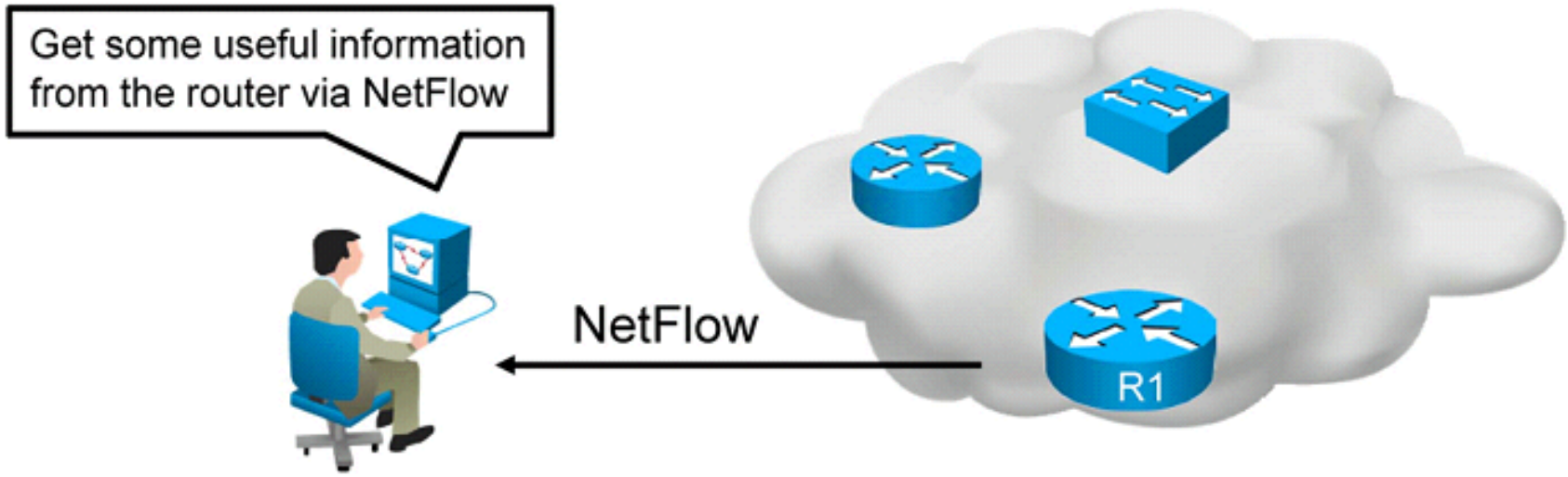
Cisco defines a flow as a unidirectional sequence of packets with seven common values:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- ToS
- Input logical interface

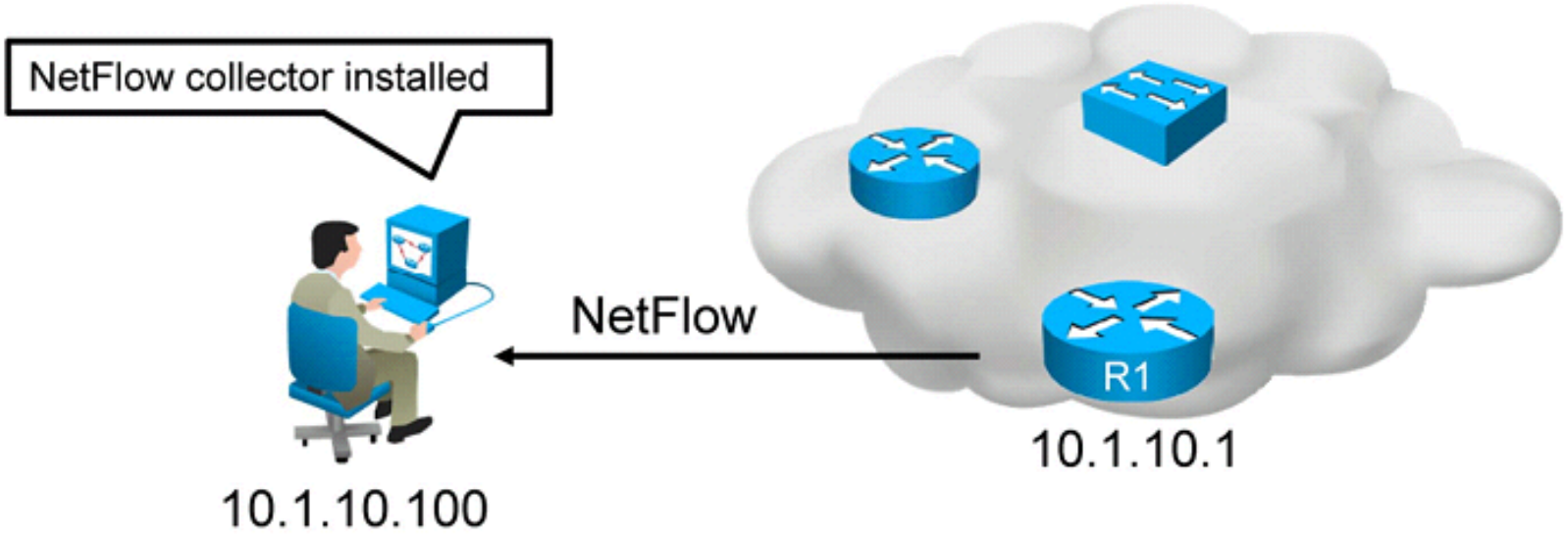


NetFlow Configuration

- Configure NetFlow data capture
- Configure NetFlow data export
- Configure NetFlow data export version
- Verify NetFlow, its operation, and statistics



NetFlow Configuration (Cont.)




```
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config-if)#exit
R1(config)#ip flow-export destination 10.1.10.100 9996
R1(config)#ip flow-export version 9
```

- Configuration of NetFlow on router R1

NetFlow Configuration (Cont.)

```
R1#show ip interface GigabitEthernet0/1
<output omitted>
  Input features: Ingress-NetFlow, MCI Check
  Output features: Access List, Post-Ingress-NetFlow, Egress-NetFlow
```

- Displays whether NetFlow is enabled on an interface

```
R1#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  10.1.10.100 (9996)
  Version 9 flow records
  43 flows exported in 15 udp datagrams
```

- Displays the status and the statistics for NetFlow data export

NetFlow Configuration (Cont.)

```
Branch#show ip cache flow
<output omitted>
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 31 added
  6374 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 31 added, 31 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:49:48
Protocol      Total    Flows   Packets   Bytes  Packets Active(Sec) Idle(Sec)
--------      Flows     /Sec    /Flow    /Pkt    /Sec      /Flow      /Flow
TCP-Telnet    19       0.0        19      58      0.1       6.5        11.7
TCP-WWW       14       0.0         8     202      0.0       0.0         1.5
TCP-other      2       0.0        19      98      0.0       2.2         8.9
<output omitted>

SrcIf       SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Gi0/1       172.16.1.100    Gi0/0.10       10.1.10.100     01 0000 0000  1341
```

- Displays a summary of the NetFlow accounting statistics

QoS

La Qualité de service

Traffic Characteristics

Data

- Smooth/bursty
- Benign/greedy
- Drop-insensitive
- Delay-insensitive
- TCP retransmits

Voice

- Smooth
- Benign
- Drop-sensitive
- Delay-sensitive
- UDP priority

One-Way Requirements

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%
- Bandwidth (30–128 Kbps)

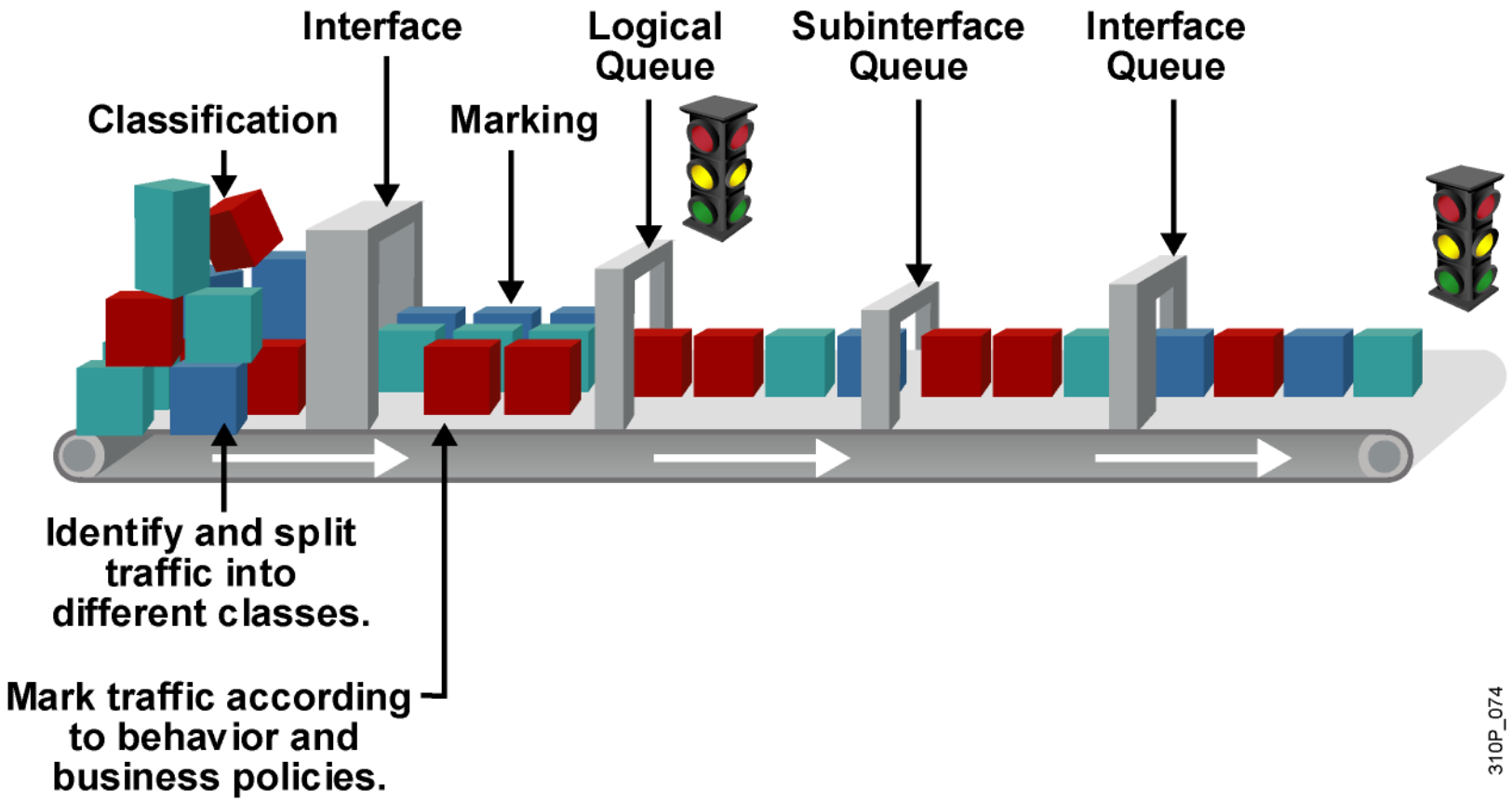
Video

- Bursty
- Greedy
- Drop-sensitive
- Delay-sensitive
- UDP priority

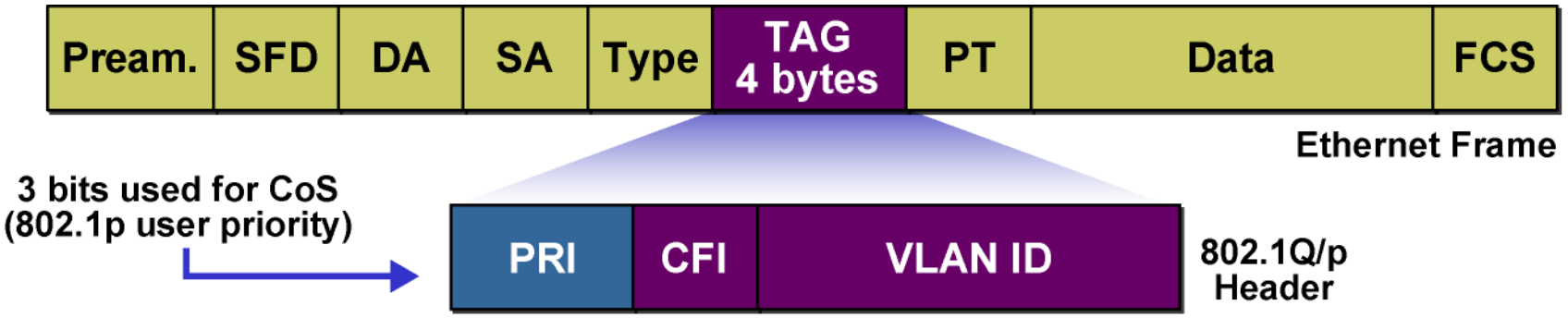
One-Way Requirements

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 0.1–1%
- Bandwidth (384 Kbps–20+ Mbps)

Classification et marquage



Marquage en couche 2 : 802.1p, CoS

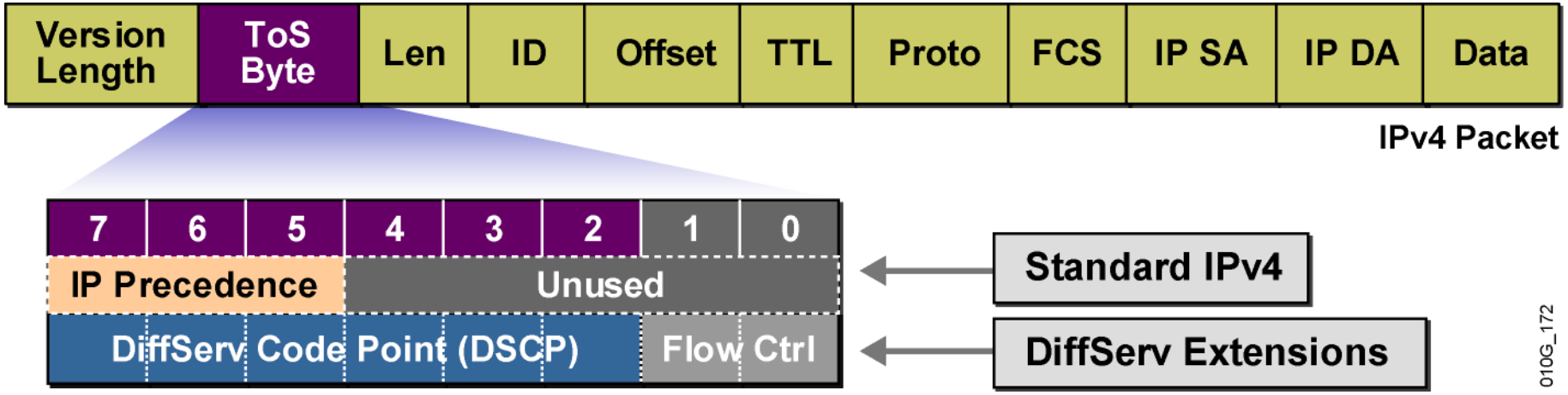


CoS	Typical Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data

010G_171

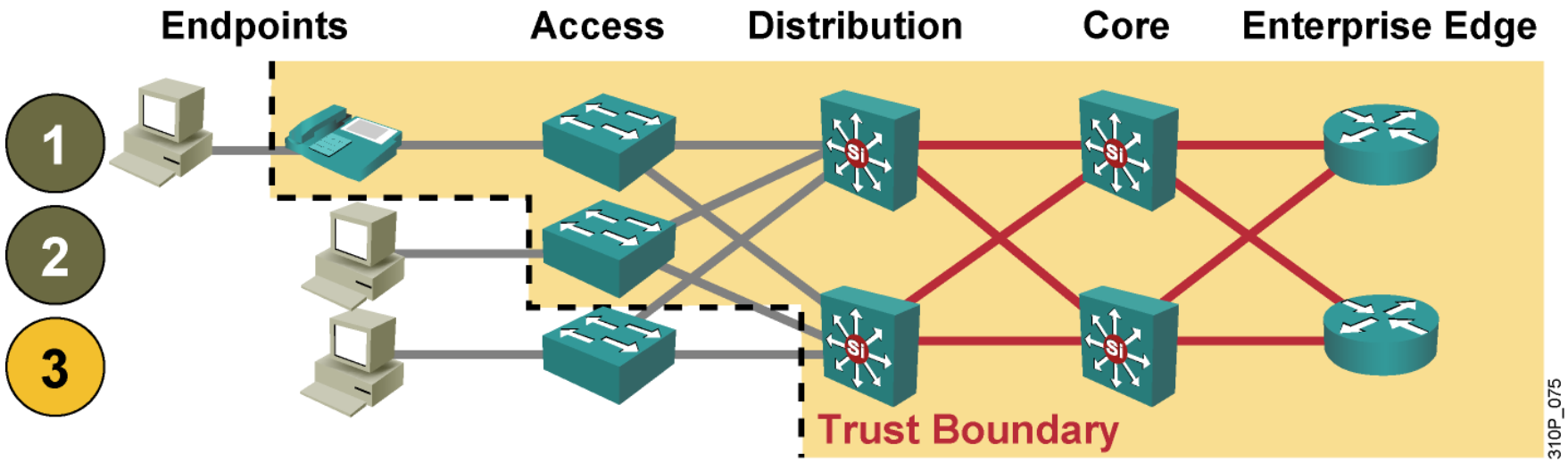
- 802.1p est aussi appelé Classe de Service
- Chaque type de trafic se voit assigné d'une valeur CoS.
- Les CoS 6 et 7 sont réservés aux protocles de routage et supervision

Marquage en couche 3 : IP Precedence, DSCP



- IPv4
  - Les 3 premiers bits du champ ToS sont appelés IP précédence.
  - Les autres bits ne sont pas utilisés
- DiffServ
  - Les 6 premiers bits du champ ToS sont appelés DiffServ Code Point (DSCP).
  - DSCP est compatible avec la précédence.
  - Les deux derniers bits sont utilisés pour le contrôle de flux

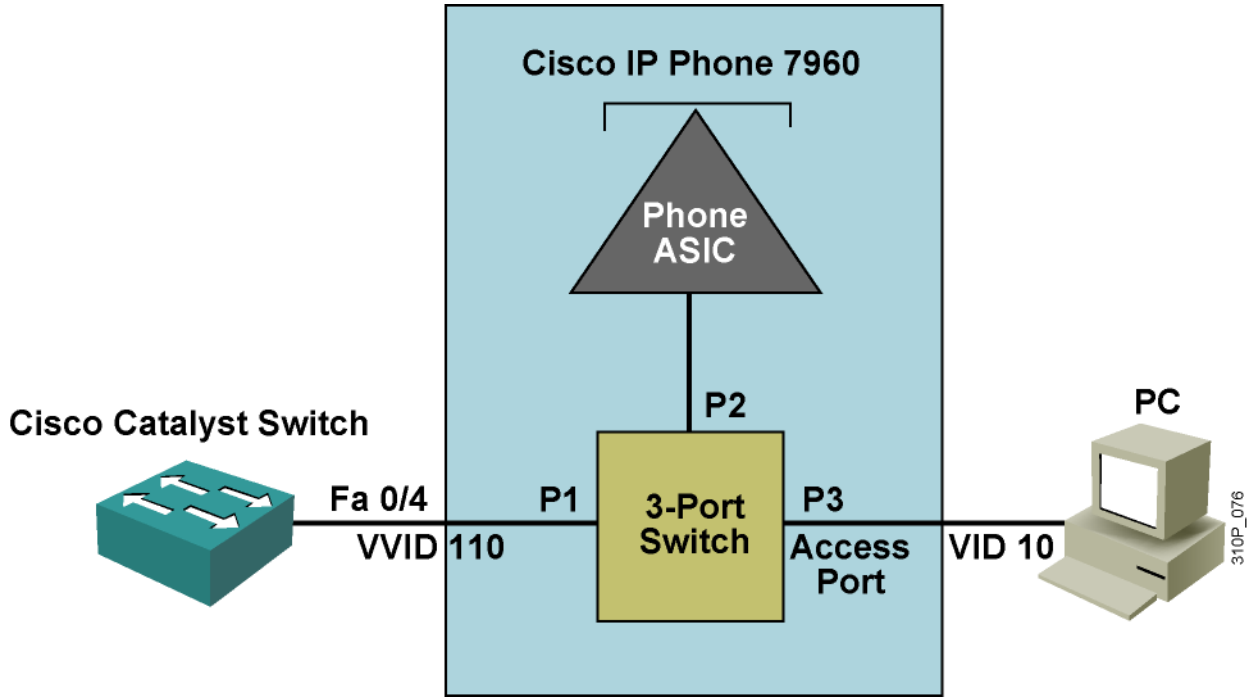
Frontières de la Classification



- Un équipement de confiance traite correctement les paquets.
- La classification doit être aussi proche de la source que possible
- 1 et 2 sont optimales, 3 est acceptable, si le switch d'accès n'est pas capable de faire de la classification

Configuration d'un switch pour la Voix

- Le traffic est marqué prioritaire sur le VLAN voix



Commandes de base pour un Téléphone

Configuration du “voice VLAN”

- switchport voice vlan 110

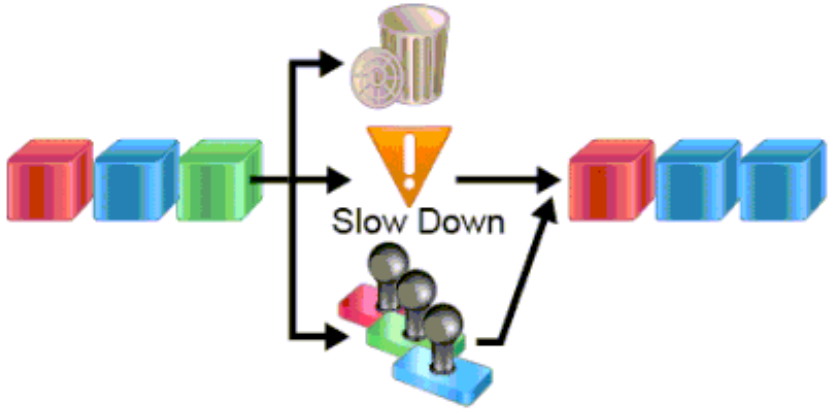
Vérification de la configuration

- show interfaces fa 0/4 switchport

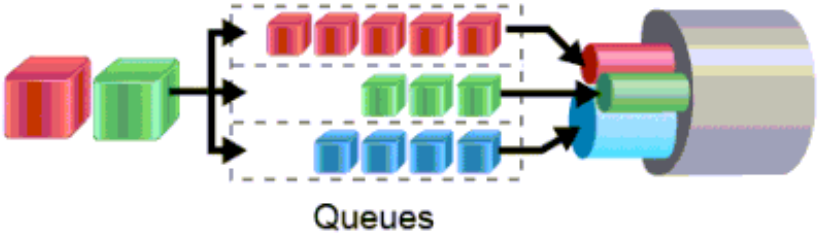
QoS Mechanisms Overview

Classification and Marking

Policing, Shaping, and Re-Marking



Congestion Management or Scheduling Tools



Link-Specific Tools (e.g. Fragmentation)

QoS Mechanisms—Classification and Marking

Various Layer 2 and Layer 3 fields for marking traffic:

- **CoS** = class of service
  - Layer 2, Ethernet marking
- **ToS** = type of service
  - Layer 3, IP packet
  - For IPv4, it is called "ToS." For IPv6, it is called "Traffic Class."
- **DSCP** = differentiated services code point
  - The value that is used to describe the meaning of ToS
- **CS** = Class Selector
  - Subset of DSCP fields
- **TID** = traffic identifier
  - What CoS is for wired Ethernet, TID is for wireless Ethernet.

Classification Tools

There are three general ways to classify traffic:

- **Markings:**
  - Looks at header information.
  - Classification is done based on the existing markings.
- **Addressing:**
  - Looks at header information.
  - Classification is done based on the source/destination port, interface, Layer 2 address, or Layer 3 address.
- **Application signatures:**
  - Looks at the content of the payload.

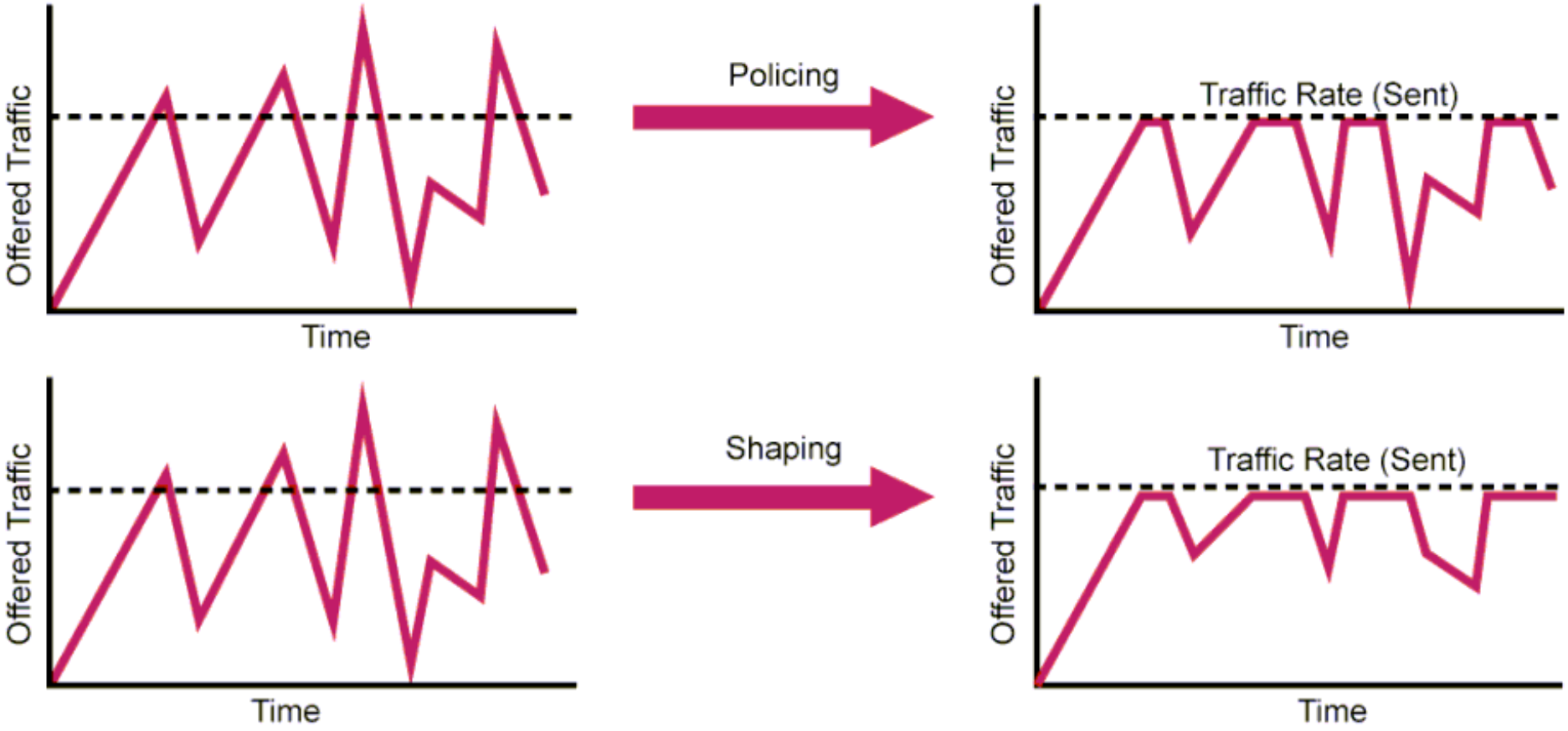
Classification Tools (Cont.)

Example of advanced classification tool: NBAR

- Layers 4 to 7 deep-inspection classifier.
- While most applications can be identified by inspecting Layers 3 and 4 information, this kind of identification is not always possible.
- NBAR classifies applications by looking into the packet payload and comparing the content against its signature database.

QoS Mechanisms—Policing, Shaping, and Re-Marking

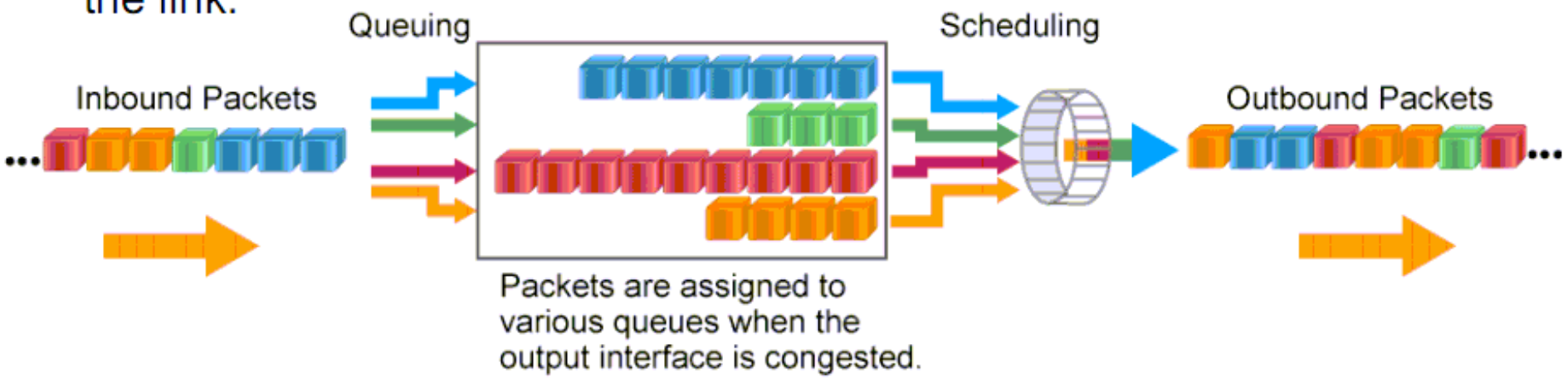
Policers and shapers are both rate-limiters, but they differ in how they treat excess traffic; policers drop it and shapers delay it.



Tools for Managing Congestion

Congestion management includes:

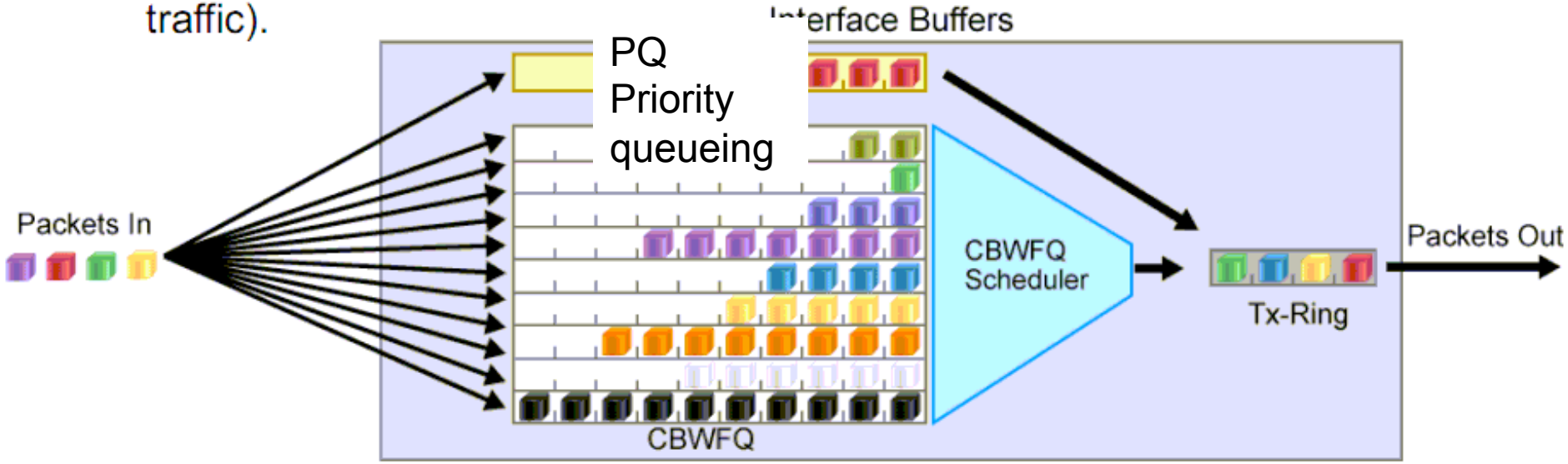
- **Queuing** (or buffering) is the logic of ordering packets in output buffers. It is only activated when congestion occurs. When queues fill up, packets can be reordered so that the higher-priority packets can be sent out of the exit interface sooner than the lower priority ones.
- **Scheduling** is a process of deciding which packet should be sent out next. Scheduling occurs regardless of whether there is congestion on the link.



Tools for Managing Congestion (Cont.)

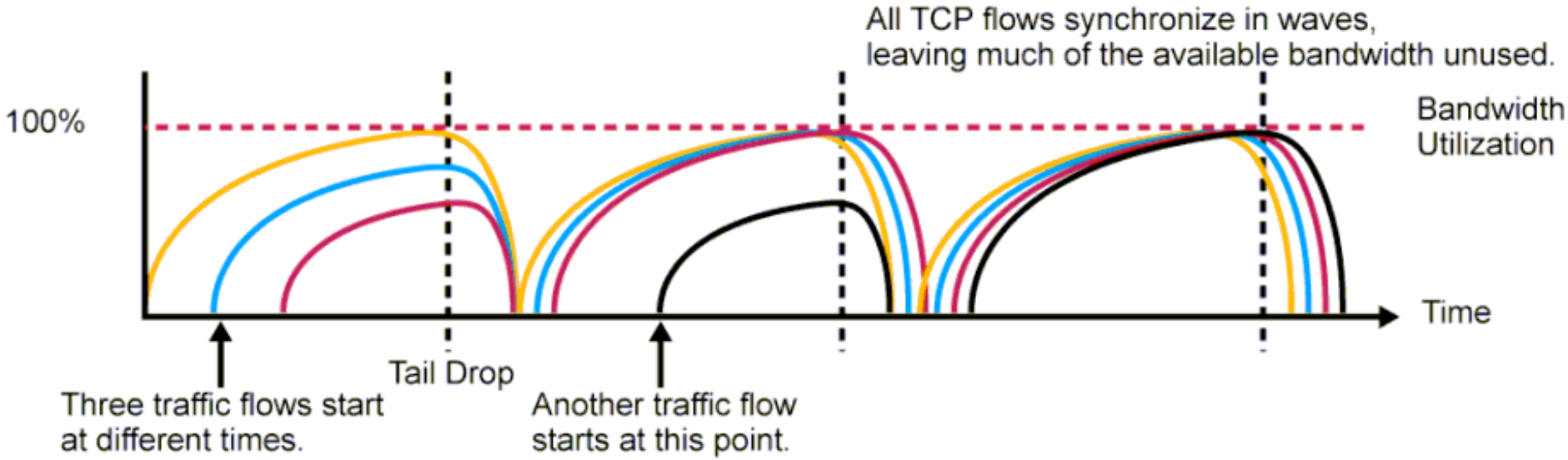
There are many queuing mechanisms. Two modern examples from Cisco are as follows:

- **Class-based weighted fair queuing:**
  - Traffic classes get fair bandwidth guarantees.
  - No latency guarantees—only suitable for data networks.
- **Low-latency queuing:**
  - Takes the previous model and adds a queue with strict priority (for real-time traffic).



Tools for Congestion Avoidance

- **Tail drop:**
  - When a queue fills up, it drops packets as they arrive.
  - It can result in waste of bandwidth if TCP traffic is predominant.
- **Congestion avoidance:**
  - It drops random packets before a queue fills up.
  - Cisco uses WRED (drops packets randomly, but "randomness" is skewed by traffic weights).



Test

Which feature can you implement to reserve bandwidth for VoIP calls across the call path?

A. PQ
B. CBWFQ
C. round robin
D. RSVP

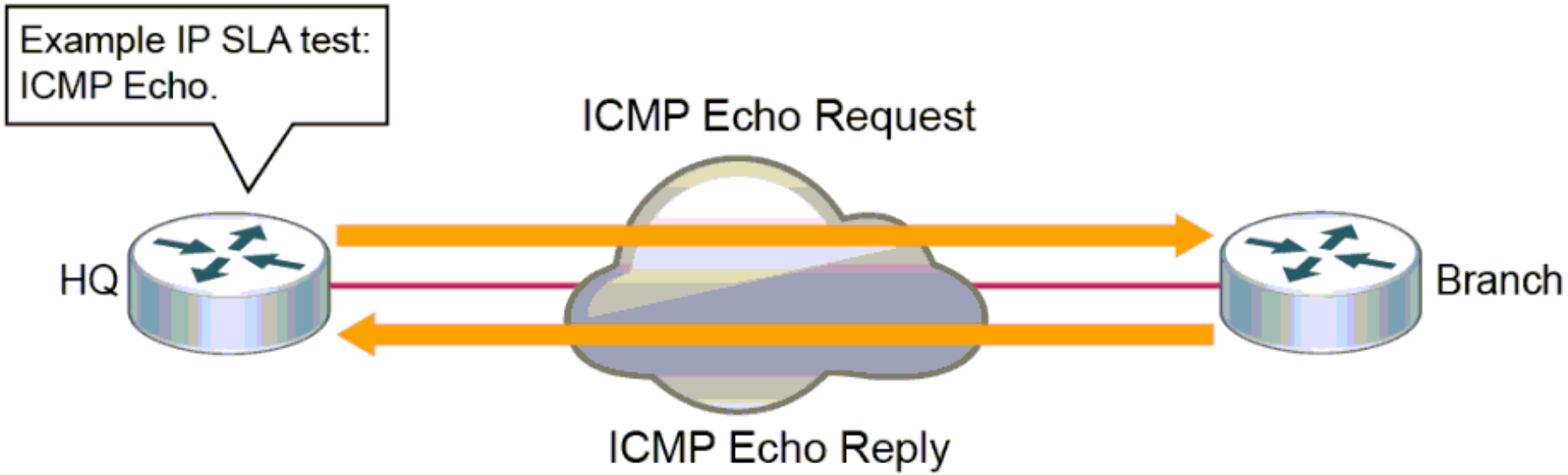
- Réponse : D

IP SLA

Service Level Agreement

Using IP SLA for Troubleshooting

IP SLA can use ICMP Echo Request and Response packets to test availability.



Step 4 Access the console of R1 and configure an IP SLA ICMP Echo test to the SRV1 IP addres (10.10.3.30).

Define the IP SLA with the number 1 and set the frequency to 10 seconds.

```
R1# conf t
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 10.10.3.30
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit
```

Step 5 Schedule IP SLA 1 on R1 to perform an ICMP Echo test forever and to start running now.

```
R1(config)# ip sla schedule 1 life forever start-time now
R1(config)# exit
```

Félicitations

Vous avez suivi avec succès

cette formation