

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, Etherchannels, FHRP

3. Routage :
 - Subnetting, statique, dynamique, DV, LS, RIP

4. Sécurité & administration :
 - ACL, NAT, SNMP, Logging, NetFlow

5. Routage : OSPF & EIGRP

6. IPv6 : adressage & routage

7. Architectures LAN, WAN & Cloud

8. Réseaux intelligents & automatisation

9. Divers:

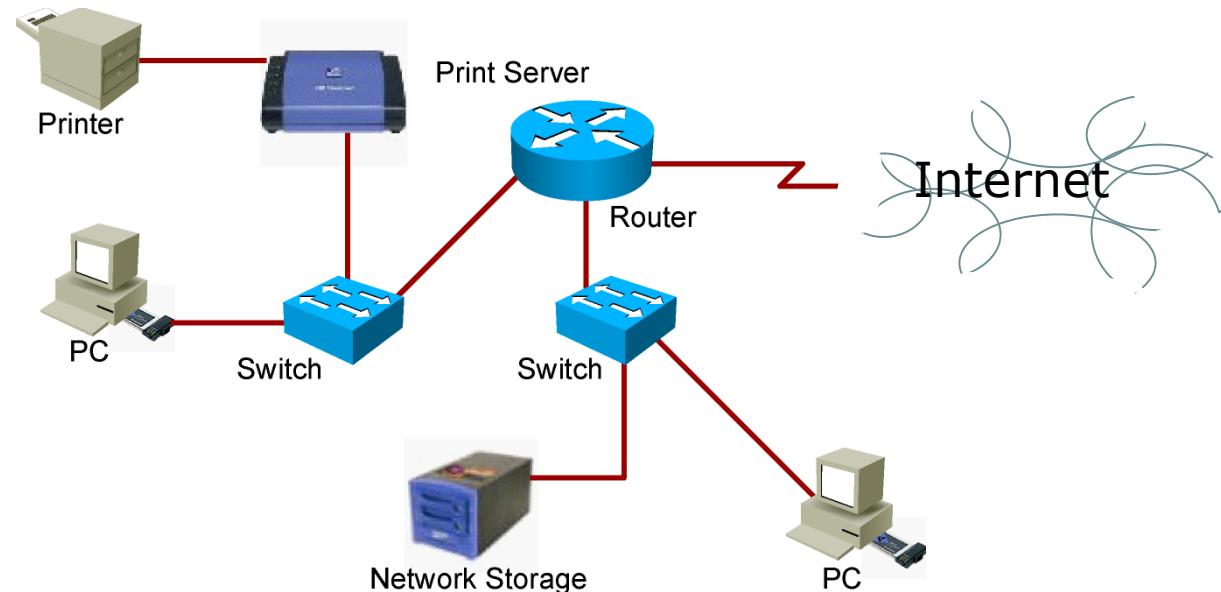
- Wi-Fi, QoS,

Seconde
semaine

Introduction aux réseaux

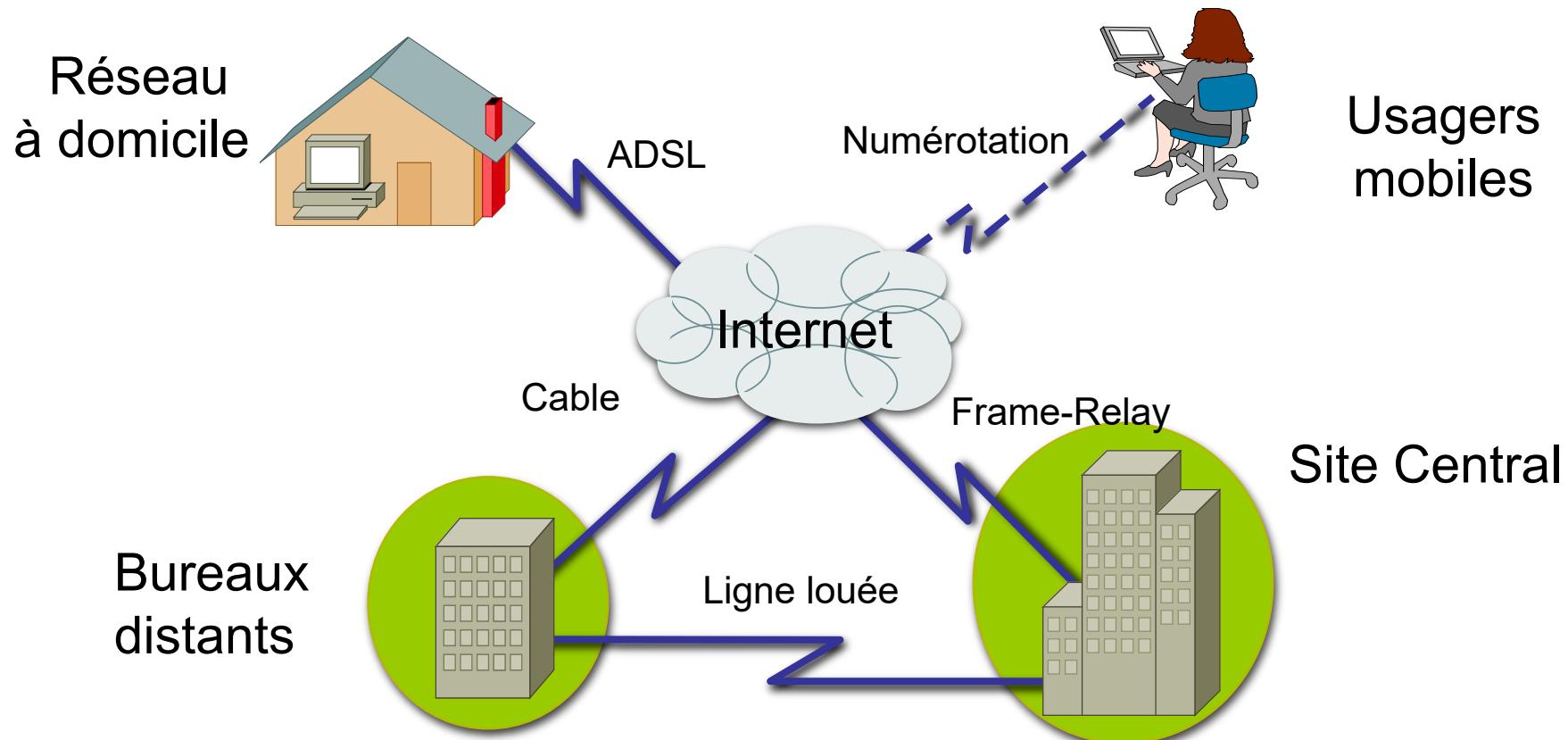
Présentation générale

LAN : Partage des ressources locales



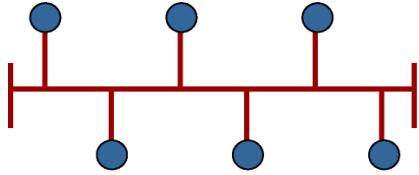
- Réseaux Locaux (LAN)
 - Partage d' applications et de données
 - Stockage
 - Accès à l' Internet

WAN : Accès aux réseaux étendus

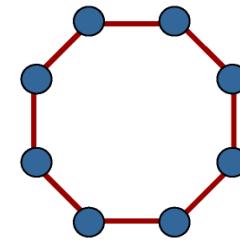


- Les réseaux étendus (WAN) connectent à l' Internet
- Ils peuvent aussi interconnecter des sites
- Il existe de nombreuses technologies d' accès : DSL, Cable...

Les topologies d'accès

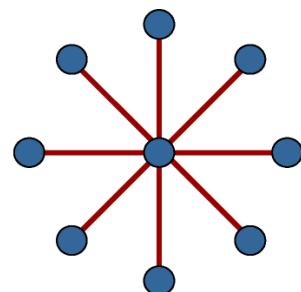


Topologie en bus
Ethernet

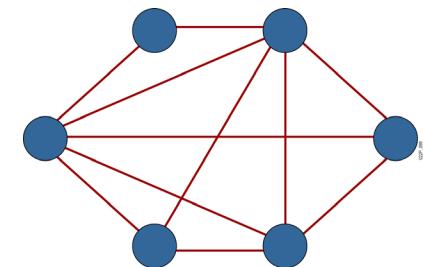


Anneaux
Token Ring

Réseaux locaux (LAN)



Topologie en étoile
Hub and Spoke



Topologie maillée
Circuits virtuels

Réseaux étendus (WAN)

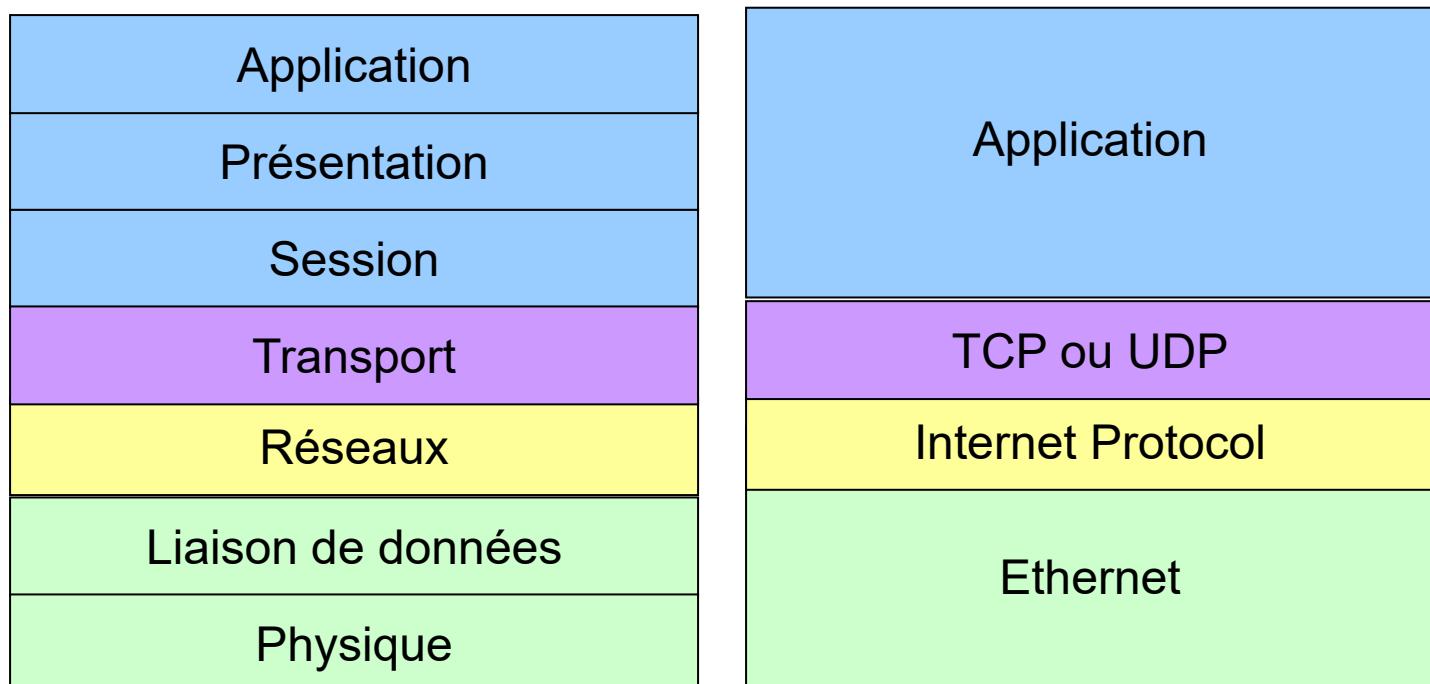
Les modèles OSI et TCP/IP

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 **spécifier** 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

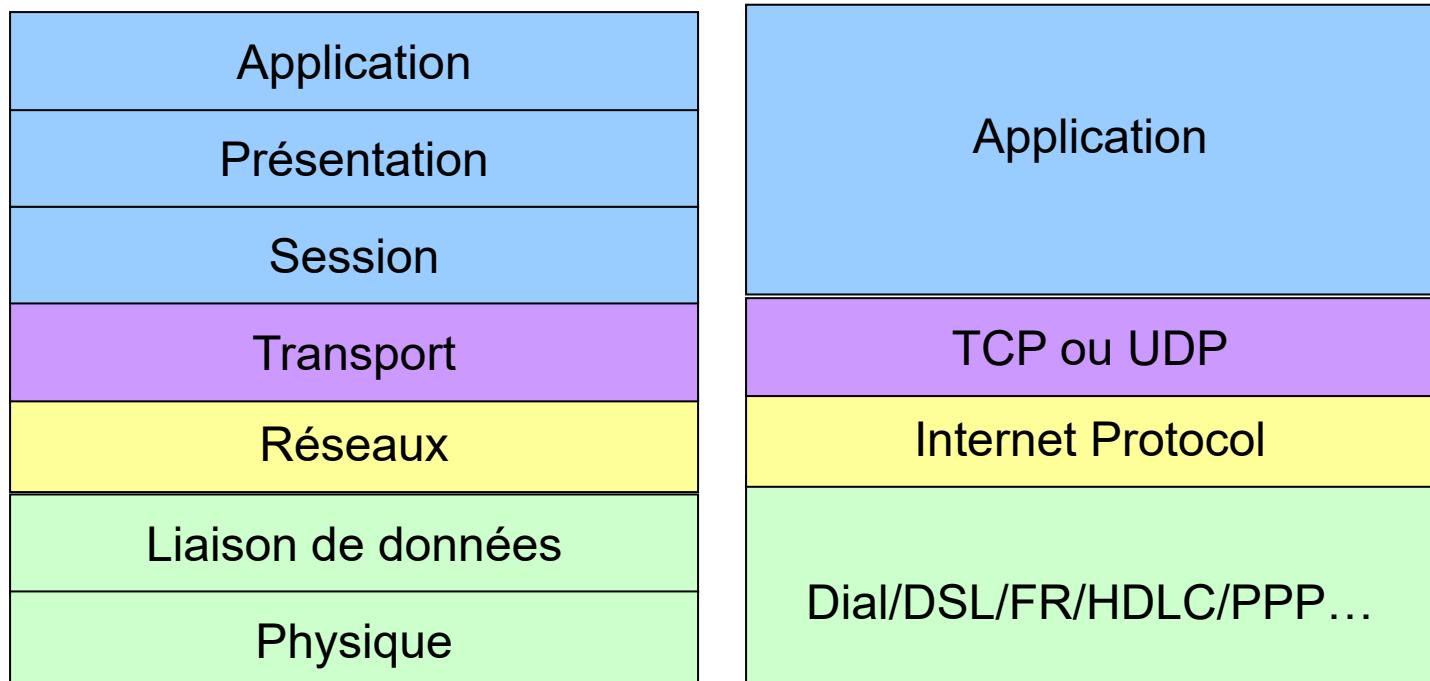
Comparaison de OSI et TCP/IP dans le LAN

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



Comparaison de OSI et TCP/IP dans le WAN

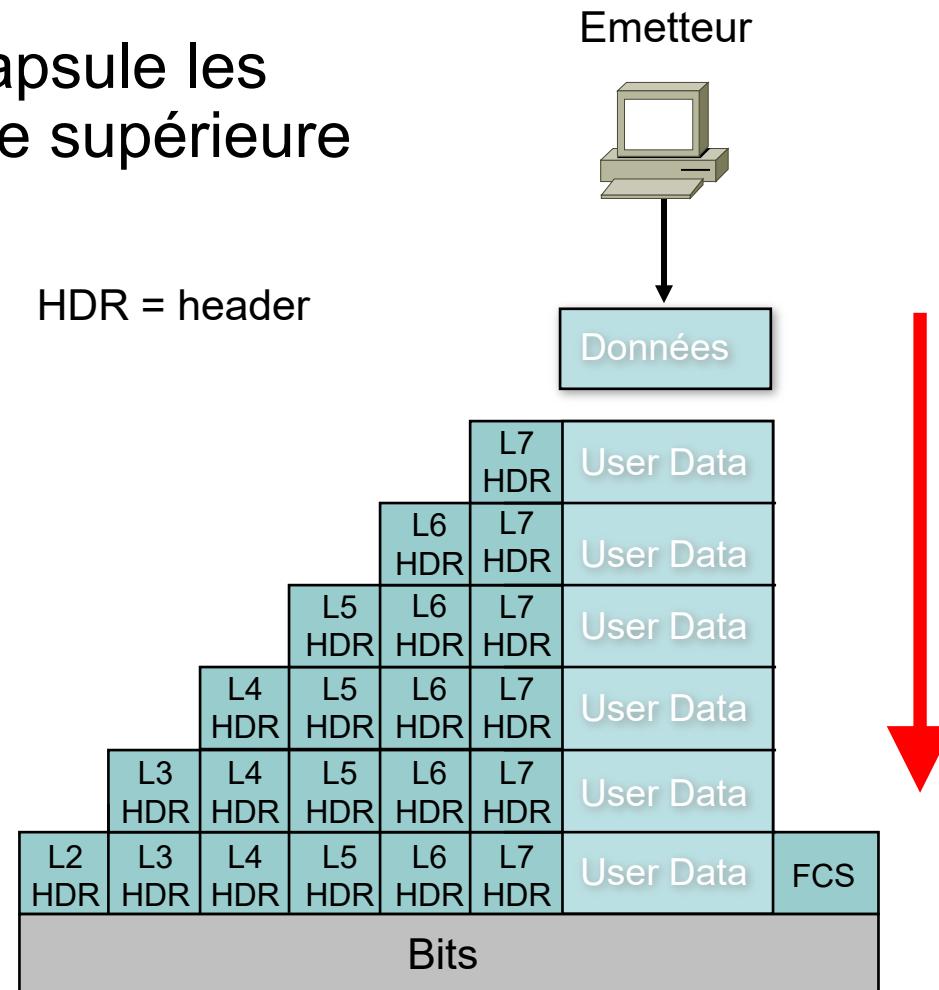
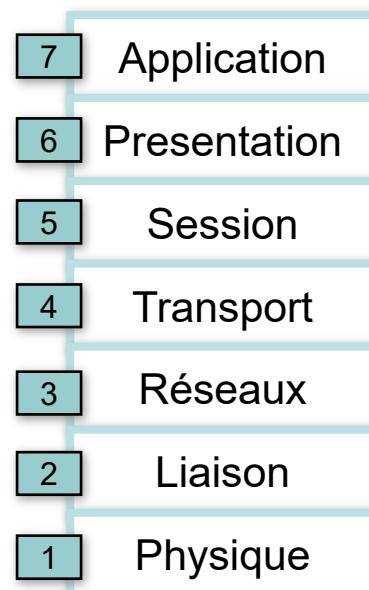
Le réseau étendu est caractérisé par les deux premières couches



Encapsulation et dé-encapsulation

L'encapsulation des données

- Chaque couche encapsule les données de la couche supérieure

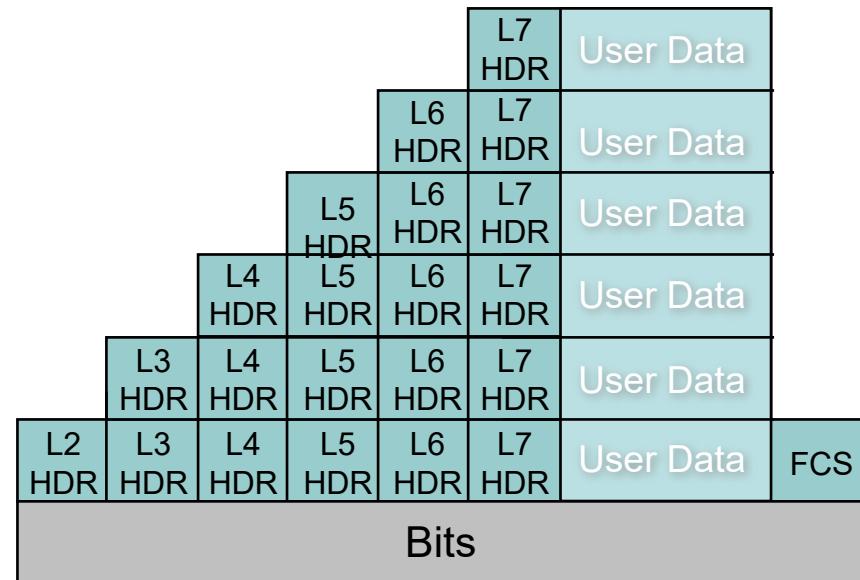


Dé-encapsulation des données

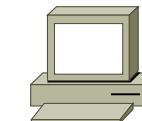
- Chaque couche dé encapsule les données de la couche inférieures



HDR = header



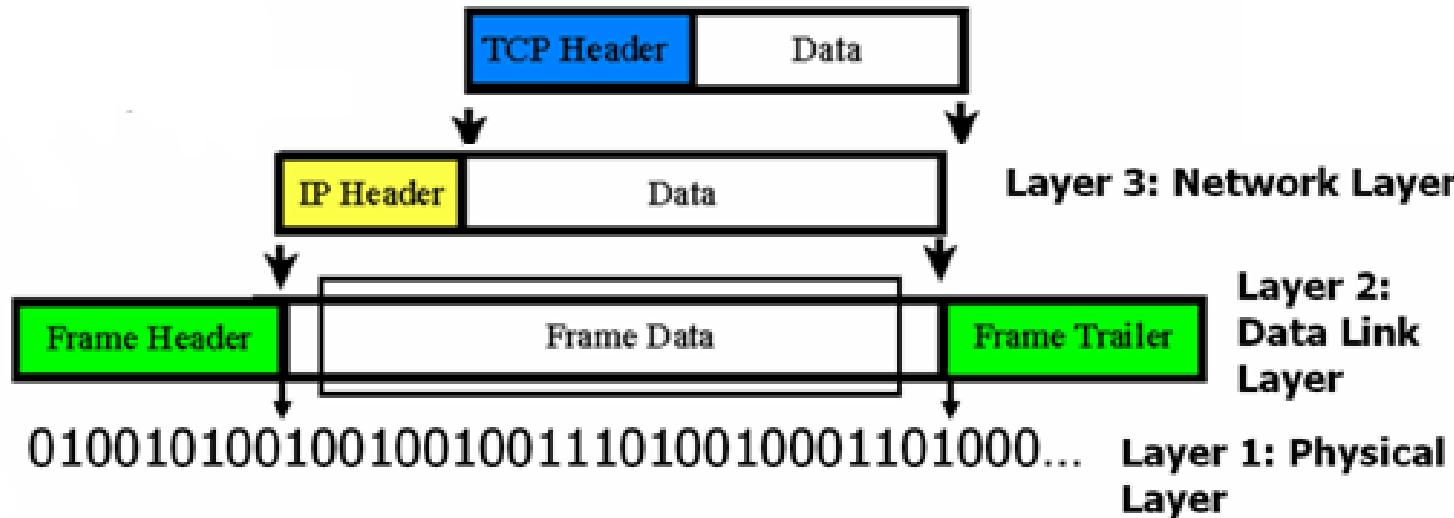
Récepteur



Données

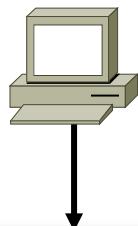
Data encapsulation avec TCP/IP

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



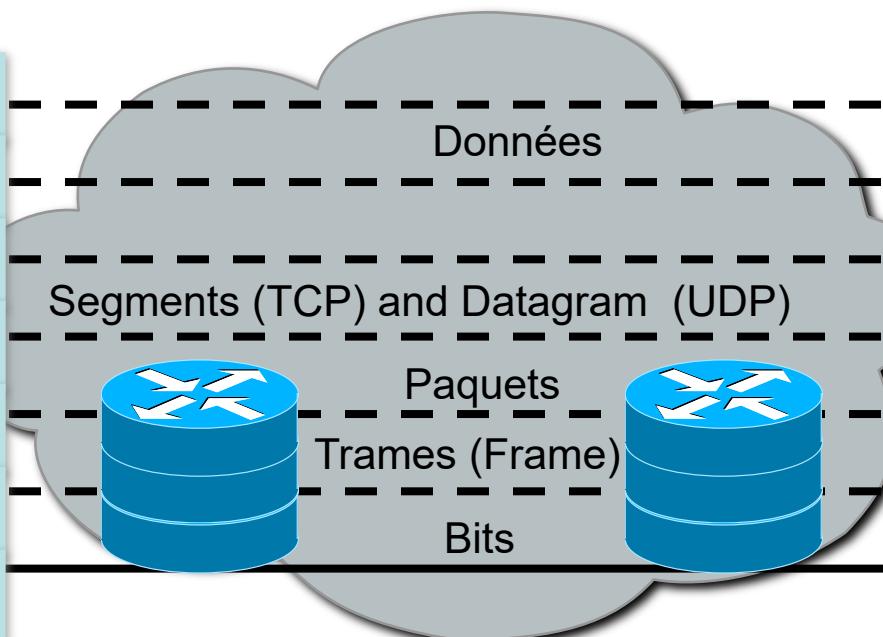
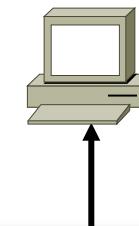
Communication pair à pair

Emetteur



Chaque couche communique avec son pair

Récepteur



OSI couche 1 : la couche physique

OSI couche 1 - Couche physique

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

- 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)

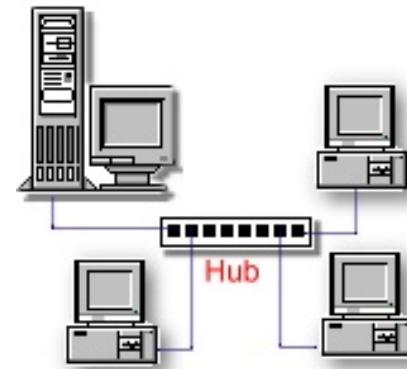
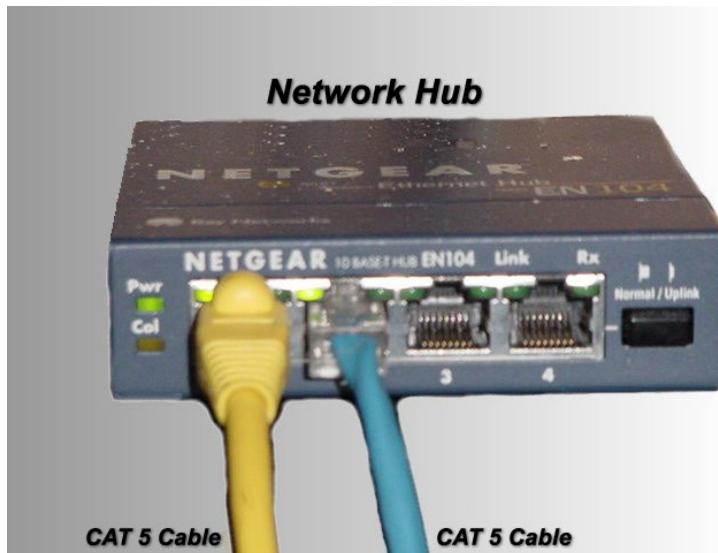
101100111100001011001

Le répéteur



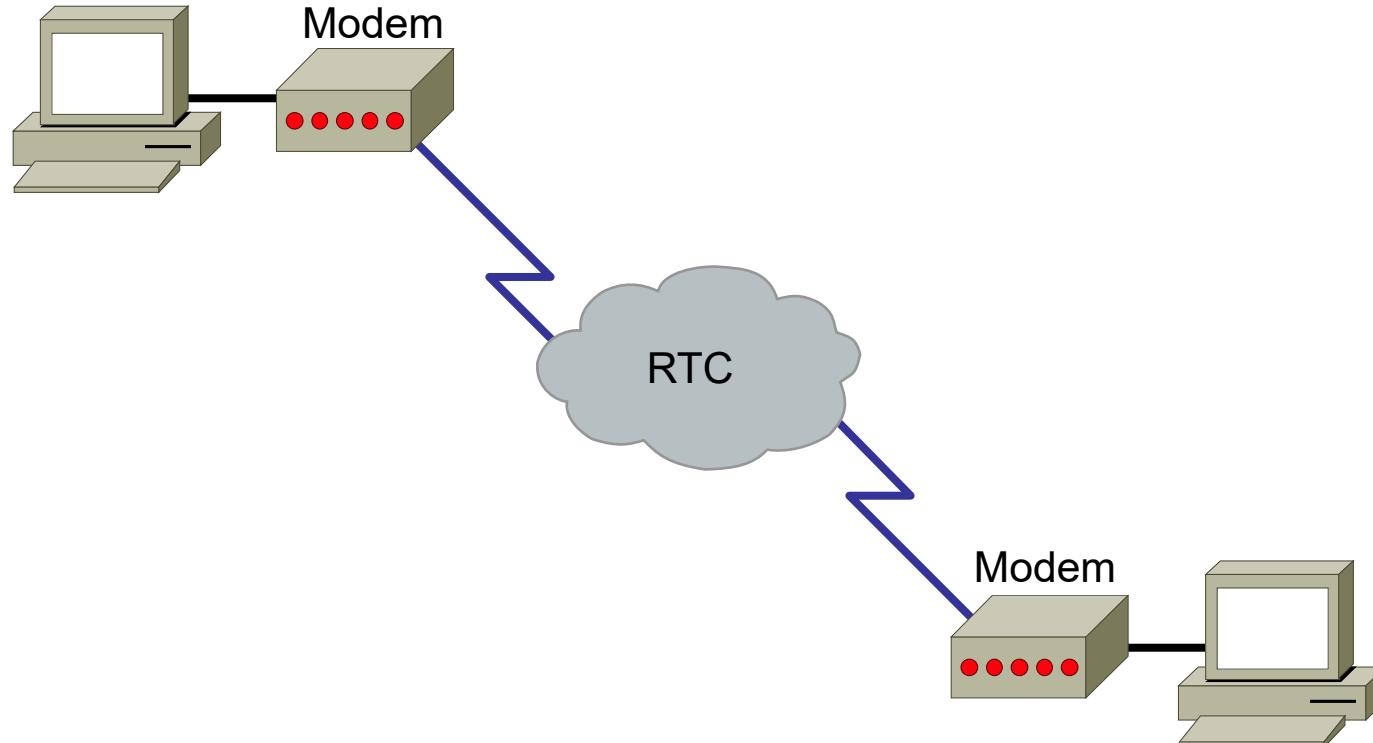
- Equipement de couche 1 qui combat l'atténuation.
- Le répéteur:
 - Récupère le signal atténué
 - Le régénère (détection d'erreurs)
 - Le retransmet sur le réseau

Le concentrateur



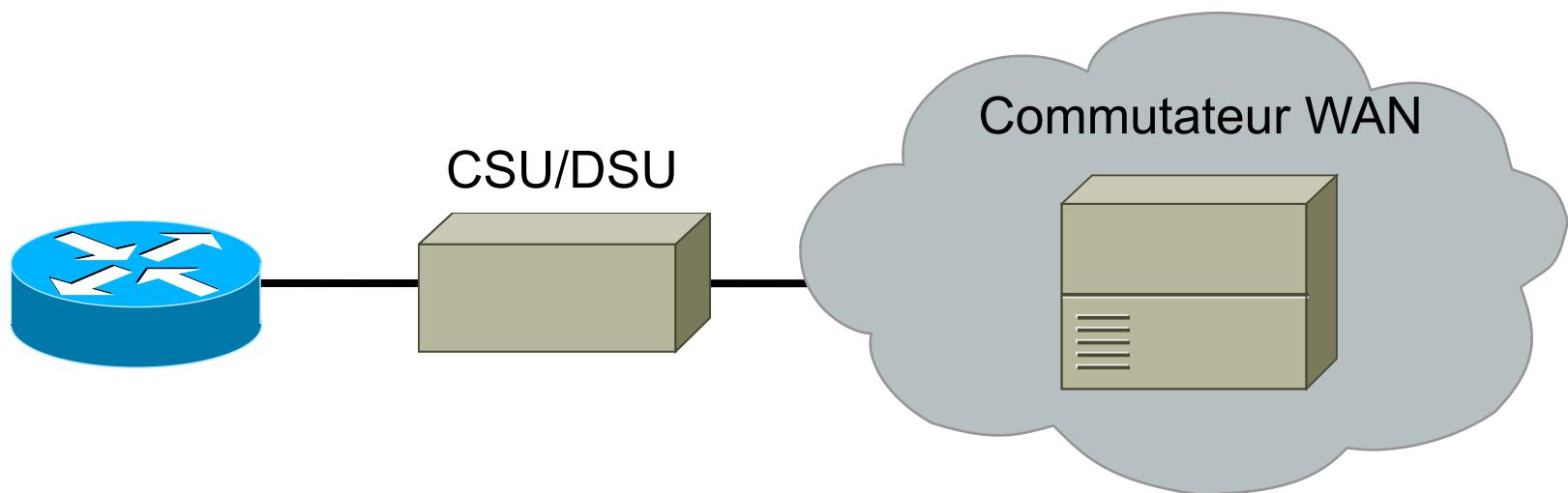
- Permet d'interconnecter plusieurs équipements
- Régénère le signal, comme le répéteur
- C'est un répéteur multiport

Le Modem



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

CSU/DSU ou ETTD/ETCD

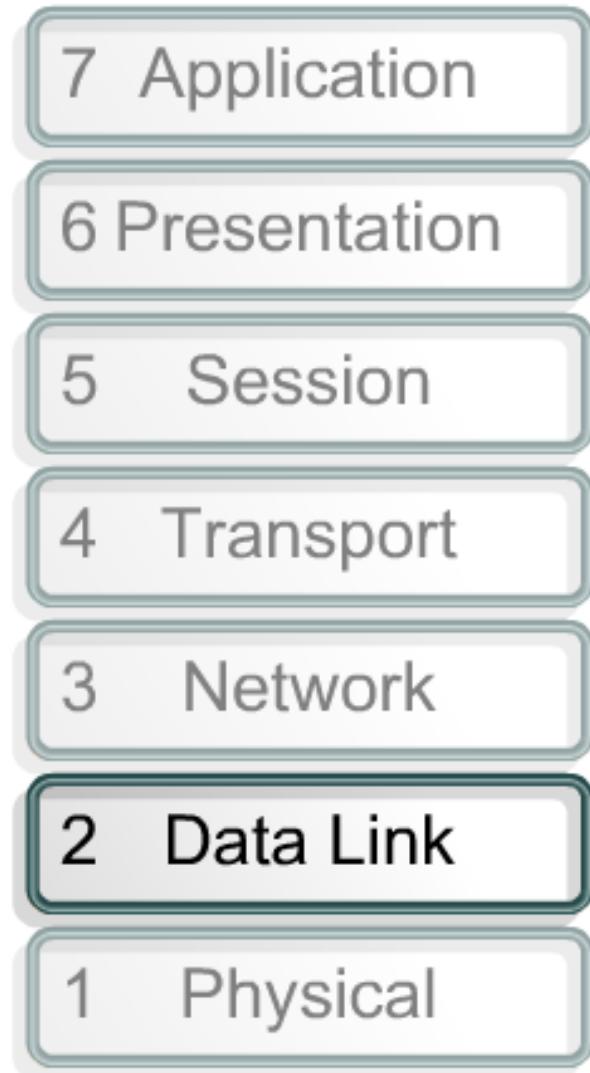


C'est un modem utilisé par les liaisons spécialisées et Frame-Relay

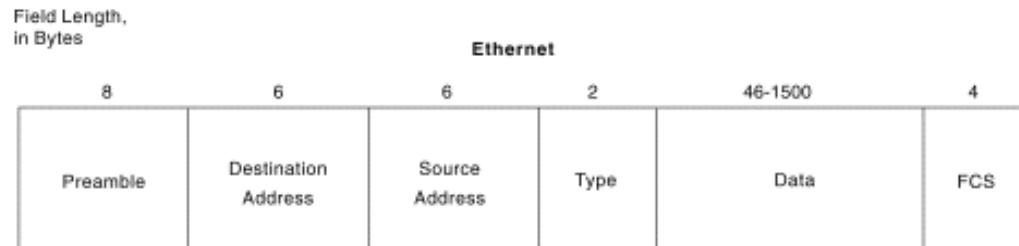


OSI couche 2 : Liaison de données

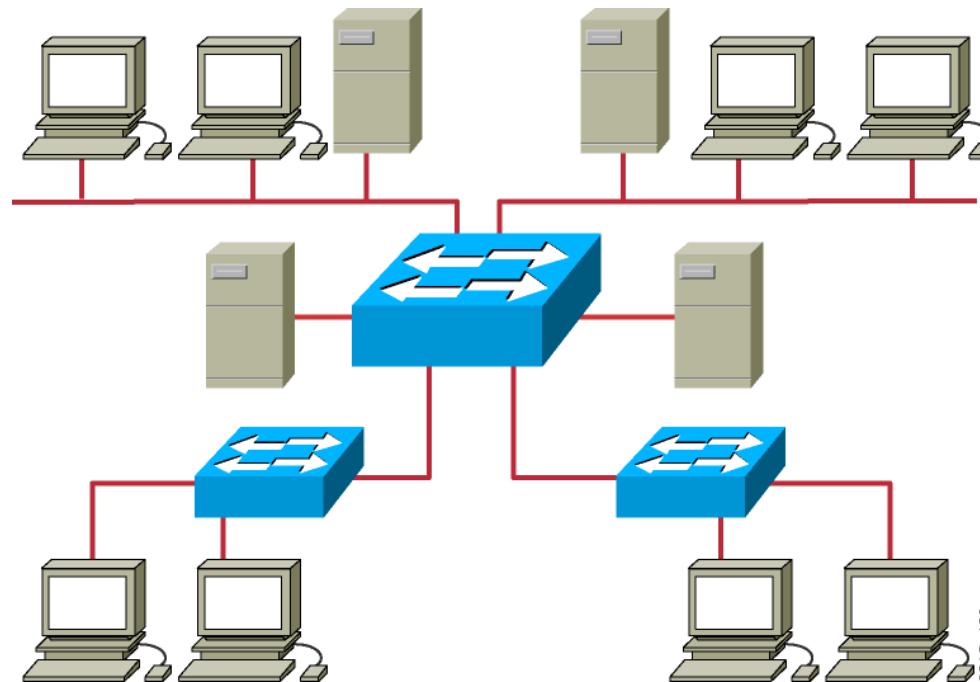
OSI couche 2 - Liaison des données



- 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



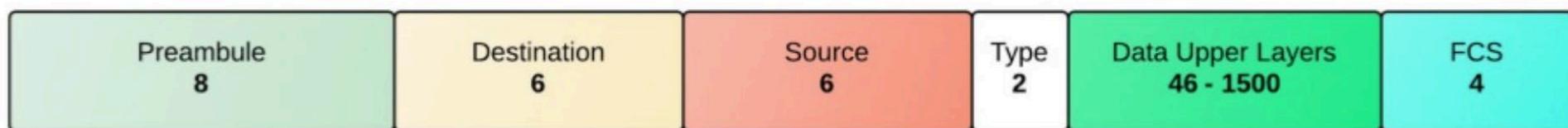
Equipements de couche 2 : le commutateur



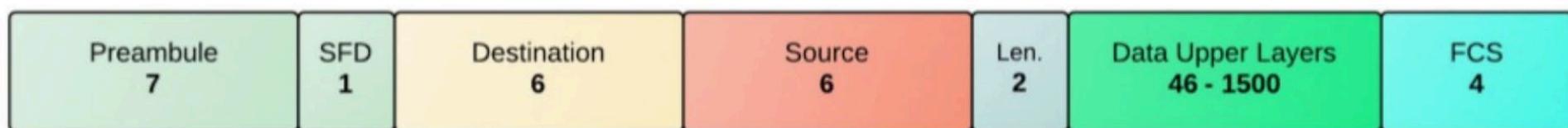
- Le commutateur apprend les adresses MAC en silence
- Cet apprentissage permet, par la suite, de copier les trames uniquement sur le port concerné

Exemple de protocole couche 2 : Ethernet

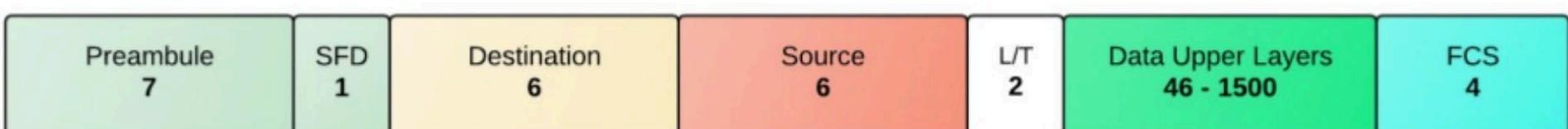
DIX



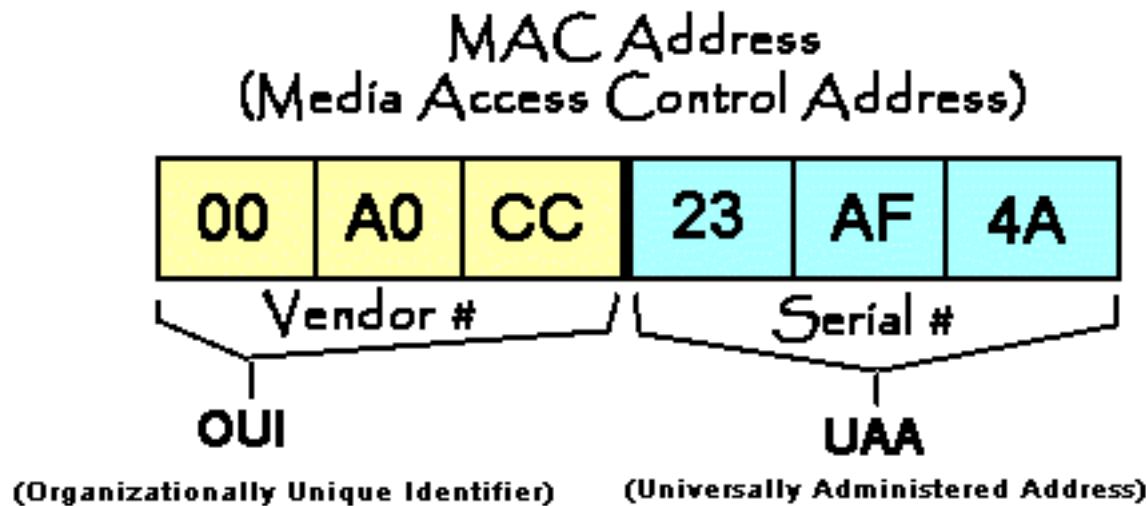
IEEE 802.3 original



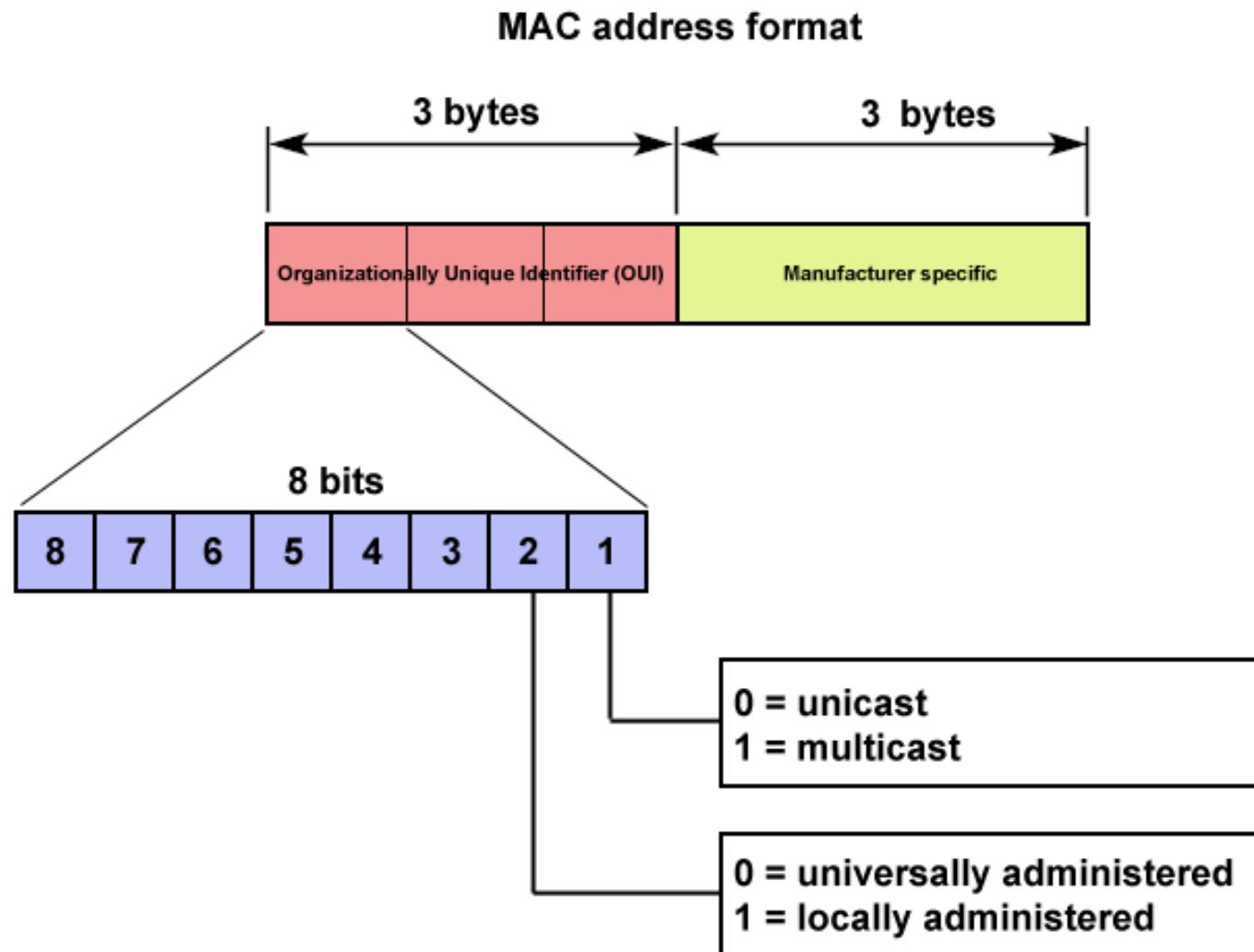
IEEE 802.3 révisé



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

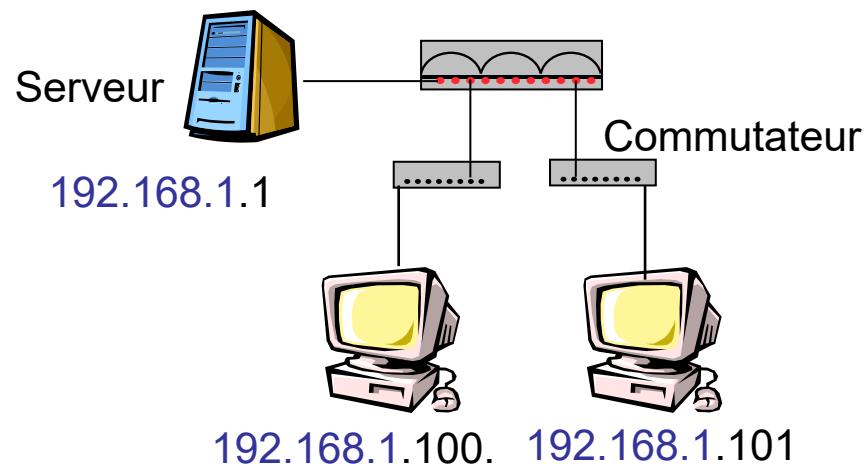
- Couche 3 du modèle OSI
- Non fiable (best effort) : pas de garantie que les paquets soient bien arrivés, ni qu'ils arrivent dans l'ordre dans lequel ils ont été envoyés
- Chaque paquet est traité indépendamment : 2 paquets dont les adresses source et destination sont identiques peuvent emprunter des 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 représentée sur 4 octets en décimal

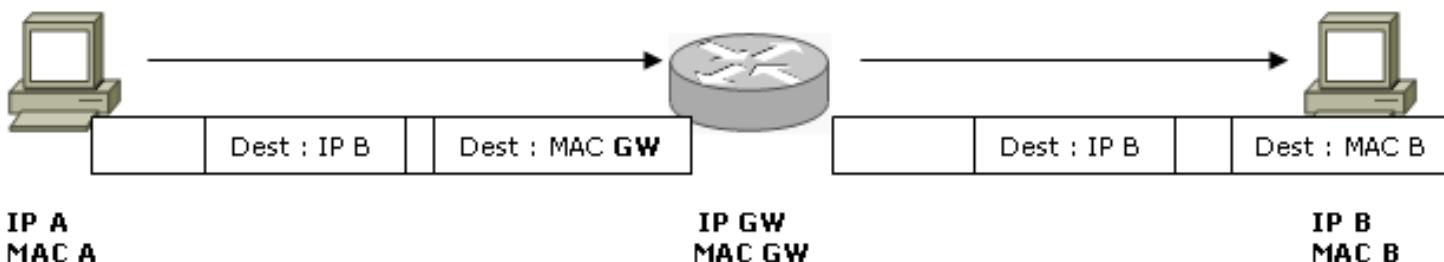
réseau.hôte

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

LAN 1

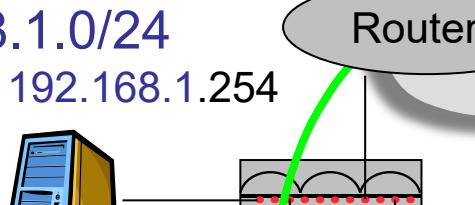
Réseau IP :

192.168.1.0/24

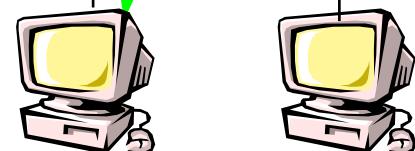
192.168.1.254

Serveur

192.168.1.1



192.168.1.100. 192.168.1.101



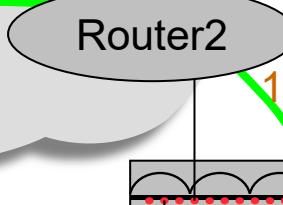
Internet

LAN 2

Réseau IP :

183.8.8.0/24

183.8.8.254



183.8.8.1 183.8.8.2



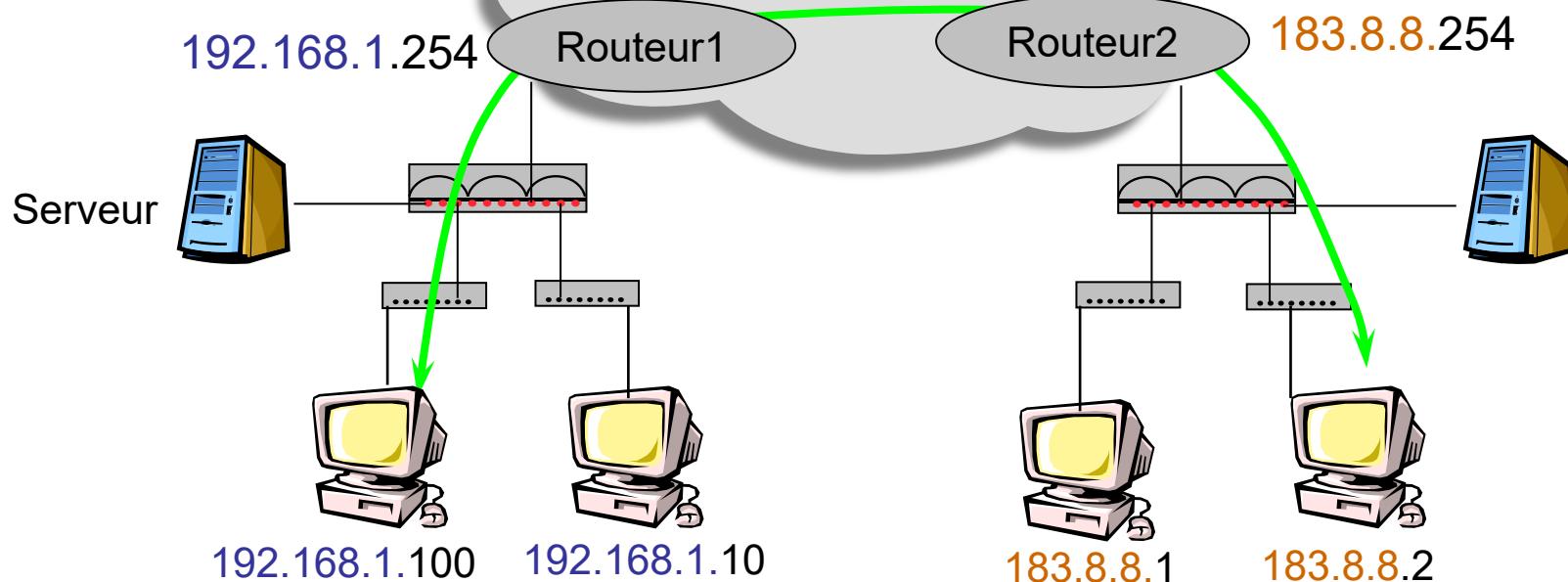
- Chaque host a une adresse IP
- Toutes les adresses IP d'un même site appartiennent au même réseau

Le routeur est la passerelle par défaut

LAN 1
(couche 2)

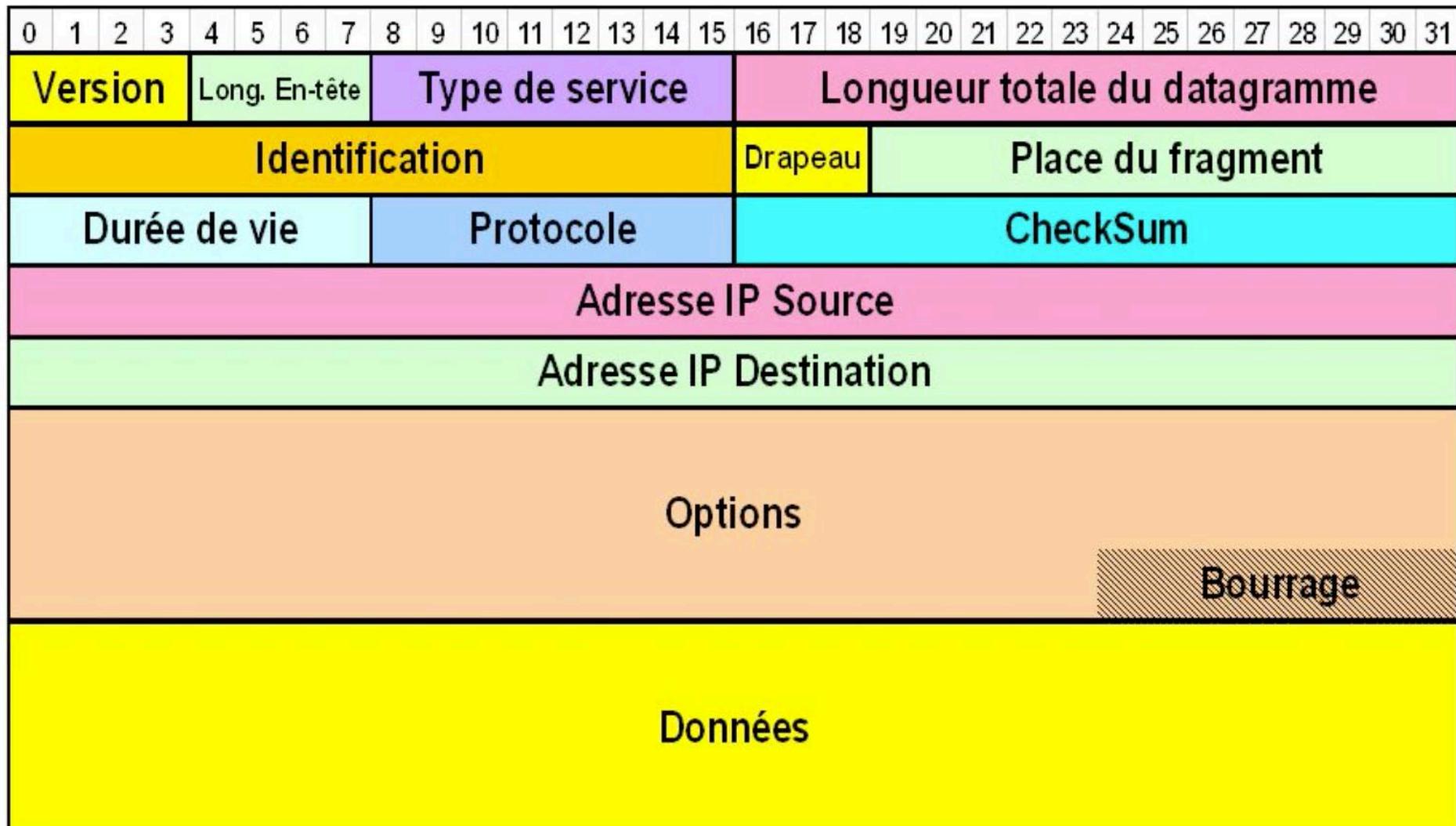
Internet Protocol
(couche 3)

LAN 2
(couche 2)

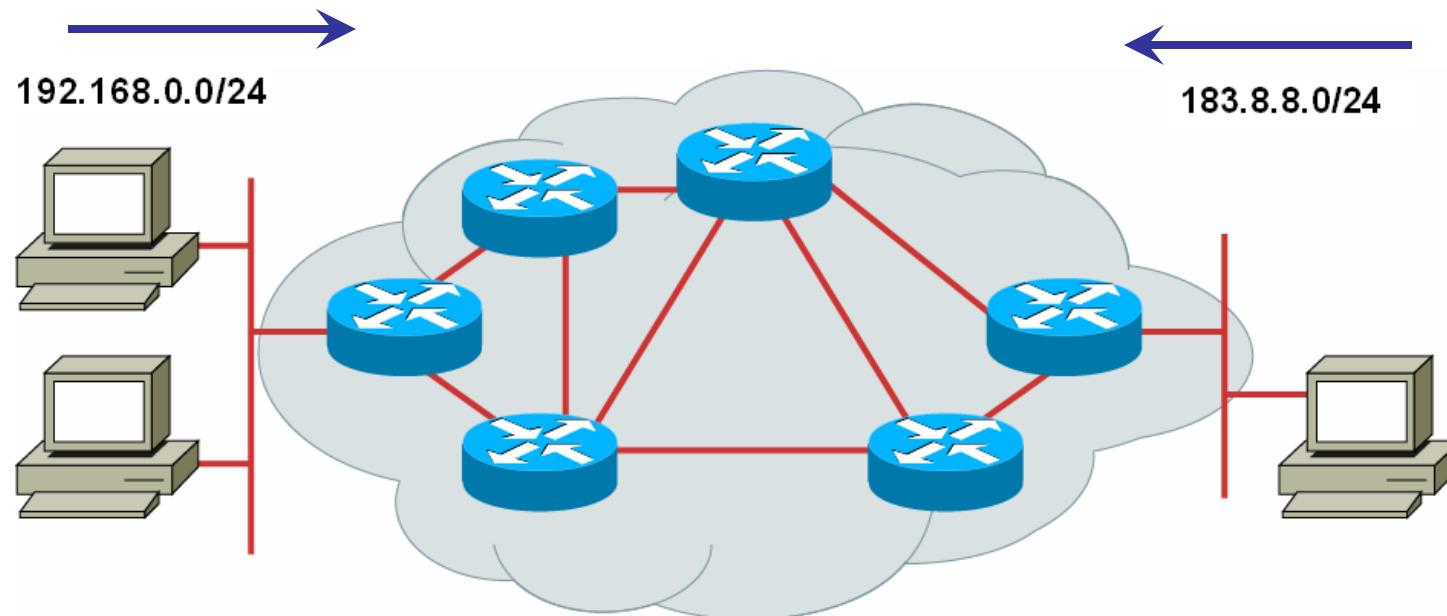


- Internet Protocol (IP) interconnect les LAN (Ethernet)
- Le routeur est la passerelle par défaut du LAN

L'entête IP



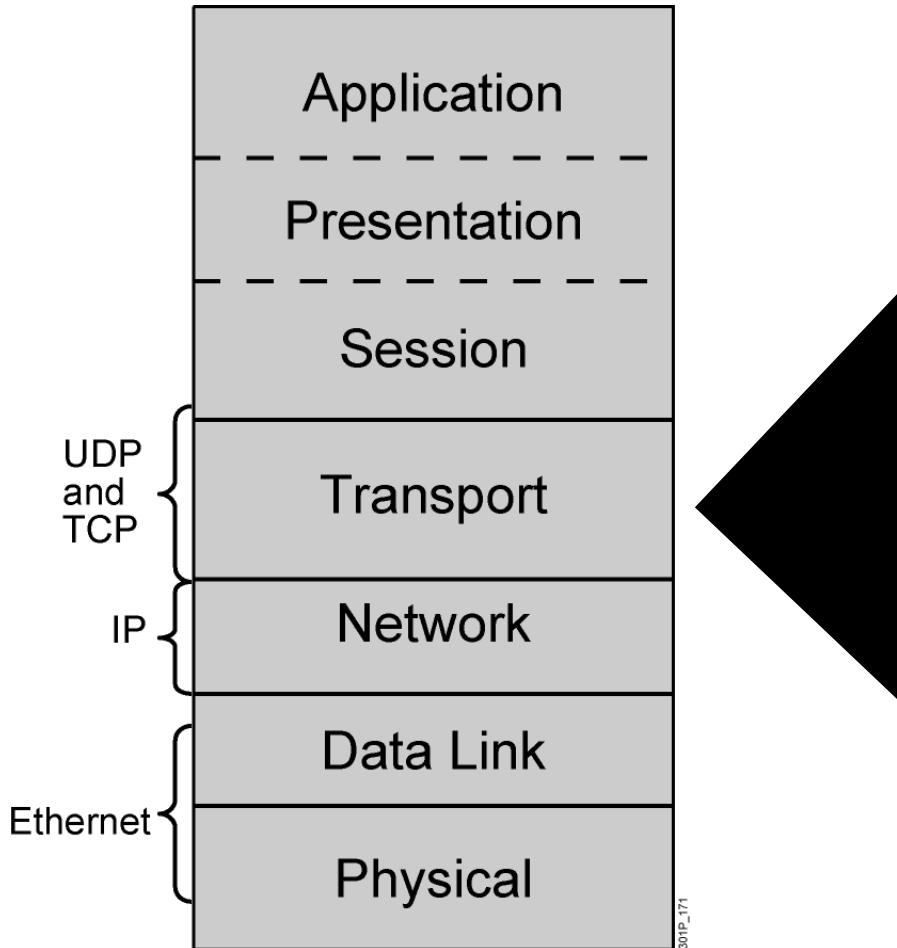
Les protocoles de routage



- 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)
- Contrôle de flux (TCP)
- Orienté connexion (TCP)
- Fiabilité (TCP)

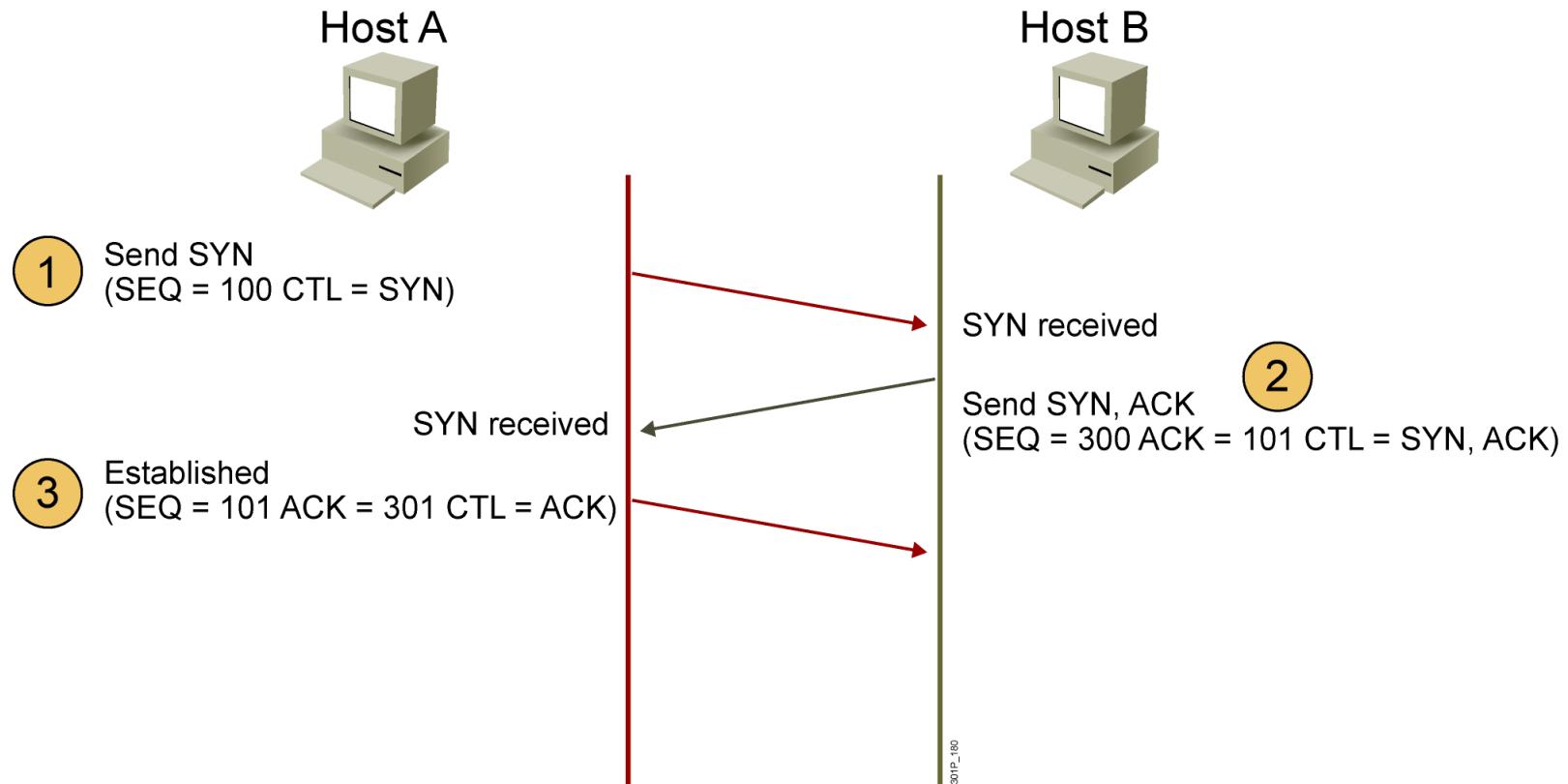
Caractéristiques de UDP

- 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

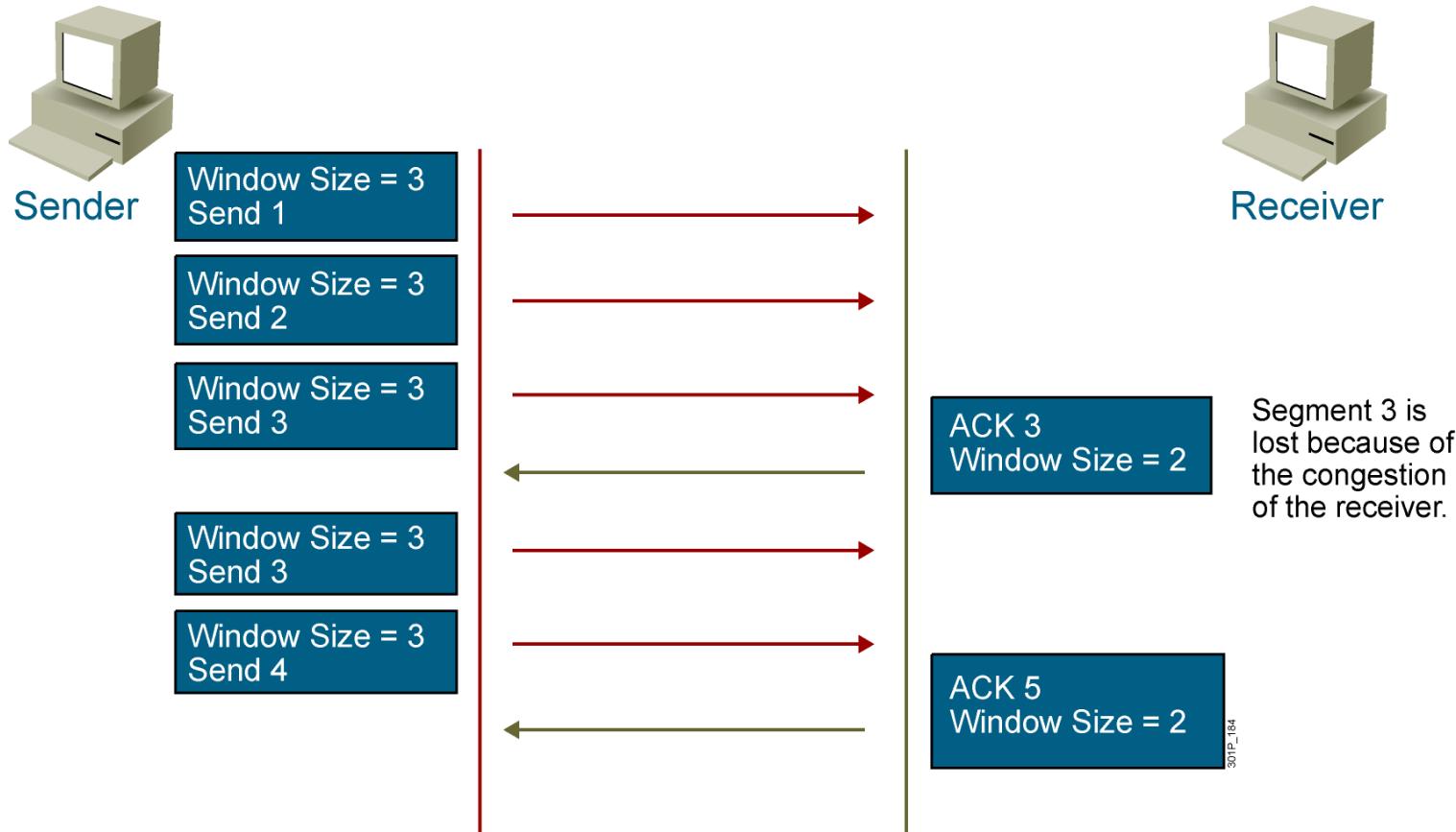
Protocol à trois poignées de main



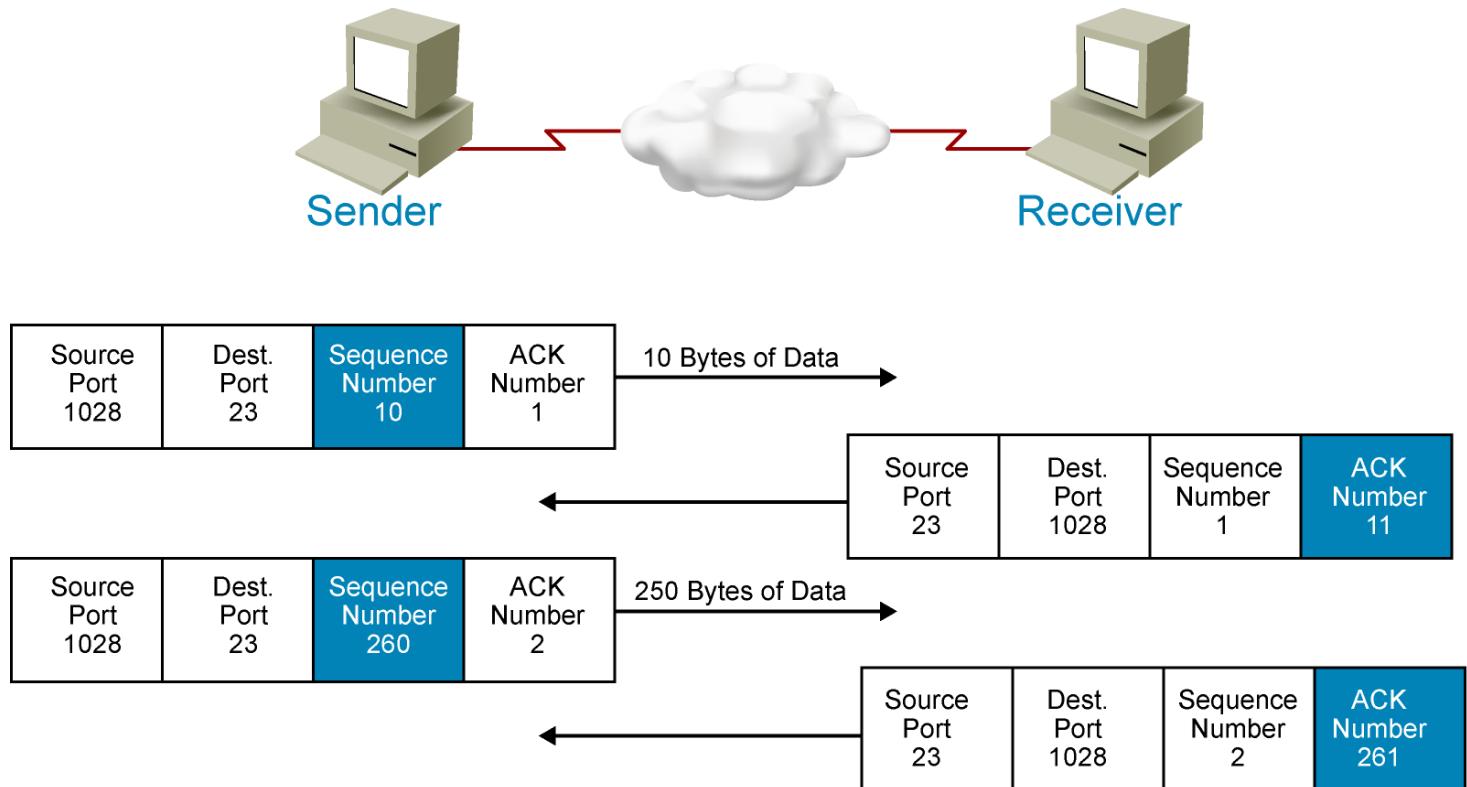
Acquittement TCP



La fenêtre glissante

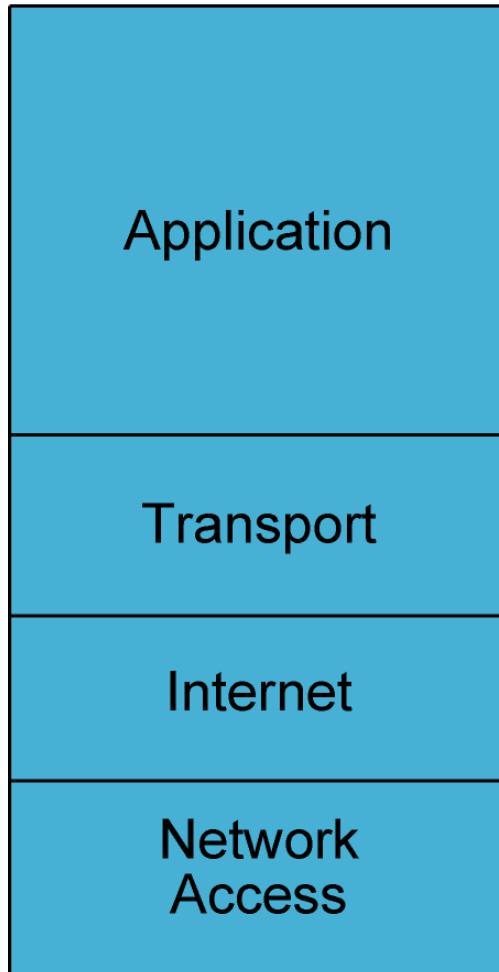


Numéros de séquence



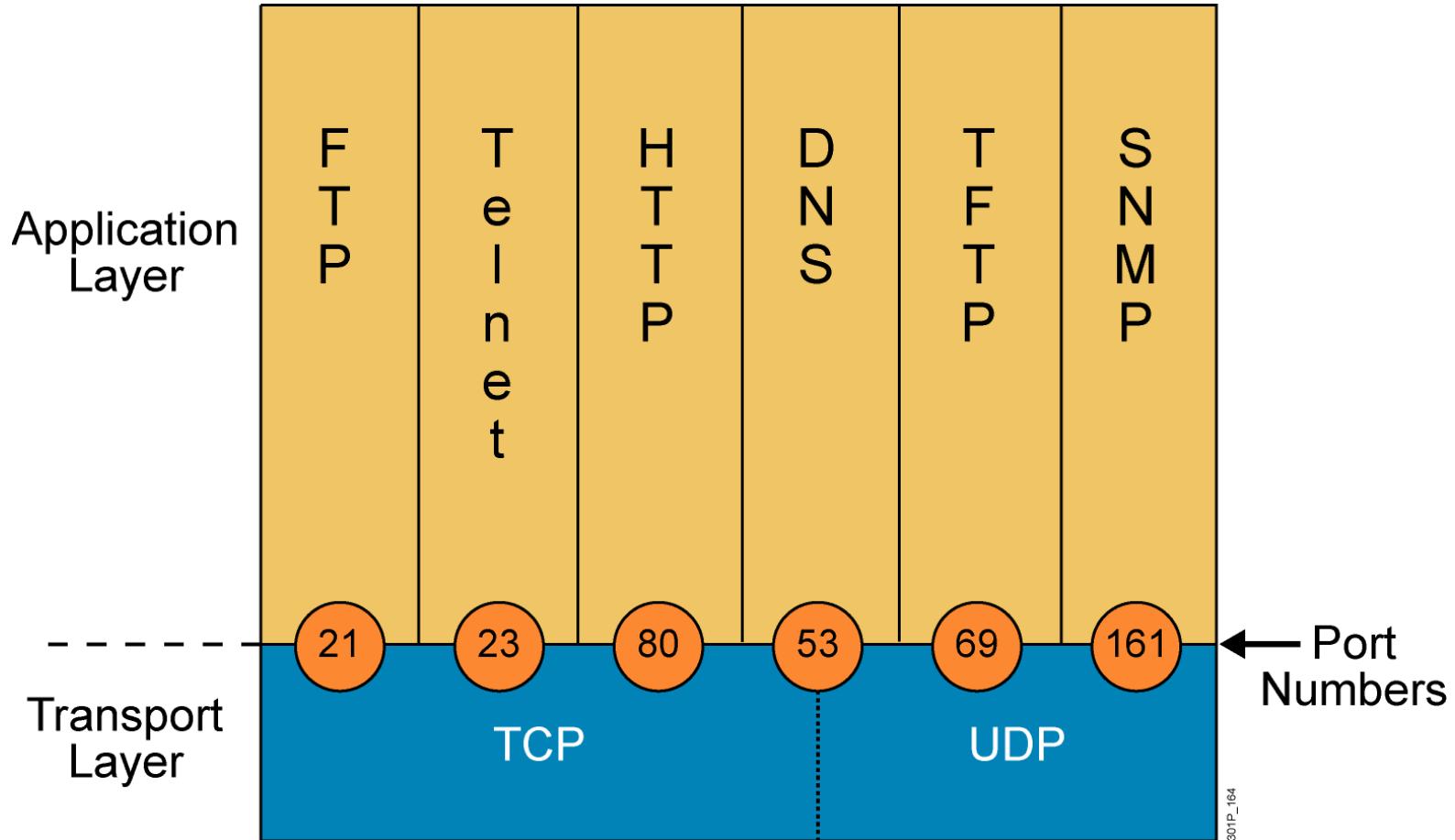
OSI couche 7 : Application

Les applications TCP/IP

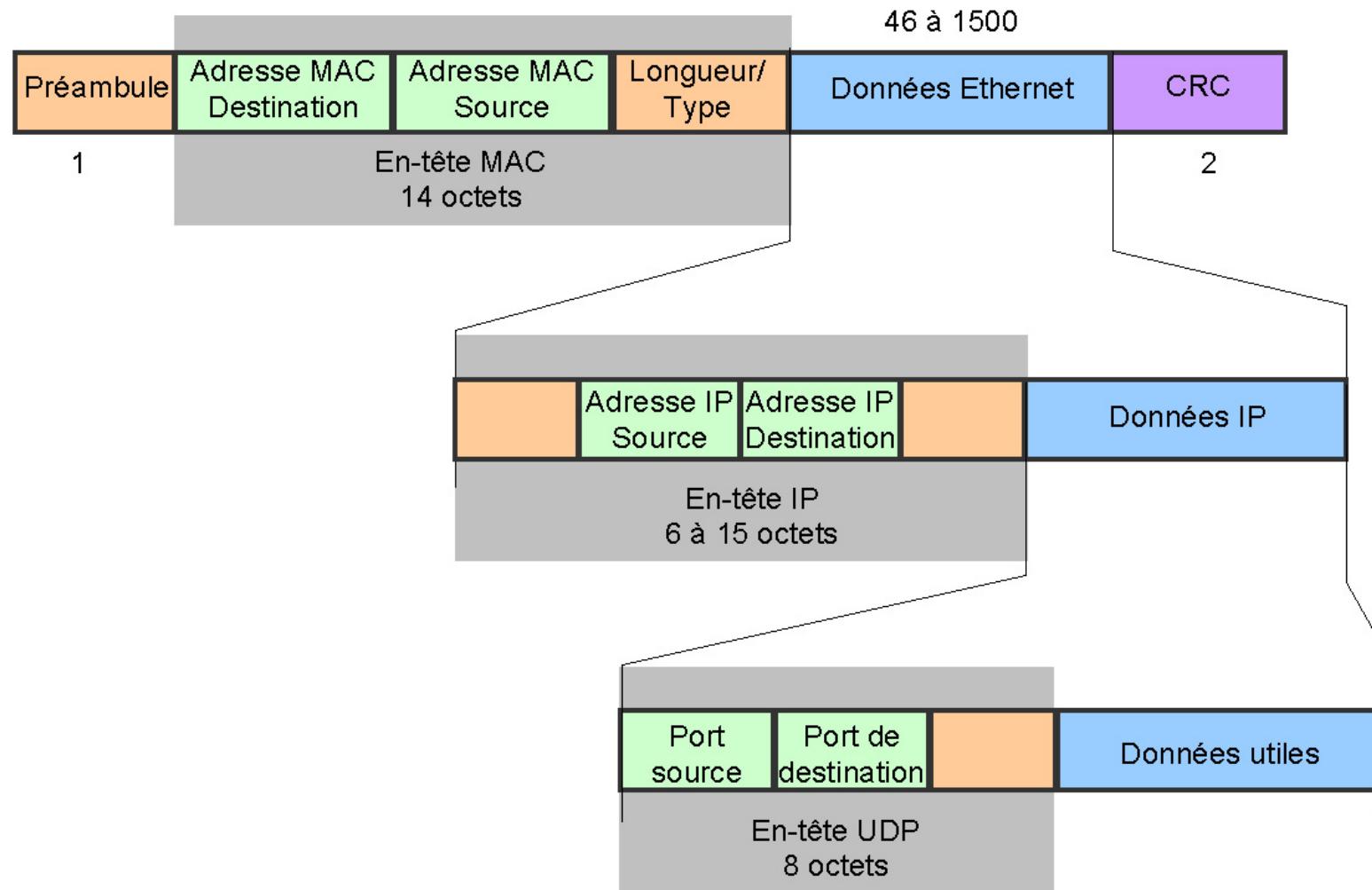


- Transferts de fichiers
 - FTP
 - TFTP
 - Network File System
- E-mail
 - Simple Mail Transfer Protocol
- Accès distant
 - Telnet
 - rlogin
- Gestion des réseaux
 - Simple Network Management Protocol
- Gestion des noms
 - Domain Name System

Les numéros de port des applications



Bilan des couches

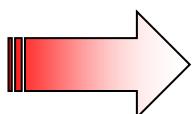


Subnetting

Première partie

Subnetting sur octet entier

L'adresse de couche 3:

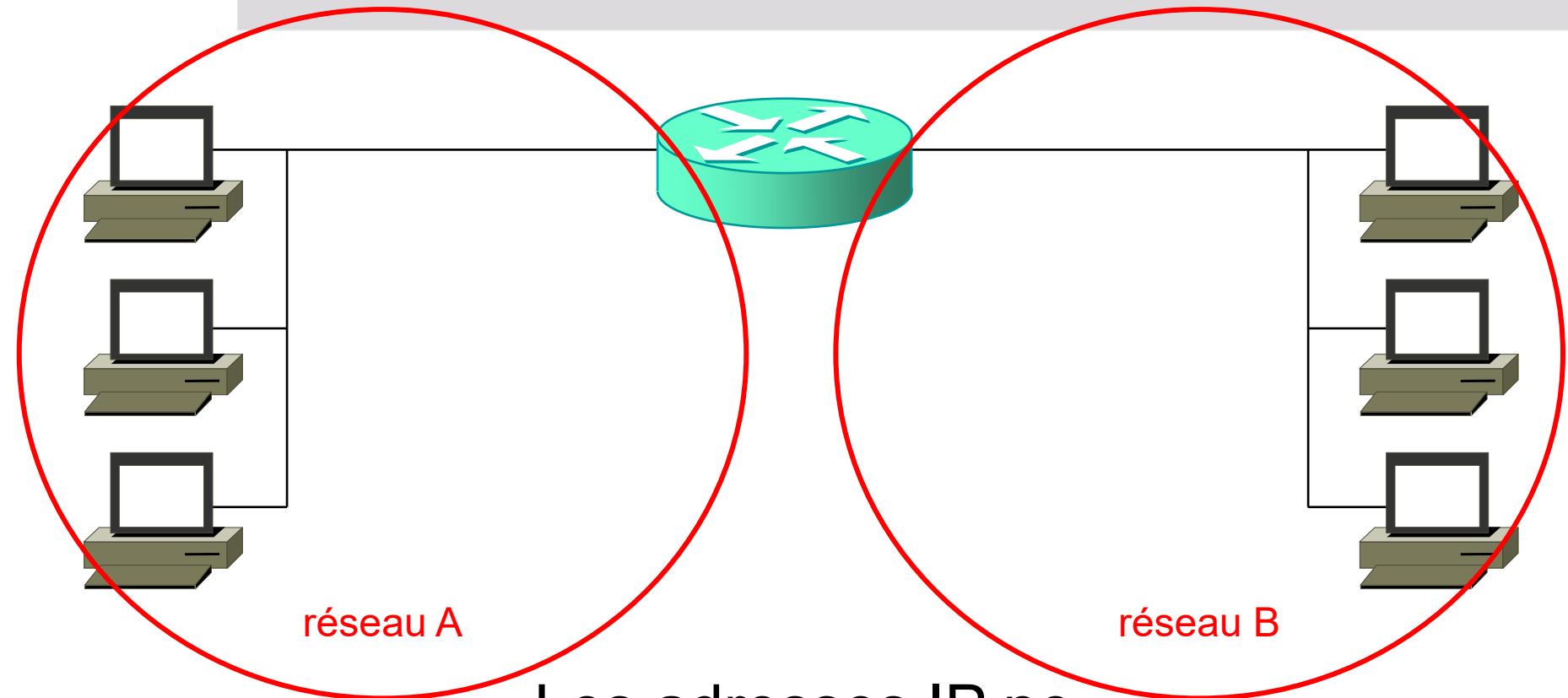


1. L'adresse IP et son masque
2. Les adresses réservées
3. Les classes
4. Le nombre d'adresses par réseau
5. Le subnetting sur un octet entier
6. Le subnetting sur un octet partiel

L'adresse IP

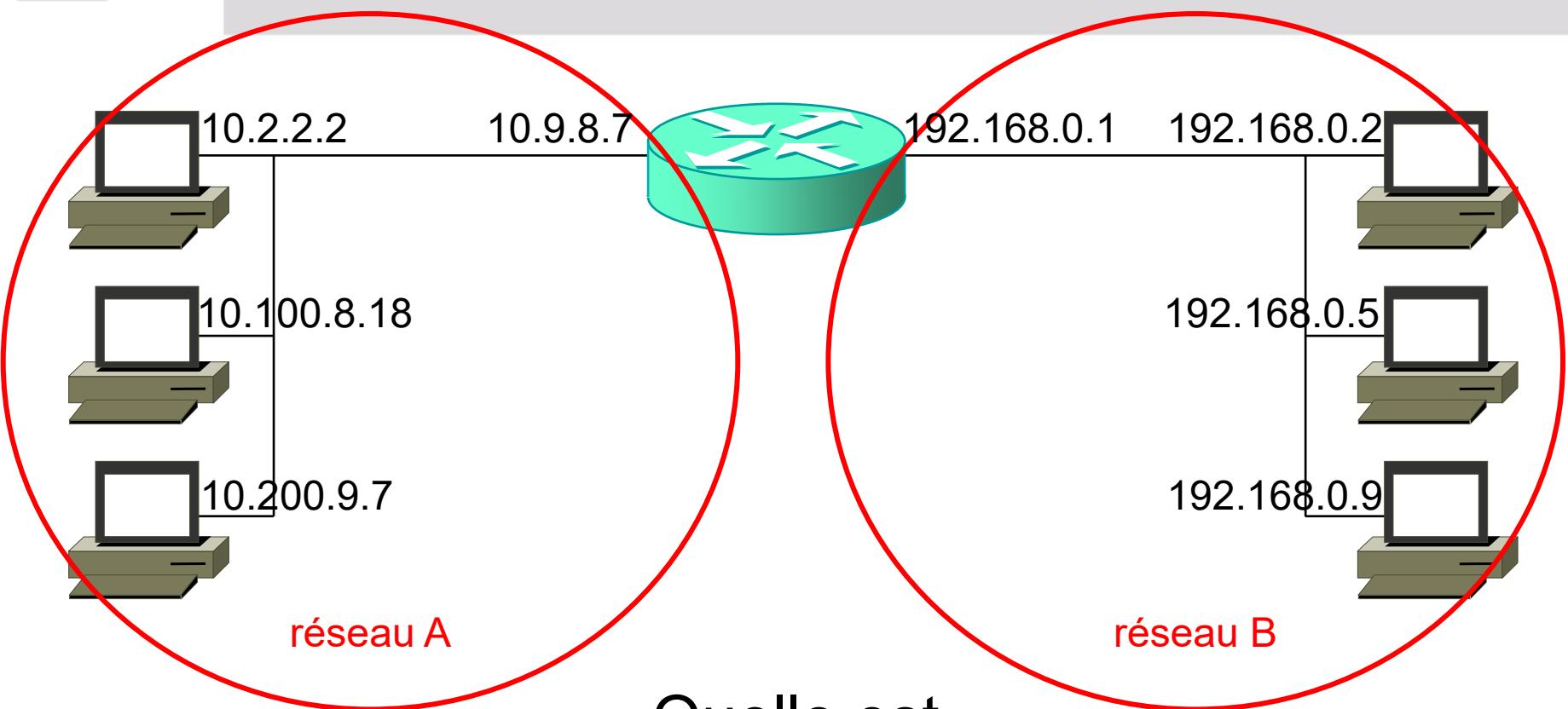
- Une adresse IP, c'est 4 octets : **192.168.4.6**
 - **192** = 1^{er} octet
 - **168** = 2^{ème} octet
 - **4** = 3^{ème} octet
 - **6** = 4^{ème} octet
- Un octet = 8 bits
 - donc une adresse IP = $8 \times 4 = 32$ bits

Deux réseaux



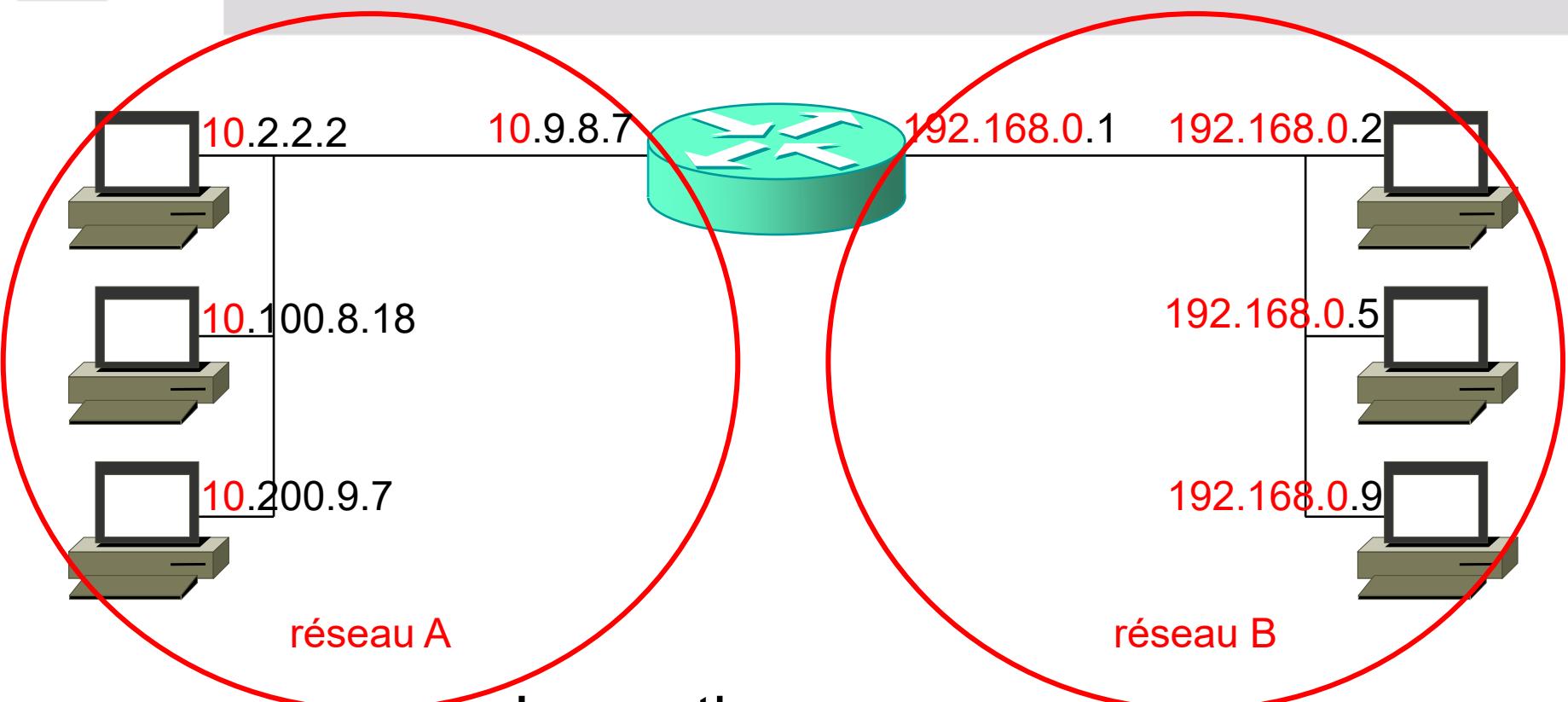
Les adresses IP ne
pourront pas être
attribuées de manière
quelconque !

Identifiez la partie commune !



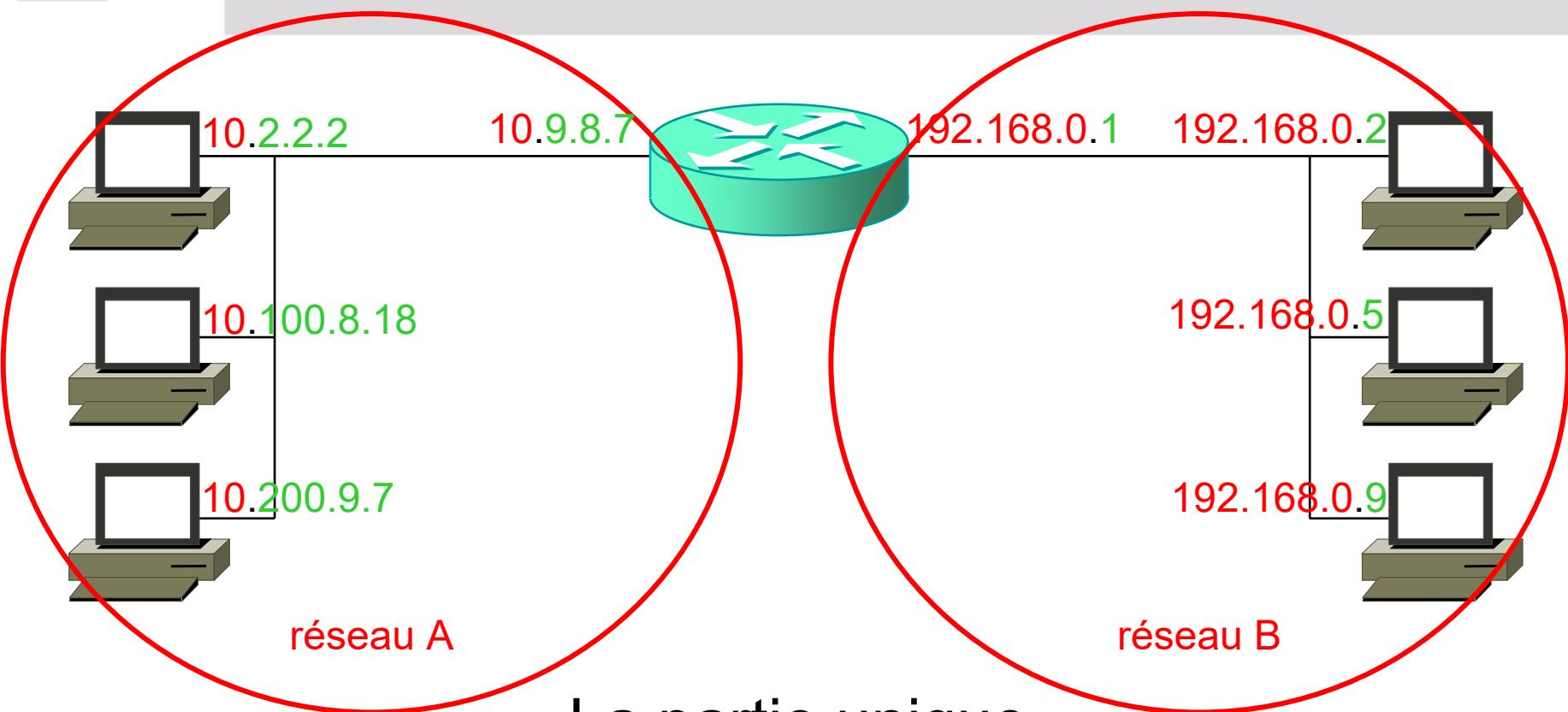
Quelle est
la partie **commune**
dans chaque réseau ?

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 !

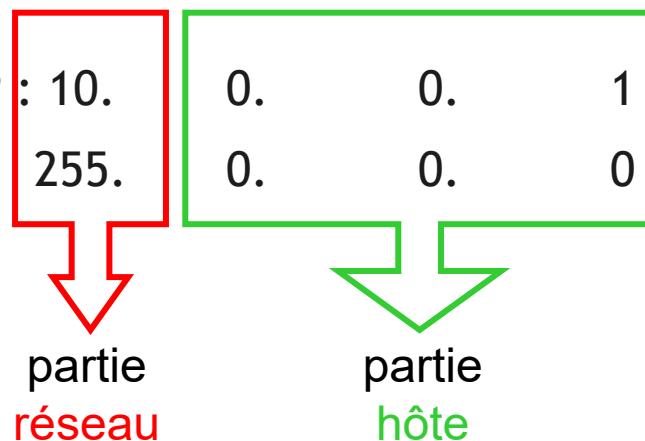
- Comment distinguer la partie ‘réseau’ de la partie ‘hôte’ ?
- → à l’ aide du **masque**
- Exemples de masques :
 - 255.0.0.0
 - 255.255.0.0
 - 255.255.255.0

Application du masque décimal

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

- Exemple :

- Adresse IP : 10.
255.
- Masque : 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

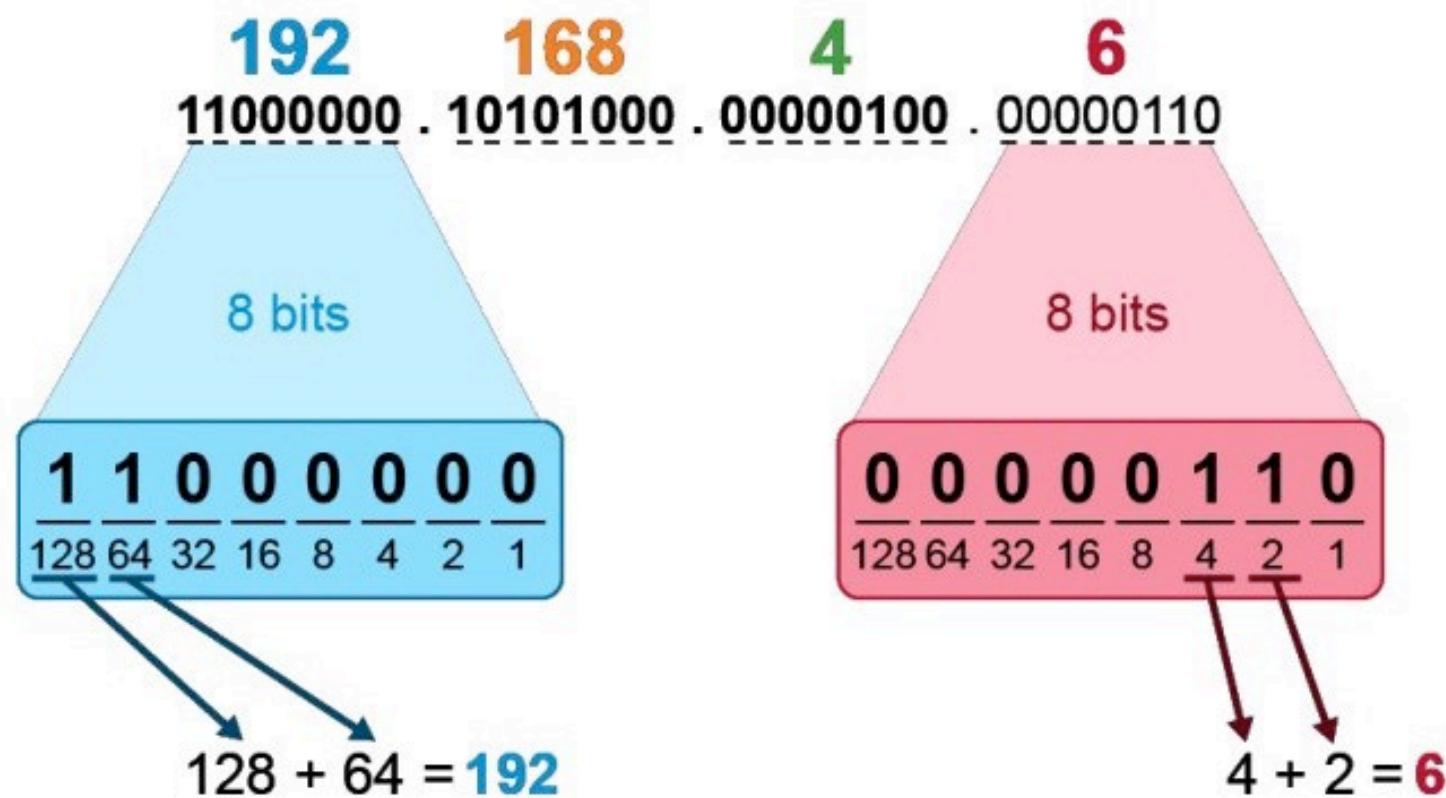
Solution

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

IP Address **192.168.4.6**

=



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 \Leftrightarrow 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

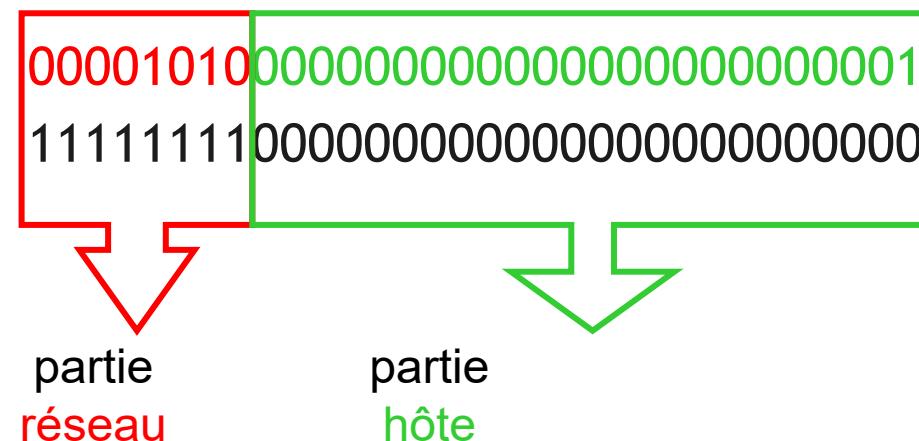
- Le masque est une suite de 32 bits.
 - Dès qu'un bit est à **0**, tous les bits suivants sont à 0.
- Exemples :
 - 00000000000000000000000000000000
 - 11000000000000000000000000000000
 - 11111111000000000000000000000000
 - 11111111111111110000000000000000
 - 1111111111111111111111111111111100000000
 - 11

Application du masque binaire

- Le masque est **superposé** à l' adresse IP.

- Exemple :

- Adresse IP : 00001010000000000000000000000001
- Masque : 11111111000000000000000000000000



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’écritra /0
 - 11111111.00000000.00000000.00000000 s’écritra /8
 - 11111111.11111111.00000000.00000000 s’écritra /16
 - 11111111.11111111.11111111.00000000 s’écritra /24
 - 11111111.11111111.11111111.11111111 s’écritra /32

Exercice : identifiez la partie réseau

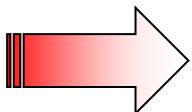
Adresse IP				Masque
10	1	2	3	/8
19	19	19	19	/8
150	150	150	150	/16
200	201	202	203	/24

Solution

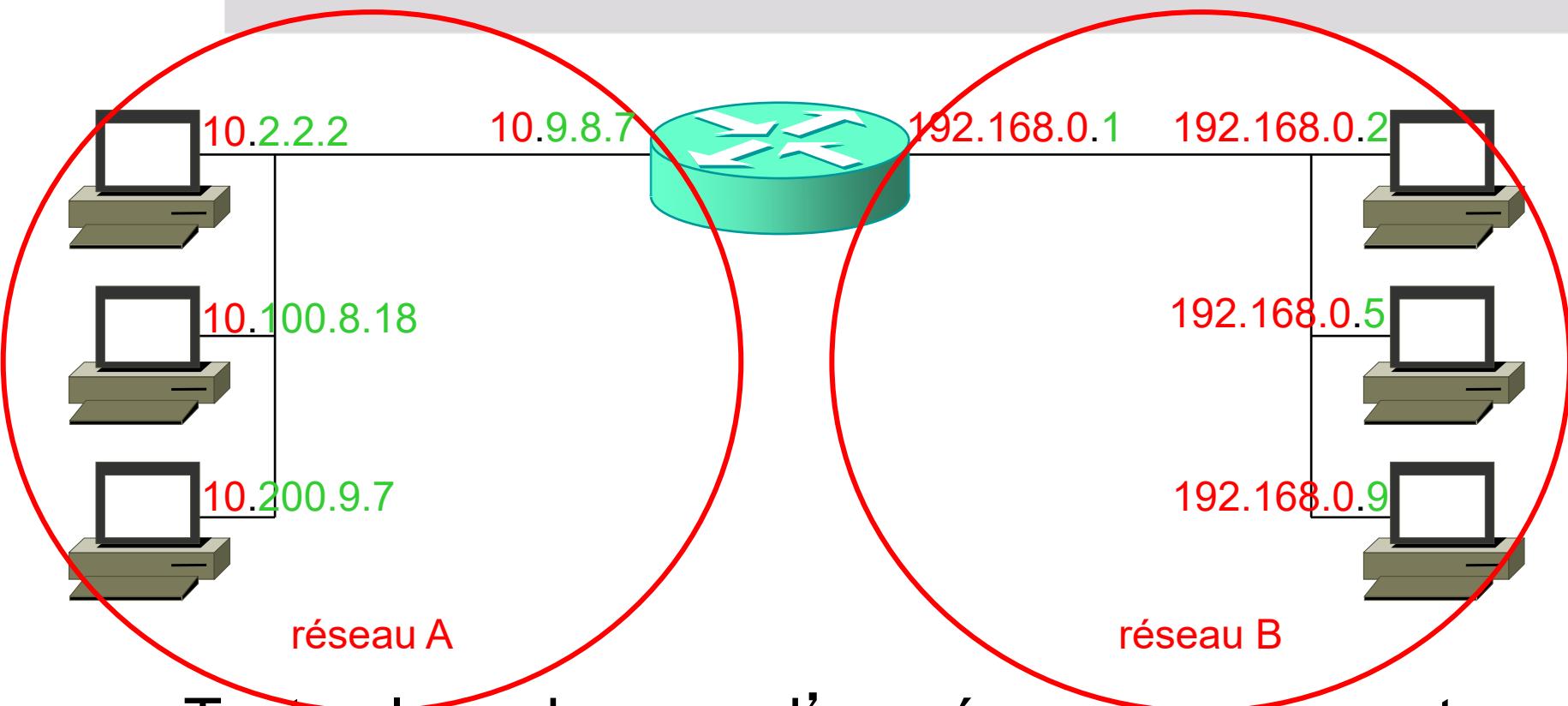
Adresse IP				Masque
10	1	2	3	/8
19	19	19	19	/8
150	150	150	150	/16
200	201	202	203	/24

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

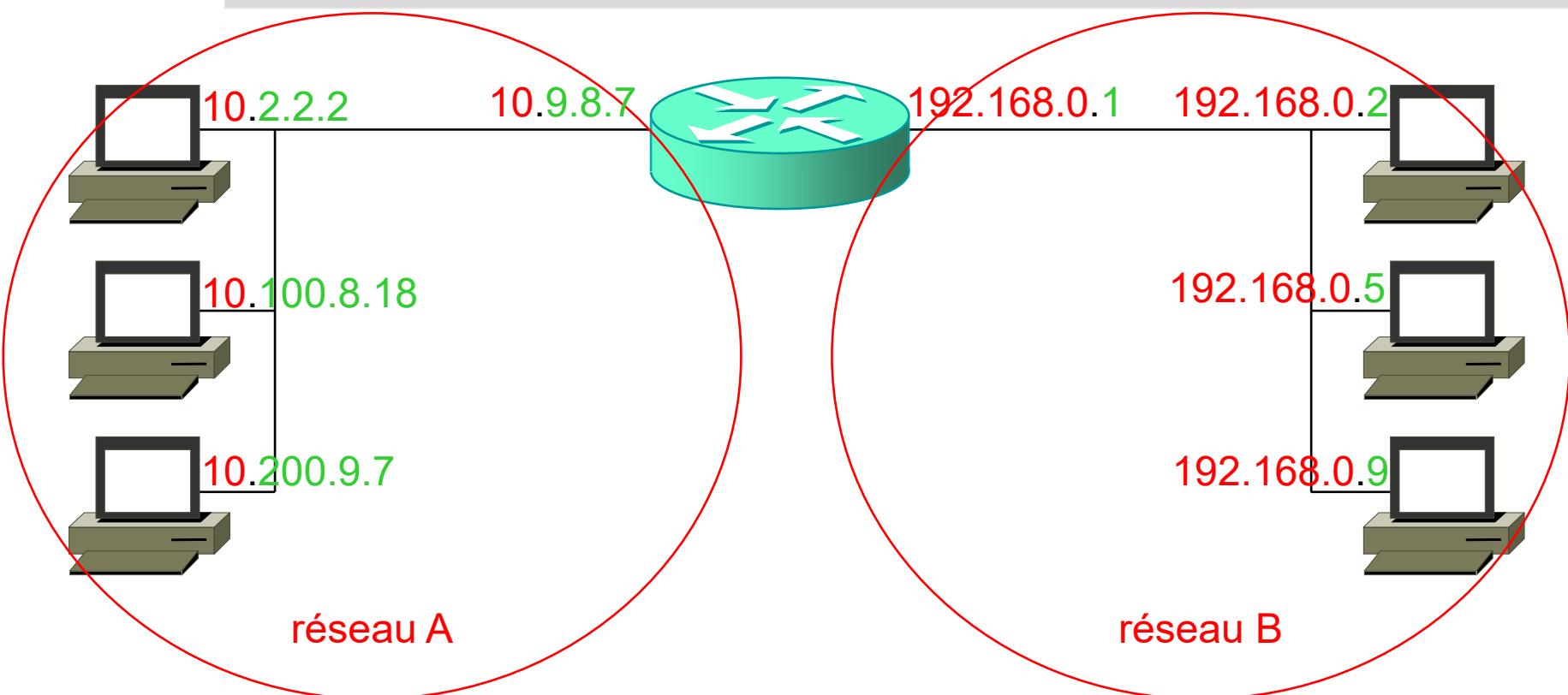
Exemples d'adresses broadcast

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.

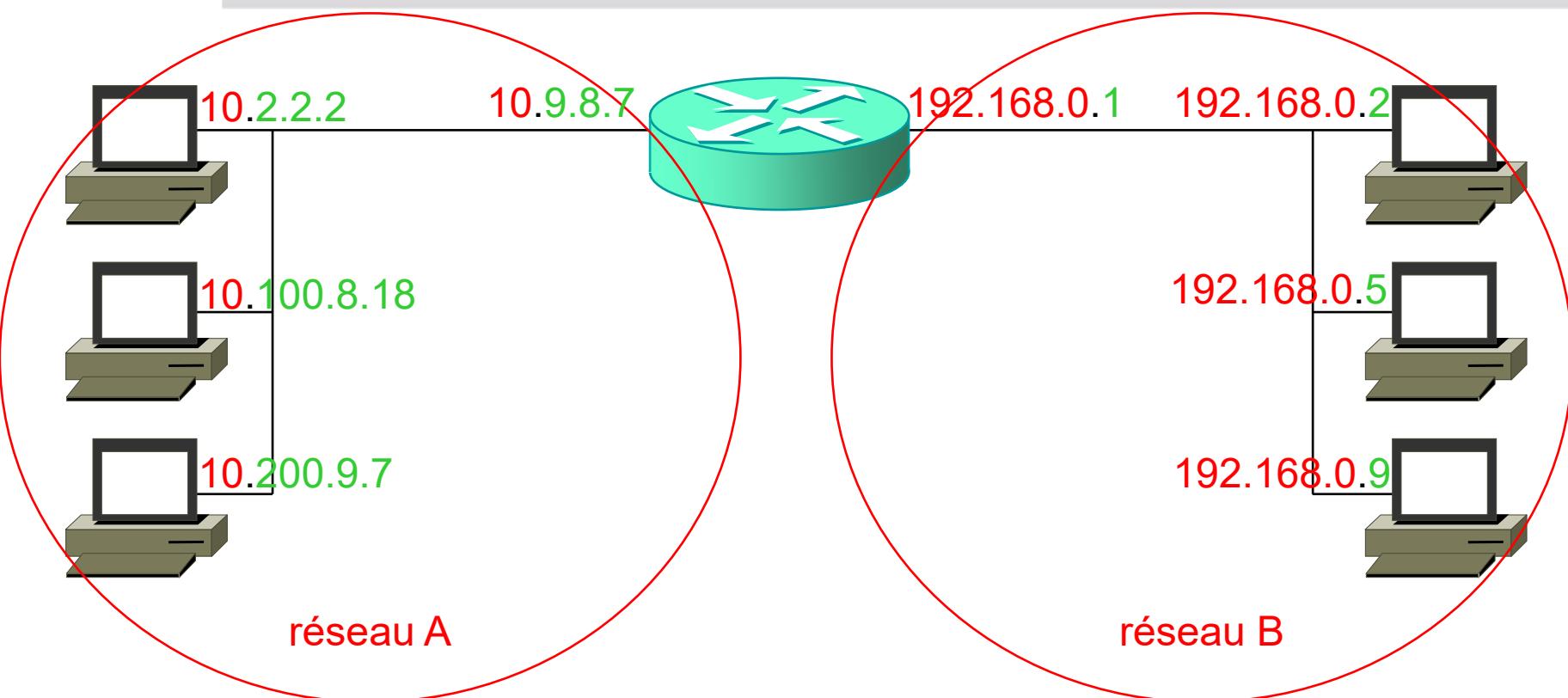
Adresse réseau de A et B



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

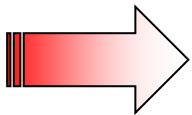
Exercice : déterminez les adresses interdites

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

Le subnetting :

1. L'adresse IP et son masque
2. Les adresses réservées
3. Les classesA large red arrow pointing to the right, positioned next to the third item in the list.
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	xxxxxxx	xxxxxxx	xxxxxxx
B	10xxxxxx	xxxxxxx	xxxxxxx	xxxxxxx
C	110xxxxx	xxxxxxx	xxxxxxx	xxxxxxx
D	1110xxxx	xxxxxxx	xxxxxxx	xxxxxxx
E	1111xxxx	xxxxxxx	xxxxxxx	xxxxxxx

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	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX
B	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX
C	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX
D	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX
E	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX

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

Cisco IOS

Se connecter à l'équipement

Connexion physique du port CONSOLE

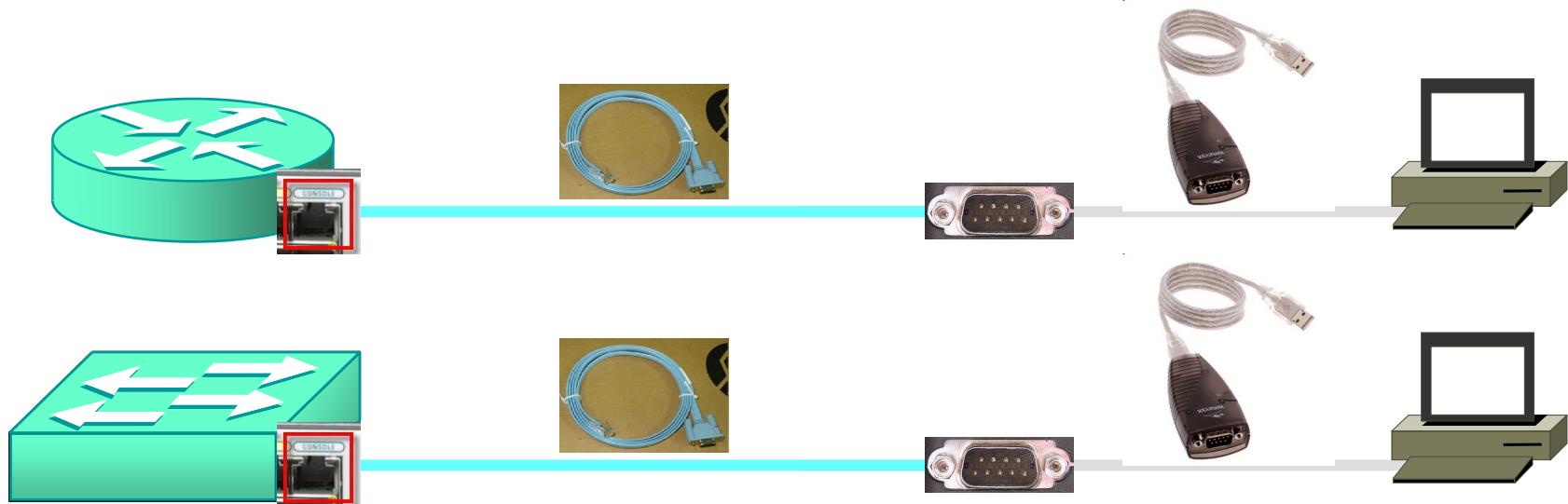
Le port CONSOLE

- 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 :



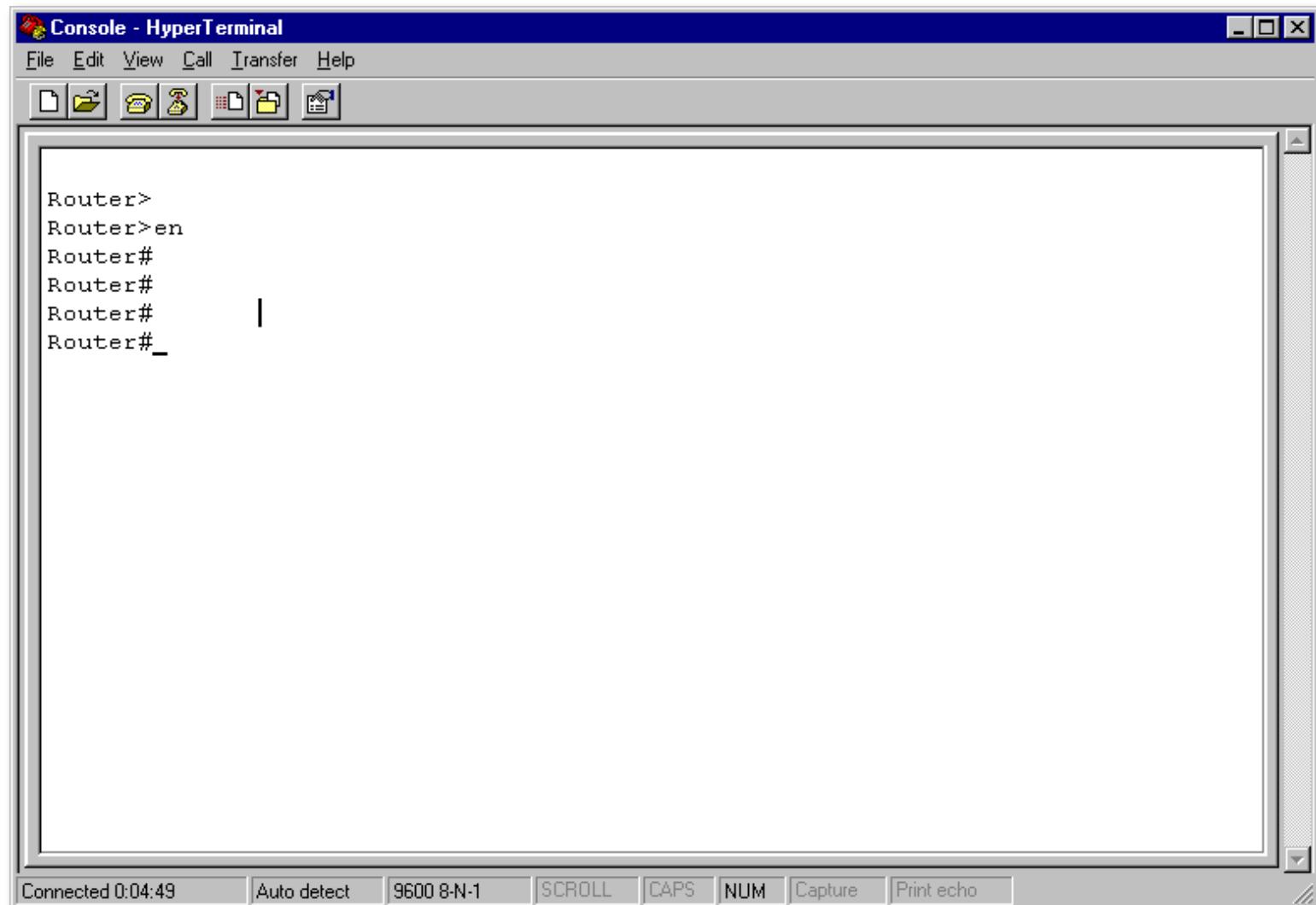
Se connecter à l'équipement

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 réservé

- 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 [Ctrl] + ‘**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
- Ils 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#



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 startup-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**' supplémentaire afficher 1 **ligne**
 - appuyer sur '**Barre d' espace**' supplémentaire afficher 1 **page**
 - 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-clé d'une commande si 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 :
 - config 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
```

[tabulation]

[tabulation]

Exemple 2

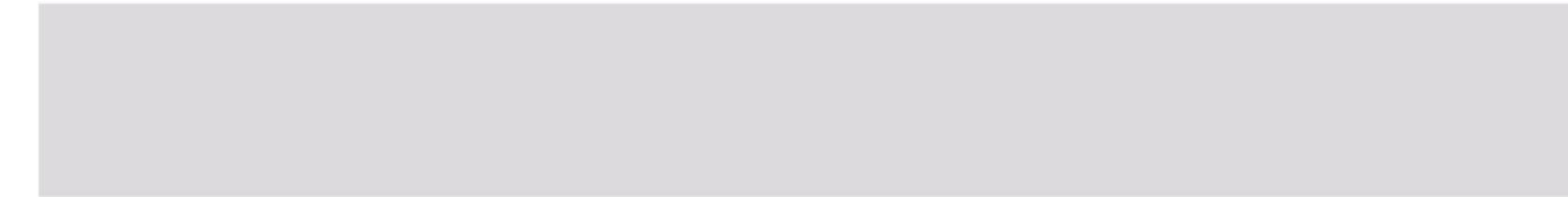
- L'auto-completion permet d'éviter les erreurs de frappe. Exemple :

```
TOTO#sh▶
```

```
TOTO#show ip in▶
```

```
TOTO#show ip interface br▶
```

```
TOTO#show ip interface brief
```



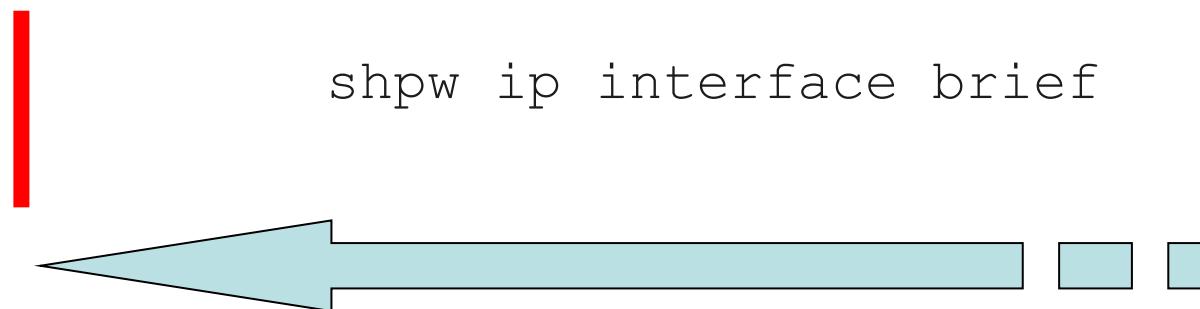
Les aides de la CLI

Positionner le curseur

Comment corriger une commande

```
shpw ip interface brief
```

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

[*Ctrl*] + ‘a’

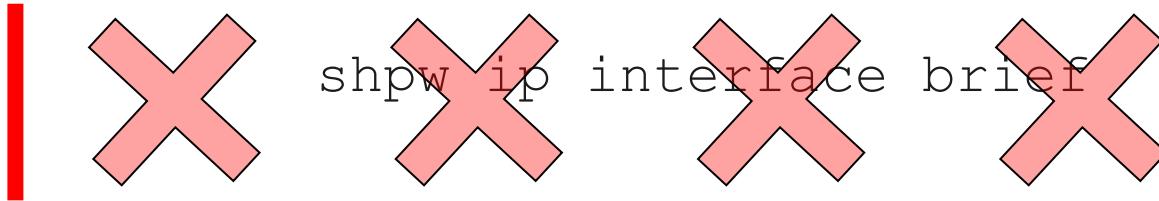
Positionne le curseur en **début de ligne**

[*Ctrl*] + 'e'

```
shpw ip interface brief
```



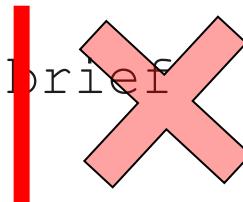
Positionne le curseur en **fin** de ligne

[*Ctrl*] + 'x'

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

[*Ctrl*] + ‘w’

shpw ip interface brie



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)#+
```

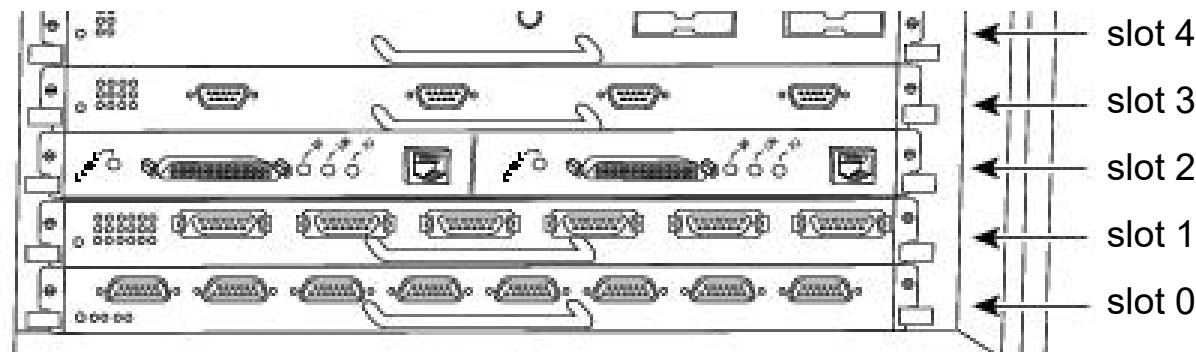
Configurations de base

Configurer une interface

Spécifier une interface

- Enable
conf t
interface [TYPE] [NUMERO]
 - Ethernet
 - FastEthernet
 - GigabitEthernet
 - Serial
 - Loopback
 - Tunnel
 - etc ...
- Exemples :
 - interface Ethernet 0
 - interface Fastethernet 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

Diagram illustrating the output:

- The "Status" column (highlighted with a red border) contains the value "up". A callout box labeled "le statut de l'interface" points to this cell.
- The "Protocol" column (highlighted with a green border) contains the value "up". A callout box labeled "le statut de la ligne" points to this cell.

	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*

- 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.

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

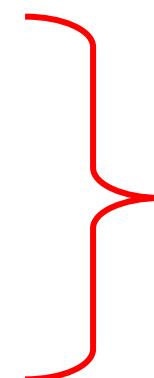
CDP

Cisco Discovery Protocol

- 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

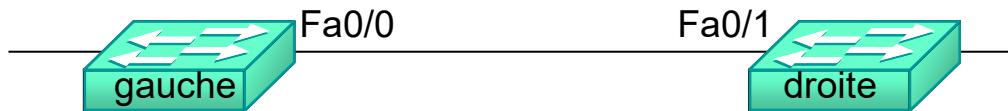
```
R1#configure terminal  
R1(config)#no cdp run  
R1(config)#cdp run
```

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

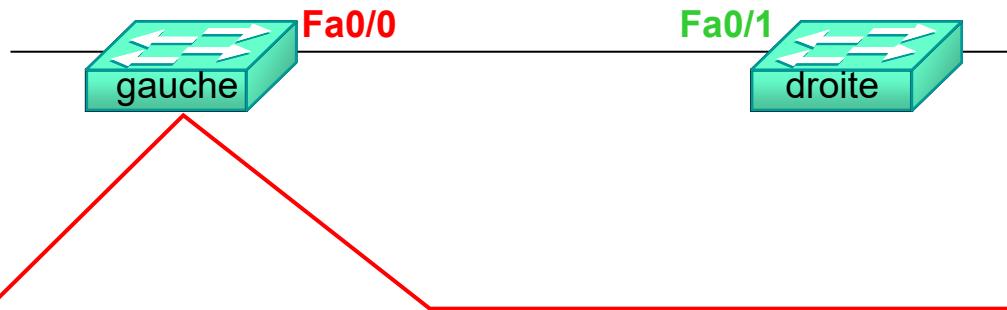


```
gauche#show cdp neighbors
```

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.

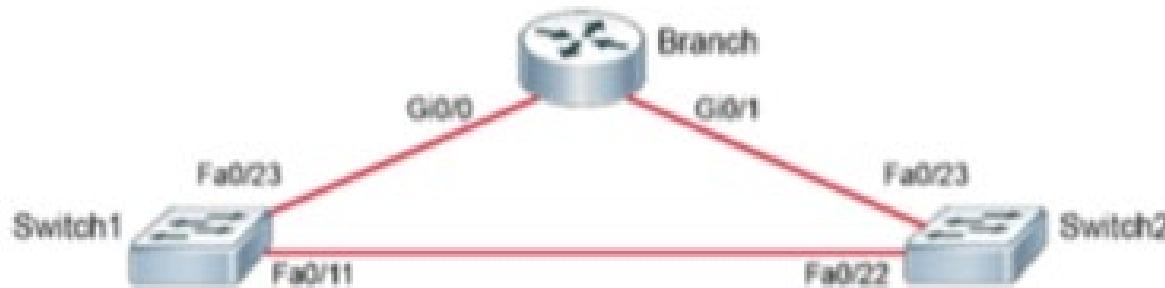
```
[no] lldp run
```

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 gerreddy

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)

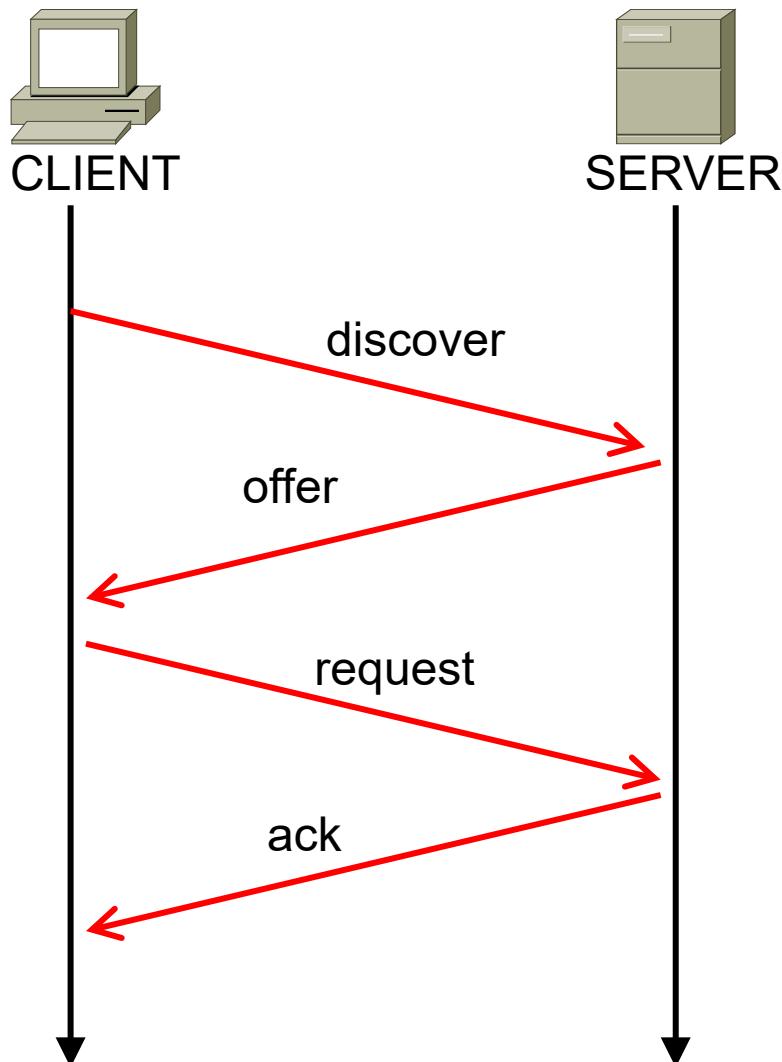
Media Attachment Unit type: 16

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

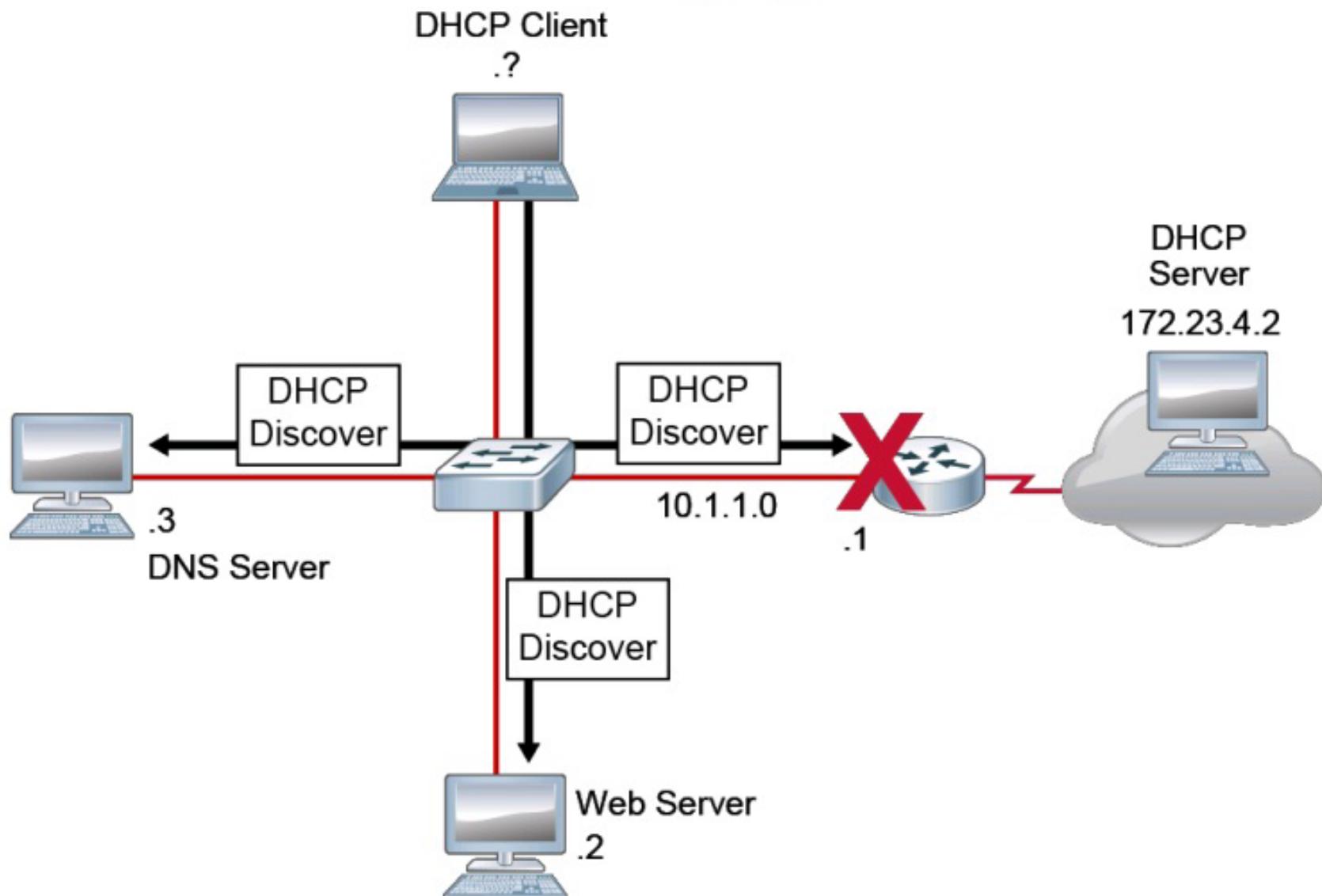
Router = server DHCP

- conf t
 - ip dhcp excluded-address 192.168.10.1 192.168.10.5
 - 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

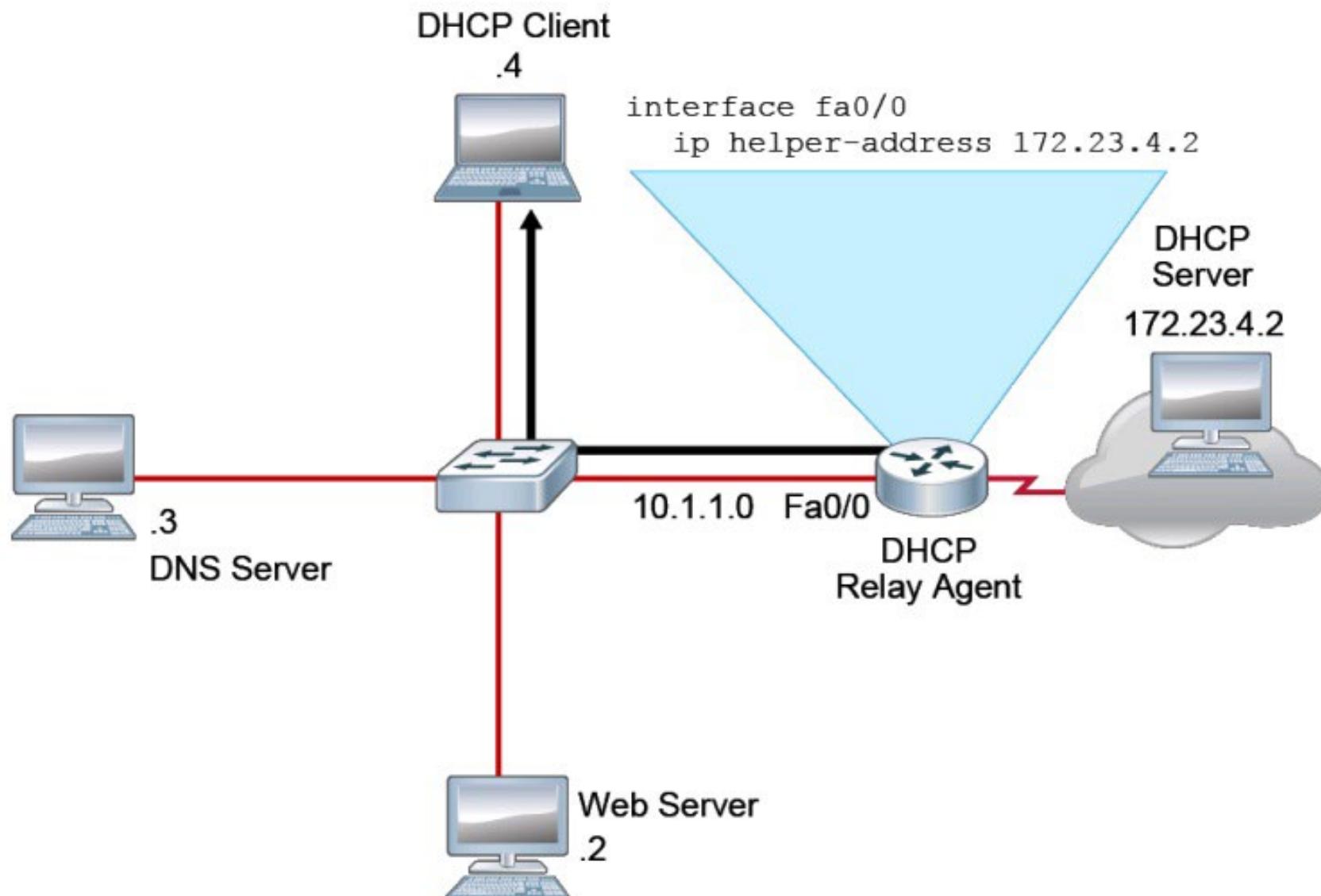
Activer la fonction DHCP

- 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).

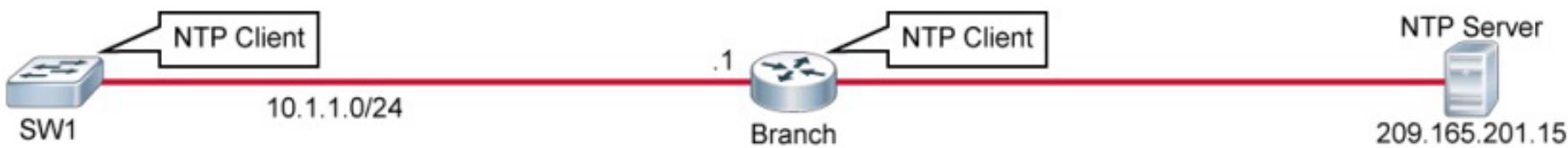
Configuring NTP

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.

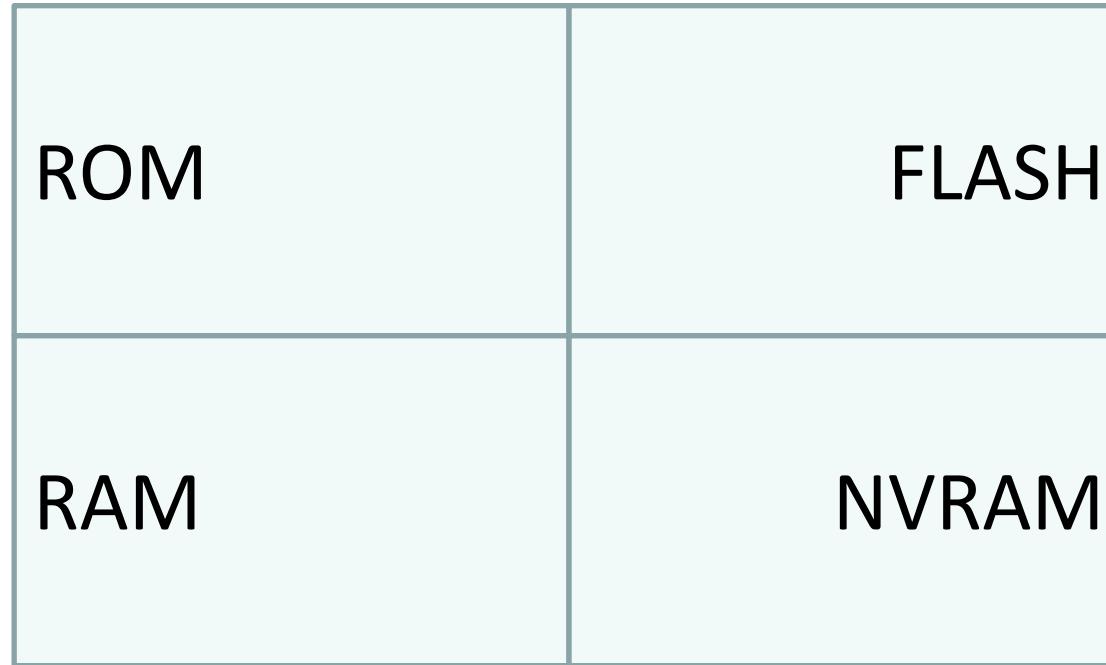
```
R1(config)# clock timezone CET 2
```

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

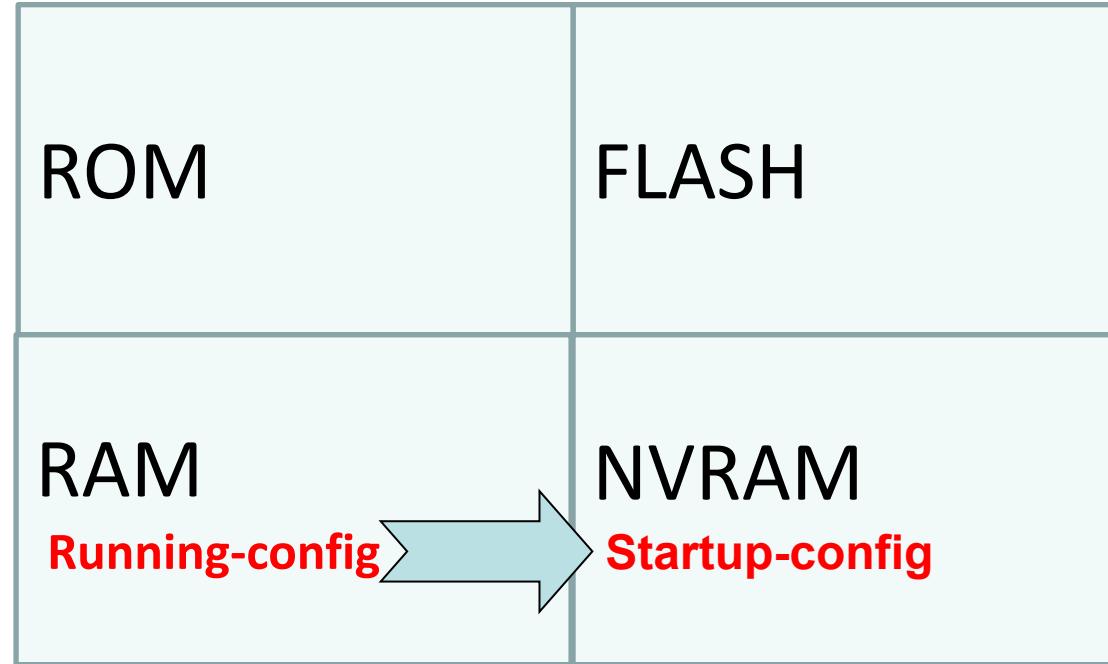
ROM	Image = IOS
RAM	NVRAM

NVRAM

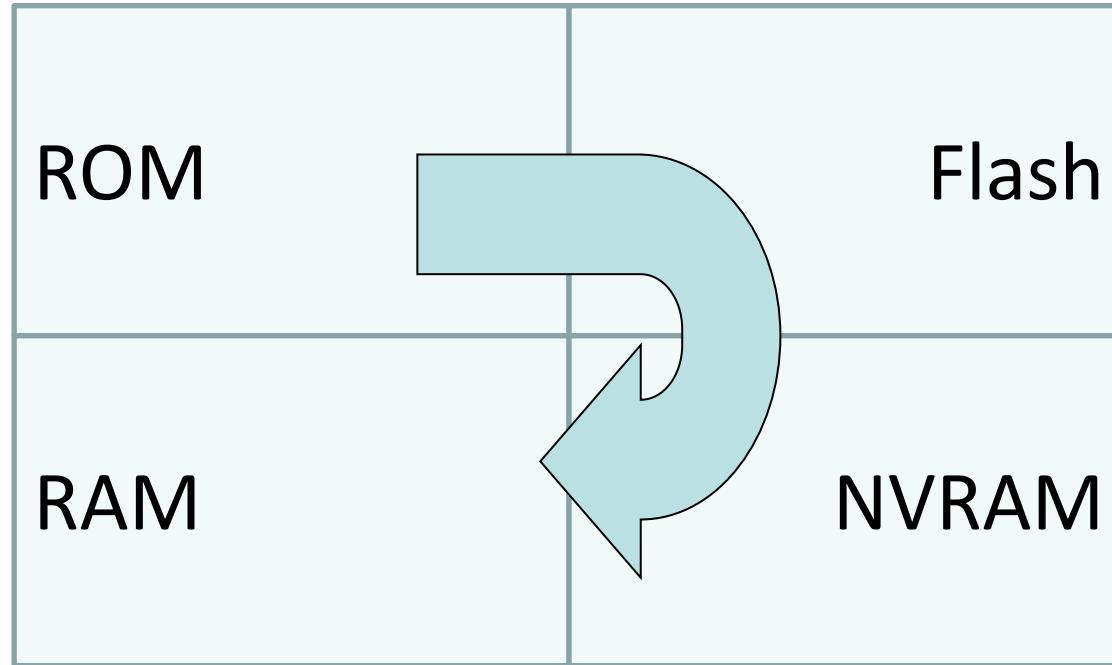


ROM	FLASH
<ul style="list-style-type: none">• Running-config• Table d'@MAC• Table de routage• Paquets etc....	NVRAM

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
 - 0x210**0** ne prendre aucune image
 - 0x210**1** prendre la 1ère image de la Flash
 - 0x210**2** 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
 - 0x21**0**2 prendre la startup de la NVRAM
 - 0x21**4**2 ne pas charger de startup
- Quelle utilité de modifier ce registre ?

Perte de mot de passe

1. Séquence < break >
2. Rommon 1>confreg 0x21**42**
3. Rommon 2>reset (ou i, ou redémarrer)
4. Enable
5. Copy start run
6. Conf t
7. Enable secret TOTO
8. Config-register 0x21**02**
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)

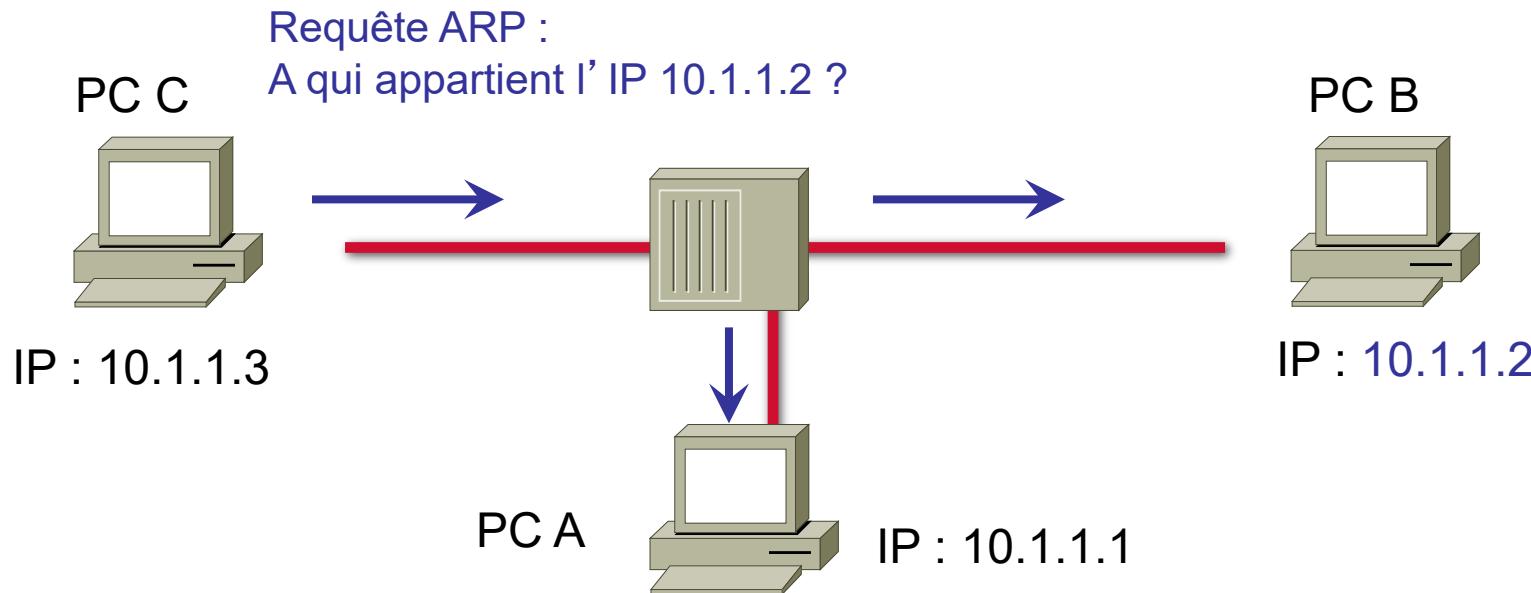
Configuration register is 0x2102

Address Resolution Protocol

Adresse physique et adresse logique

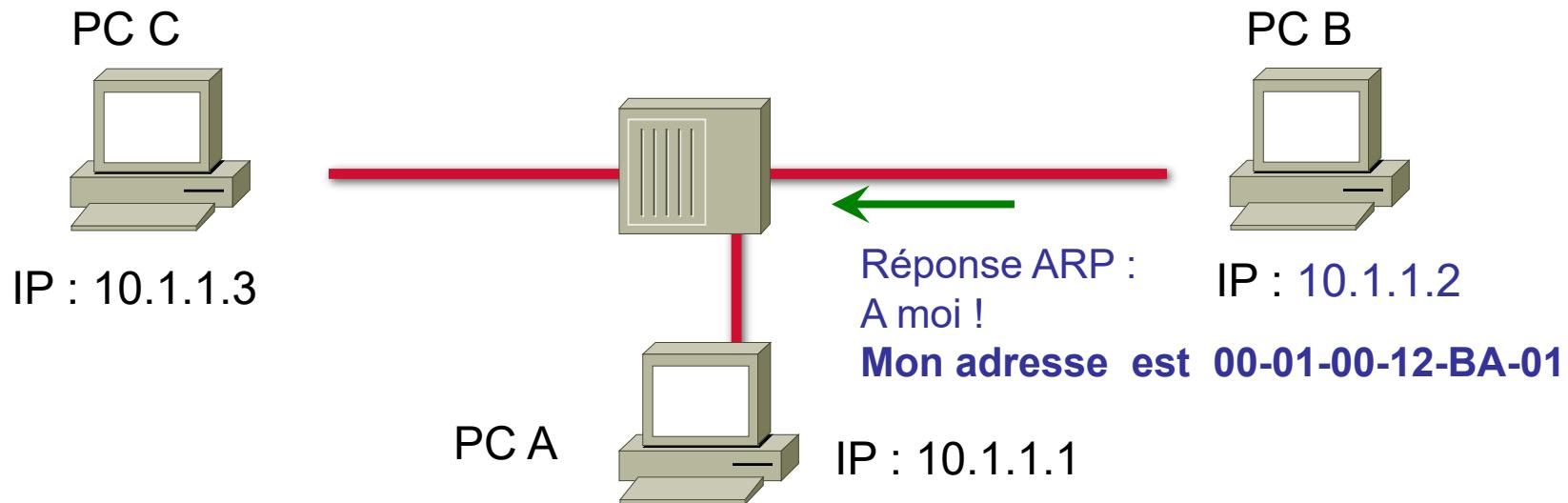
- Chaque noeud du réseau a deux adresses :
 - Une adresse physique appelée adresse MAC
 - Une adresse logique appelée adresse IP
- L'adresse **MAC** est gravée dans la carte réseau. Si l'on change cette carte, l'adresse MAC change
- L'adresse **IP** est configurée par l' administrateur et ne dépend pas 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



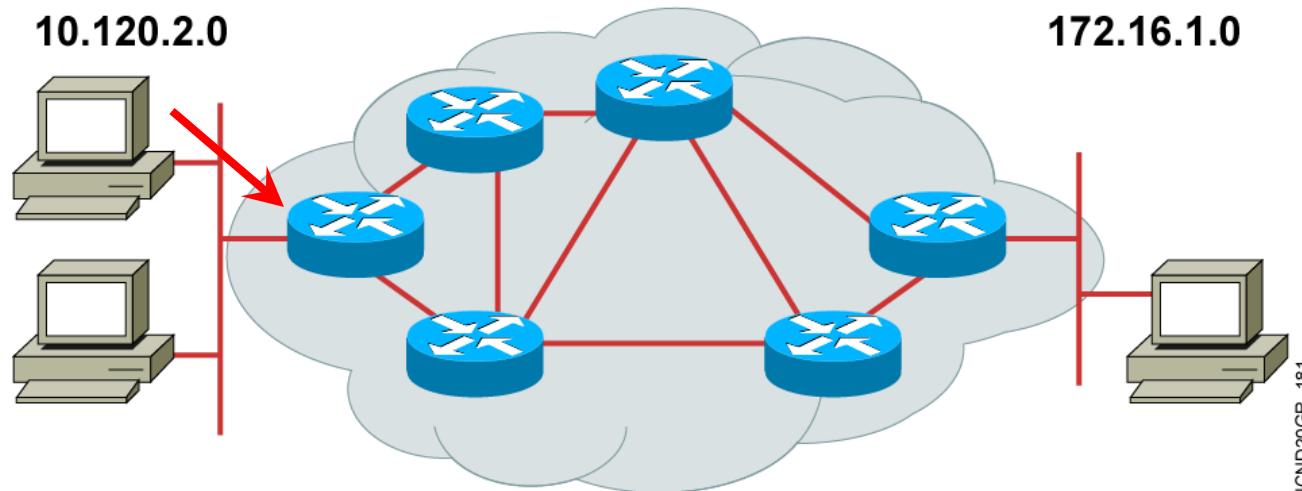
- Une requête ARP est un **broadcast** et tous les PCs du LAN le reçoivent

Réponse ARP



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

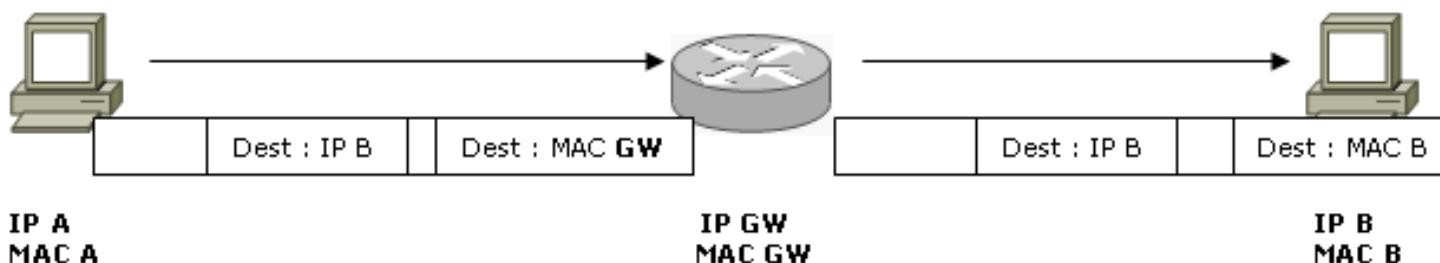
La requête ARP ne sort pas du LAN



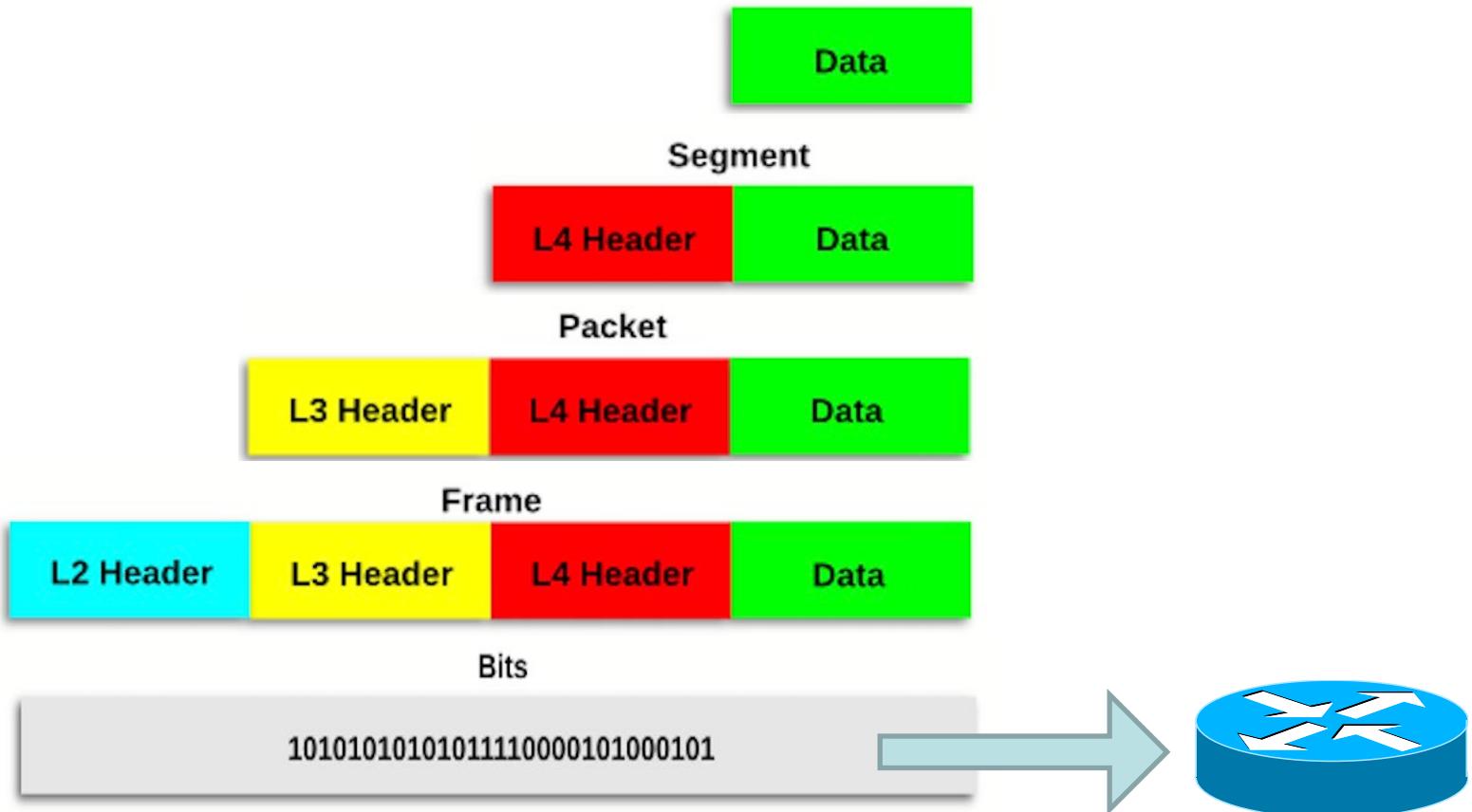
- Par défaut, les routeurs filtrent les broadcasts
- Si la destination nécessite de traverser des routeurs, ARP est inopérant

Rappel !

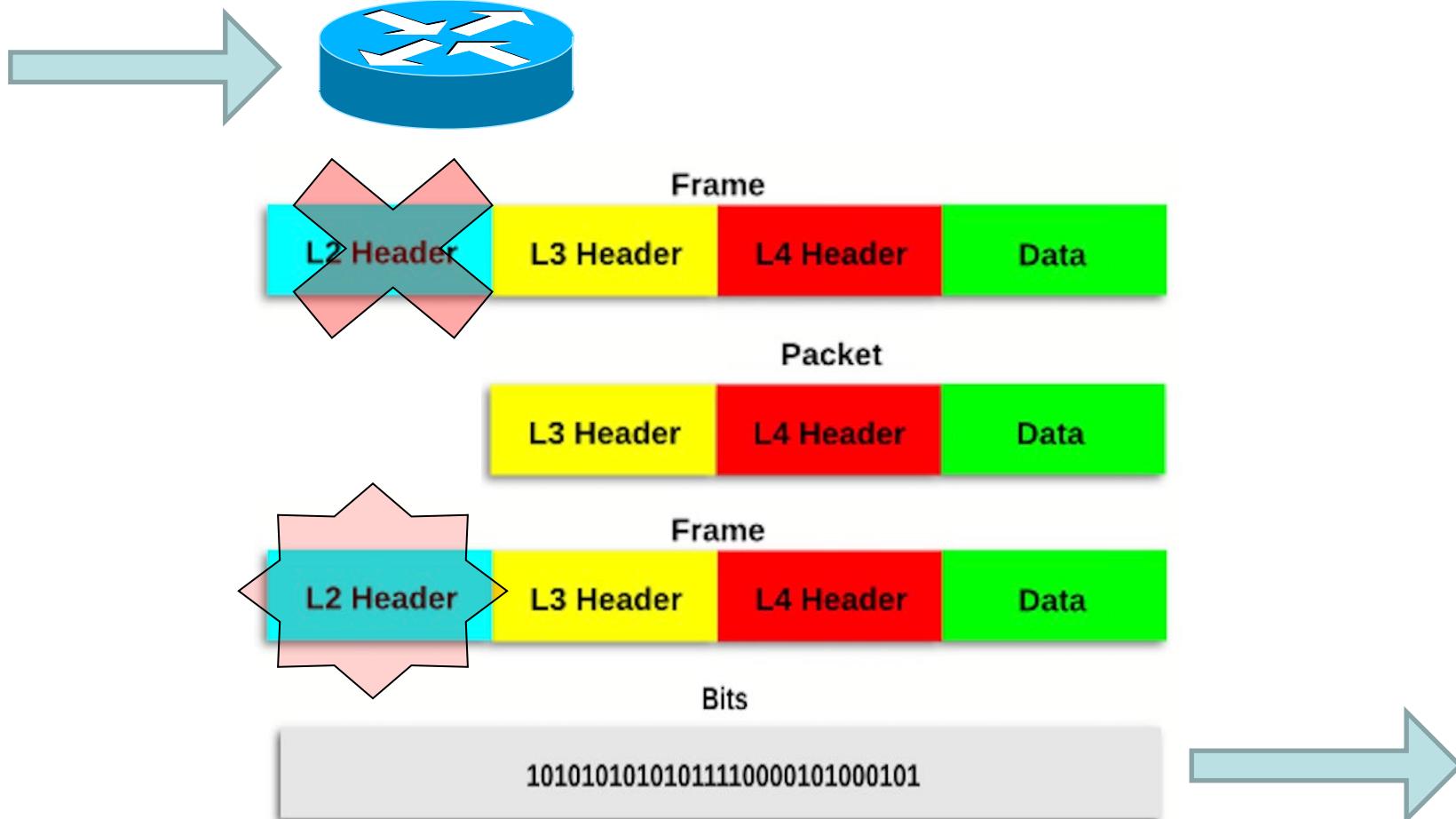
- Si deux PC ne sont pas sur le même réseau, ils sont séparés par un routeur.
 - Ce routeur est la passerelle de chaque PC
- Les entêtes IP ne sont **pas modifiées** par le routeur
- Les entêtes Ethernet sont **reconstruites** par le routeur



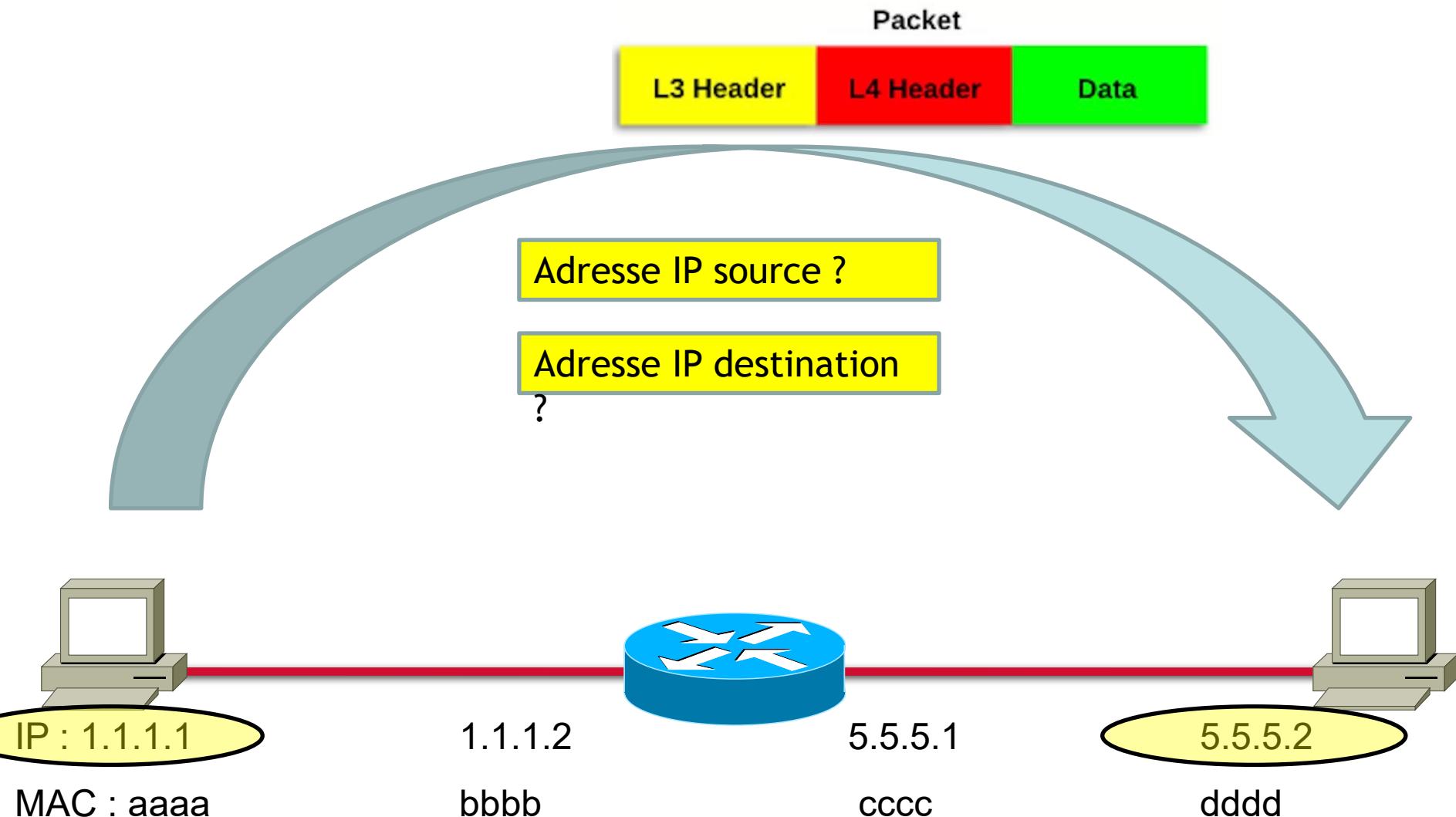
Rappel !



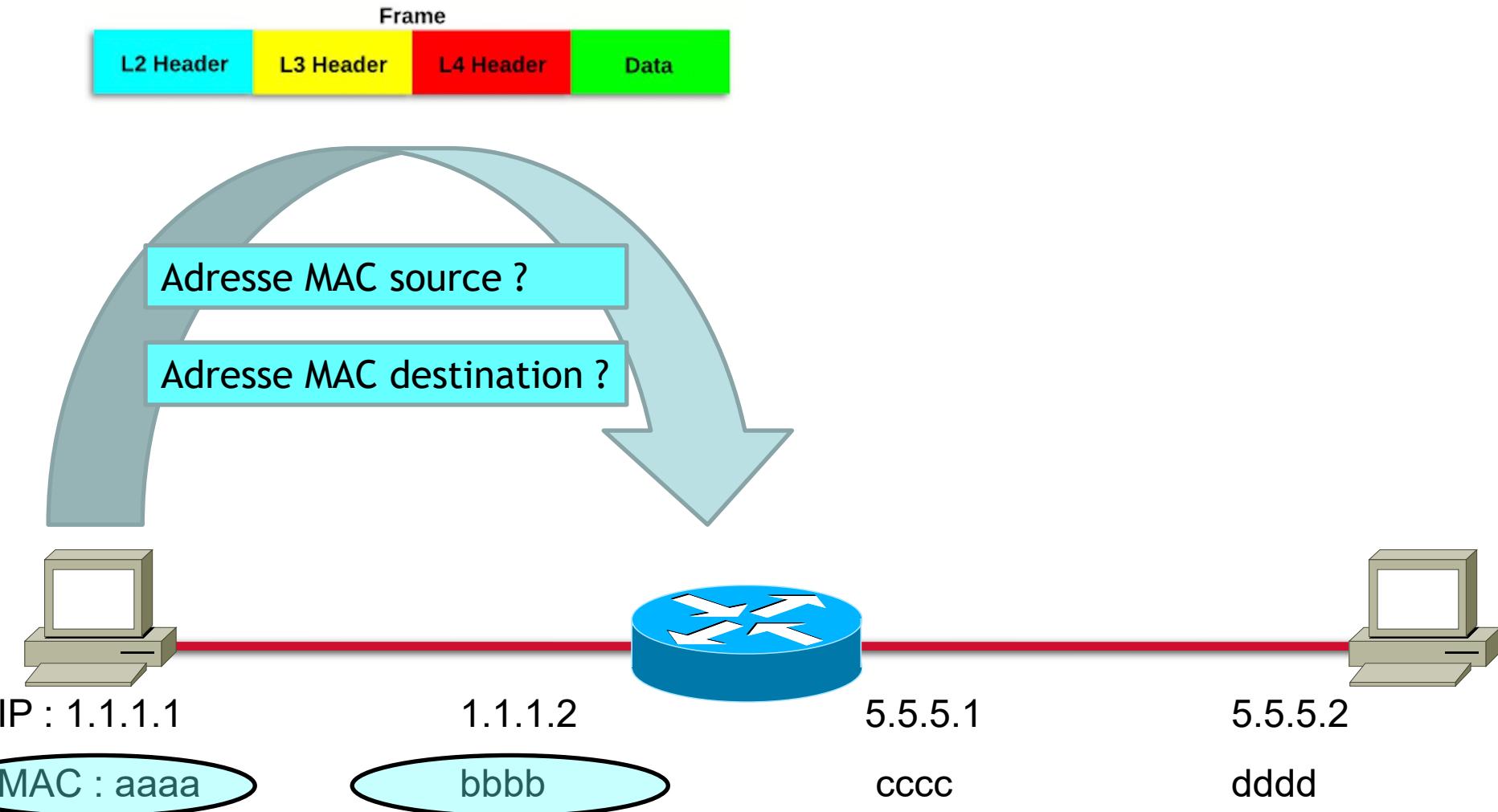
Rappel !



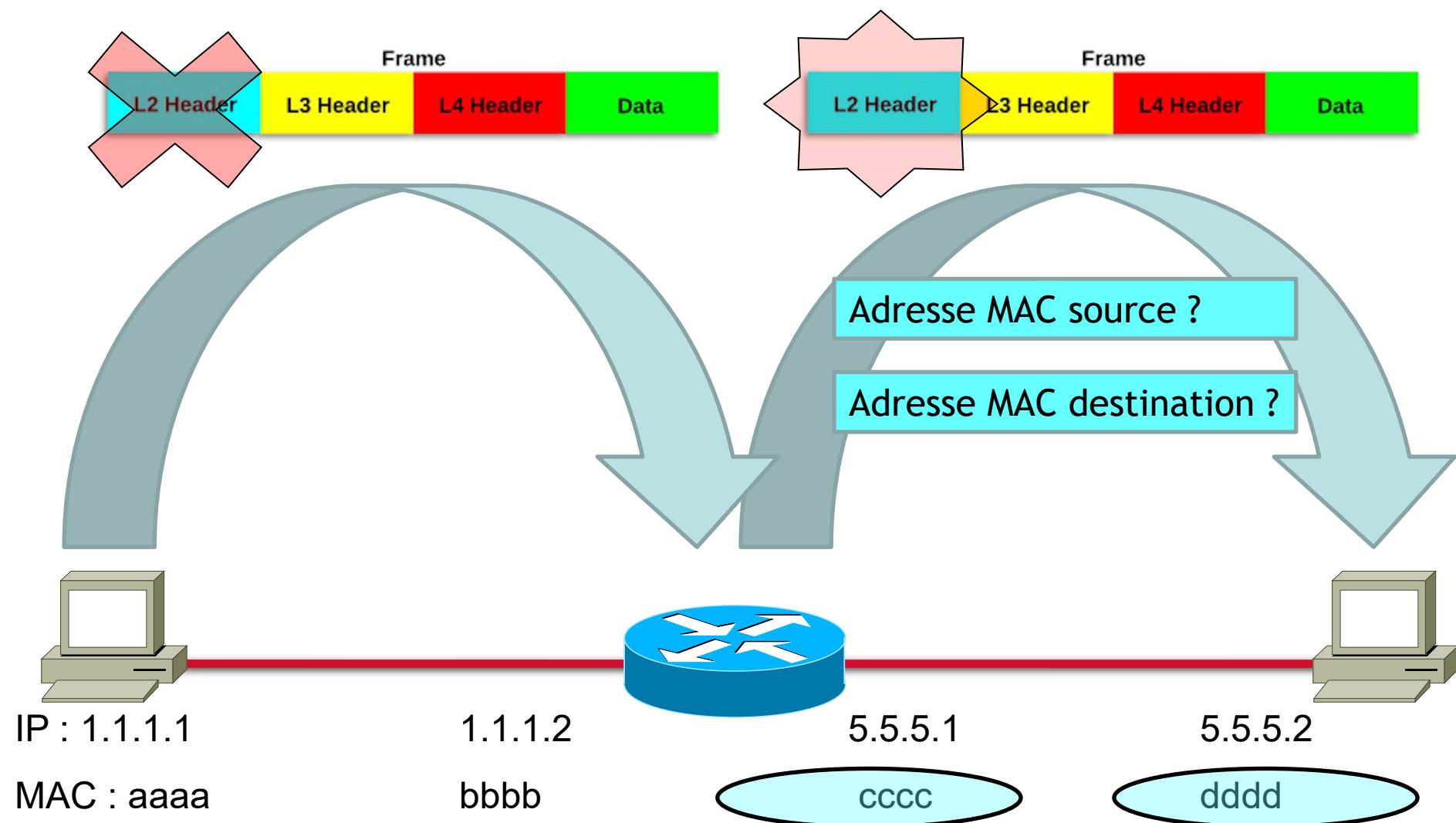
Envoi d'un paquet à travers un routeur



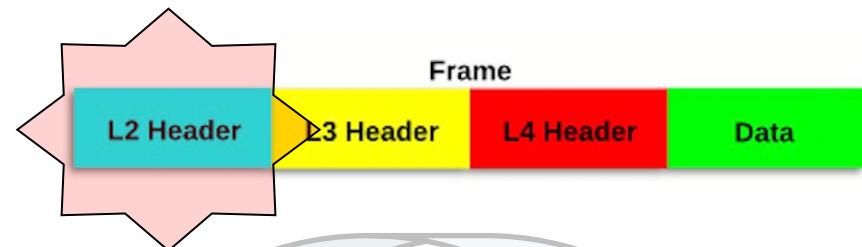
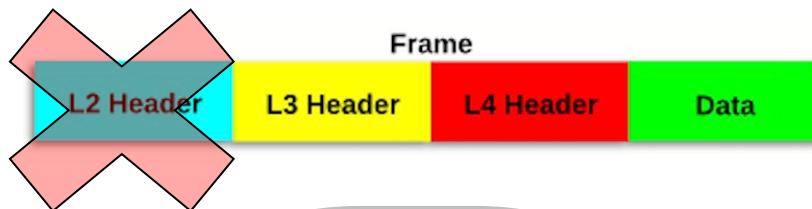
Envoi d'un paquet à travers un routeur



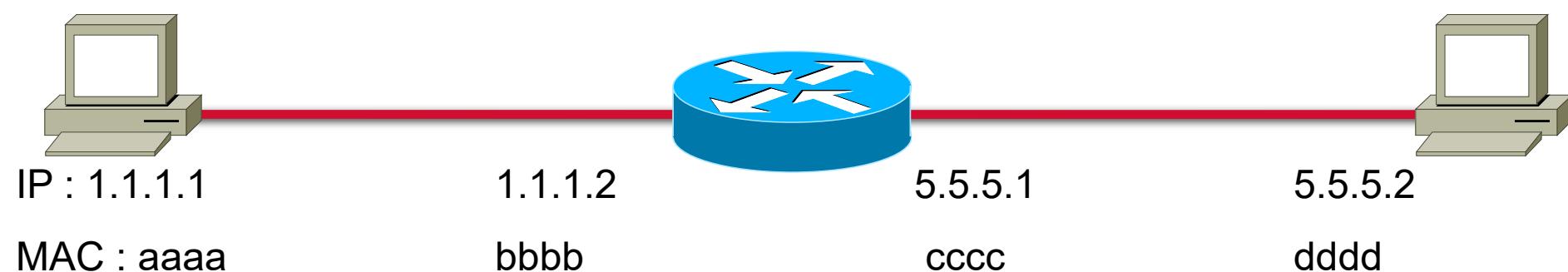
Envoi d'un paquet à travers un routeur



Envoi d'un paquet à travers un routeur

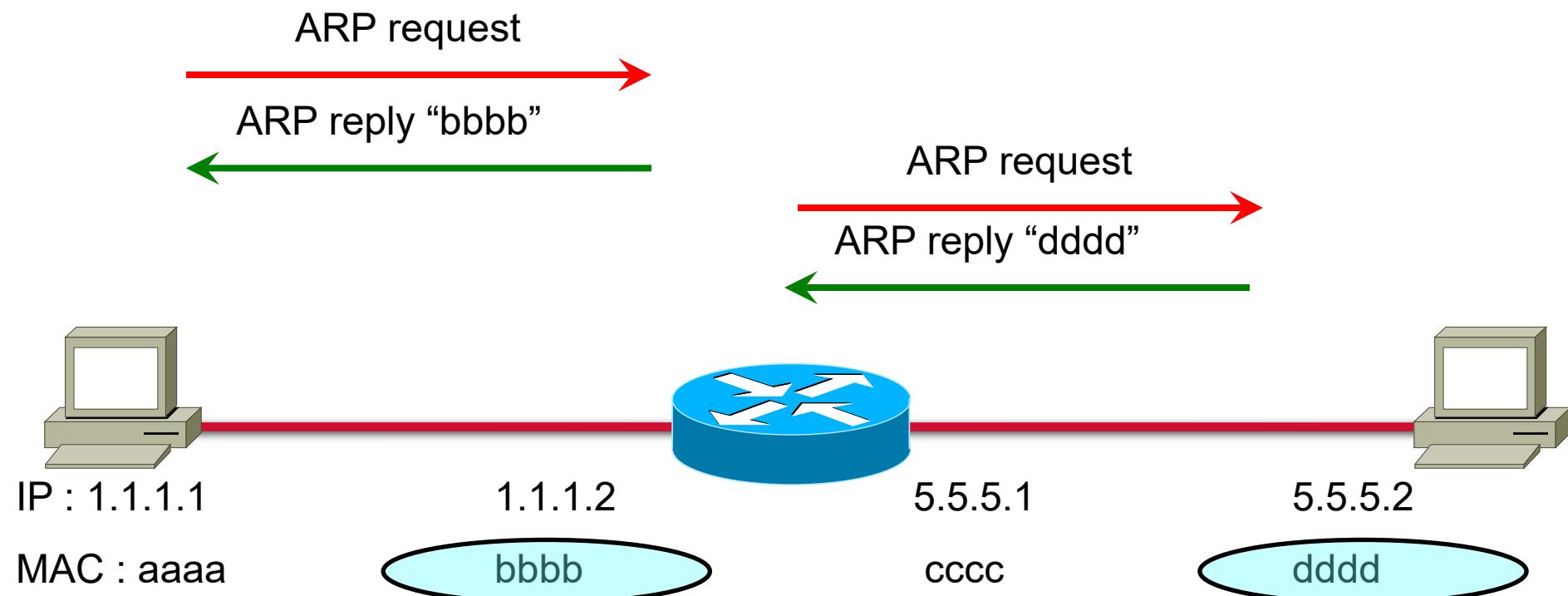


- Les adresses **MAC** des trames (L2) **changent** à chaque saut
- Les adresses **IP** des paquets (L3) sont **conservées**



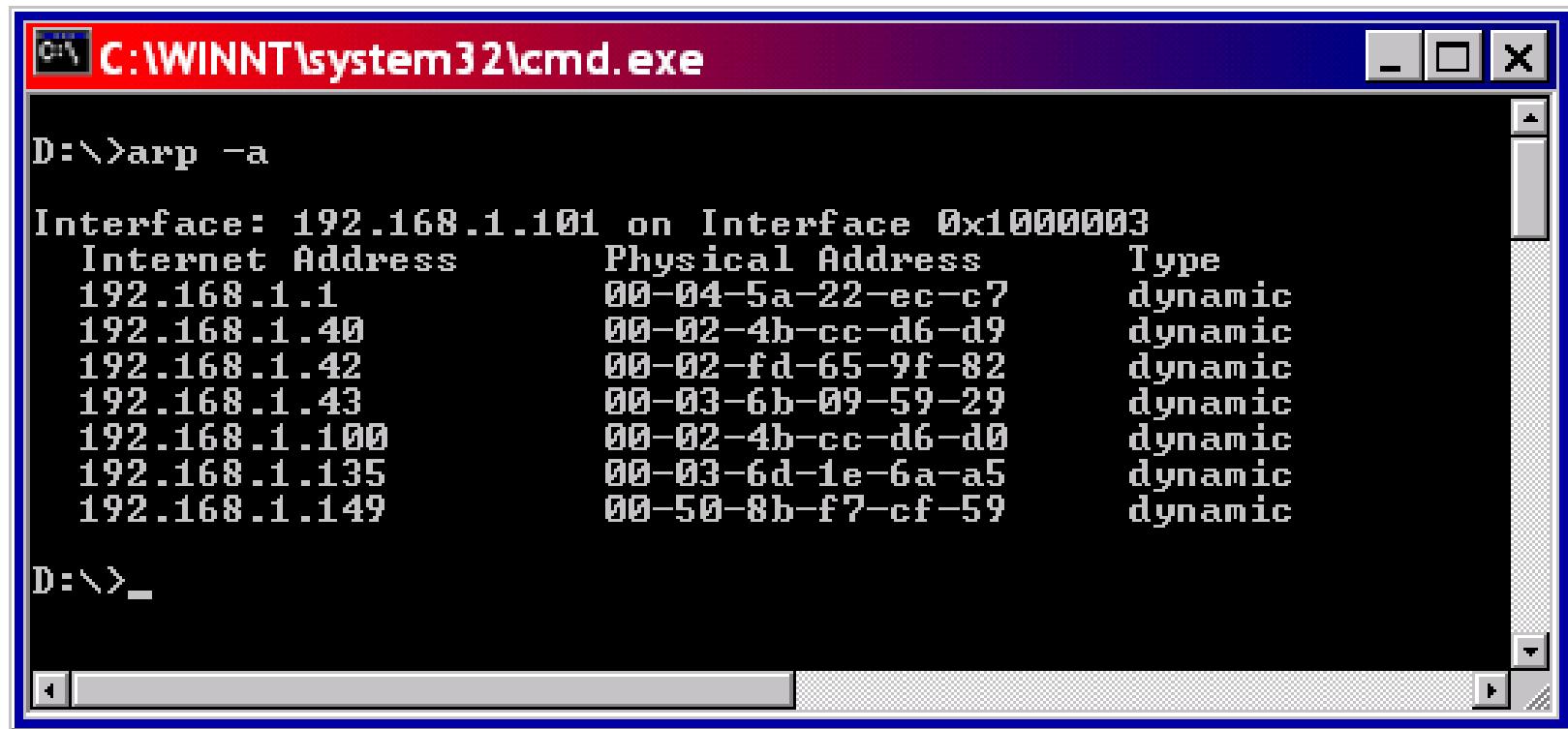
Deux requêtes ARP sont nécessaires

- 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



C:\WINNT\system32\cmd.exe

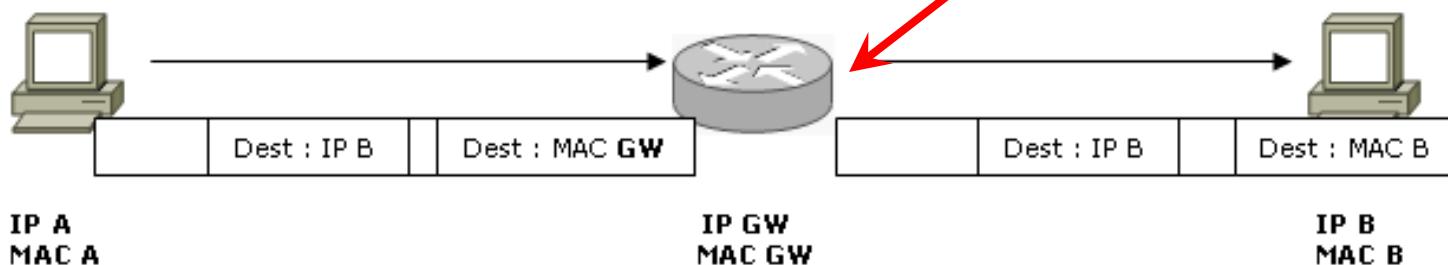
```
D:\>arp -a

Interface: 192.168.1.101 on Interface 0x10000003
  Internet Address      Physical Address          Type
  192.168.1.1            00-04-5a-22-ec-c7    dynamic
  192.168.1.40           00-02-4b-cc-d6-d9    dynamic
  192.168.1.42           00-02-fd-65-9f-82    dynamic
  192.168.1.43           00-03-6b-09-59-29    dynamic
  192.168.1.100          00-02-4b-cc-d6-d0    dynamic
  192.168.1.135          00-03-6d-1e-6a-a5    dynamic
  192.168.1.149          00-50-8b-f7-cf-59    dynamic

D:\>_
```

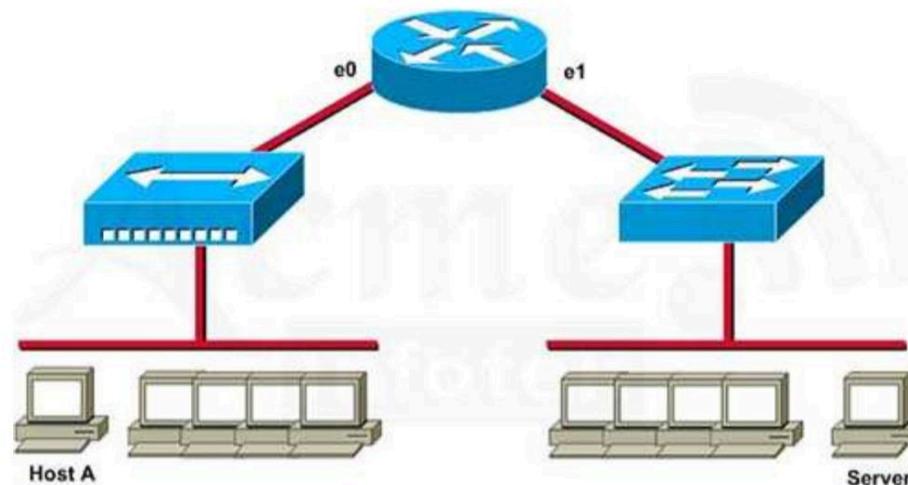
Cache ARP sur un routeur

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	-	0000.0c36.6965	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	UUUU.UcU7.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

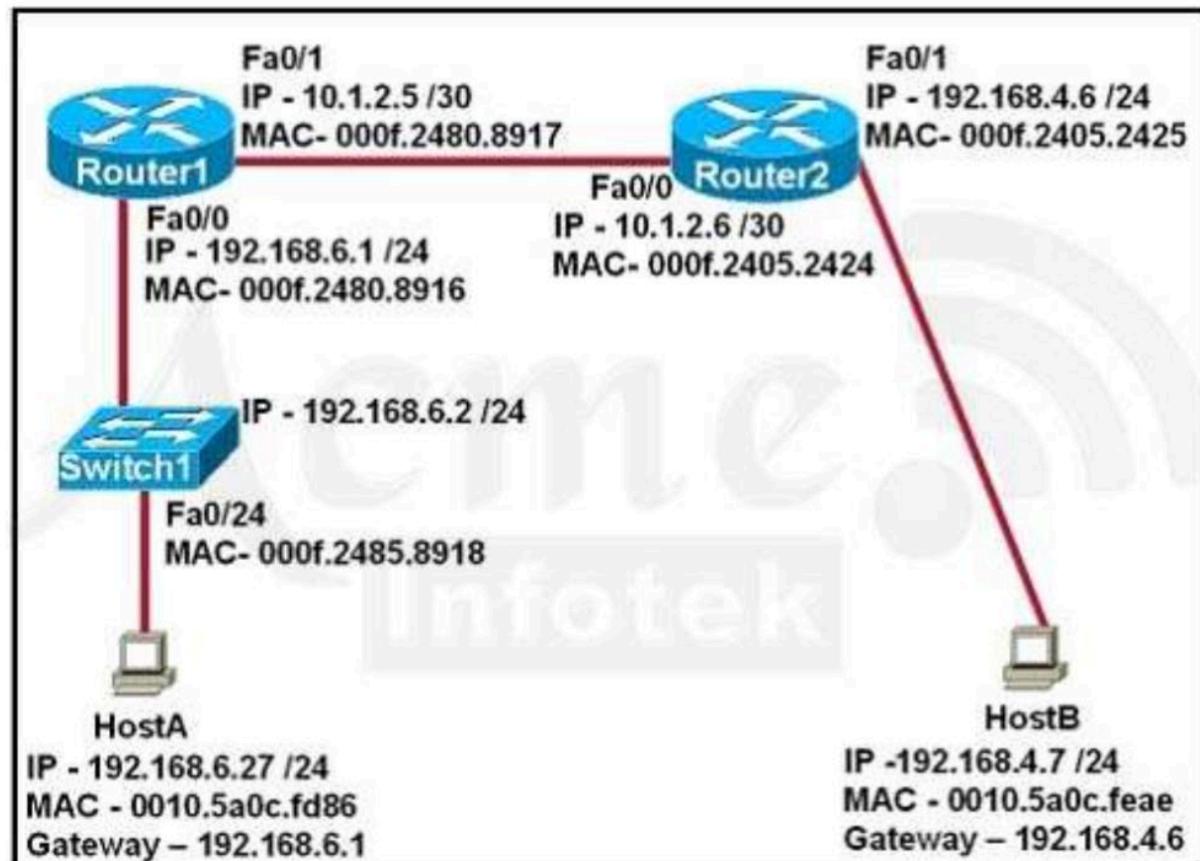
Data Frame:

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

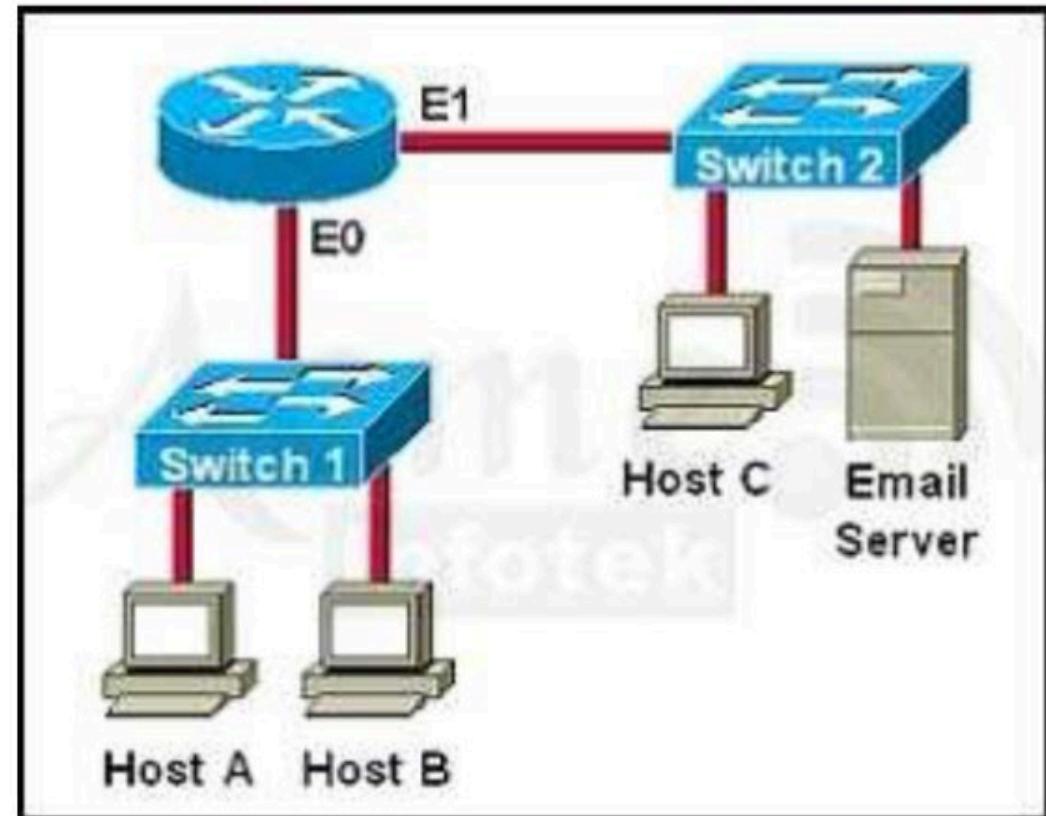
Après que A ait pingé B, quelle entrée est présente dans le cache ARP du host A ?



Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

Test

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



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

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**
 - $(256 \times 256) - 2 = 65\ 534 = 2^{16} - 2$

La Classe A

- Propriétés :

- Masque : 255.0.0.0 i.e. /8
- Nombre de bits pour la partie hôte
24 =

- Exemple :

- 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
 - $(256 \times 256 \times 256) - 2 = 2^{24} - 2$

Exercice

Adresse	Classe	Adresse réseau	1 ^{ère} 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	1 ^{ère} 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

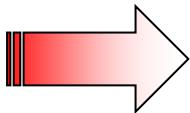
Masque	Nombre de bits dans la partie réseau	Nombre de bits dans la partie hôte	Nombre de combinaisons possibles	Nombre d' @ interdites	Nombres d' @ disponibles
/8	8	24	2^{24}	2	$2^{24}-2$
/16	16	16	2^{16}	2	$2^{16}-2$
/24	24	8	2^8	2	2^8-2

Identifier avec la « Largeur de bloc »

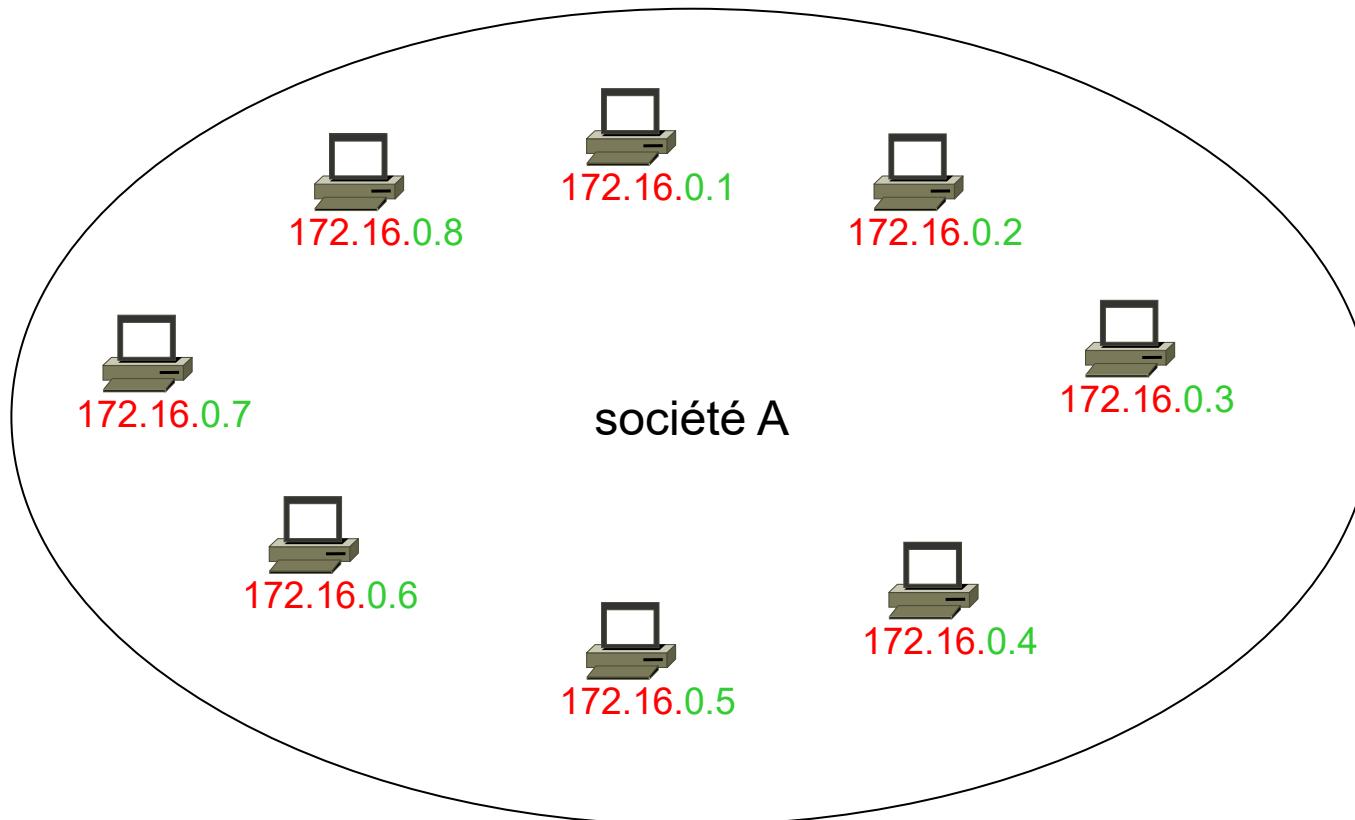
Masque	Largeur du bloc	Nombre d'hôtes
/24	255.255.255.0	$2^8=256$
/16	255.255.0.0	$2^{16}=65\ 536$
/8	255.0.0.0	$2^{24}=16\ 777\ 216$

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

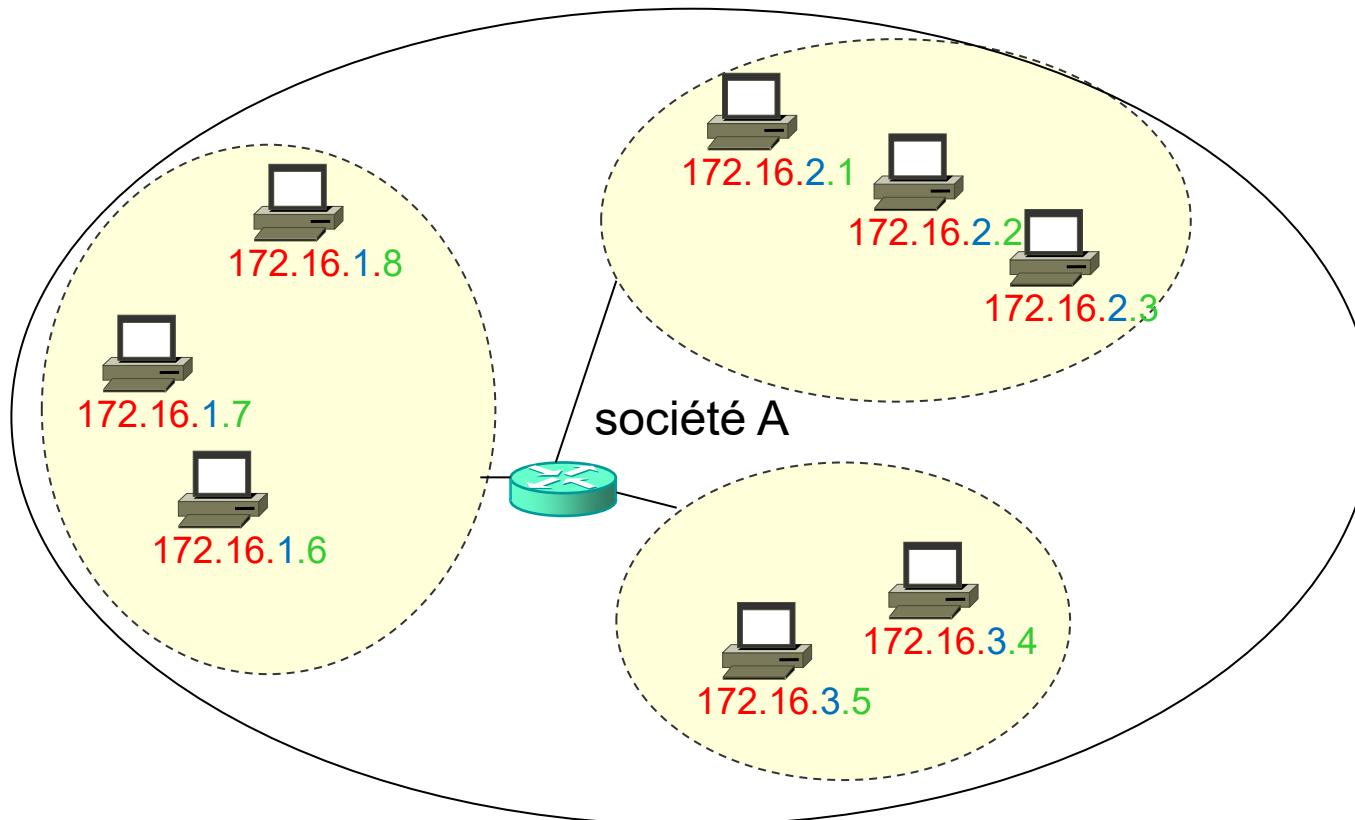


Les broadcast sans sous-réseau



- 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

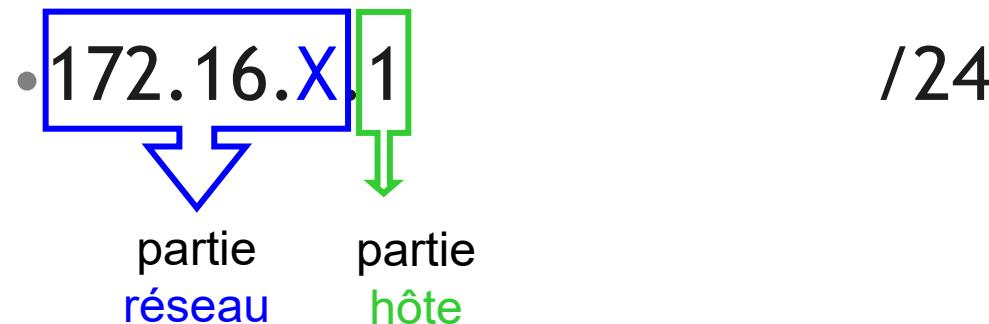
- Pour créer un sous-réseau :
 - on **allonge** la taille du masque initial
- Exemple :
 - masque initial : /16
 - masque final : /24
- En binaire :
 - masque initial : **11111111.11111111.00000000.00000000**
 - masque final : **11111111.11111111.**11111111.00000000****

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	1 ^{ère} adresse disponible
172.16.0.2	2 ^{ème} adresse disponible
172.16.0.3	3 ^{ème} 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	
172.16.1.1	1ère adresse disponible	
172.16.1.2	2ème adresse disponible	2ème sous-réseau
172.16.1....	etc...	
172.16.1.254	Dernière adresse disponible	
172.16.1.255	Adresse de broadcast	
172.16.2.0	Adresse 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	3ème sous-réseau
172.16.2.255	Adresse de broadcast	

Combien de sous-réseaux créés ?

172.16.0.0	Adresse réseau	1 ^{er} sous-réseau
172.16.1.0	Adresse réseau	2 ^{ème} sous-réseau
172.16.2.0	Adresse réseau	3 ^{ème} sous-réseau
172.16.3.0	Adresse réseau	4 ^{ème} sous-réseau
172.16.4.0	Adresse réseau	5 ^{ème} sous-réseau
172.16.5.0	Adresse réseau	6 ^{ème} sous-réseau
172.16.254.0	Adresse réseau	255 ^{ème} sous-réseau
172.16.255.0	Adresse réseau	256 ^{ème} 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 : 2^8
 - C'est le nombre de combinaisons possibles pour le 3^{ème} 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 = **11111111.11111111.1.00000000**
- Sur un octet partiel : **1111111**
 - 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 = **11111111.11111111.11111111.11000000**
- 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...10...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

	128	64	32	16	8	4	2	1	MAX	R	I	P	W	
0	0	0	0	0	0	0	0	0	0	1	256	255		255
1	1	0	0	0	0	0	0	0	128	2	128	177		255
2	1	1	0	0	0	0	0	0	192	4	64	63		255
3	1	1	1	0	0	0	0	0	224	8	32	31		255
4	1	1	1	1	0	0	0	0	240	16	16	15		255
5	1	1	1	1	1	0	0	0	248	32	8	7		255
6	1	1	1	1	1	1	0	0	252	64	4	3		255
7	1	1	1	1	1	1	1	0	254	128	2	1		255
8	1	1	1	1	1	1	1	1	255	256	1	0		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...10...00**
 - pour chaque nouveau réseau :
 - nombre d'@ consommées = **$2^{(8-N)}$**
 - nombre d'@ disponibles = **$2^{(8-N)} - 2$**

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

- 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

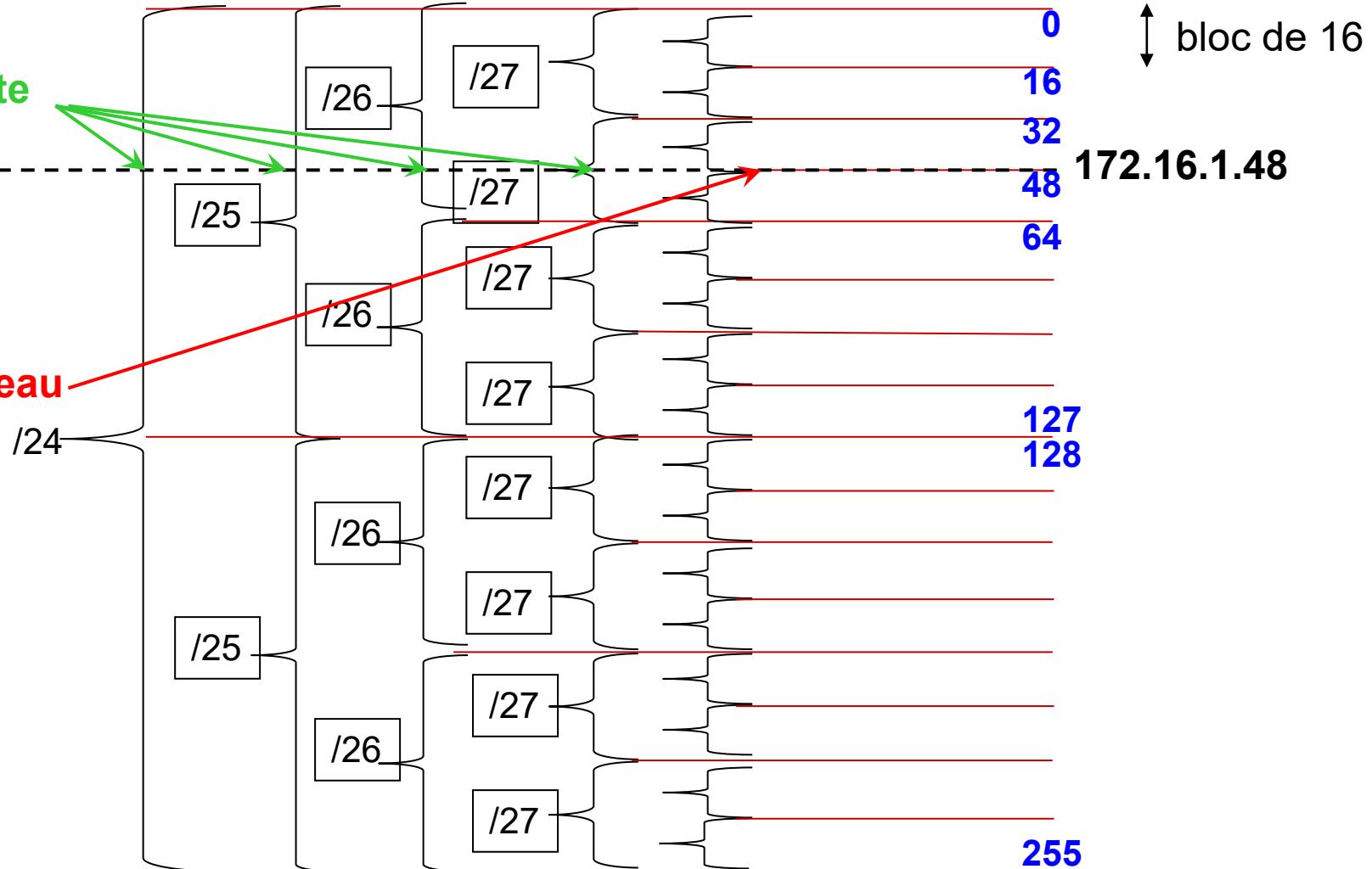
- Tout dépend du masque !!
- 172.16.1.48 /24
- 172.16.1.48 /25
- 172.16.1.48 /26
- 172.16.1.48 /27
- 172.16.1.48 /28

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

@ hôte

@ réseau



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	255.255.255.240	
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	255.255.255. 240	10.6.24.16
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

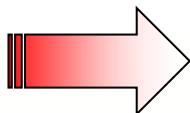
Solution 3

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

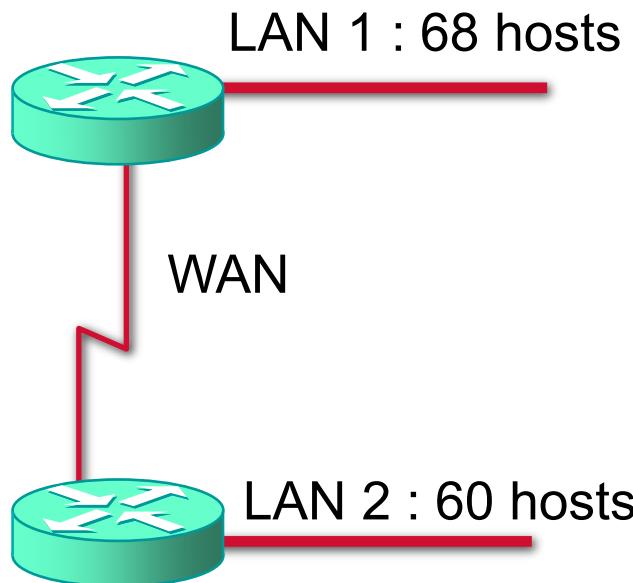
Le subnetting :

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 concrète

- 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
			1	1 ^{ère} adresse disponible
			...	2 ^{ème} adresse disponible
				3 ^{ème} adresse disponible
		63		
		64		
		65		
		...		
		126		Dernière adresse disponible
		127	▼	Adresse de broadcast
		128		
		129		
		...		
		190		
		191		
		192		
		193		
		...		
		255		

Un bloc de 128 pour le LAN 1 avec 68 hôtes

Solution 3

172	16	1	0	Adresse réseau	
			1	1 ^{ère} adresse disponible	
			...	2 ^{ème} adresse disponible	
			63	3 ^{ème} adresse disponible	
			64		
			65		
			...		
			126	Dernière adresse disponible	
			127	Adresse de broadcast	
			128	Adresse réseau	Un bloc de 128 pour le LAN 1 avec 68 hôtes
			129	1 ^{ère} adresse disponible	
			...		
			190	Dernière adresse disponible	Un bloc de 64 pour le LAN 2 avec 60 hôtes
			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

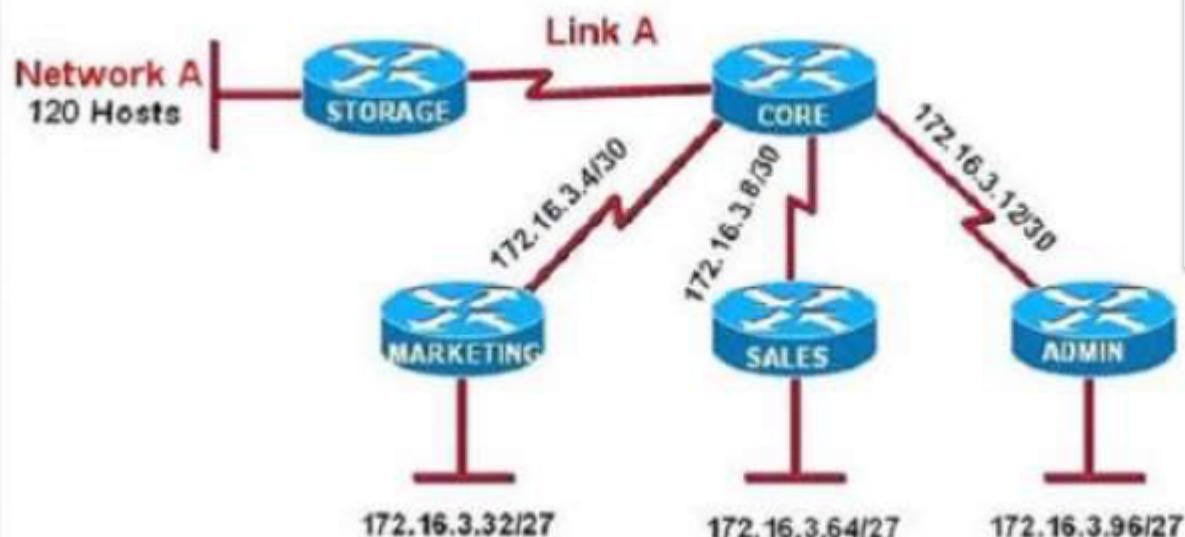
You have been asked to come up with a subnet mask that will allow all three web servers to be on the same network while providing the maximum number of subnets. Which network address and subnet mask meet this requirement?

- 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

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

La Table de Routage

Introduction

Contenu de la table de routage

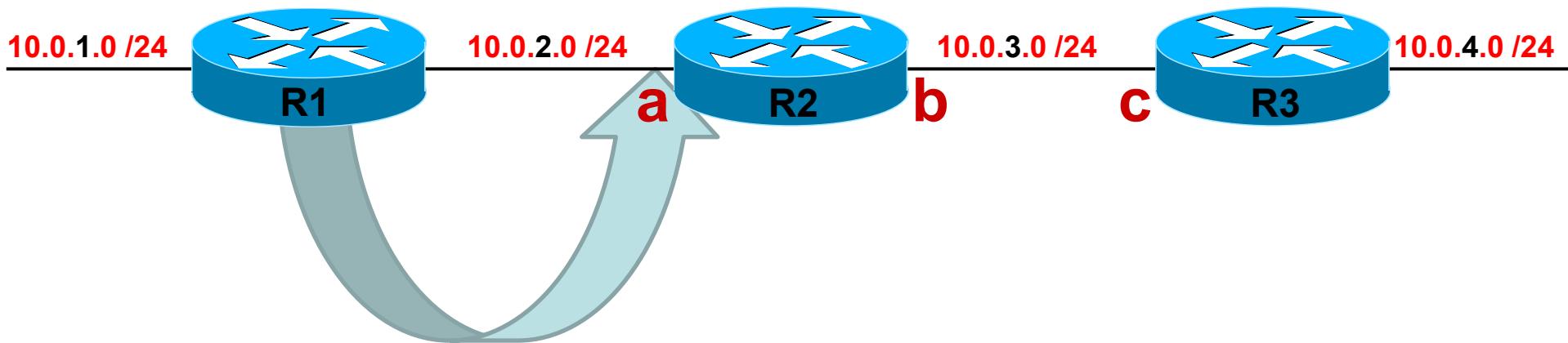
La table de routage indique **comment** acheminer les paquets :

1. Le routeur examine le champ « Adresse IP destination ».
2. Puis il cherche cette adresse dans sa Table.
3. La Table lui indique :
 - **L'interface** de sortie à utiliser
 - **Le NEXT HOP** à utiliser.

Le Next HOP est l'adresse IP du prochain saut.

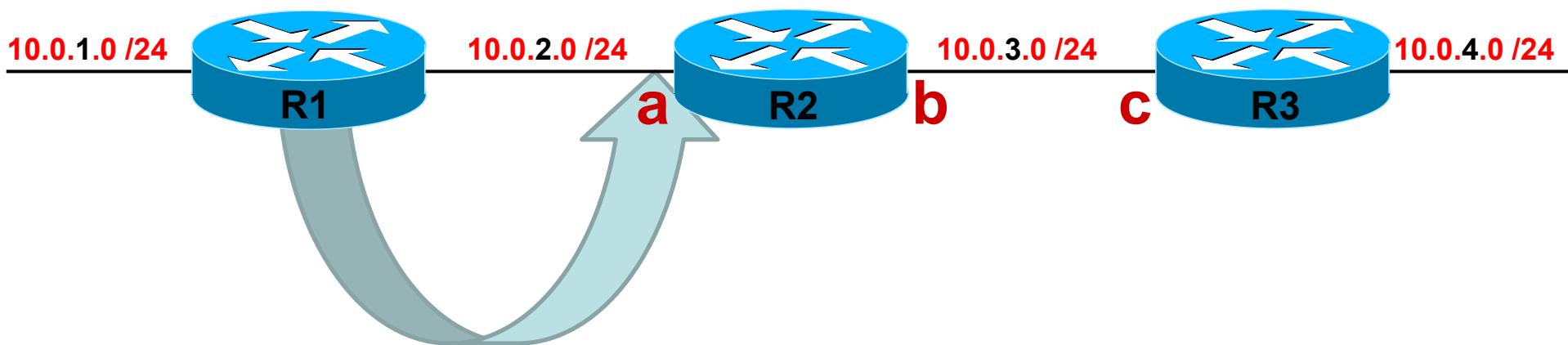
Le NEXT HOP : Exercice 1

Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.3.0 /24** ?

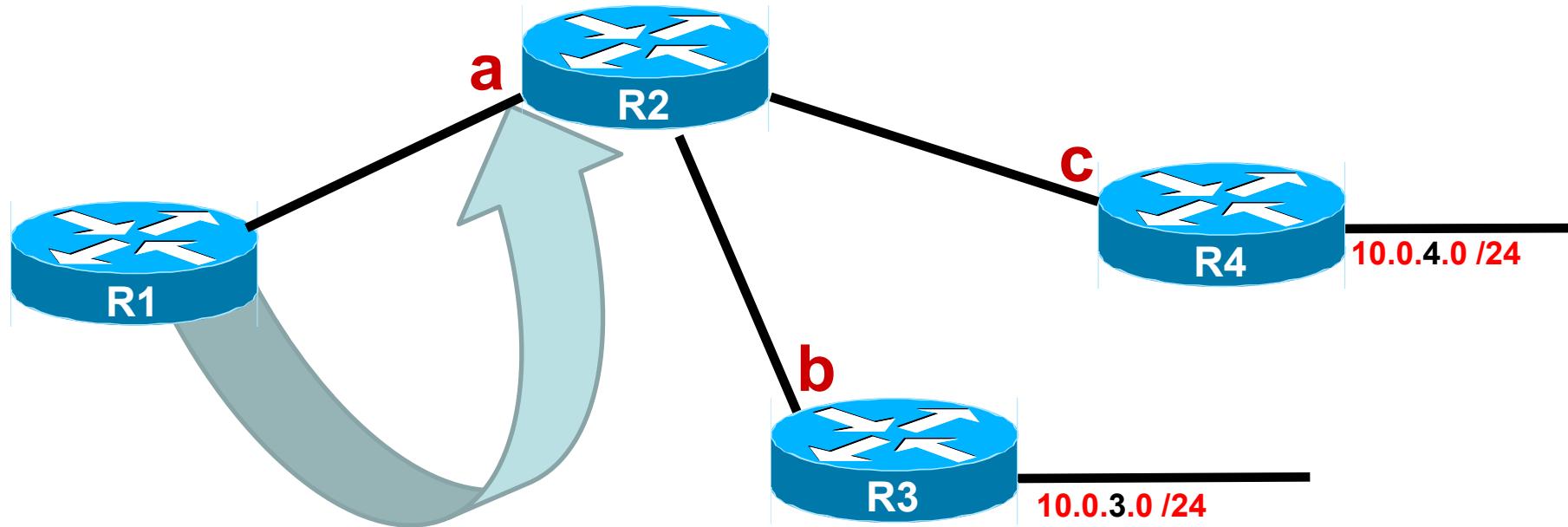


Le NEXT HOP : Exercice 2

Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.4.0 /24** ?

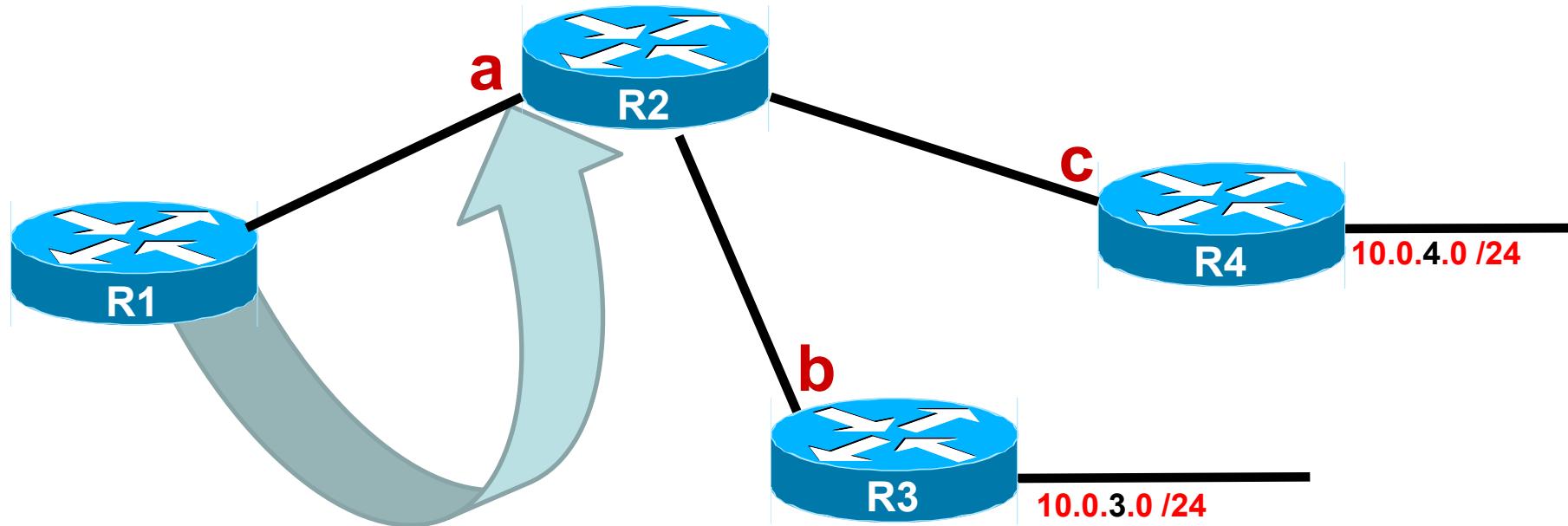


Le NEXT HOP : Exercice 3



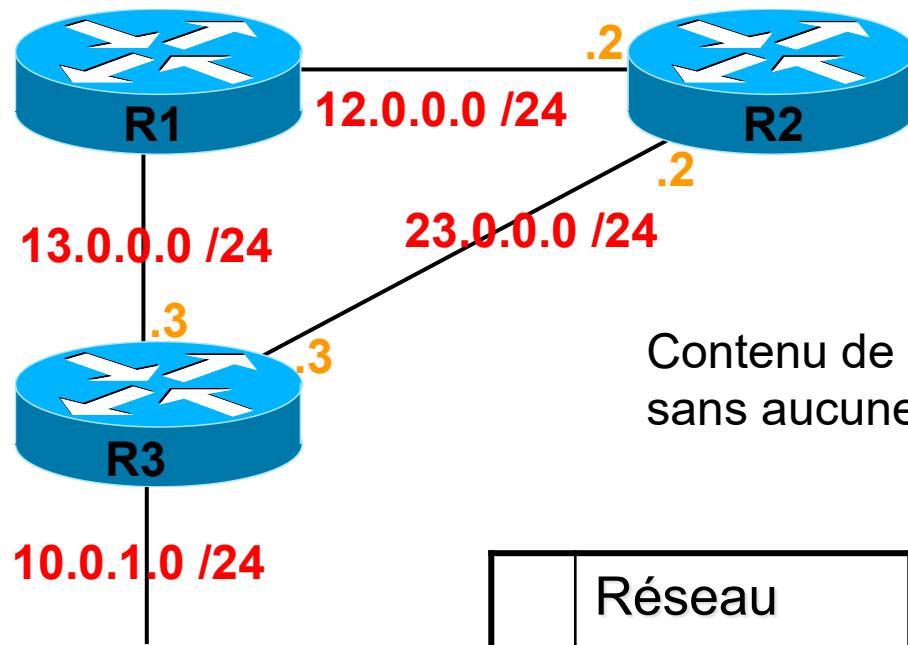
Quel NEXT HOP doit utiliser R1 pour joindre le réseau 10.0.3.0 /24 ?

Le NEXT HOP : Exercice 4



Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.4.0 /24** ?

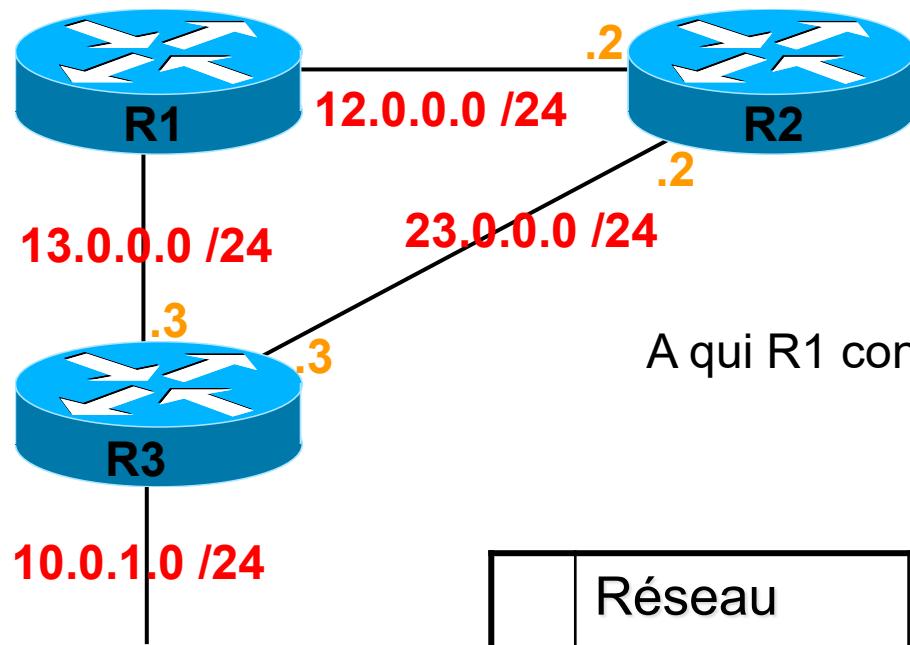
SHOW IP ROUTE



Contenu de la TABLE de ROUTAGE de R1
sans aucune route statique ni dynamique ;

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

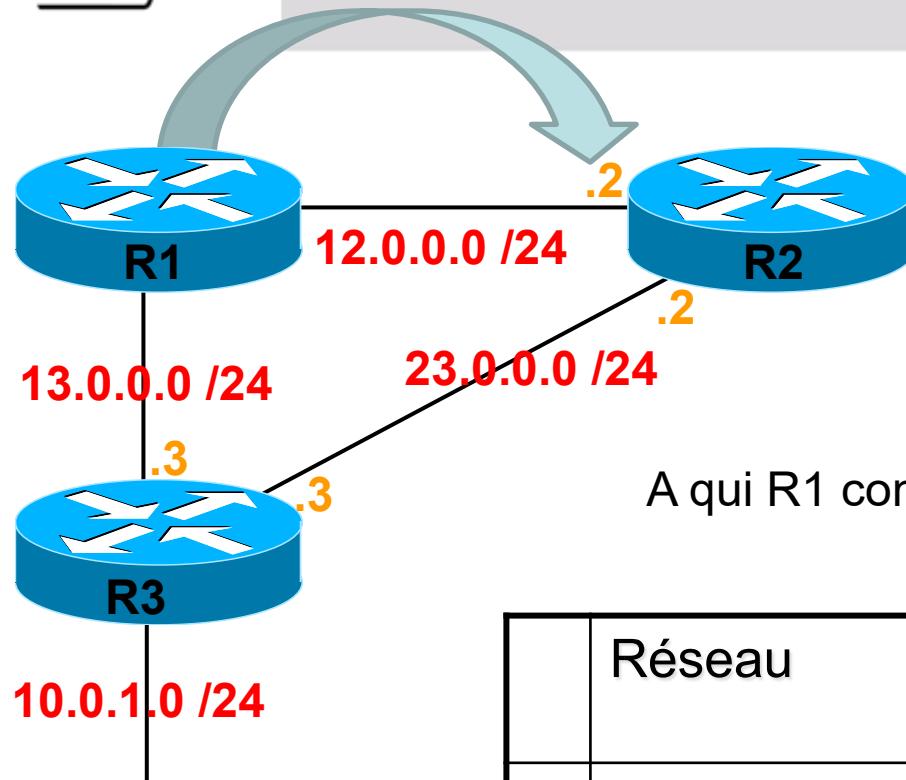
SHOW IP ROUTE : Exercice 1



A qui R1 confie les paquets à destination de 10.0.1.99 ?

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

SHOW IP ROUTE : Exercice 2



A qui R1 confie les paquets à destination de 10.0.1.99 ?

	Réseau	Masque	Next-Hop	Interface
C	12.0.0.0	/24		Fa0/2
C	13.0.0.0	/24		Fa0/0
O	10.0.1.0	/24	12.0.0.2	

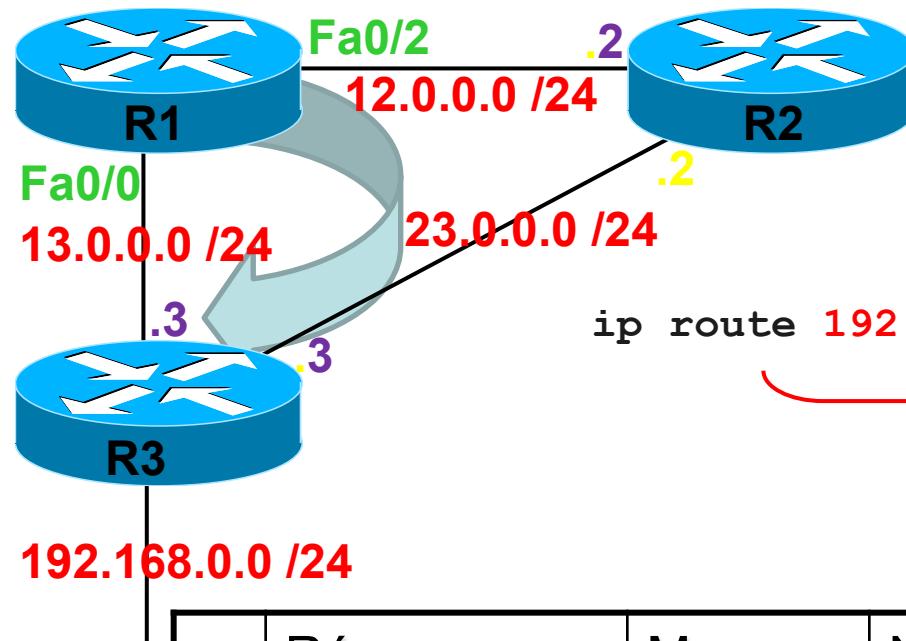
Routage statique

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



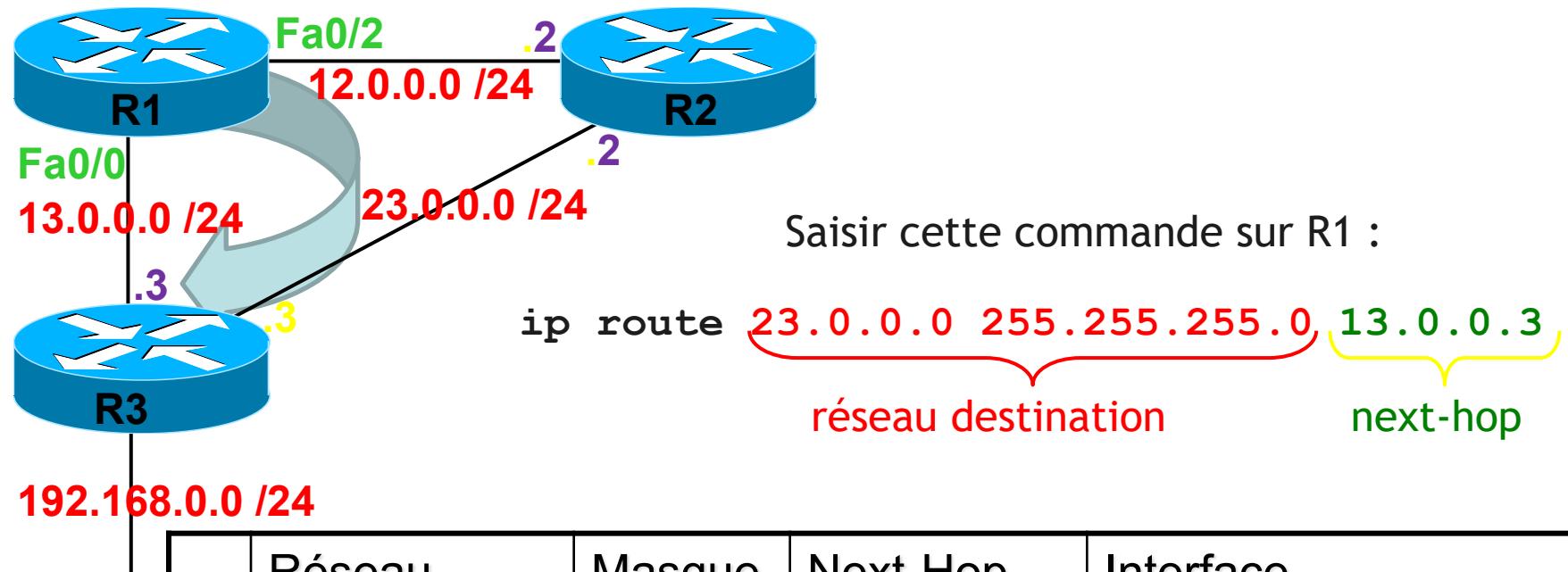
Saisir cette commande sur R1 :

```
ip route 192.168.0.0 255.255.255.0 13.0.0.3
```

réseau destination next-hop

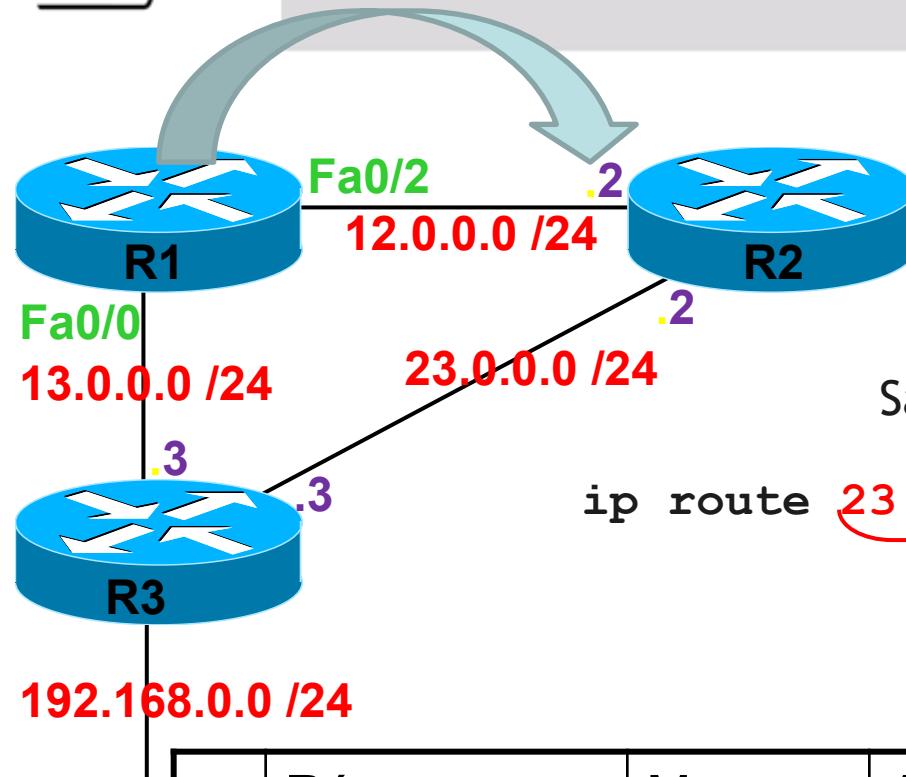
	Réseau	Masque	Next-Hop	Interface
C	12.0.0.0	/24		Fa0/2
C	13.0.0.0	/24		Fa0/0
S	192.168.0.0	/24	via 13.0.0.3	

Route statique pour 23 à partir de R1



	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

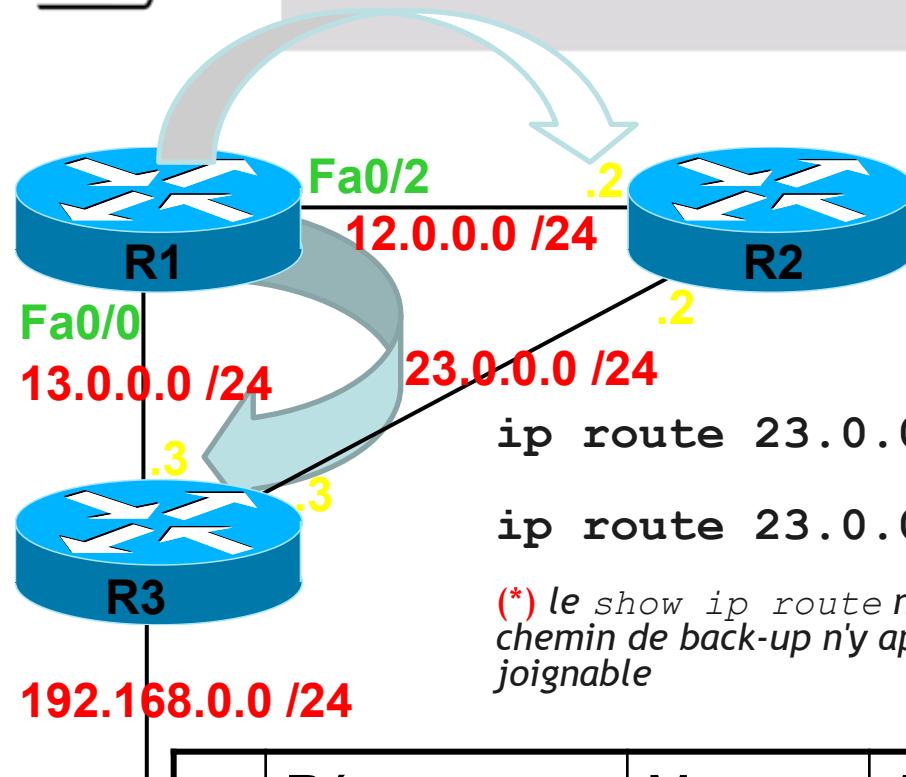


Saisir cette commande sur R1 :

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 23



```
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
```

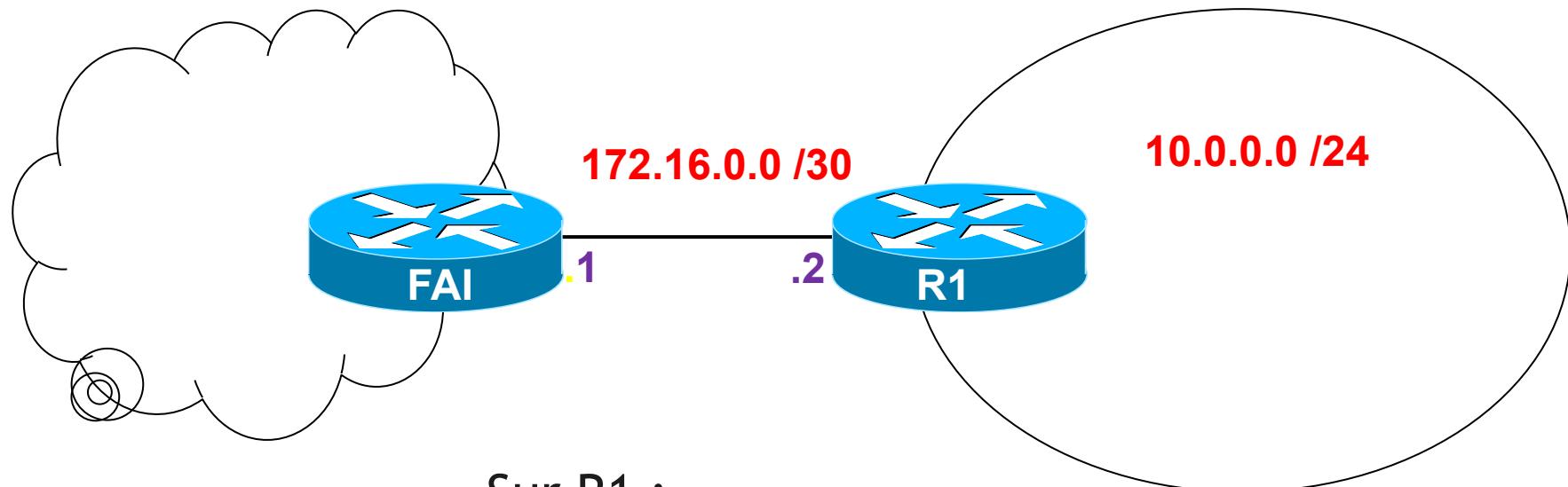
(*) le show ip route n'indique que le meilleur chemin, par conséquent le chemin de back-up n'y apparaît que lorsque le meilleur chemin n'est plus joignable

	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



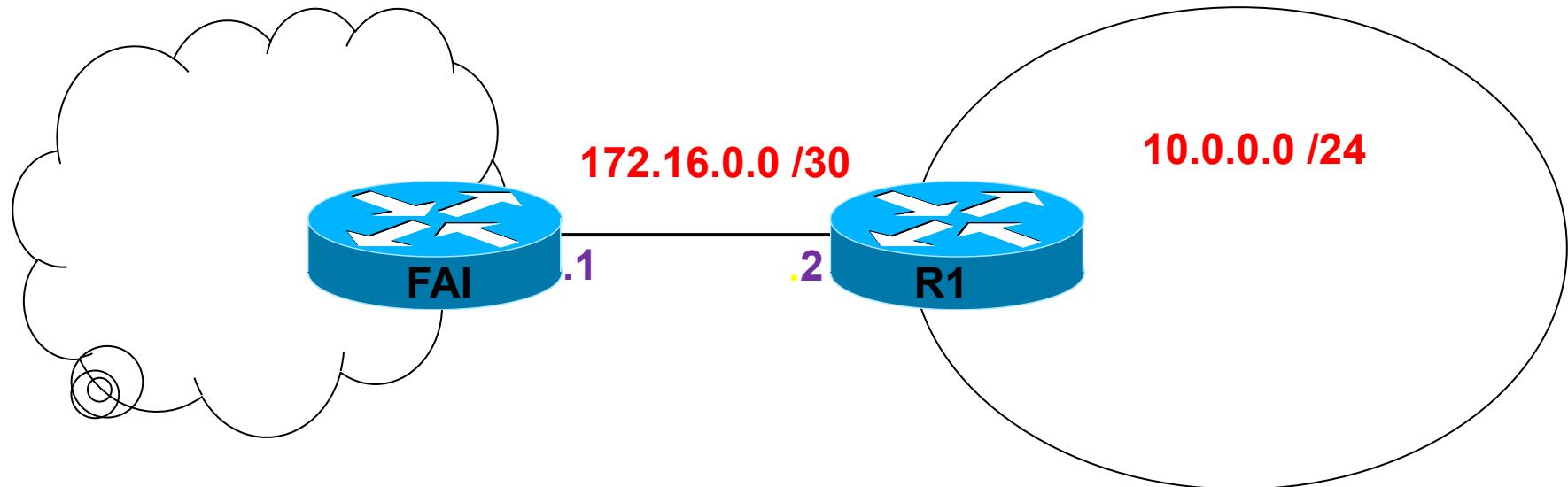
Sur R1 :

```
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
```

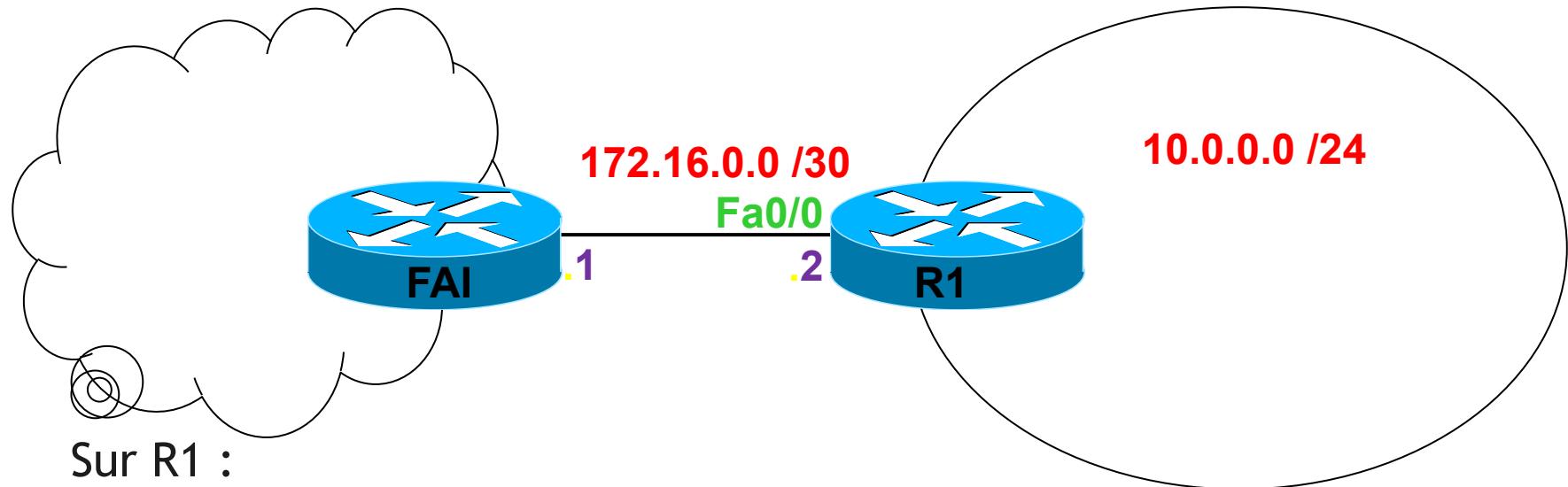
Route statique par défaut



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.

Routeage dynamique

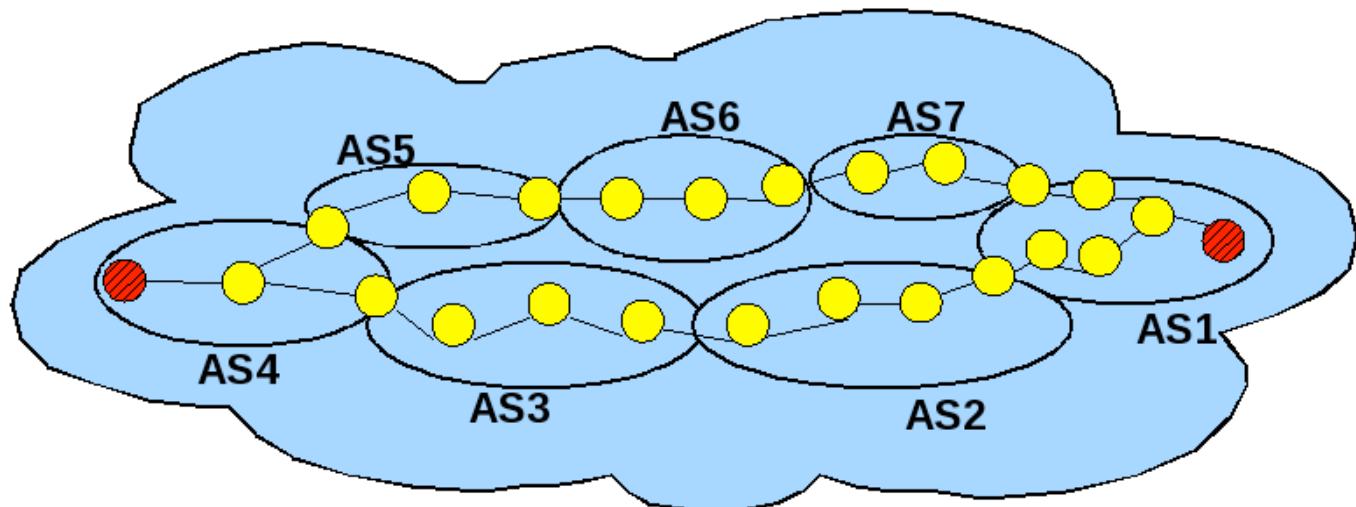
Types et familles de protocoles

Principe des Protocoles de routage

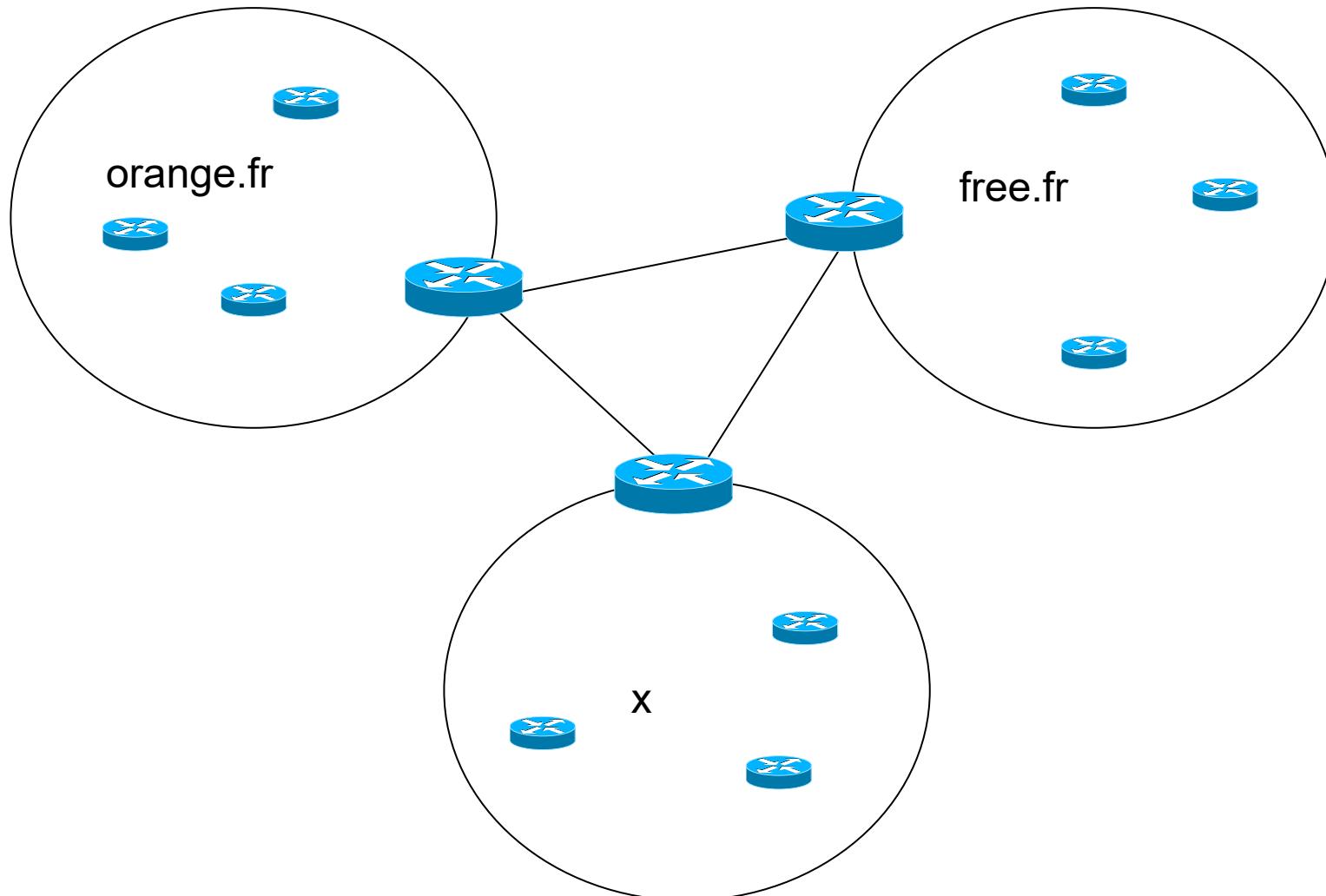
- Les routeurs échangent des informations.
- Ces échanges leur permettent d'enrichir de manière automatique leurs tables de routages.
- En cas de modification de la topologie du réseau, les tables de routage sont mises à jour de manière dynamique.

Le Système Autonome

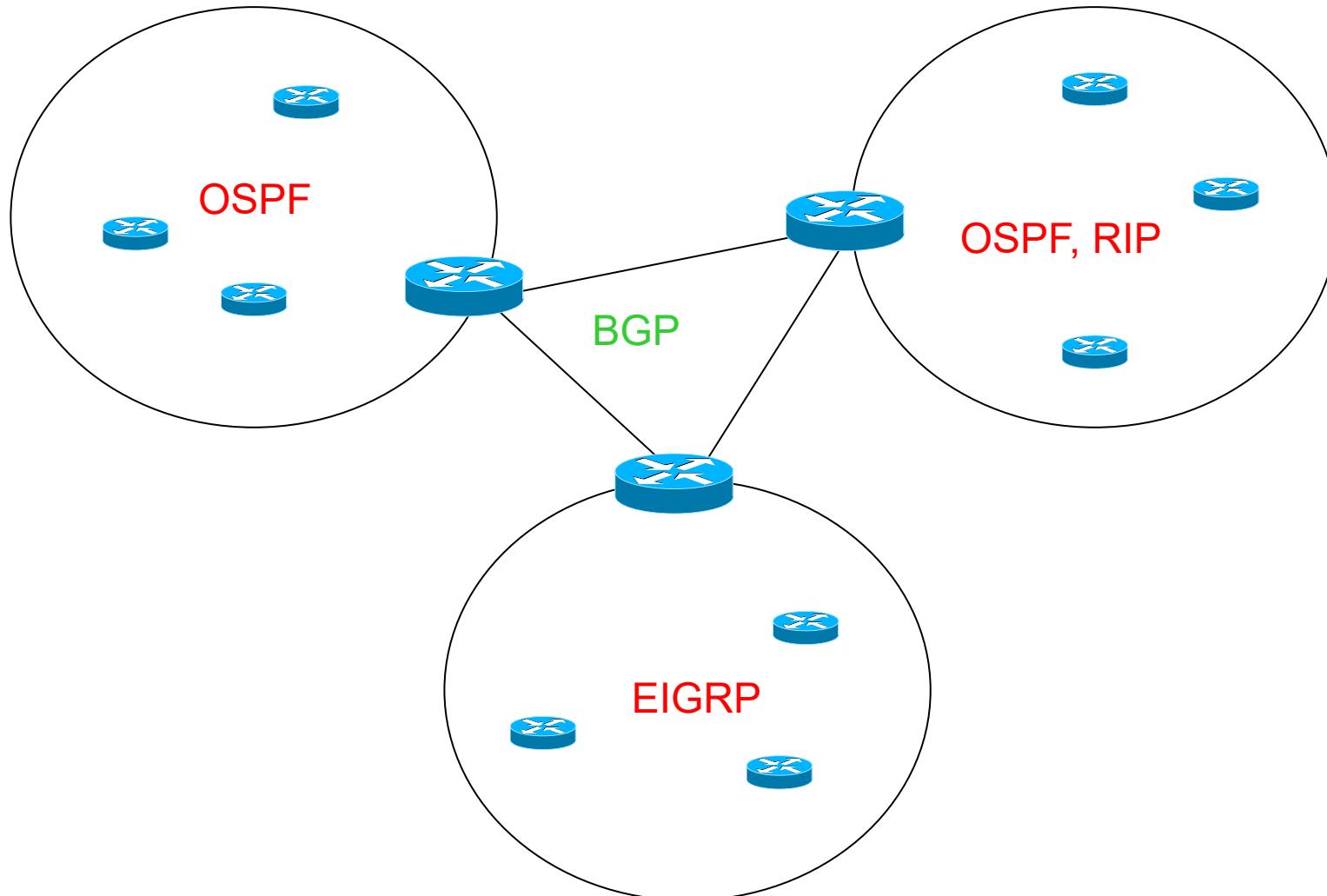
- C'est un ensemble de réseaux gérés par une seule et même entité administrative.
- C'est donc un ensemble de réseaux possédant une politique de routage qui lui est propre et indépendante.
- Internet est constitué de Systèmes Autonomes.
- Un AS est identifié par un numéro entre 1 et 65535.



Exemple



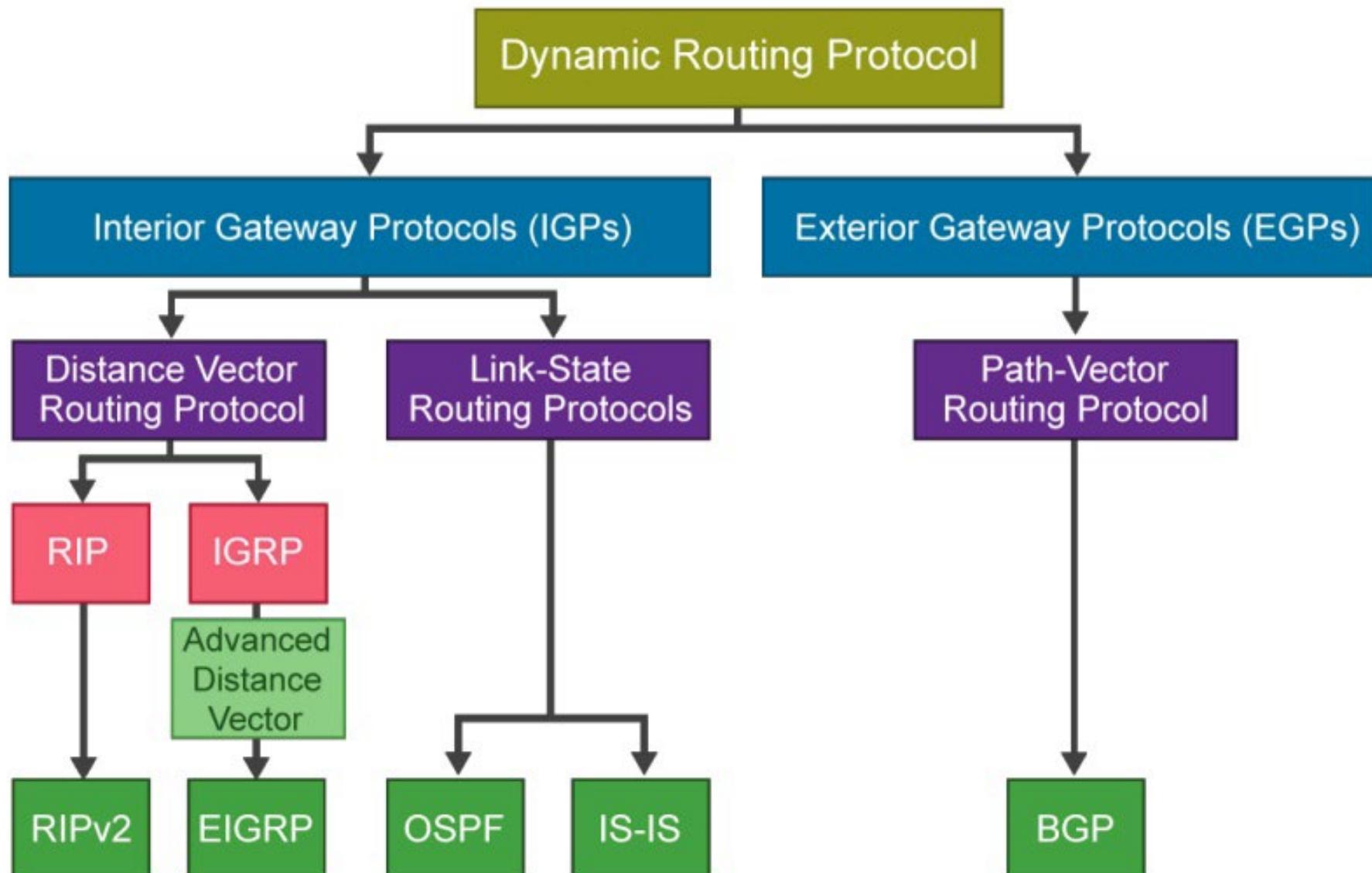
2 familles de protocoles de routage



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



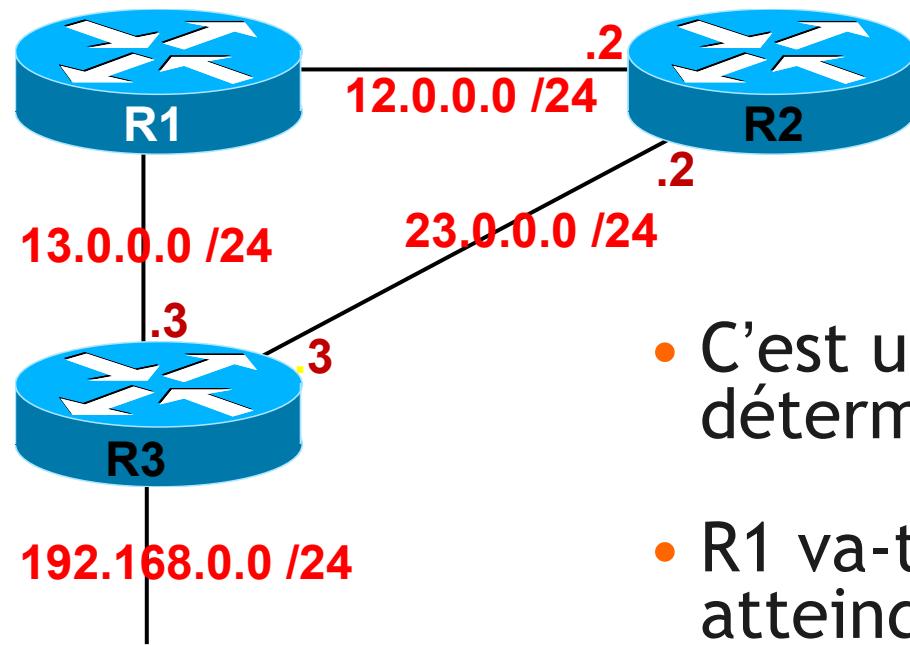
2 types de protocoles de routage

- 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

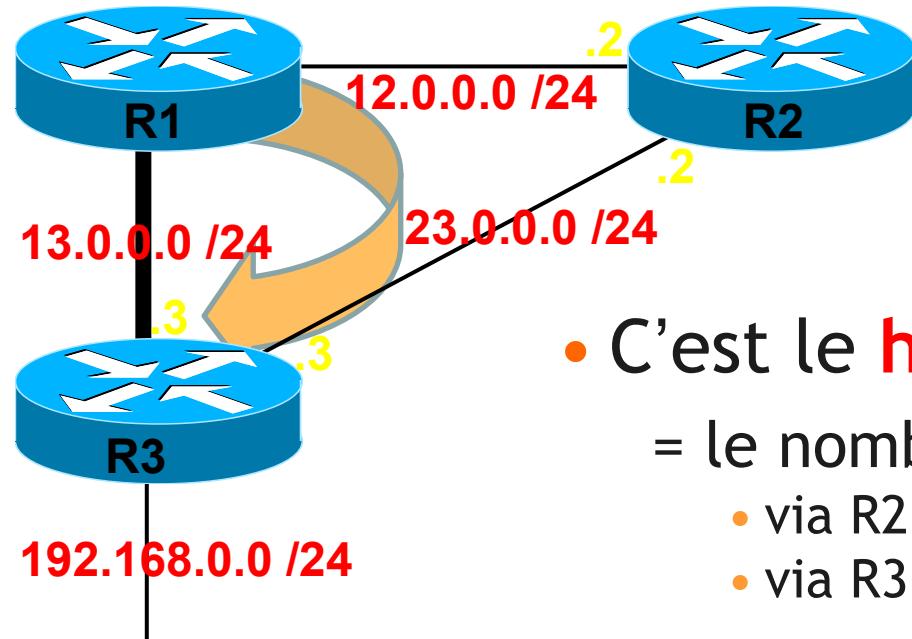
Métrique et AD

La métrique



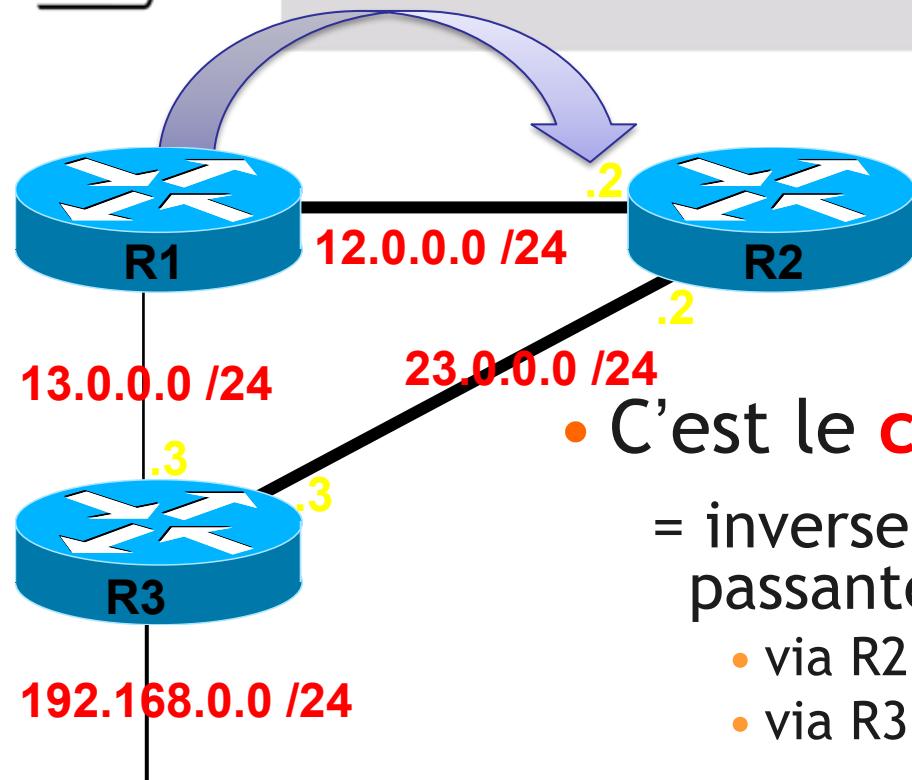
- C'est un critère utilisé pour déterminer le 'meilleur' chemin.
- R1 va-t-il passer par R2 ou R3 pour atteindre le réseau 192.168.0.0/24 ?
- R1 prendra le chemin dont la métrique est la plus **petite**.

La métrique de RIP



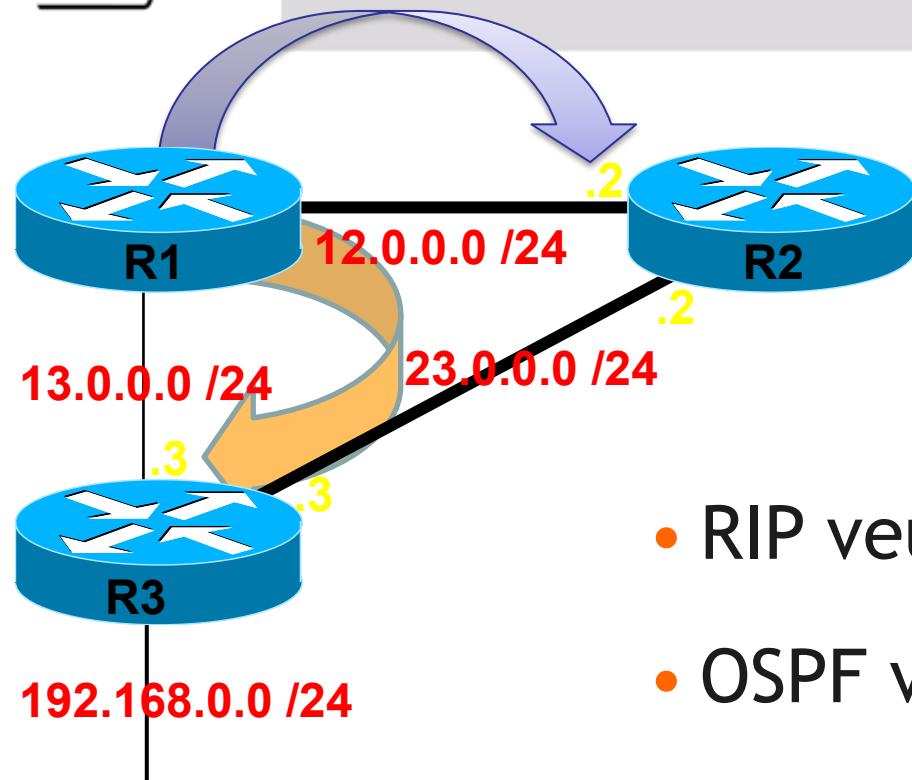
- C'est le **hop-count** :
 - = le nombre de routeurs à traverser.
 - via R2 : métrique = 2
 - via R3 : métrique = 1
- RIP indique à R1 de passer par **R3**.
- Se peut-il que RIP lui indique de passer par **R2** ?

La métrique d'OSPF



- C'est le **coût** :
 - = inversement proportionnel à la bande passante de chaque segment traversé
 - via R2, supposons une métrique de 7
 - via R3, supposons une métrique de 10
- OSPF indique à R1 de passer par **R2**.

Que DECIDE R1 ?

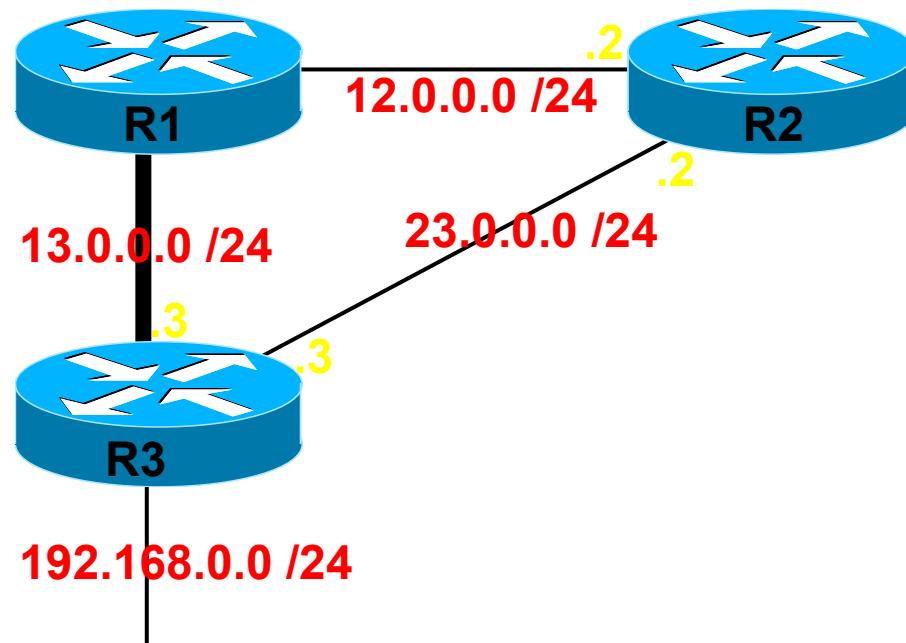


- RIP veut passer par 13.0.0.3
- OSPF veut passer par 12.0.0.2
- R1 reçoit donc 2 informations contradictoires

Comparer 2 protocoles de routage

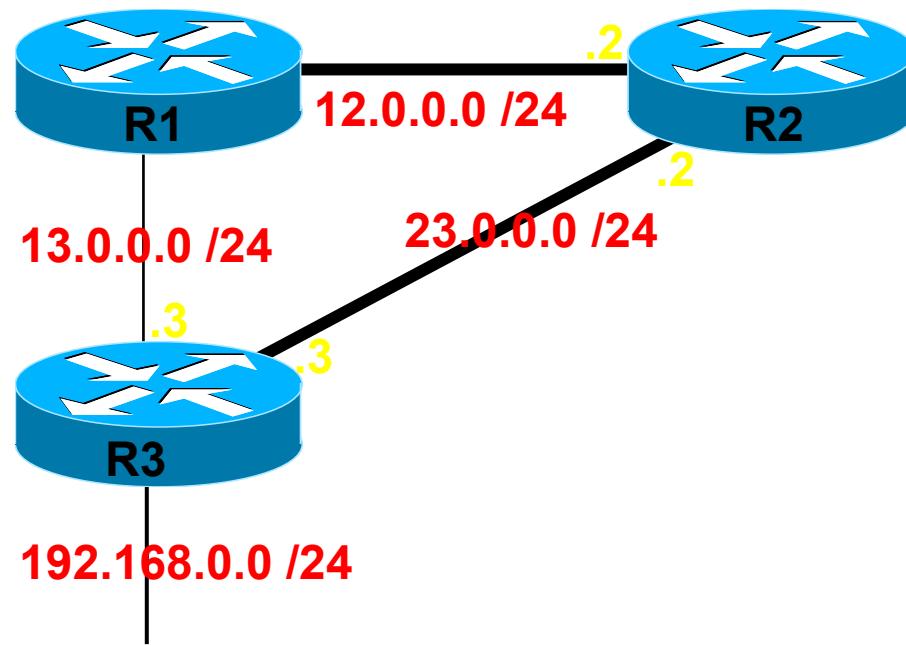
- A chaque protocole est attribué une **Distance administrative** arbitraire.
- Si 2 protocoles sont en concurrence, le routeur préfère le chemin dont la Distance administrative est la plus **petite**.
 - RIP = 120
 - OSPF = 110
 - EIGRP=90
- La distance administrative d'une route statique :
 - avec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

Show ip route avec RIP



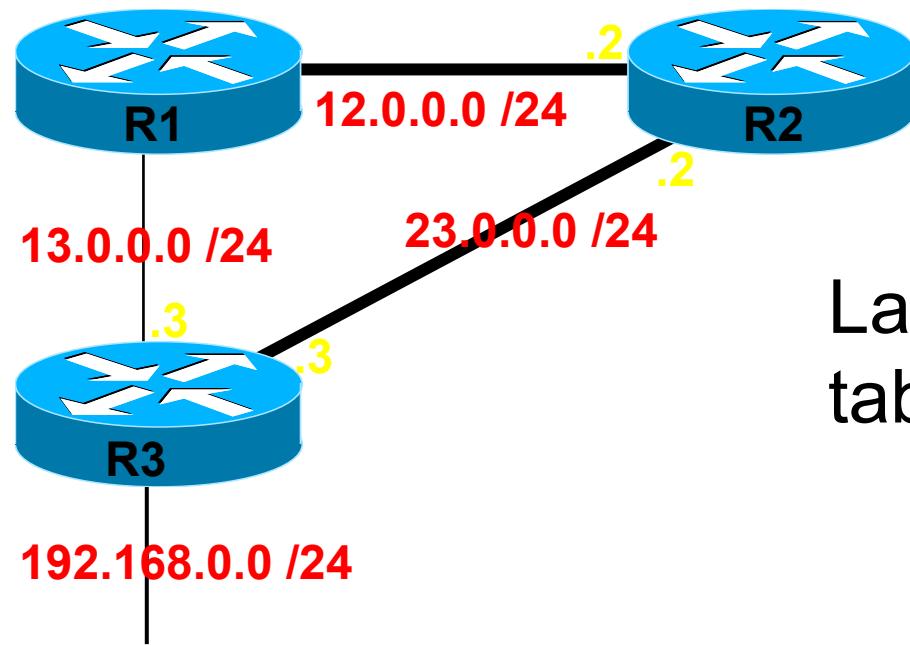
	Réseau	Masque	AD / métrique	Next-Hop	Interface
C	12.0.0.0	/24			Fa0/2
C	13.0.0.0	/24			Fa0/0
R	192.168.0.0	/24	[120 / 1]	via 13.0.0.3	

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 / 7]	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

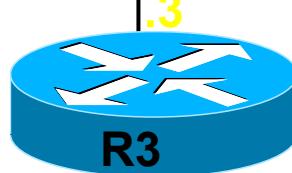
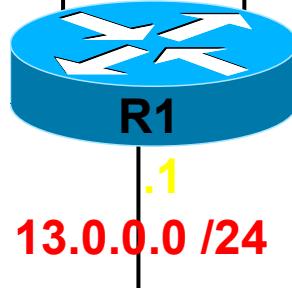
Sans summarization

réseau A
192.168.0.0 /25

réseau B
192.168.0.128 /25

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

réseau A
192.168.0.0 /25

réseau B
192.168.0.128 /25

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

13.0.0.0 /24

.3

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
- Le 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 /8
- Le 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**

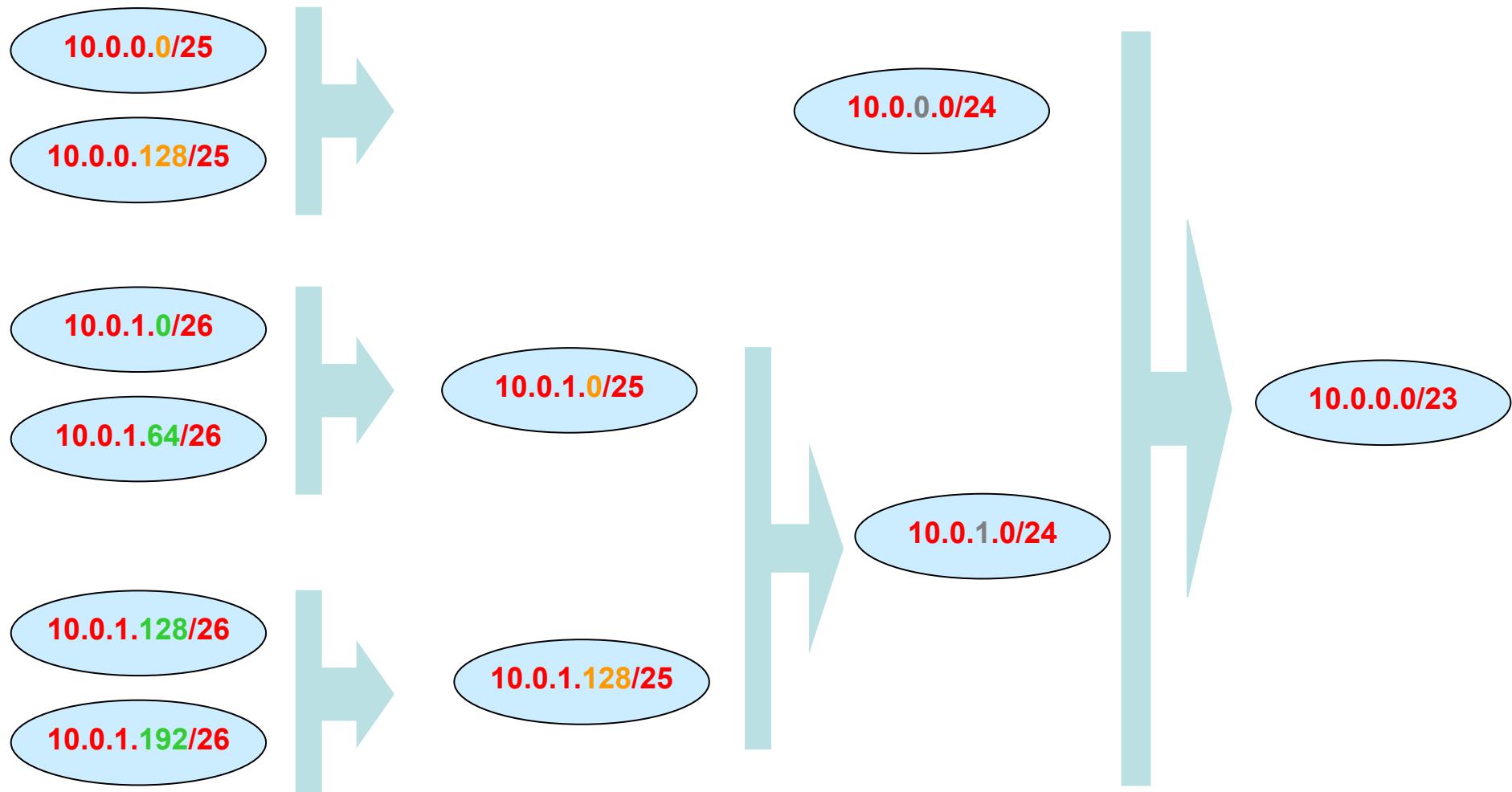
Exercice 6

- 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

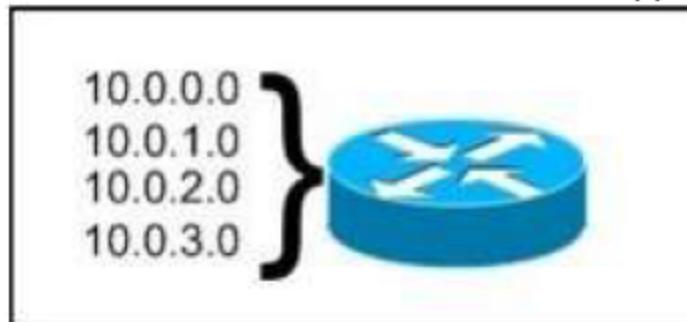
- Sous-réseaux initiaux :
 - 192.168.0.**0/26**
 - 192.168.0.**64/26**
 - 192.168.0.**128/26**
 - 192.168.0.**192/26**
- La meilleure summarization possible est :
 - 192.168.0.**0/24**

Summarizations hiérarchiques



Test

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



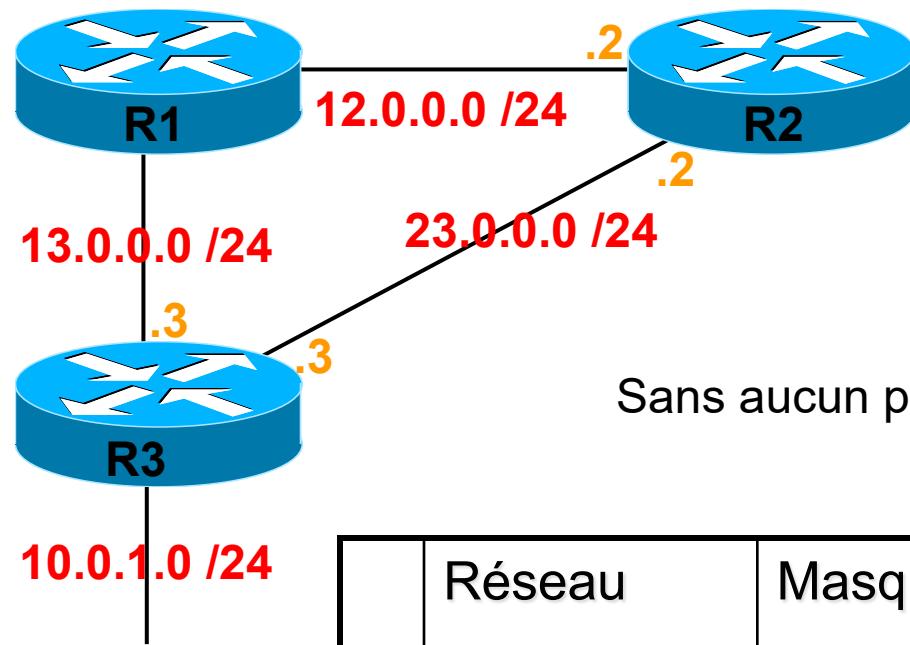
- A. 10.0.0.0 /21
- B. 10.0.0.0 /22
- C. 10.0.0.0 /23
- D. 10.0.0.0 /24

Correct Answer: B

Routage dynamique

Maîtriser la Table de routage

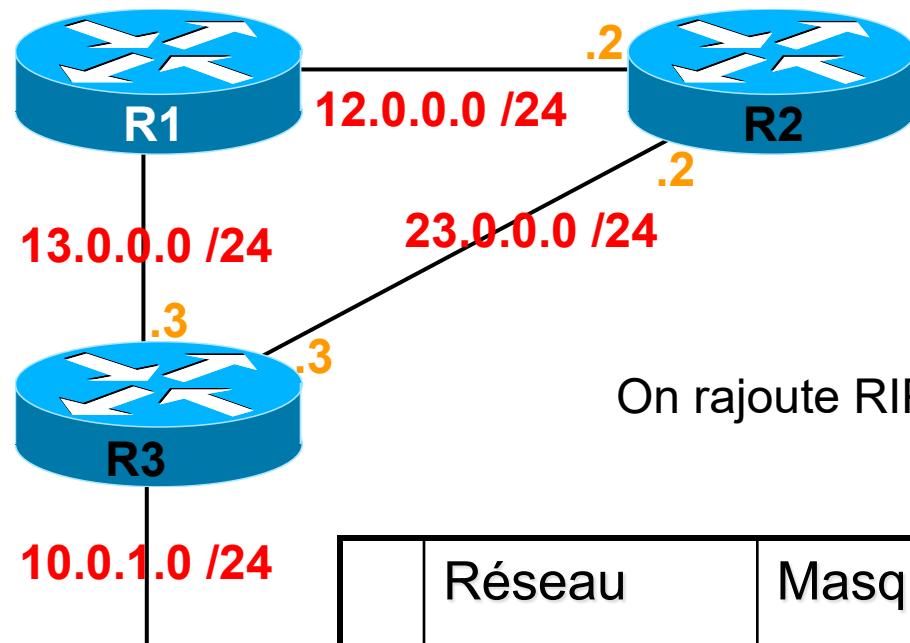
Exemple 1/3



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

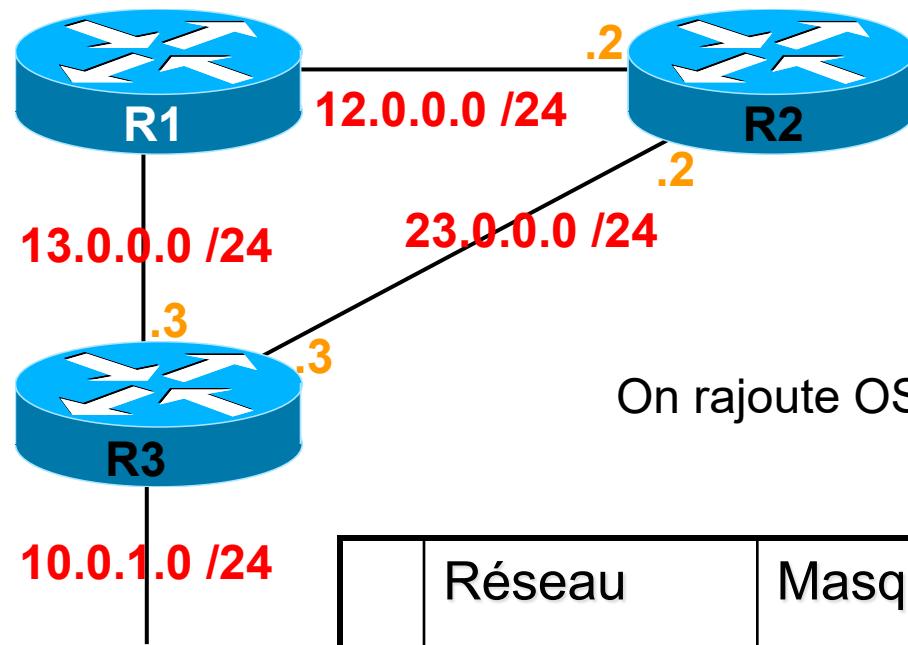
Exemple 2/3 sur R1



On rajoute RIP entre R1, R2 et 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	

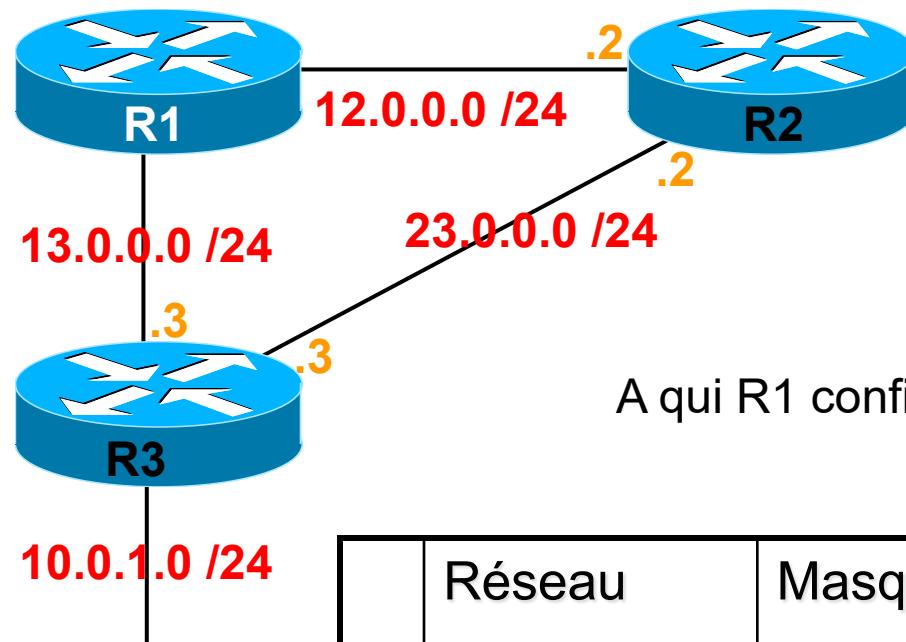
Exemple 3/3



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	

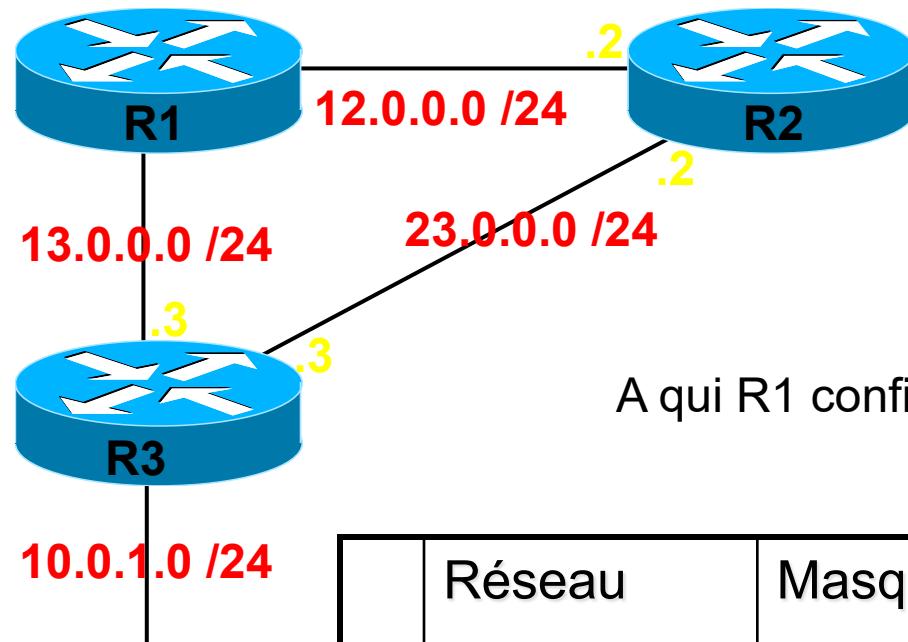
Exploitation de la table - Cas 1



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	Fa0/0
O	10.0.1.0	/24	[110 / 20]	12.0.0.2	Fa0/2

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	

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.

Règle de sélection du meilleur chemin.

```
ROUTER# show ip route
```

```
10.0.0.0/24 is subnetted, 3 subnets,  
R      10.1.1.0/24 [120/1] via 10.1.2.2, 00:00:05, Ethernet0  
C      10.1.2.0/24 is directly connected, Ethernet0  
O      10.1.0.0/16 [110/200] via 10.1.2.3, 00:00:05, Ethernet0  
R      192.168.24.0/24 [120/2] via 10.1.2.2, 00:00:16, Ethernet0
```

**1^{er} critère :
LONGUEUR du
MASQUE**

**2^{ème}
critère :
AD**

**3^{ème}
critère :
METRIQUE**

**PARTAGE de CHARGE
entre les NEXT HOP**

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

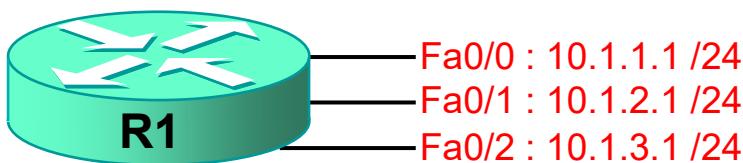
signifie :

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

Exemples

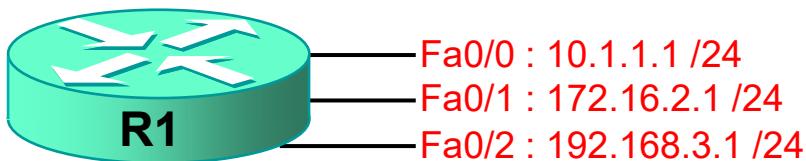
- network 11.0.0.0
- activer RIP sur toutes les interfaces en 11.0.0.0 /8
- network 111.0.0.0
- activer RIP sur toutes les interfaces en 111.0.0.0 /8
- network 131.0.0.0
- activer RIP sur toutes les interfaces en 131.0.0.0 /16
- network 211.0.0.0
- activer RIP sur toutes les interfaces en 211.0.0.0 /24

Exercice 1



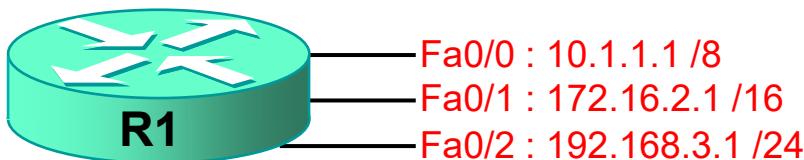
- Activer RIP sur toutes les interfaces
- `router rip`
- `network 10.0.0.0`

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

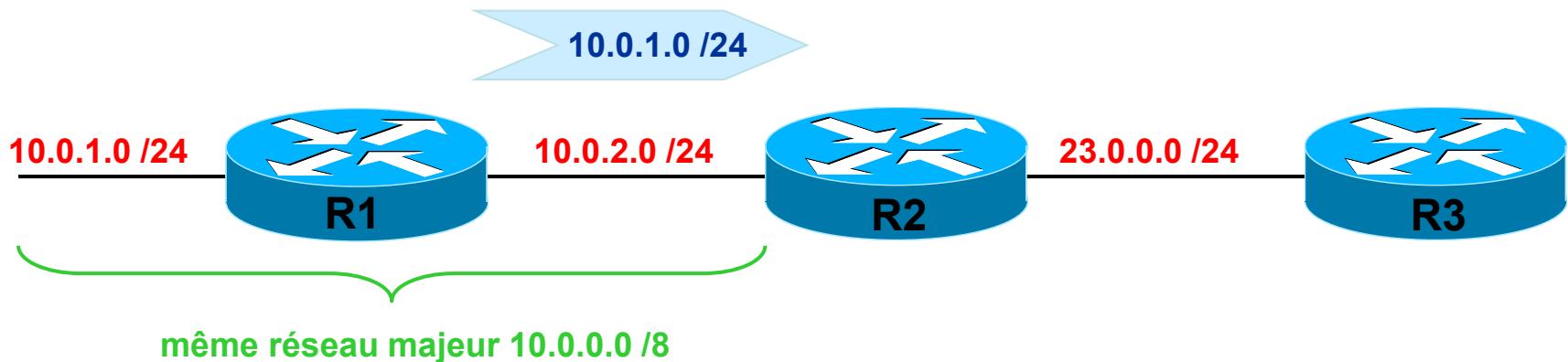
maximum-path 16

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.

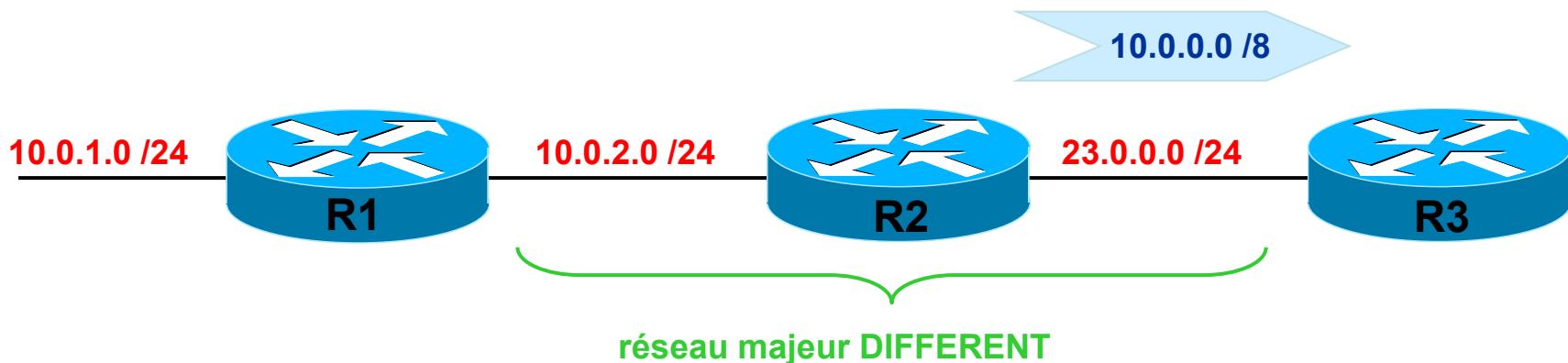
Exemple



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

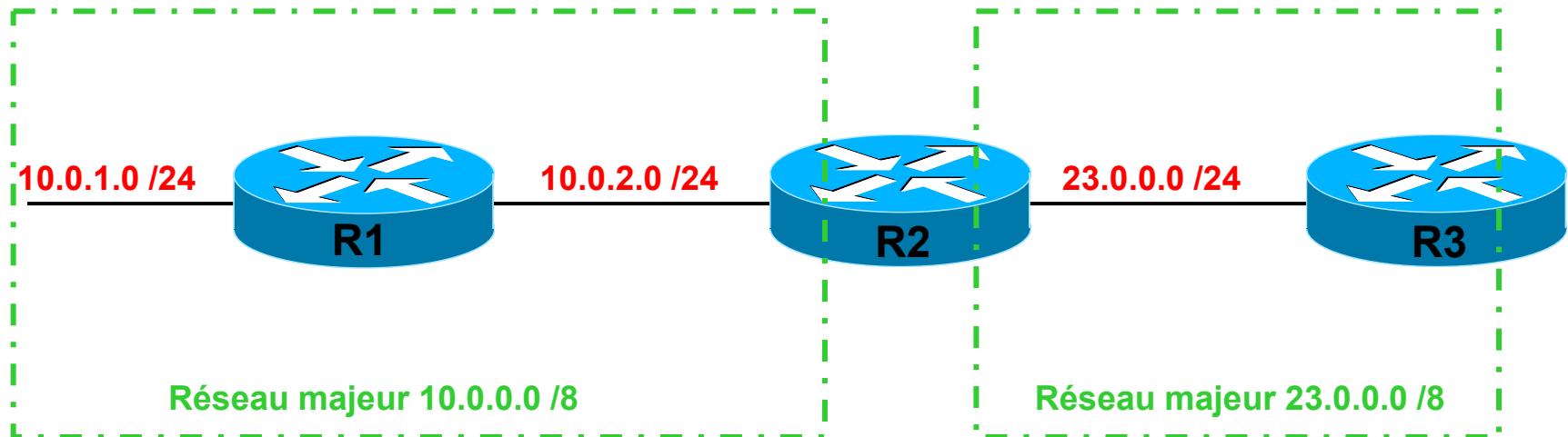
Exemple, suite



Annonce du réseau $10.0.1.0/24$ de R2 à R3 :

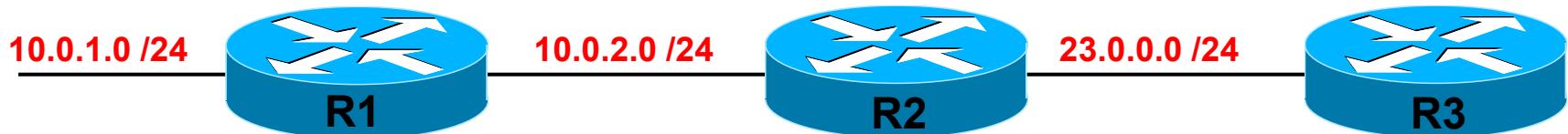
- R2 envoie cette annonce à R3.
- Le sous-réseau entre R2 et R3 est $23.0.0.0 /24$.
- $10.0.1.0/24$ et $23.0.0.0 /24$ n'appartiennent pas au même réseau majeur.
- R2 applique DONC la summarization automatique.
- R2 annonce donc $10.0.0.0 /8$ à R2

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	/8

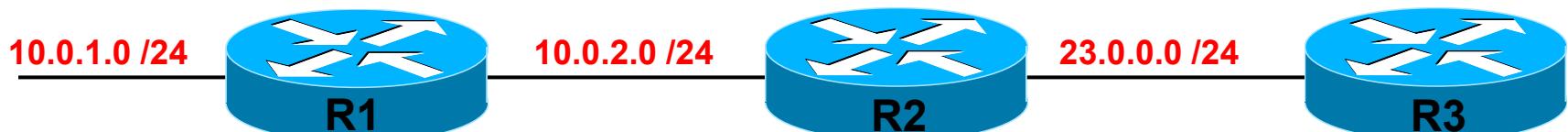
	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24

	Réseau	Masque
R	10.0.0.0	/8
C	23.0.0.0	/24

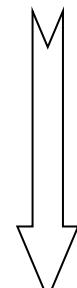
Désactiver

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

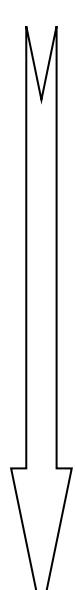
Avec no auto-summary



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

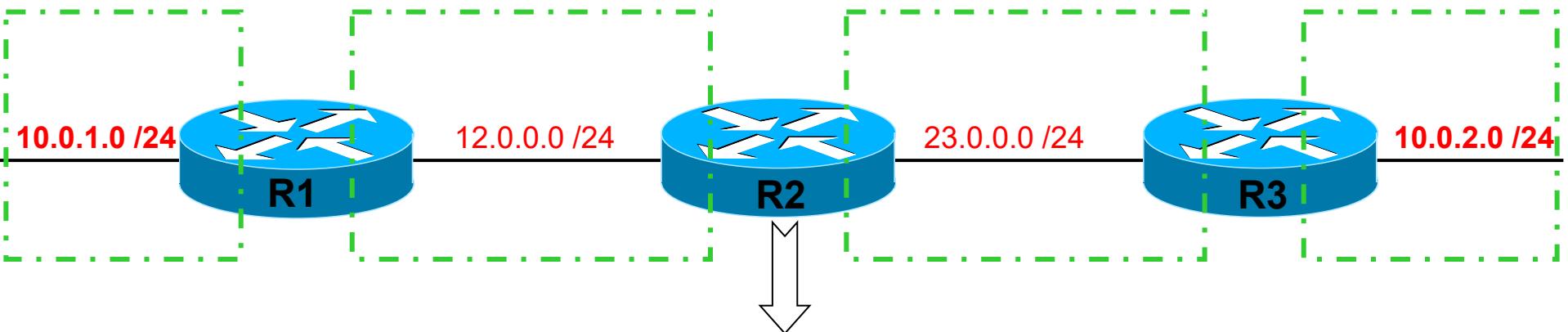


	Réseau	Masque
X	10.0.1.0	/24
C	10.0.2.0	/24
C	23.0.0.0	/24



	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

En VERSION 2, RIP sait indiquer
le masque des réseaux qu'il annonce.

Va-t-il toujours annoncer le vrai masque ?

NON !

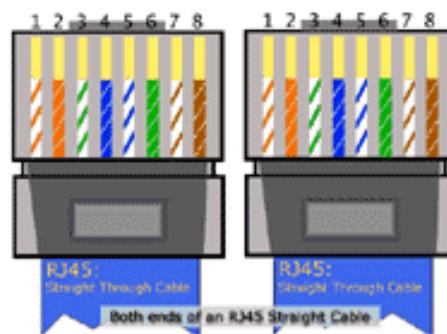
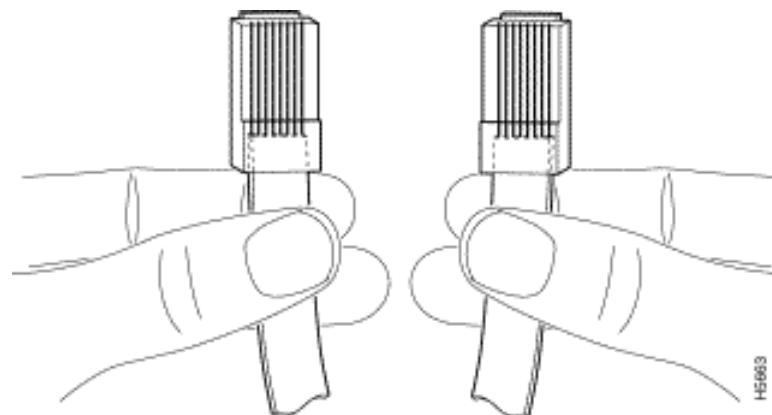
Annoncer le vrai masque

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

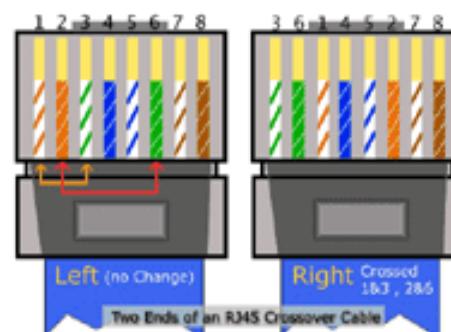
Switching

**Differents types de cables :
Droits, Croisés, Rollover**

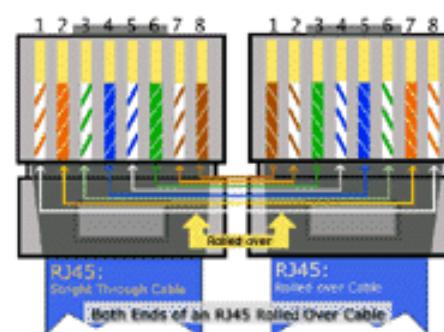
3 types de cables



droit

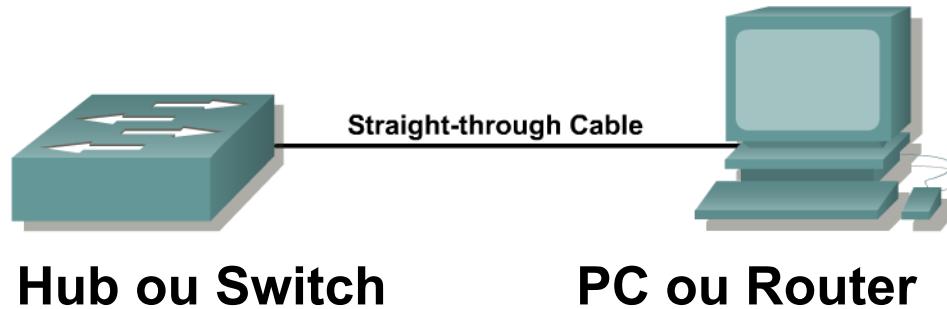


Croisé



Rollover

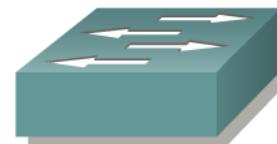
Le cable droit



- Le cable droit connecte des équipements de nature différentes.

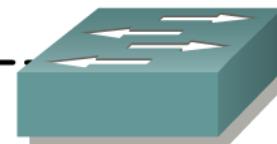
Cable croisé

Hub ou Switch



Crossover Cable

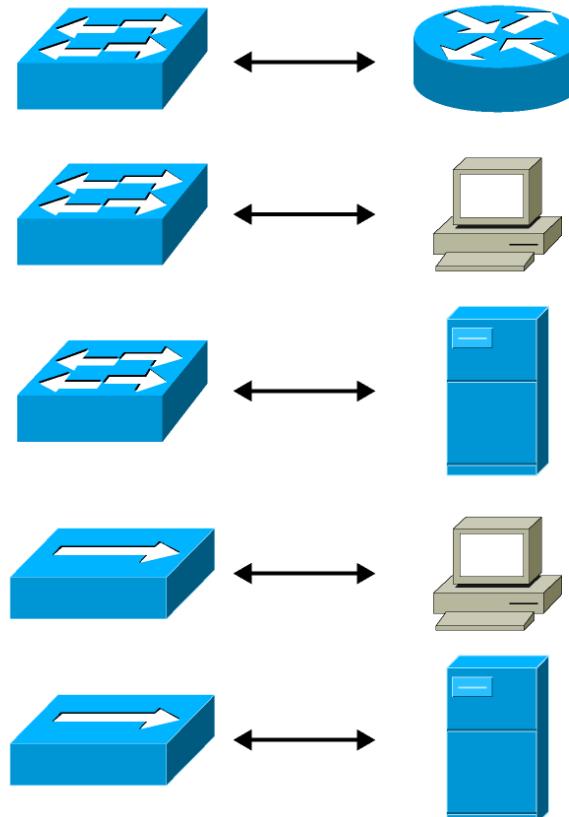
Hub ou Switch



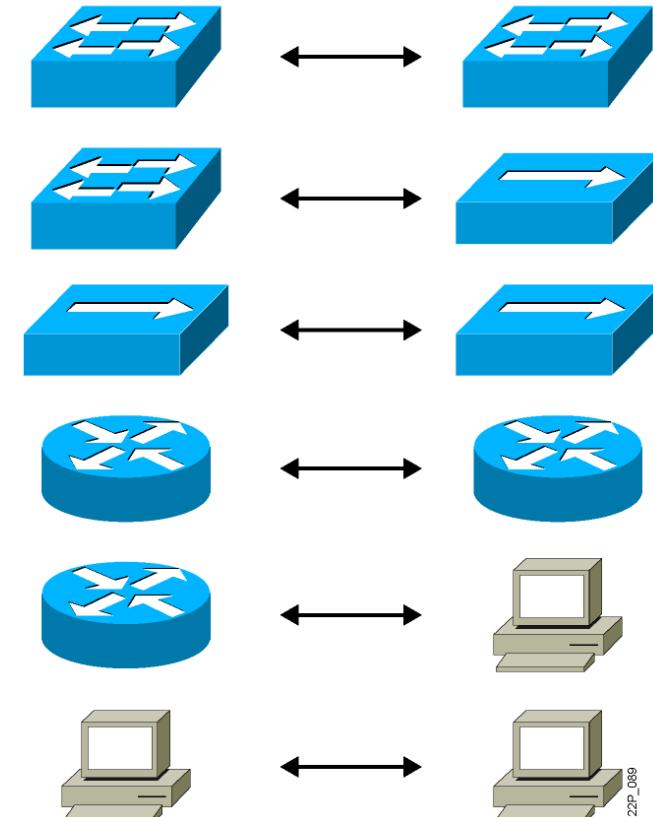
- Pour interconnecter les switchs
- Connecte les port de même nature

Droit, versus croisé

Straight-Through Cable

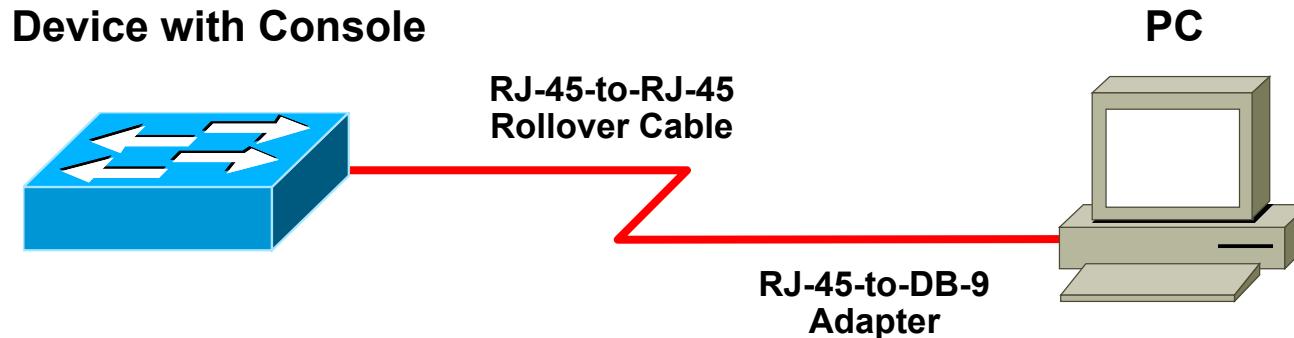


Crossover Cable



022P_089

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** :

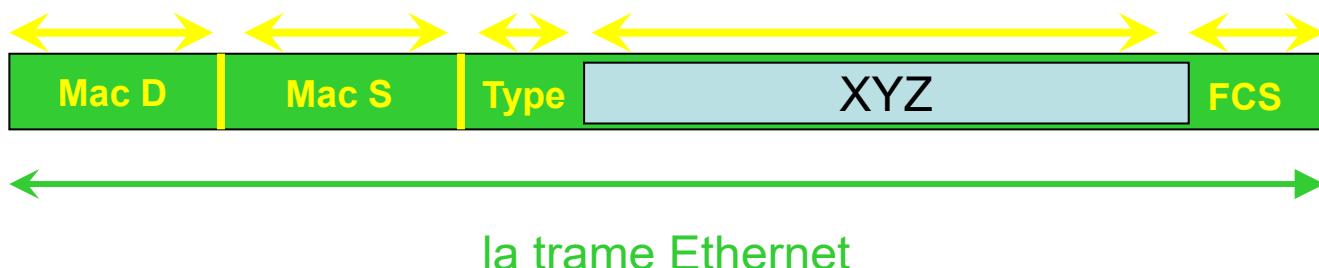


Ethernet Frame Structure

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
 - l'adresse MAC source
 - le type
- La partie **utile** entre 46 et 1500 octets
- Le pied de la trame Ethernet contient :
 - FCS, Frame Check Sequence 4 octets

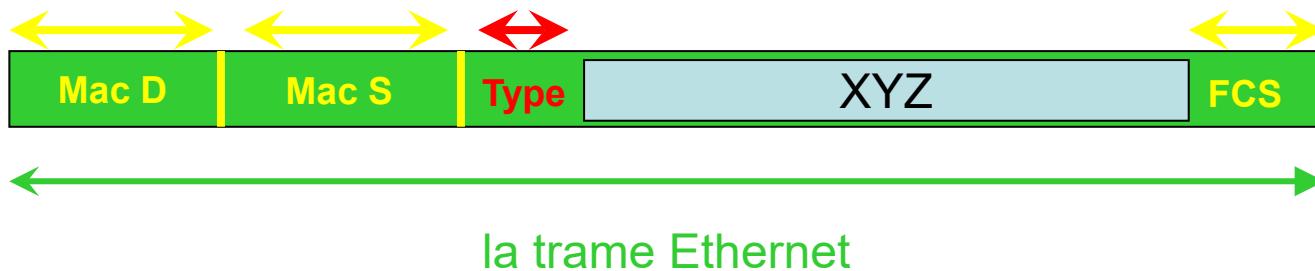


Taille de la trame

- Taille maximale de la trame :
 - $= 14 + 1500 + 4 = \textcolor{red}{1518}$ octets
- Taille minimale de la trame :
 - $= 14 + 46 + 4 = \textcolor{green}{64}$ 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'



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 hexadécimaux
 - 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 7^{ème} bit est égal à 0.

Si le 7^{ème} bit vaut 1, alors il s'agit d'une adresse MAC administrée localement.

Unicité de l' adresse MAC

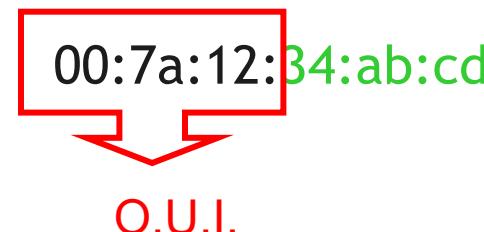
- L'adresse MAC est composée de 2 parties :
 - partie ‘O.U.I.’ :
 - Organizational Unique Identifier
 - 3 octets
 - attribués par IANA
 - partie ‘constructeur’
 - 3 octets
 - attribués par le Constructeur
- Exemples :

• 007a.12 34.abcd



The diagram shows the MAC address 007a.12 34.abcd. A red box highlights the first three segments (007a.12) and another red box highlights the last four segments (34.abcd). Two red arrows point from these boxes down to the text "O.U.I.".

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



The diagram shows the MAC address 00:7a:12:34:ab:cd. A red box highlights the first three segments (00:7a:12) and another red box highlights the last four segments (34:ab:cd). Two red arrows point from these boxes down to the text "O.U.I."

Ethernet

Les trois types de trames

Types de trames

- **Unicast**

- un équipement veut parler avec un autre équipement

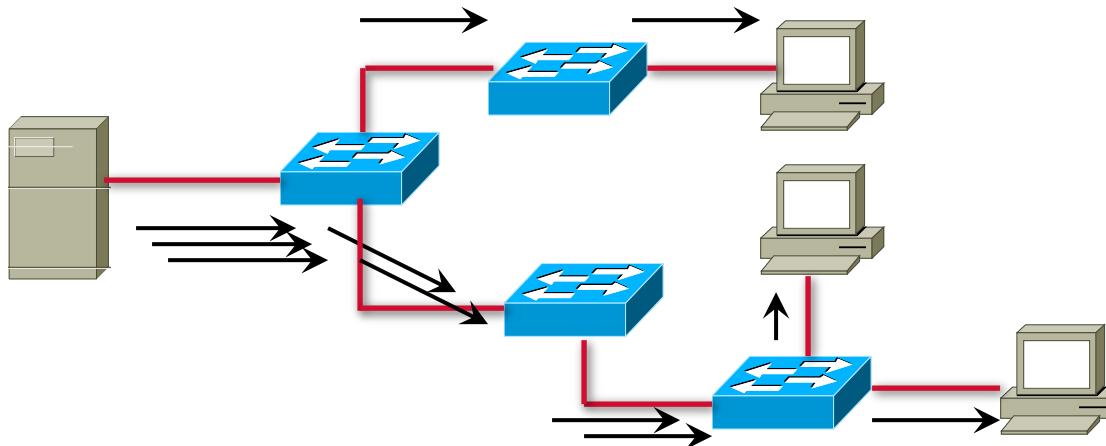
- **Broadcast :**

- un équipement veut parler avec tous les autres équipements de son réseau.

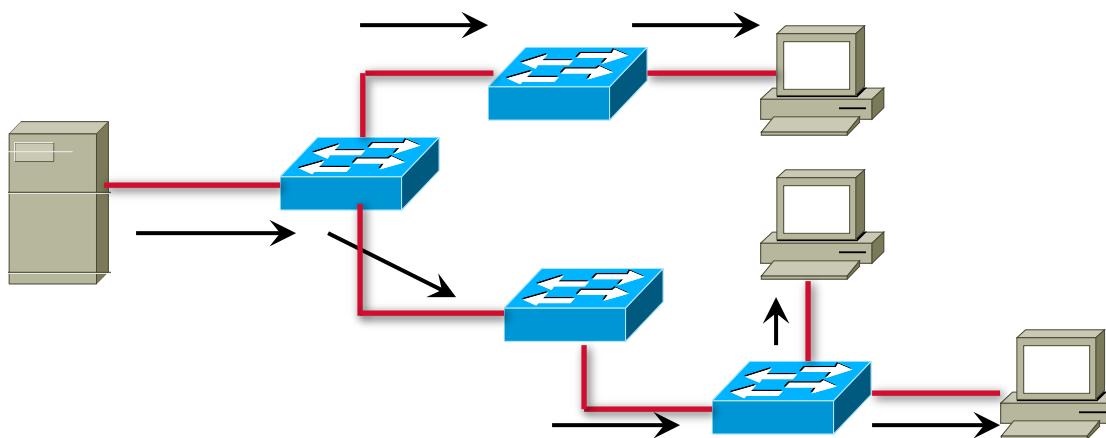
- **Multicast :**

- un équipement veut parler avec plusieurs autres équipements mais pas tous

Intérêts d' un broadcast



Unicast

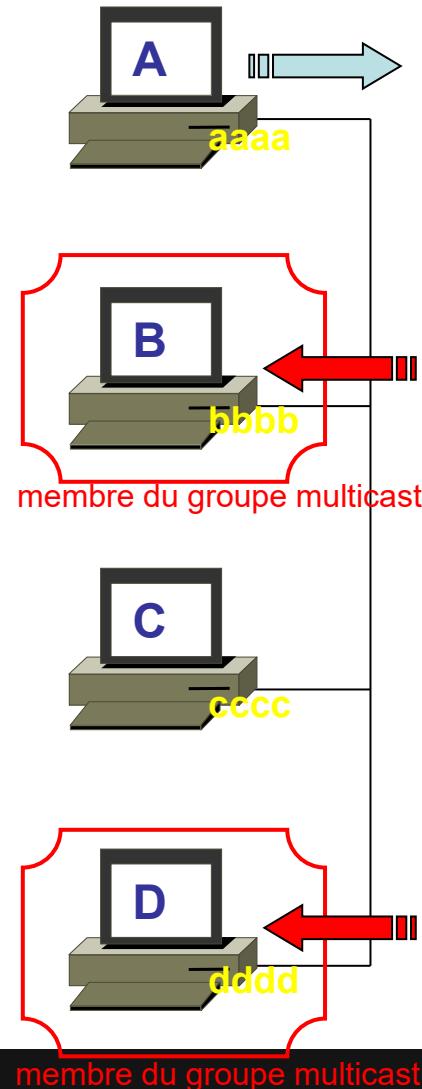


Broadcast

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



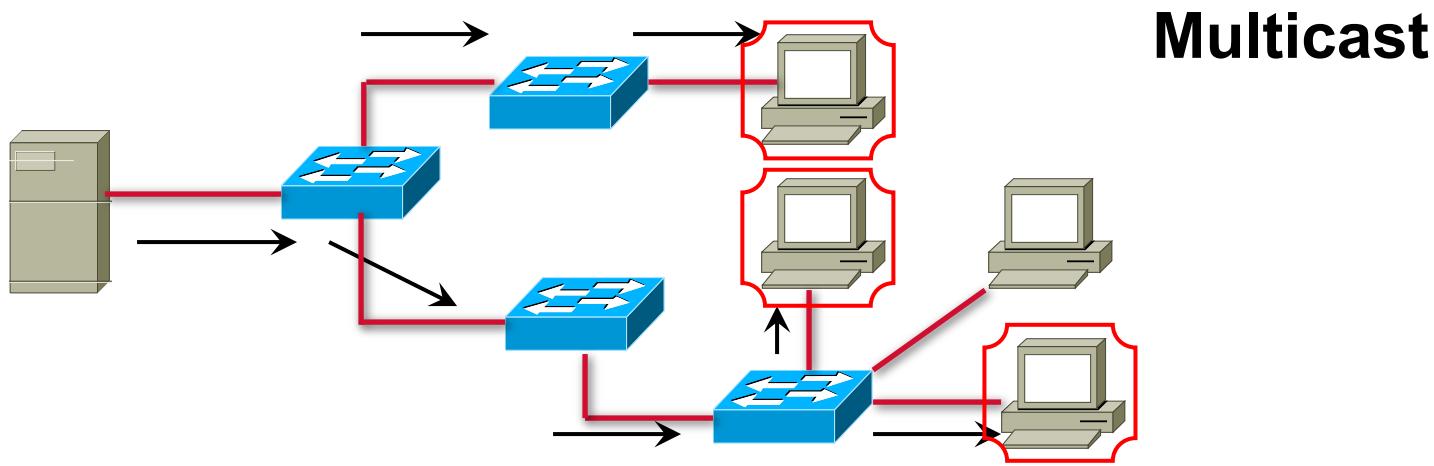
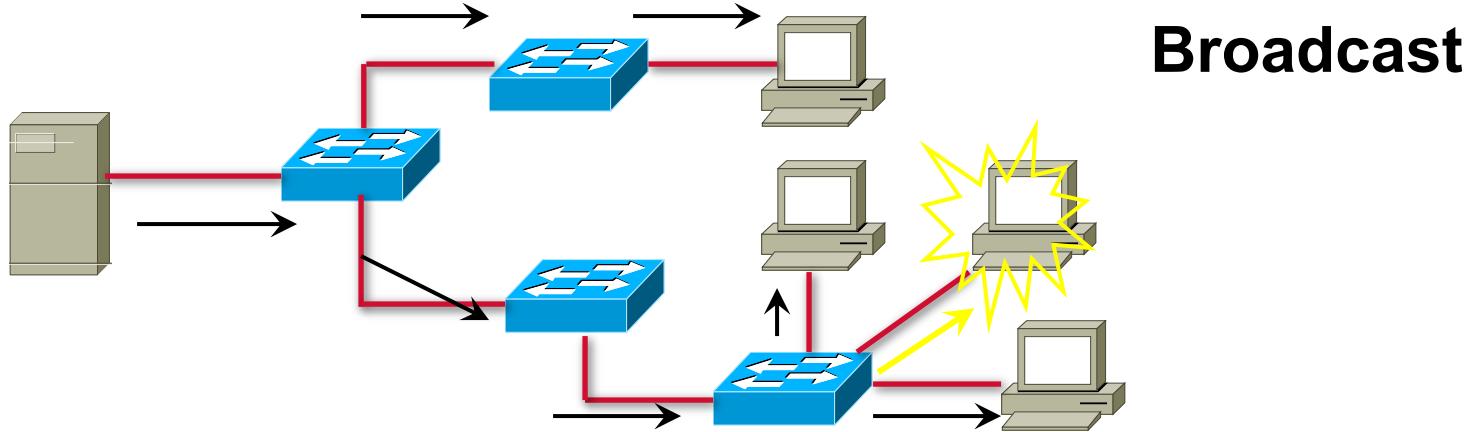
- Utiliser l'adresse MAC destinataire qui identifie les membres du groupe multicast :
 - le 8^{ème} bit est égal à 1
 - exemple : 0100.5E01.1111
- Exemple : multicast de A pour 0100.5E01.1111



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



Ethernet

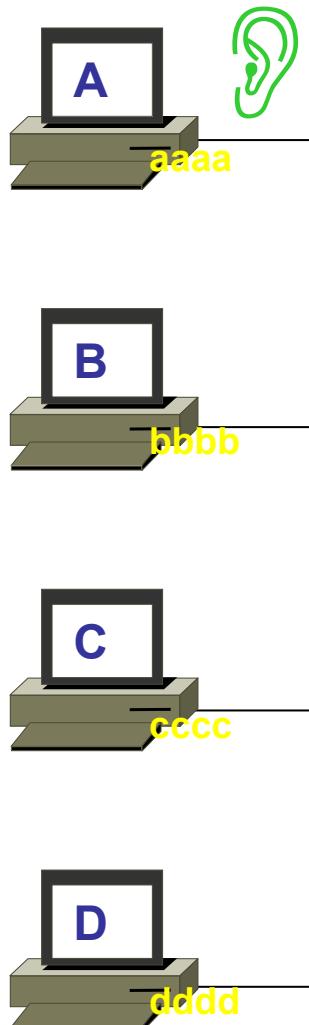
Les collisions

CSMA / CD : toutes les étapes

Un équipement veut envoyer une trame sur le réseau :

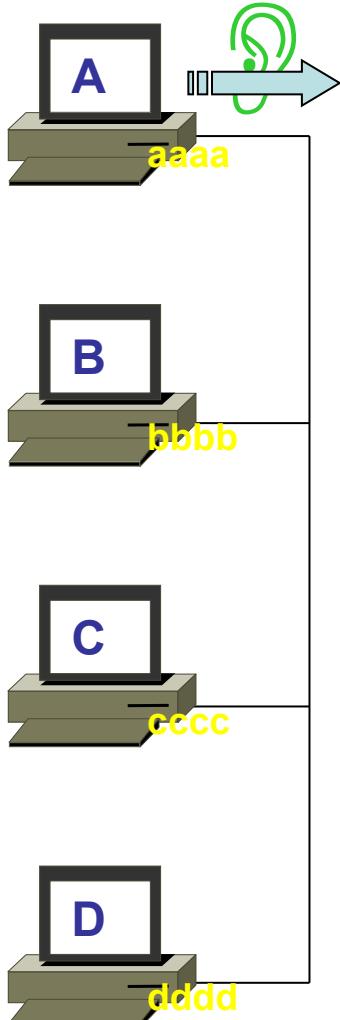
1. Il écoute le réseau pour voir s' il est libre.
2. Si le réseau est libre, il commence à déposer sa trame
3. Il continue à écouter le réseau pour vérifier qu' il est le seul à l' utiliser
 1. il compare ce qu' il dépose sur le réseau avec ce qu' il entend sur le réseau
4. S' il y a divergence, cela 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



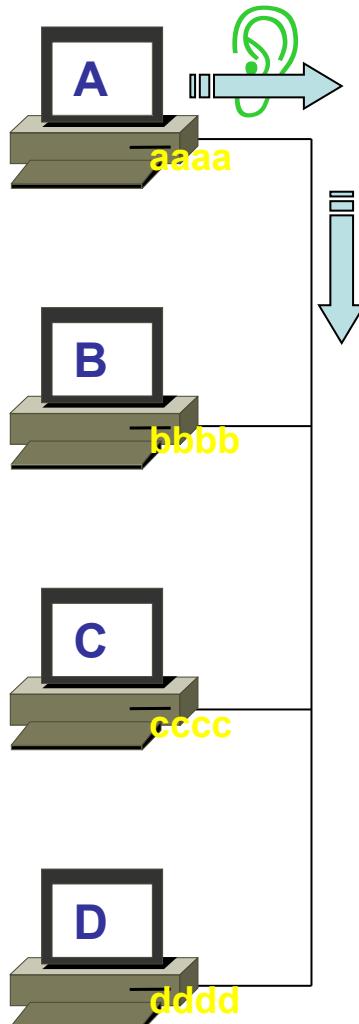
- Y a-t-il déjà du trafic sur le réseau ?

2. A dépose sa trame



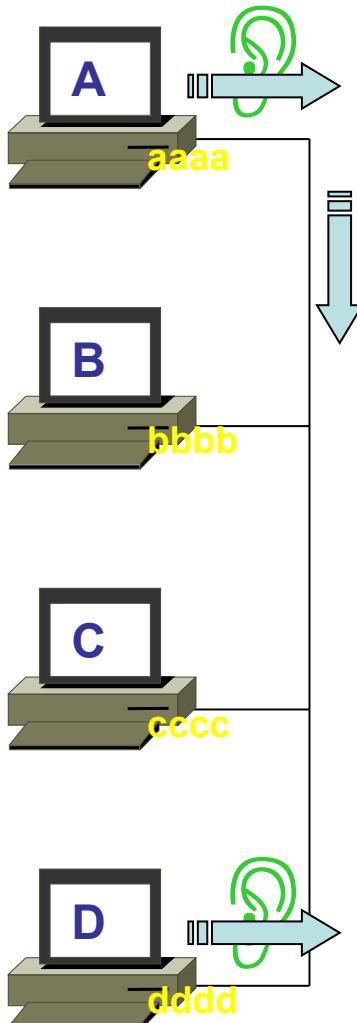
- Pas de trafic.
- La voie est libre.
- A dépose sa trame et continue à écouter
- A vérifie que ses données ne sont pas perturbées par l'émission d'un autre équipement

3. Propagation de la trame



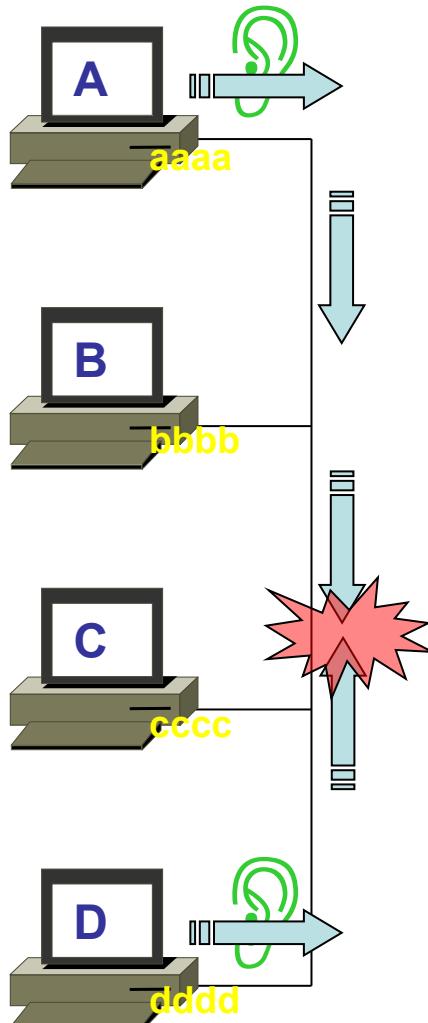
- La trame déposée par A se propage dans le réseau.
- Elle n'a pas encore atteint D
- D veut également envoyer une trame.

4. D dépose sa trame



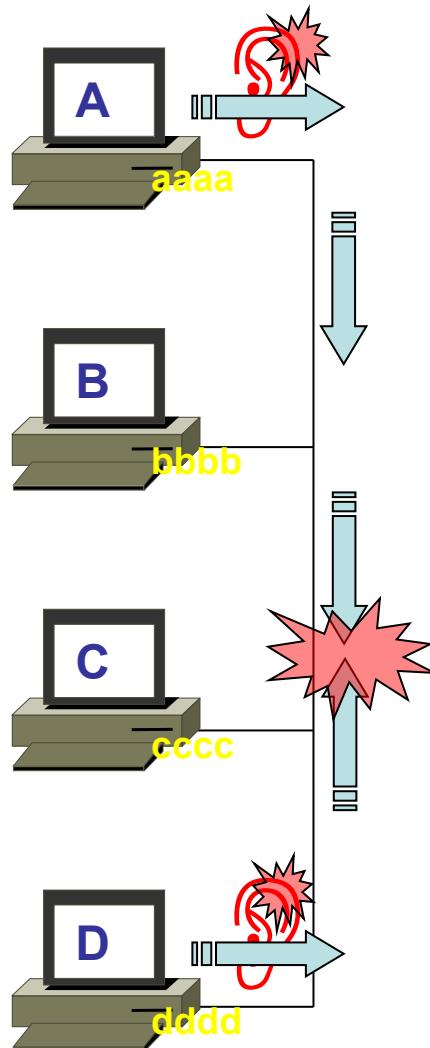
- La trame de A n'a pas atteint D.
- D écoute le réseau : il croit que le réseau est libre.
- D dépose sa trame

4. Collision



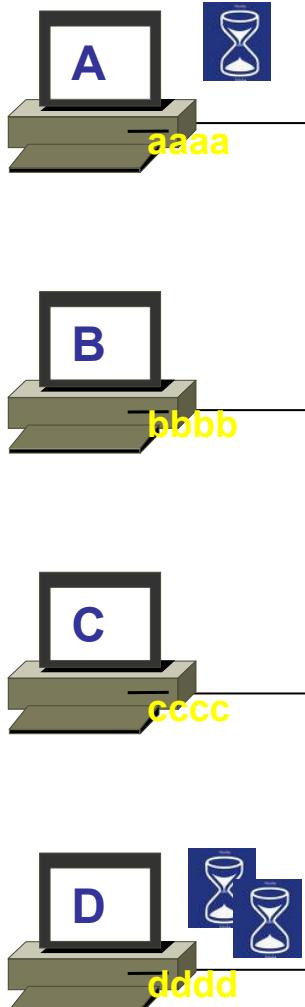
- Les 2 trames se rencontrent.
- Les trames n'ont pas pu être entièrement déposées sur le réseau :
 - on parle alors de **fragments**

5. Détection de la collision



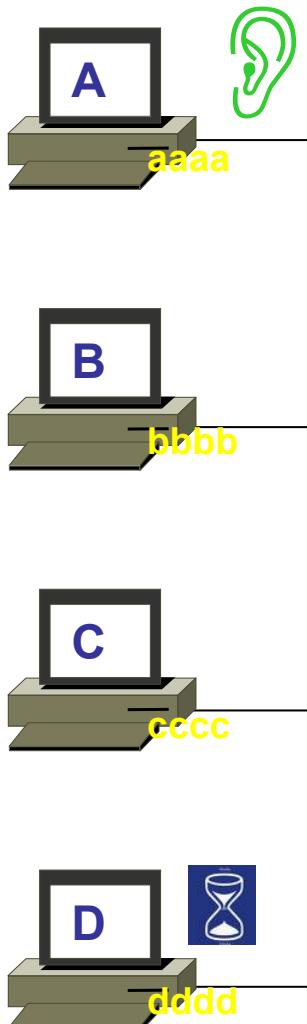
- A et D constatent qu' il y a divergence entre ce qu' ils envoient et ce qu' ils entendent.

6. Arrêt de l'émission



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

6. Nouvel essai



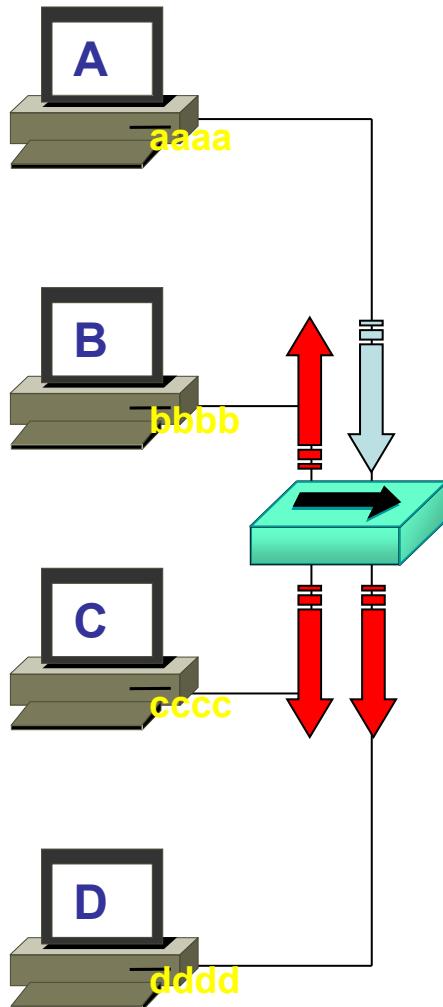
- D attend plus longtemps que A.
- Donc A essaie à nouveau d'émettre : il commence par écouter le réseau.

- 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

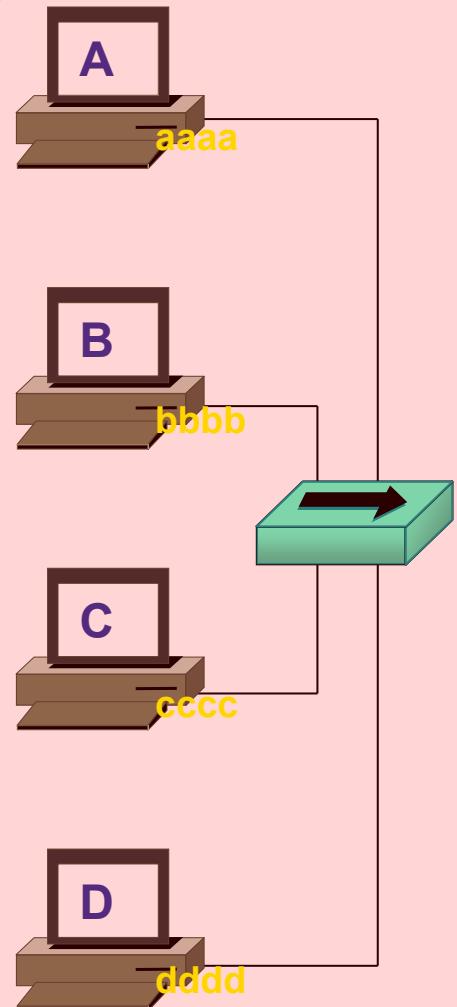
Le HUB

Fonctionnement du HUB



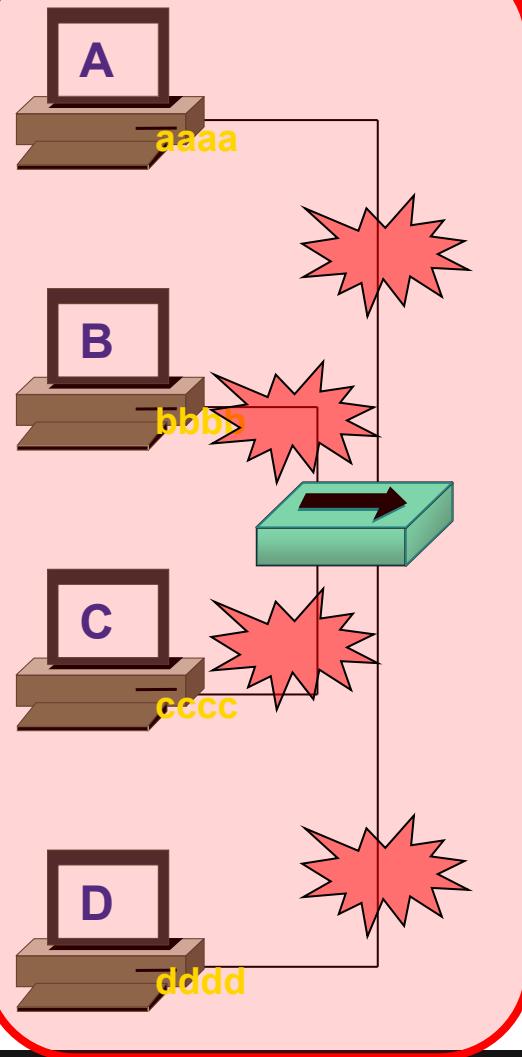
- Il reçoit une trame sur une interface.
- Il la duplique sur **toutes les autres** interfaces, quel que soit le type de trame : unicast, broadcast, multicast

Domaine de collision



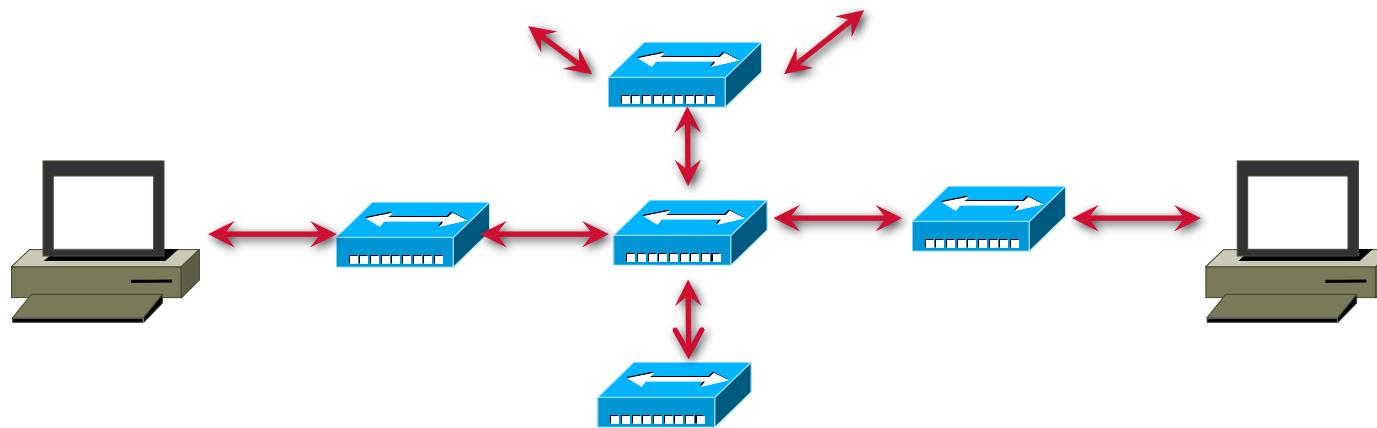
- Tous les équipements placés autour d'un même HUB peuvent avoir des collisions entre eux :
- Ils sont dans **le même domaine de collision**.

Domaine de collision

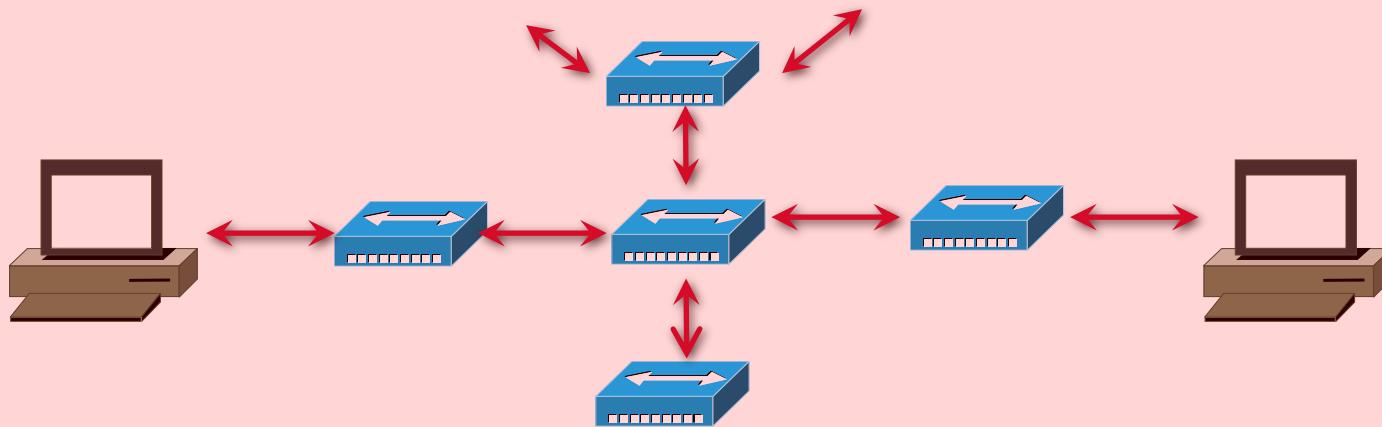


- Si une collision se produit sur un segment :
 - il se répand sur tous les segments autour du HUB
 - tout le réseau est impacté
 - aucun équipement ne peut utiliser la bande passante

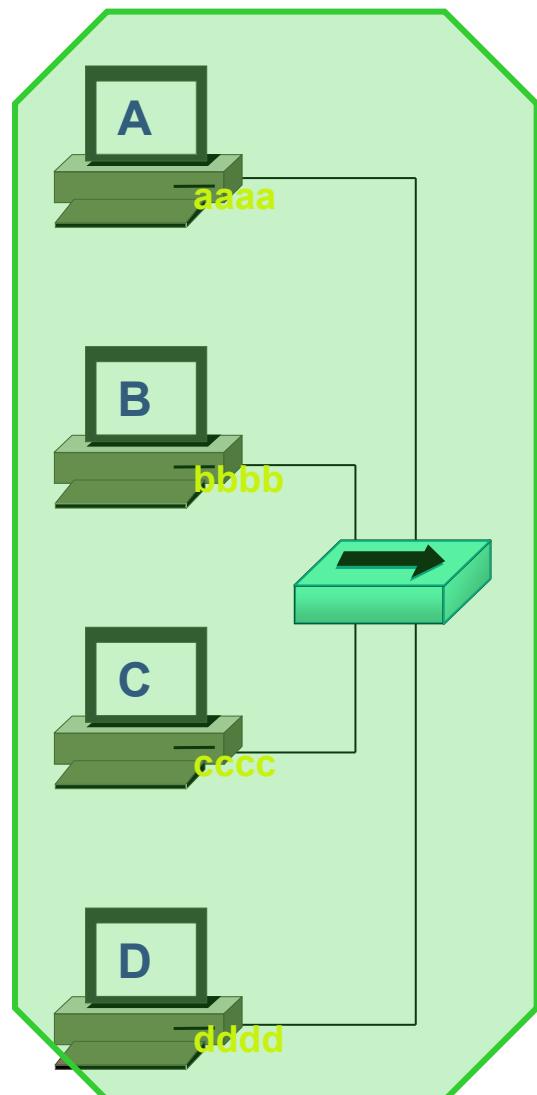
Combien de domaines de collision?



Un seul

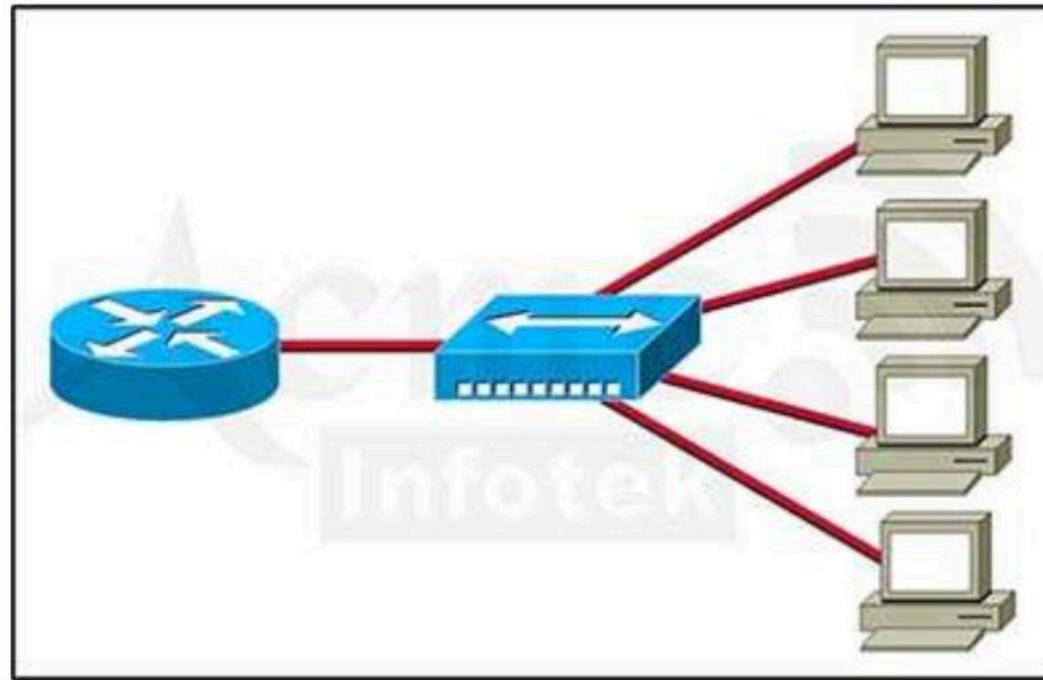


Domaine de broadcast



- Un équipement placé 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 ? • 1
- Combien de domaines de broadcast ? • 1

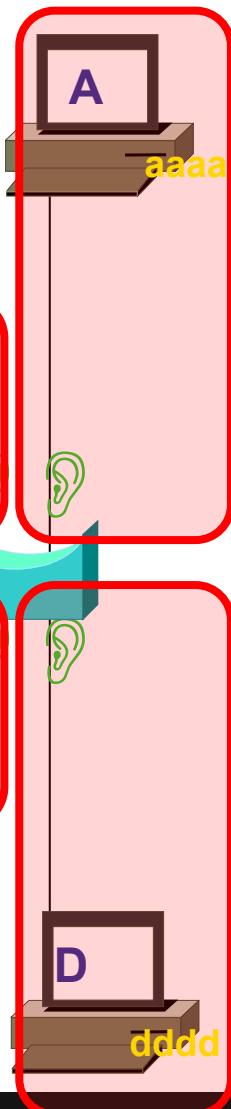
Ethernet

Le PONT

Fonctionnement du PONT

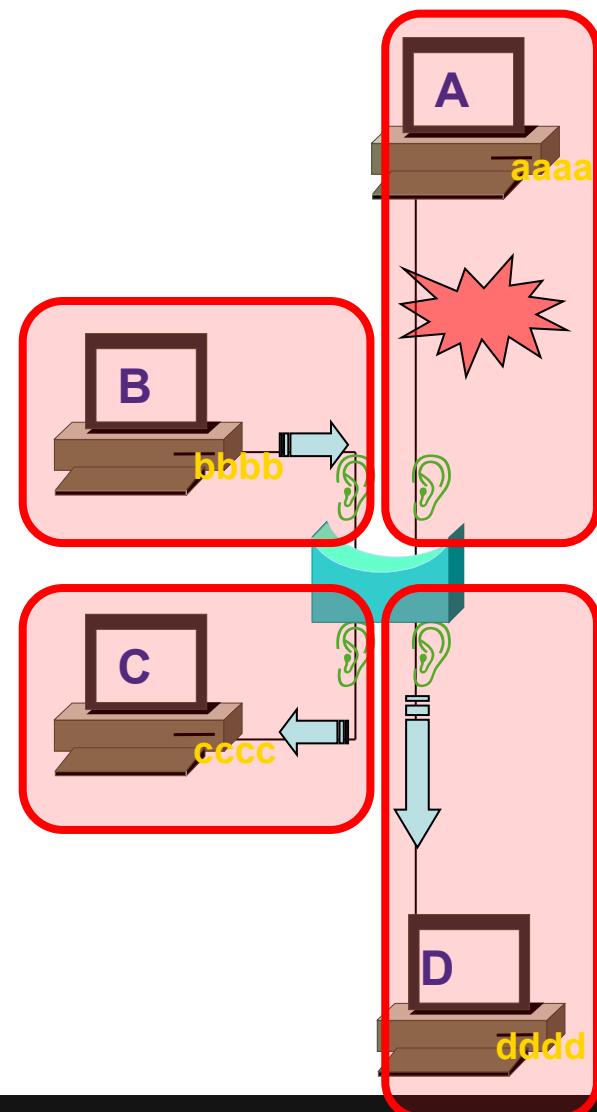
- Le PONT a une mémoire sur chaque interface.
 - Il est donc capable de conserver des trames dans cette mémoire, le temps que la voie devienne libre.
 - Il écoute sur chaque interface, avant de faire suivre une trame.
 - Les fragments restent confinés dans leur domaine de collisions.

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.**

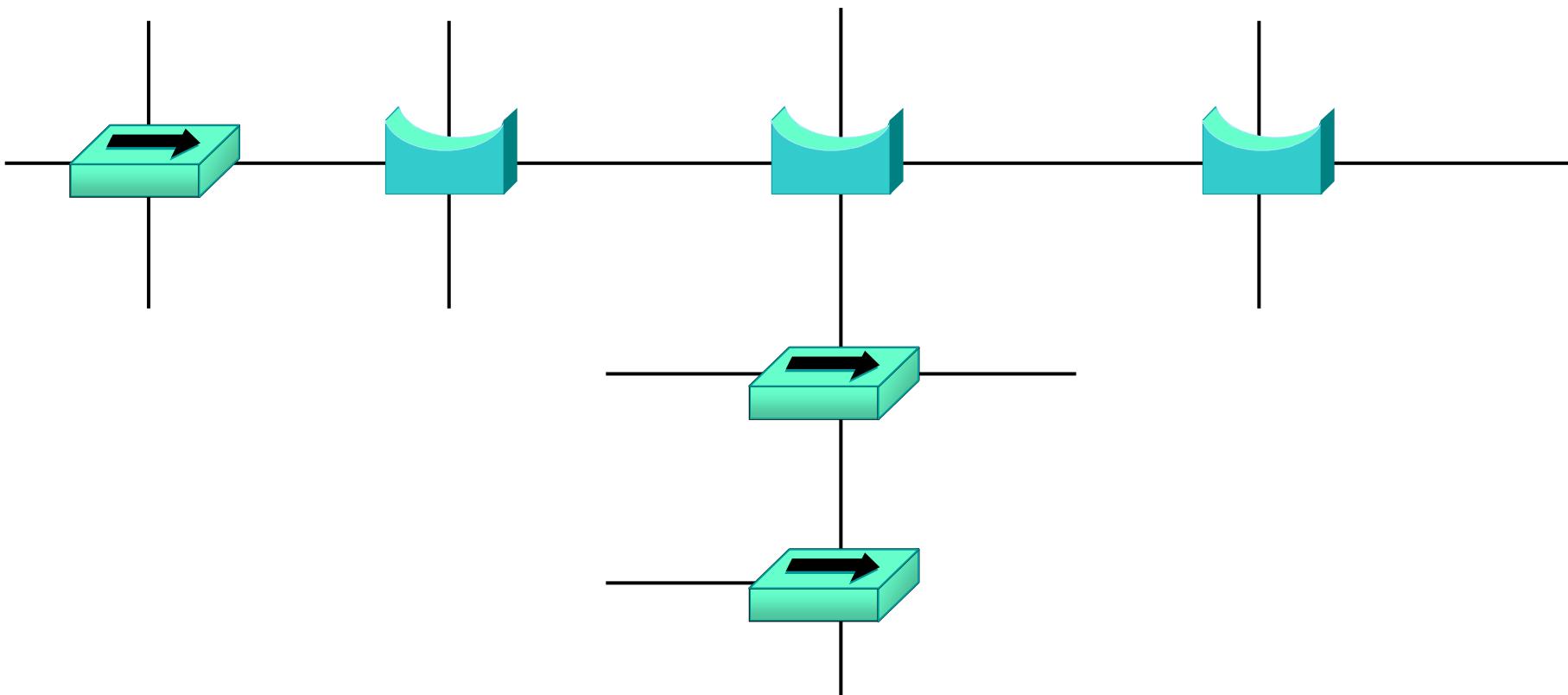
Domaine de collision



- 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.

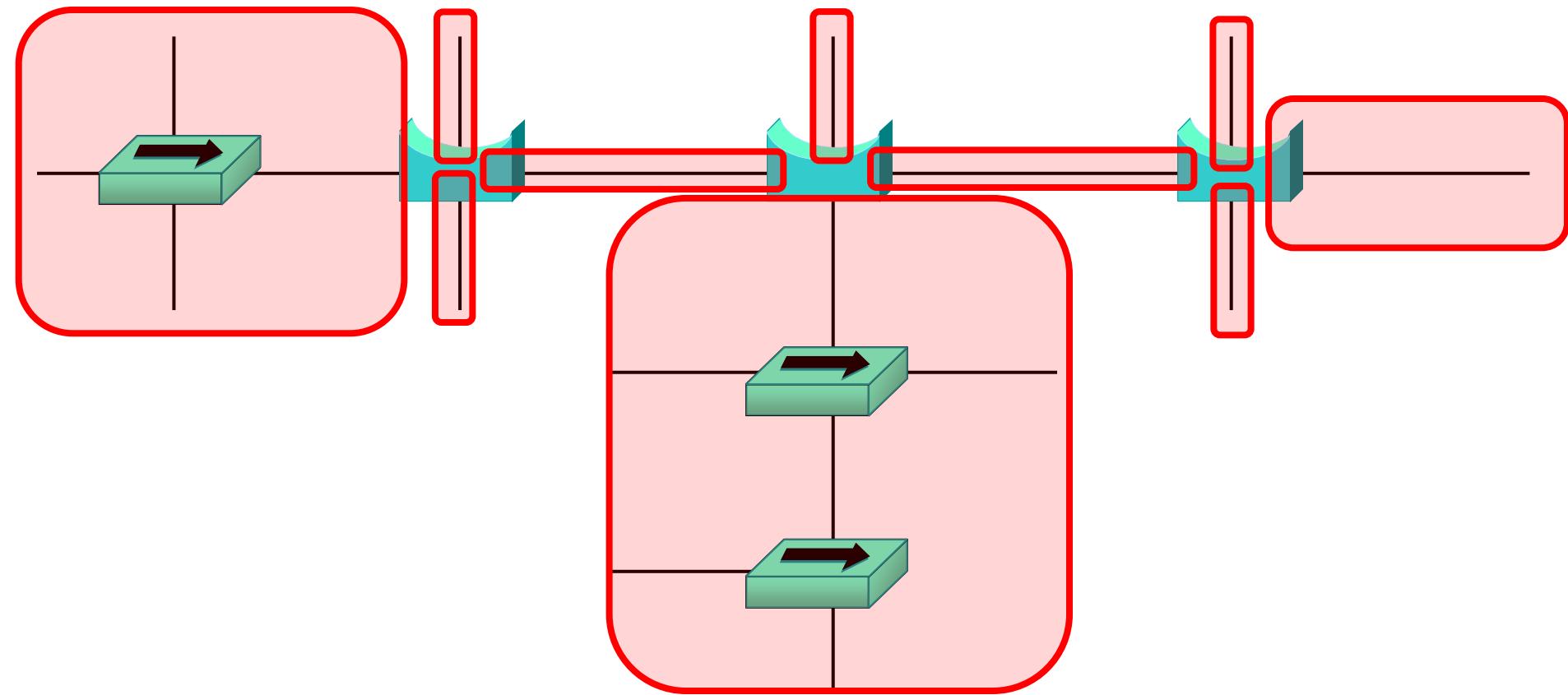
Exercice

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



Solution

10 domaines de collision.



Fonctionnement du pont

Lorsqu' il reçoit une trame :

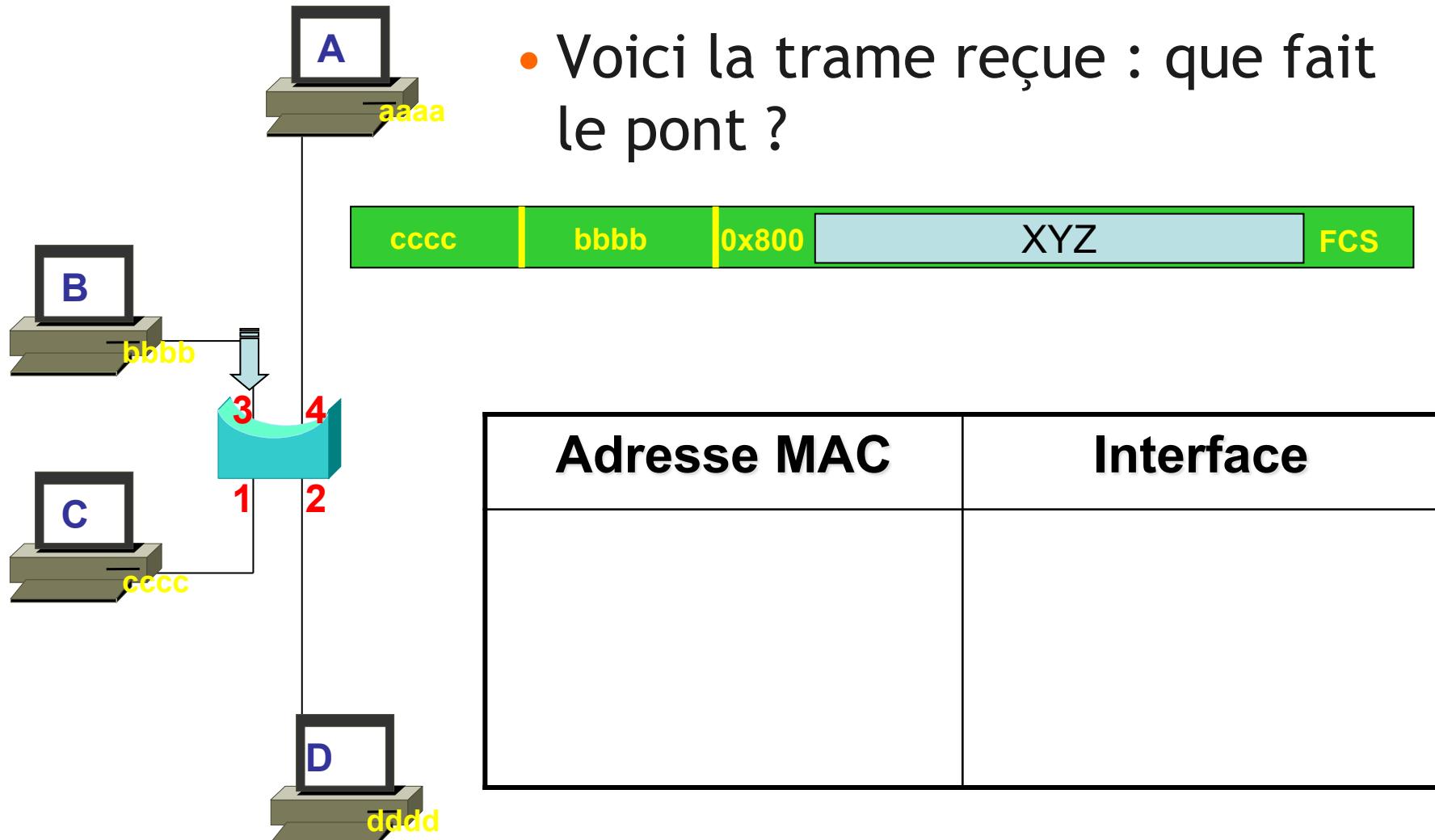
1. il regarde l' adresse MAC **source** de la trame et met à jour sa table

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

Fonctionnement du pont

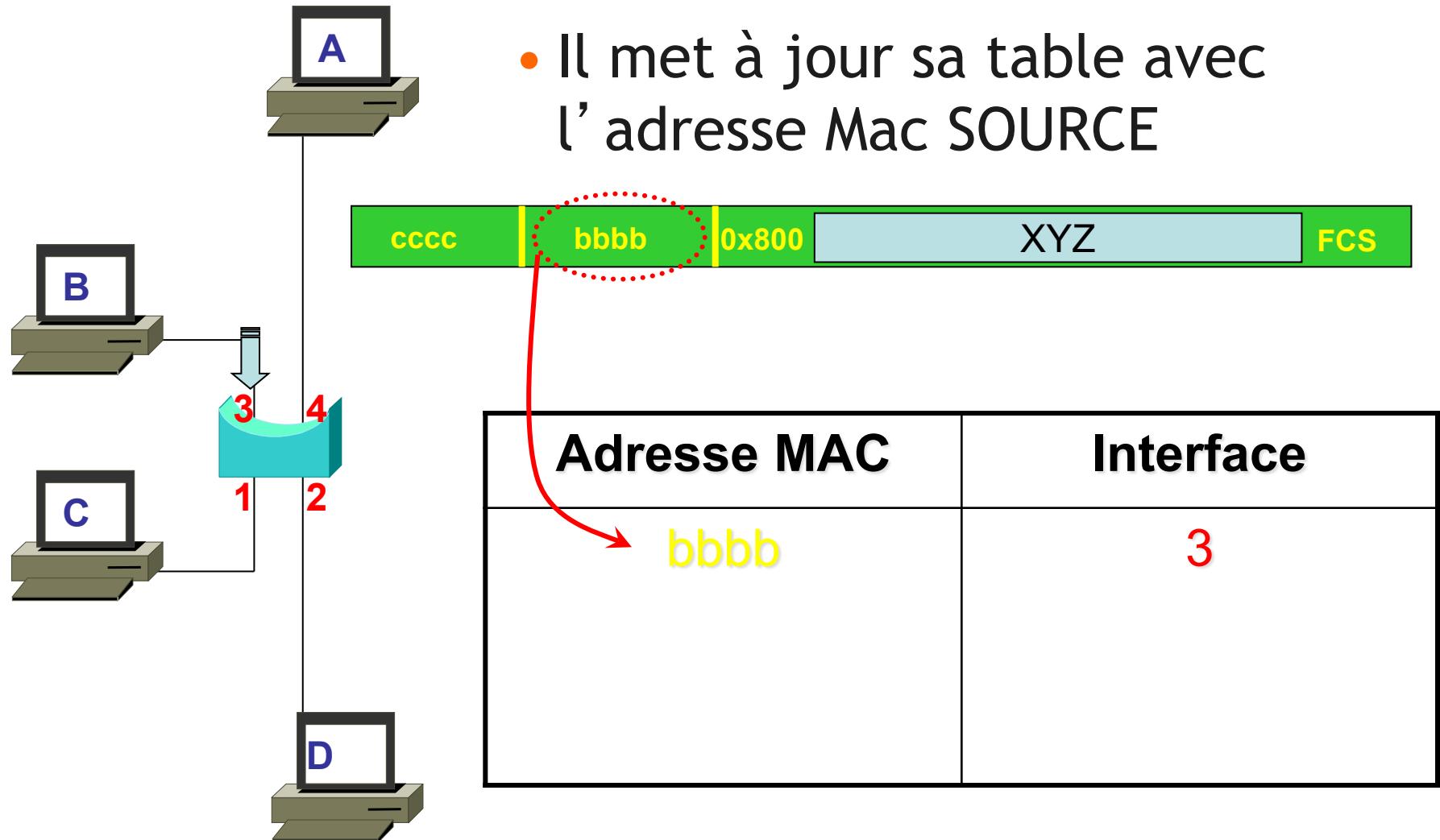
- S'il ne trouve pas l'adresse Mac destination dans sa table :
 - il s'agit d'un 'unknown unicast'
 - il **duplicre** la trame sur toutes ses interfaces, sauf celle où il l'a reçue.
 - C'est un **unicast flooding**
- Si l'adresse Mac de destination est broadcast (**FFFF.FFFF.FFFF**) ou multicast :
 -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

Exercice 1

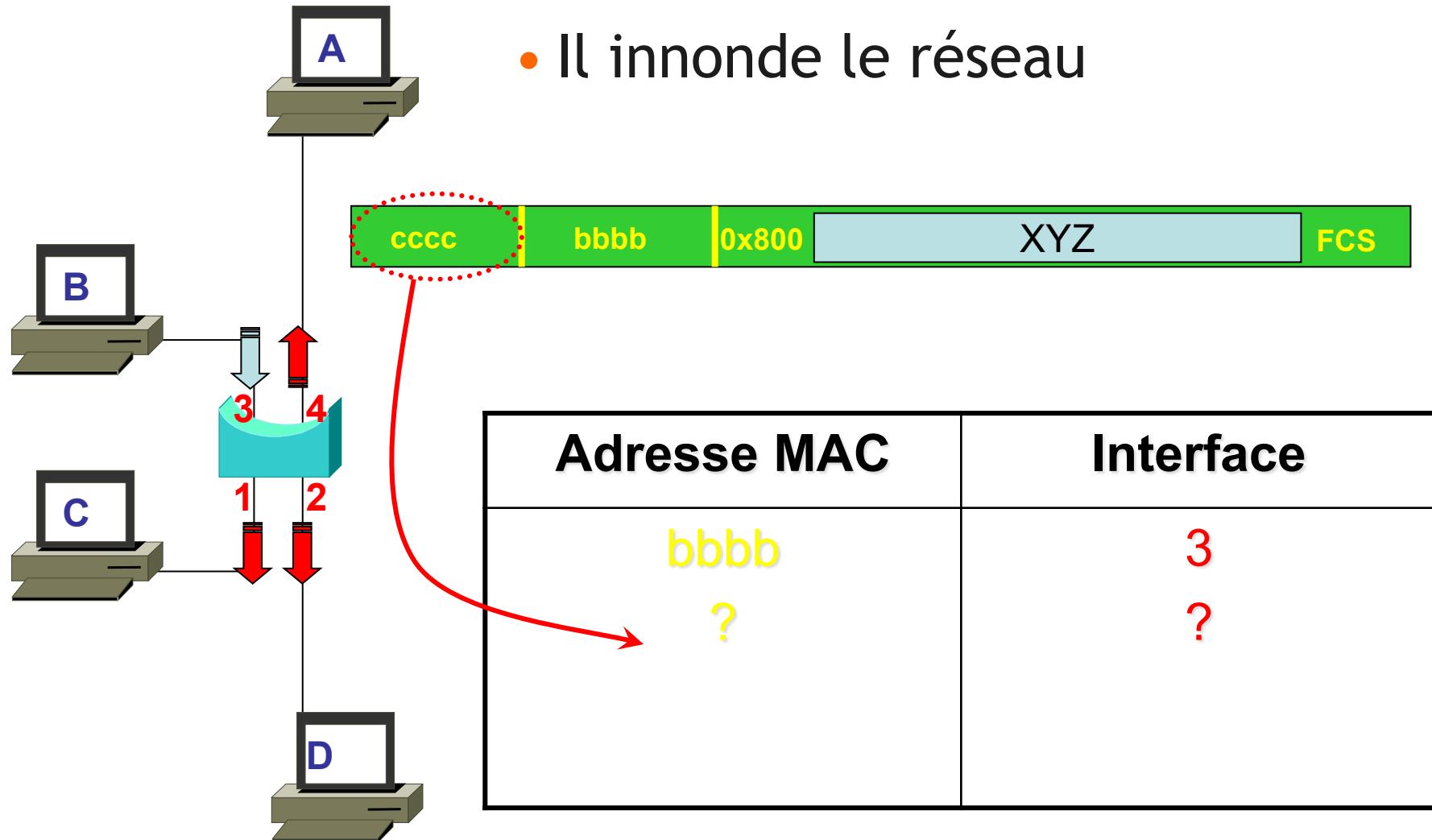


Adresse MAC	Interface

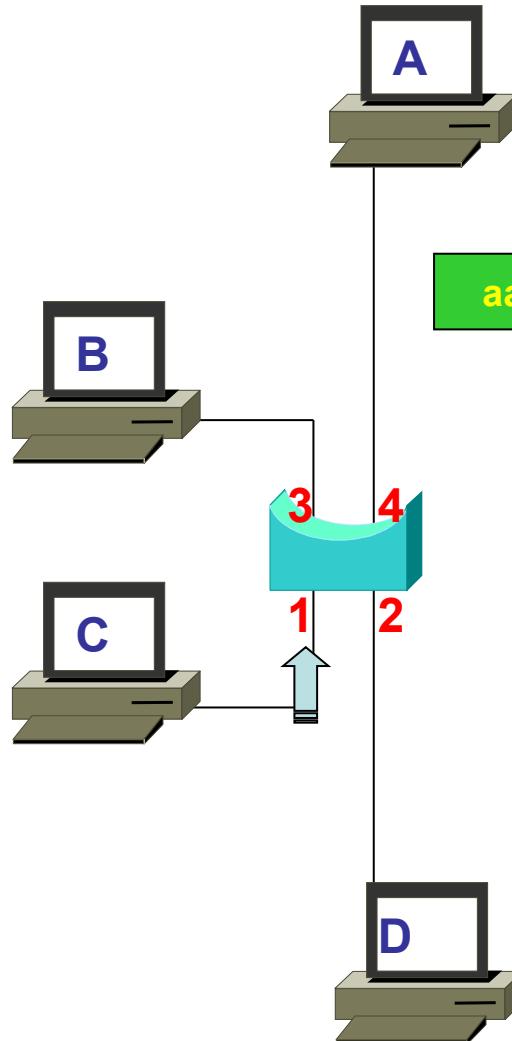
Solution 1



Solution 1, suite



Exercice 2

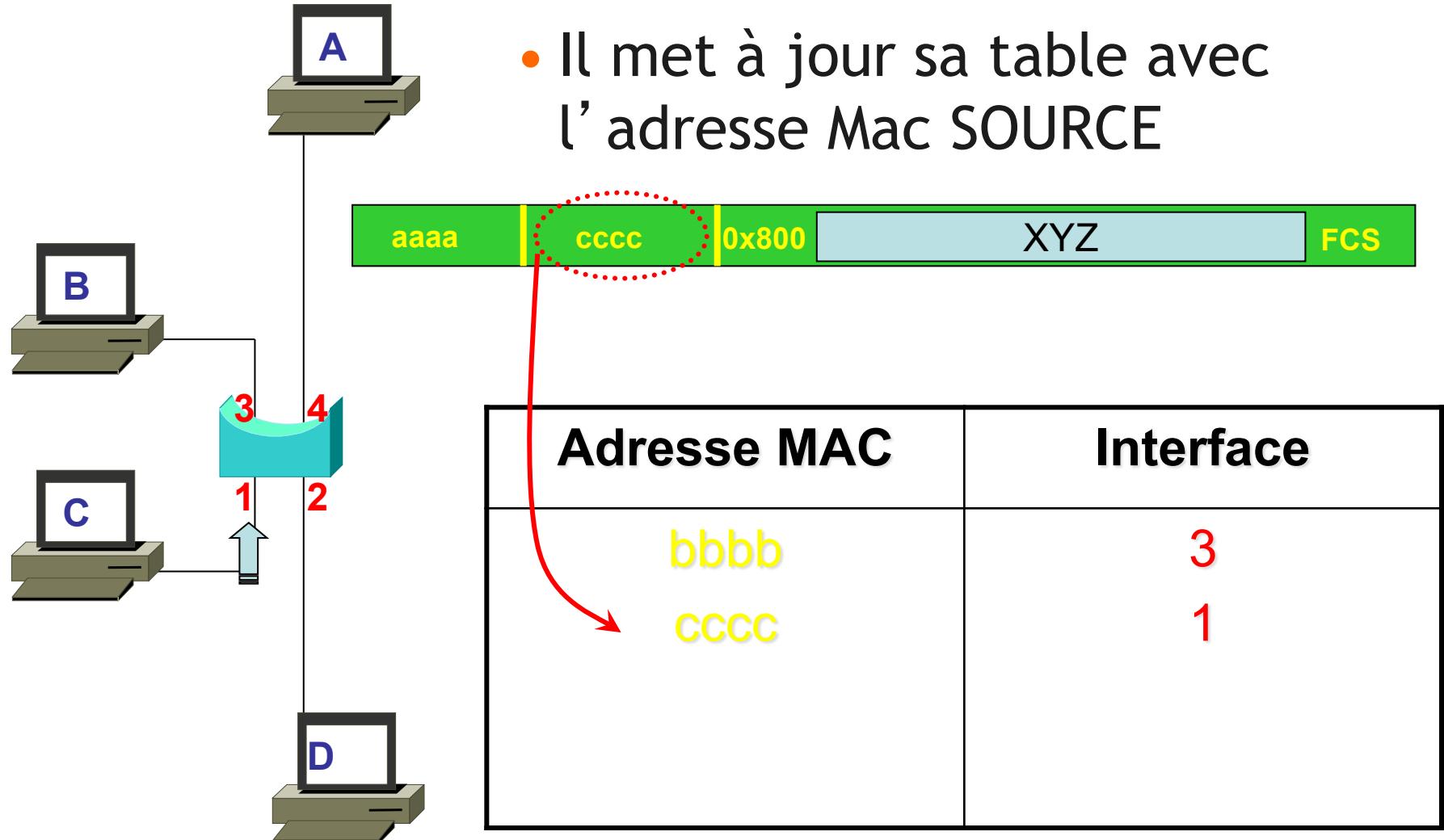


- Voici la trame reçue : que fait le pont ?

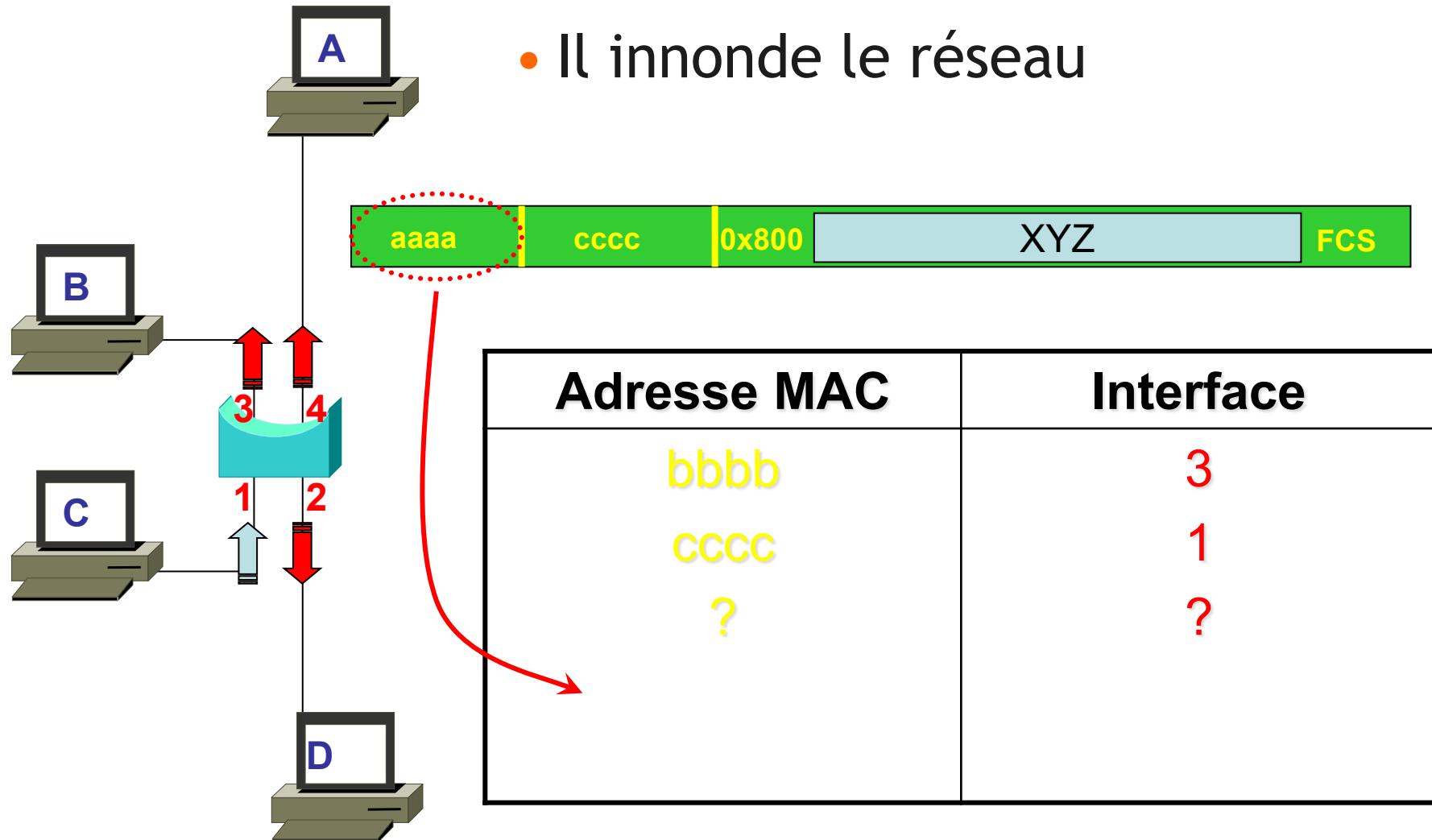


Adresse MAC	Interface
bbbb	3

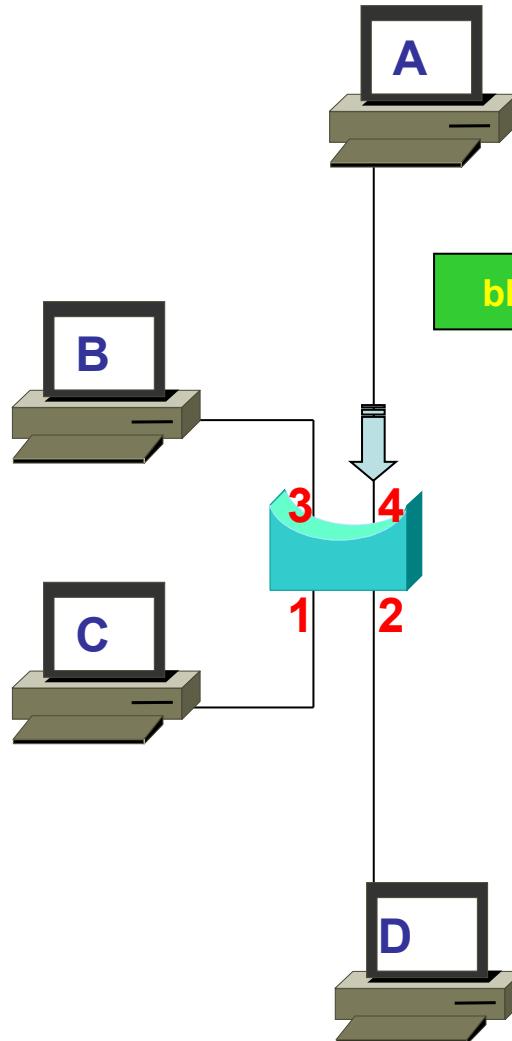
Solution 2



Solution 2, suite



Exercice 3

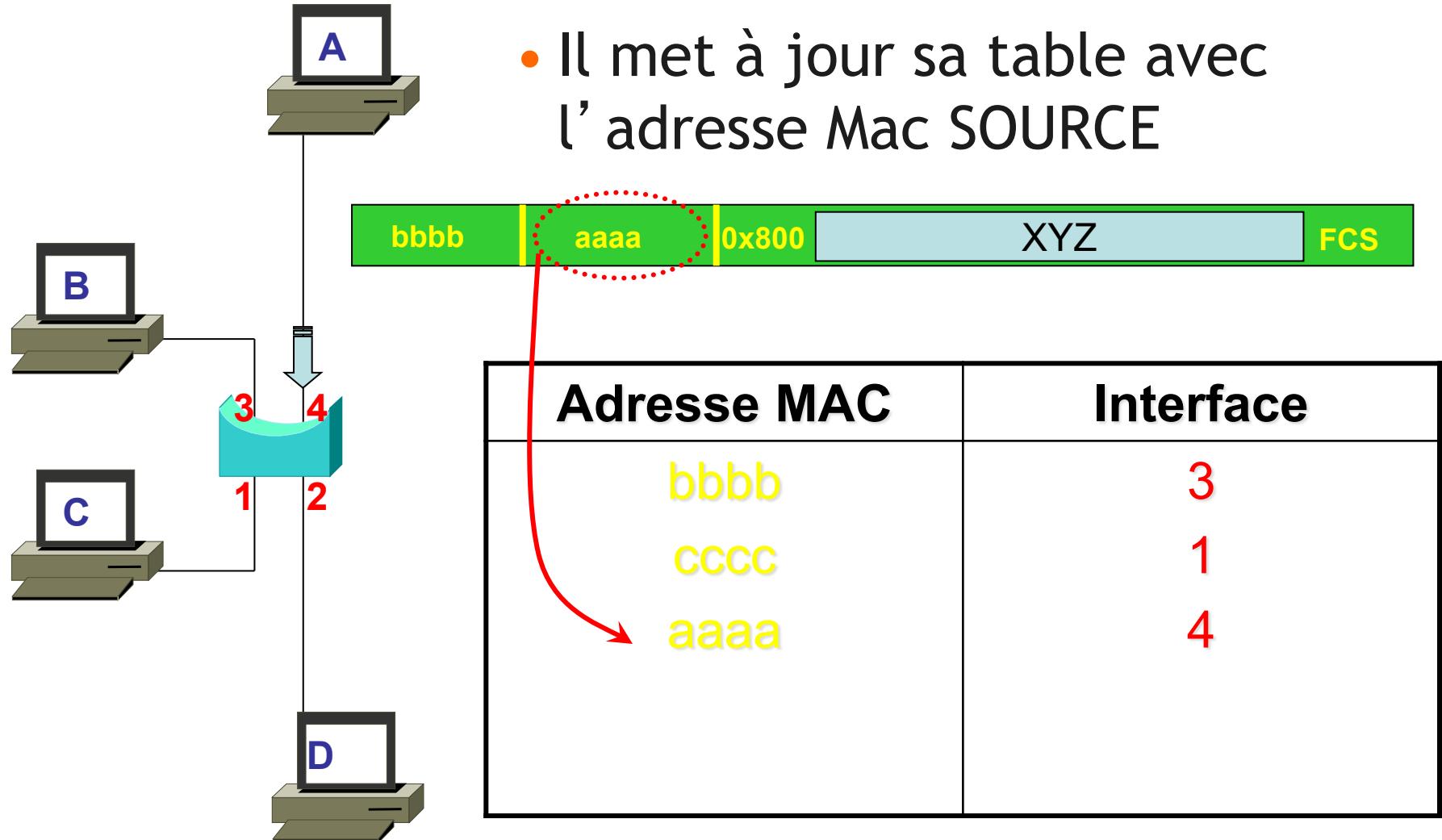


- Voici la trame reçue : que fait le pont ?

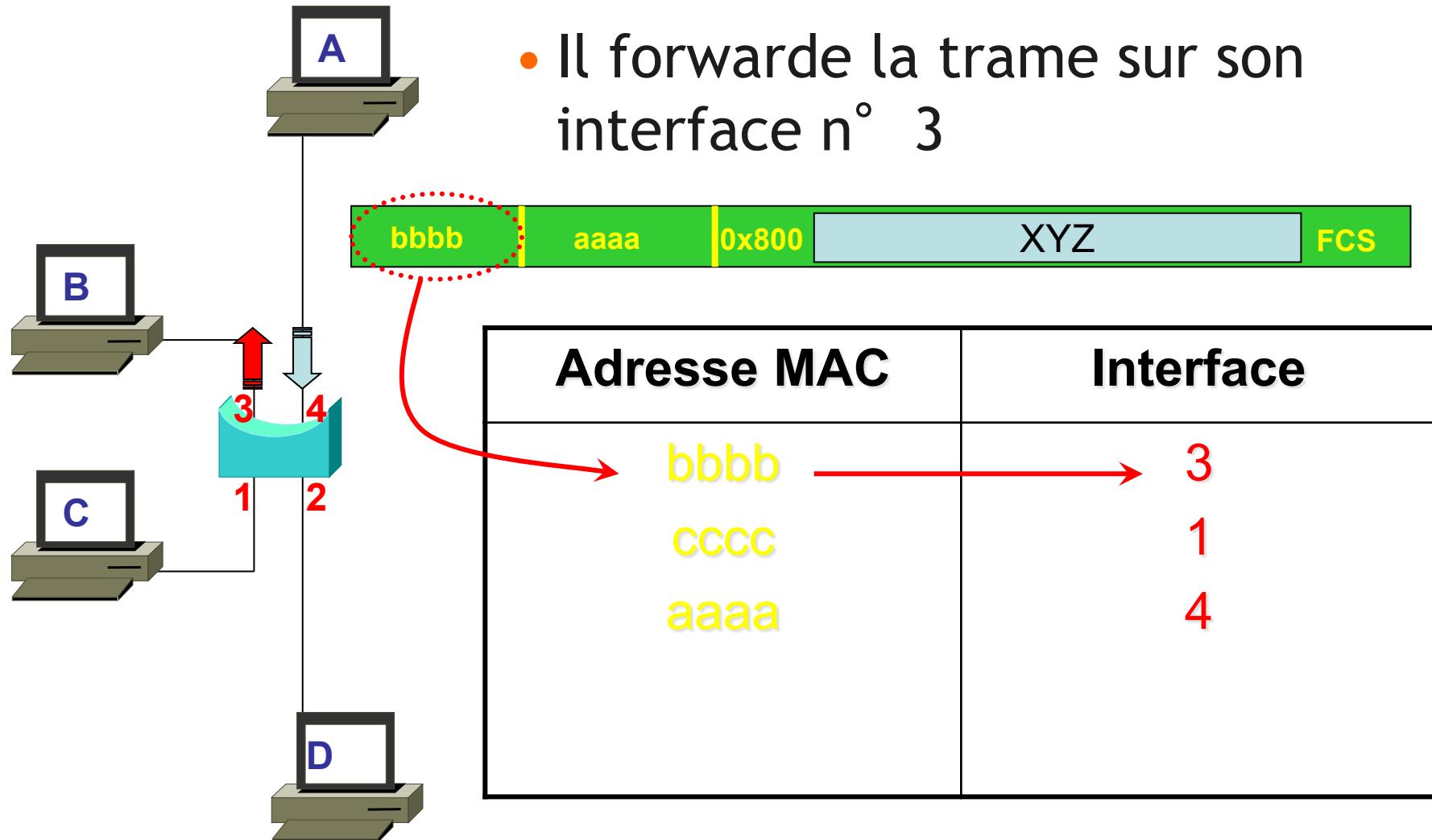


Adresse MAC	Interface
bbbb	3
cccc	1

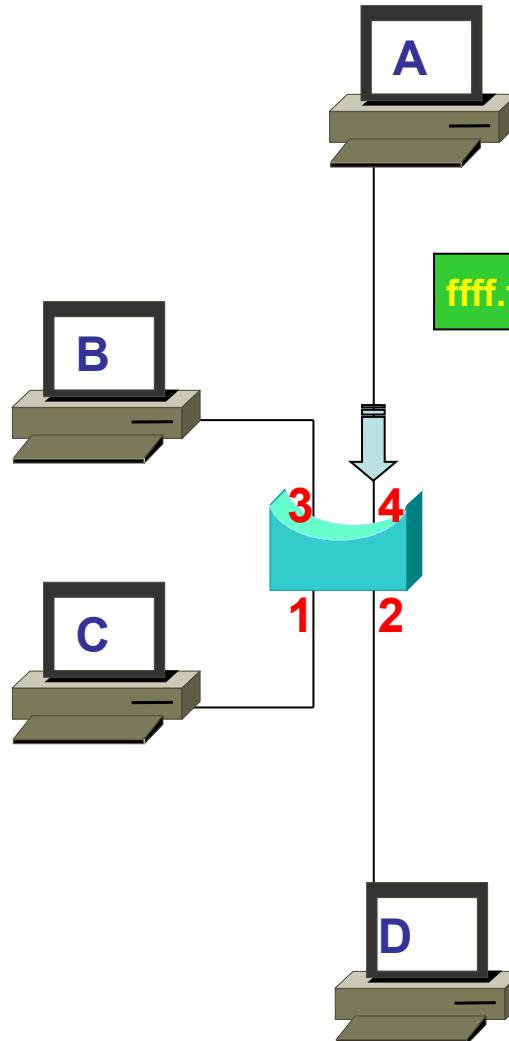
Solution 3



Solution 3, suite



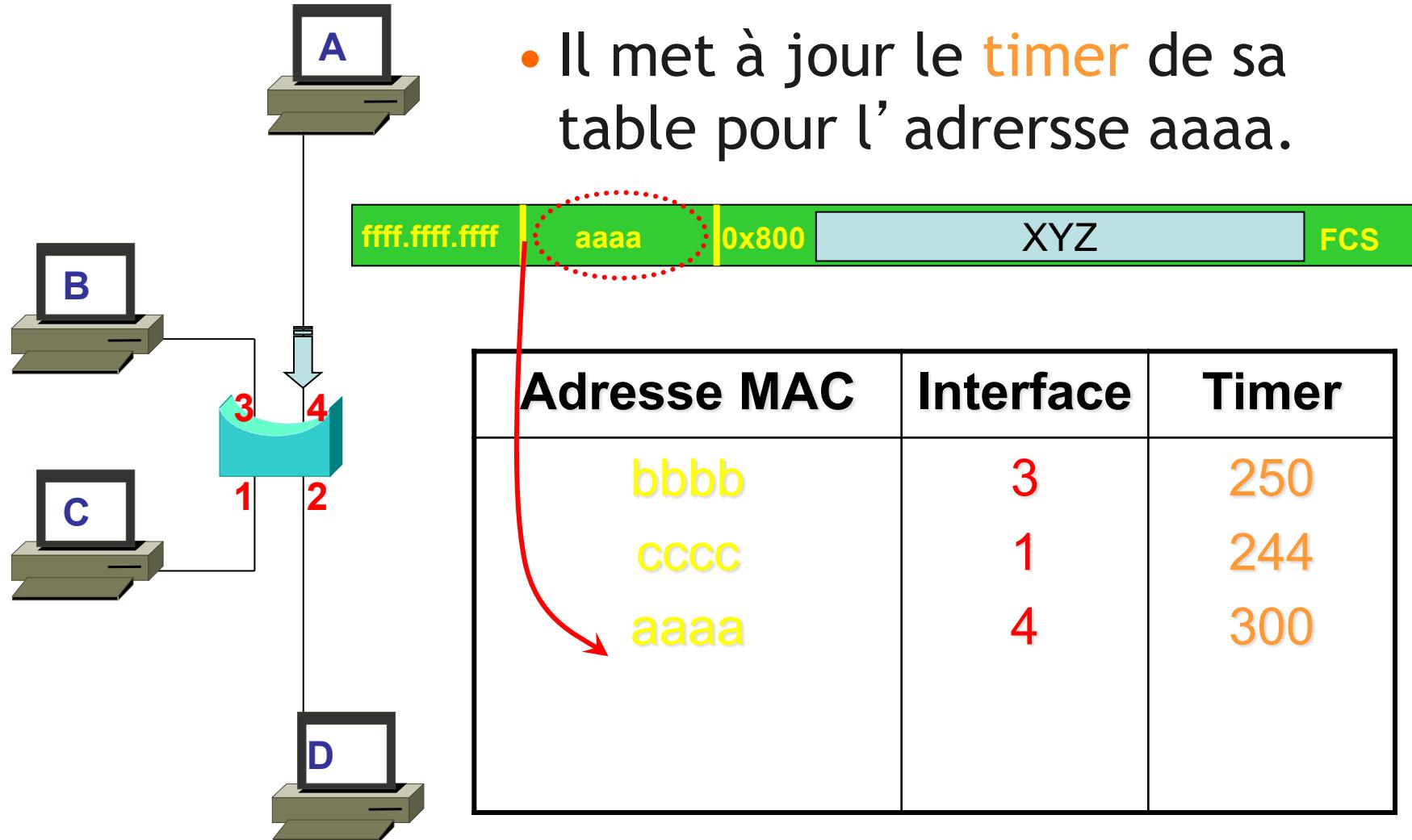
Exercice 4



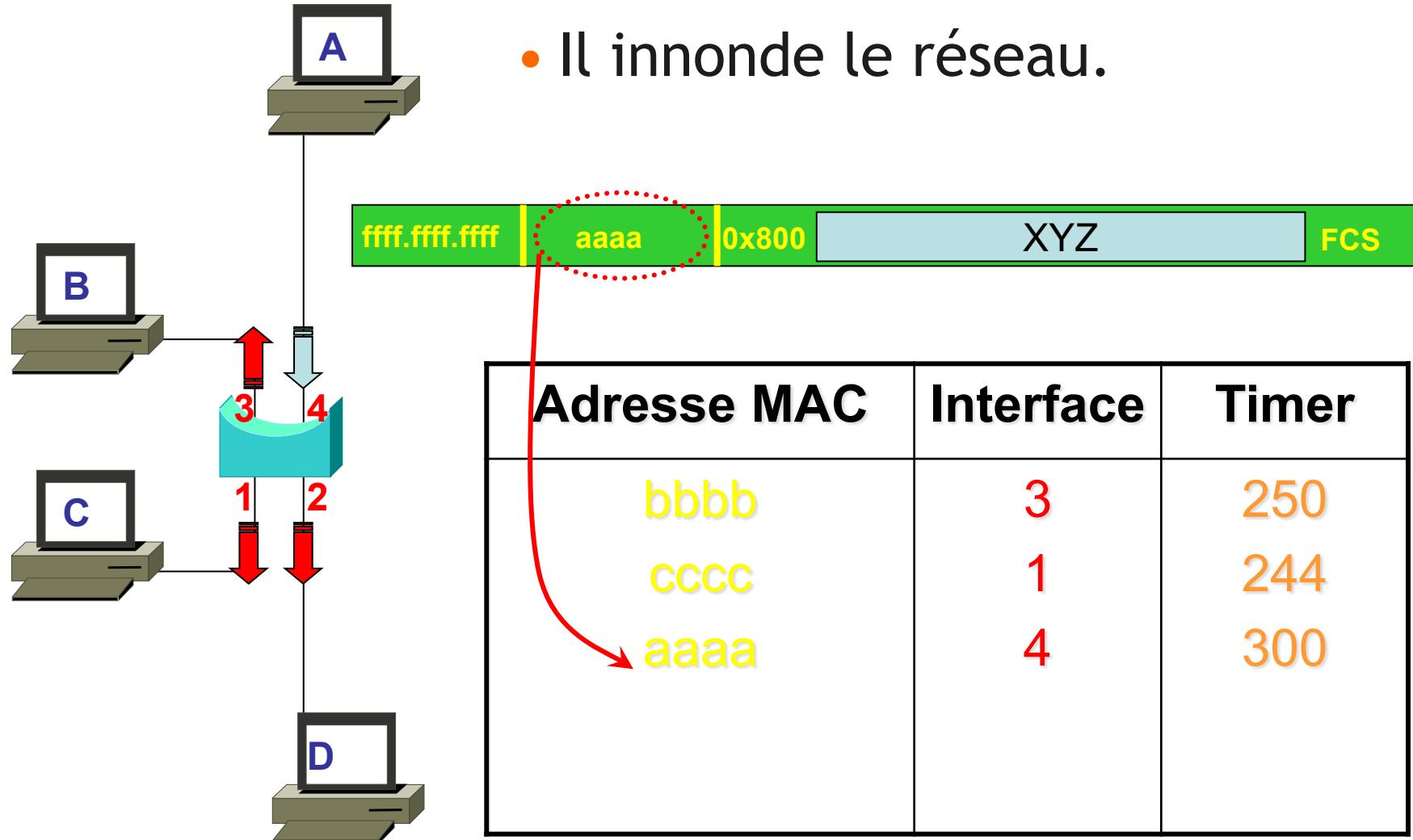
- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
bbbb	3
cccc	1
aaaa	4

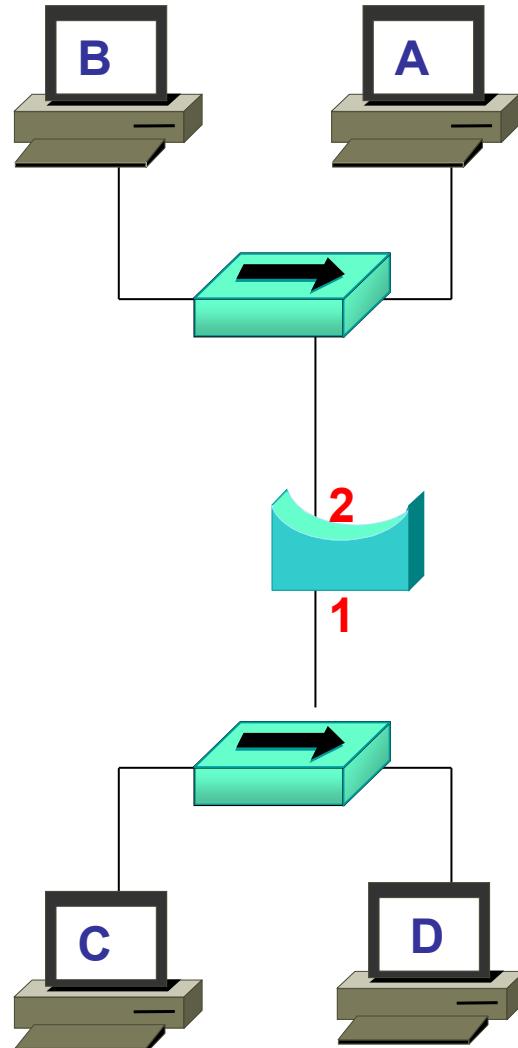
Solution 4



Solution 4, suite



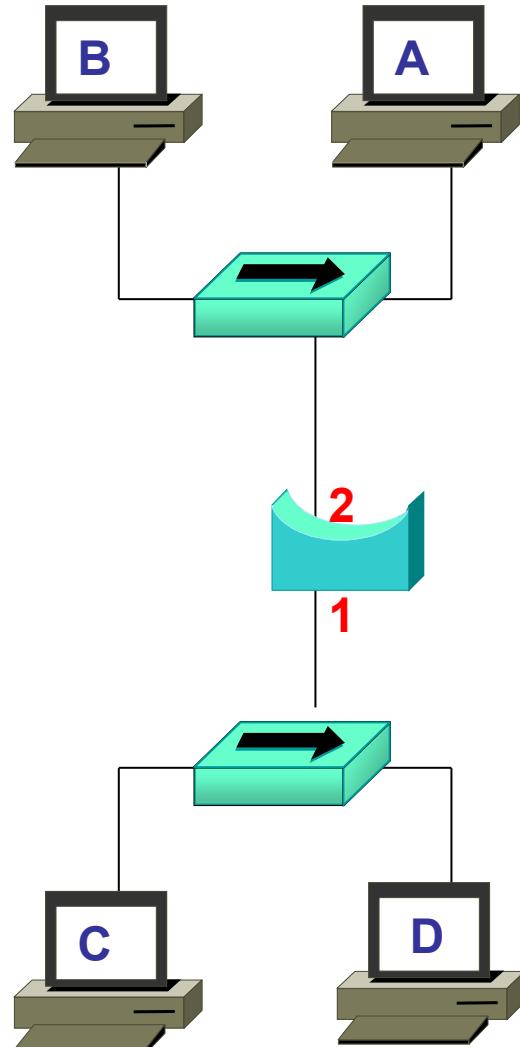
Exercice 5



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

Adresse MAC	Interface

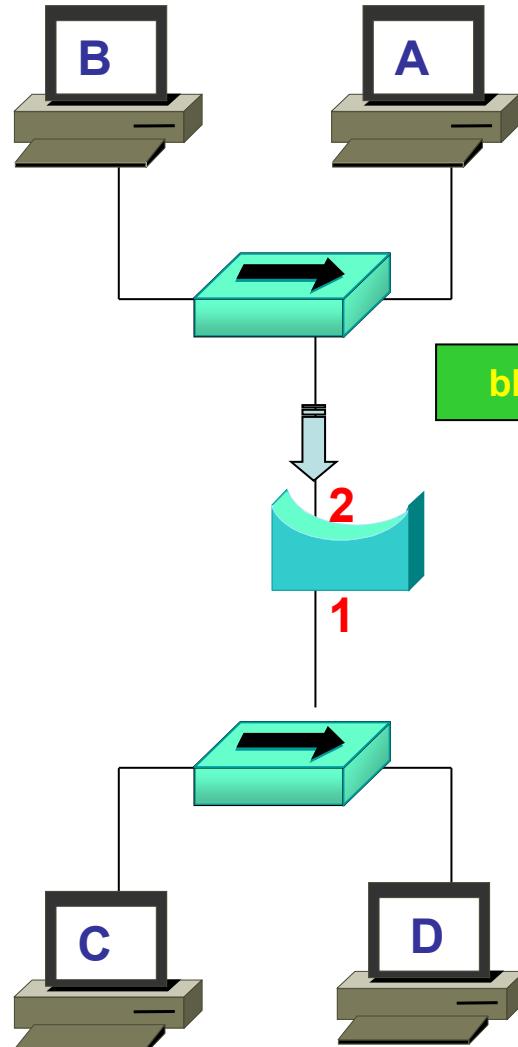
Solution 5



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

Adresse MAC	Interface
aaaa	2
bbbb	2
cccc	1
dddd	1

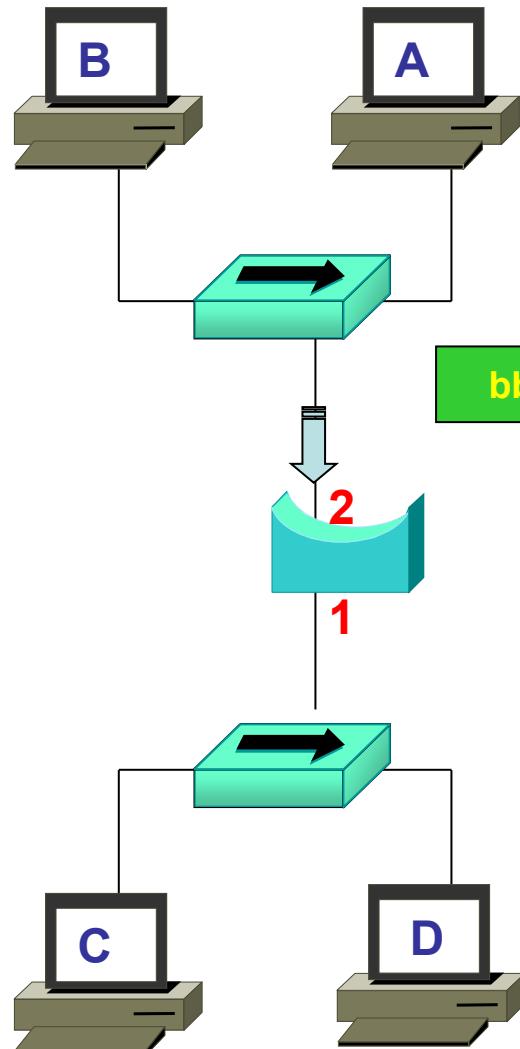
Exercice 6



- Voici la trame reçue : que fait le pont ?

Adresse MAC	Interface
aaaa	2
bbbb	2
cccc	1
dddd	1

Solution 6

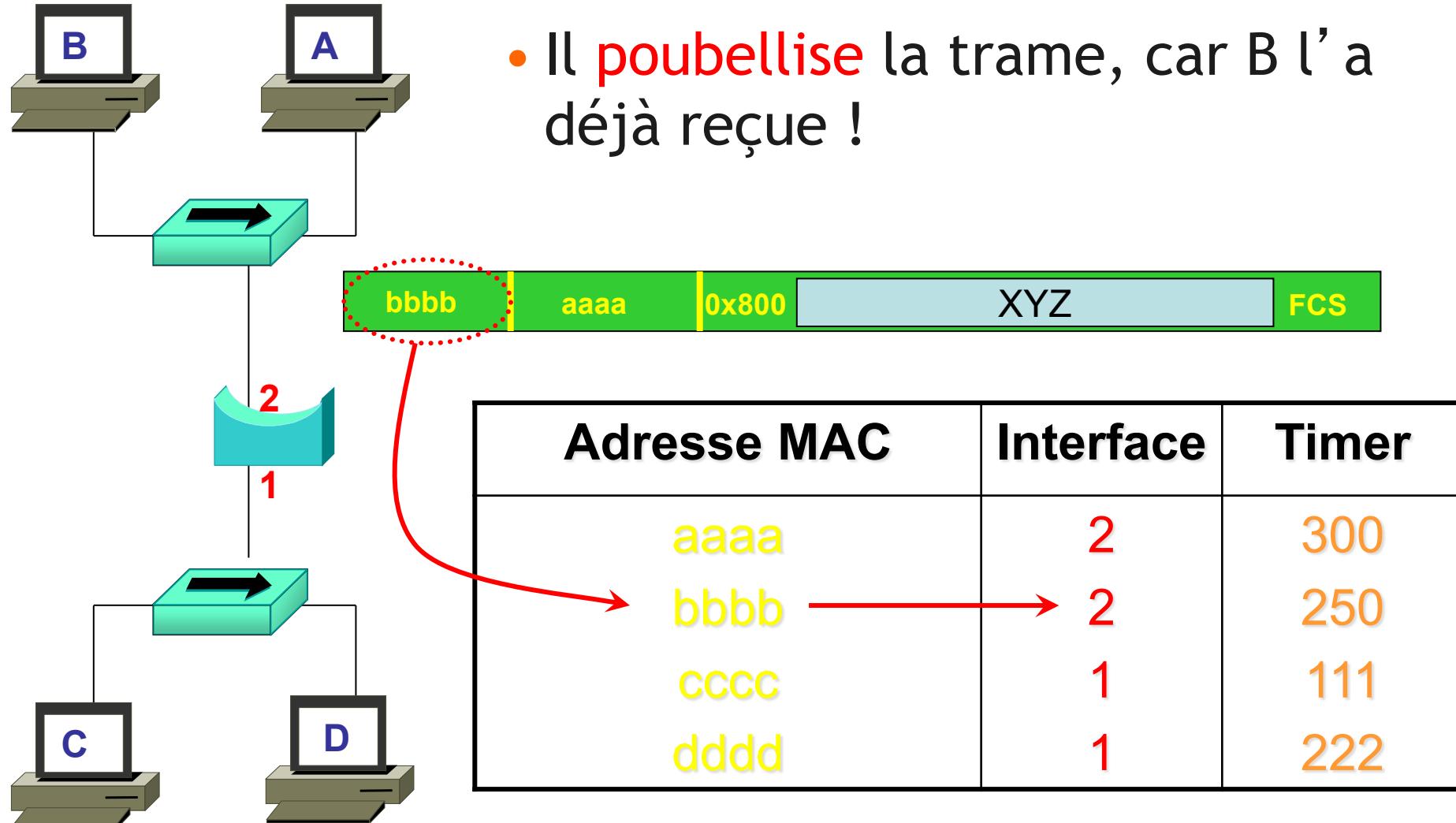


- Il met à jour le **timer** de sa table pour l'adresse **aaaa**.



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

Solution 6, suite



Bilan : l' algorithme 802.3

Je reçois une trame



J'apprends l'adresse mac SOURCE ou je mets à jour la timer 'aging'



Est-ce un broadcast ? un multicast ? ou unknown unicast ?

NON

OUI

Inonder la trame sur tous les ports (sauf celle reçue)



Les adresses Mac source et destination sont sur la même interface ?

NON

OUI

Poubelliser la trame



Copier la trame sur l'interface de sortie

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

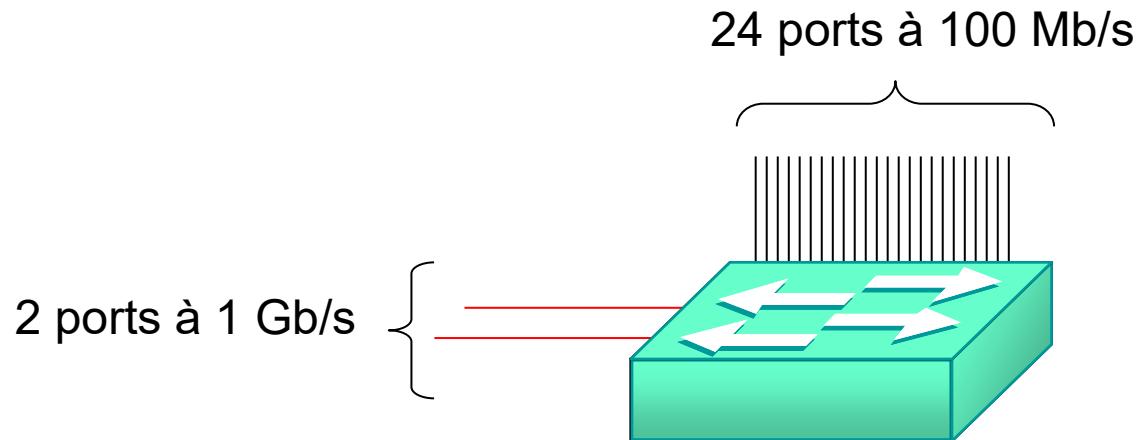
Ethernet

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’



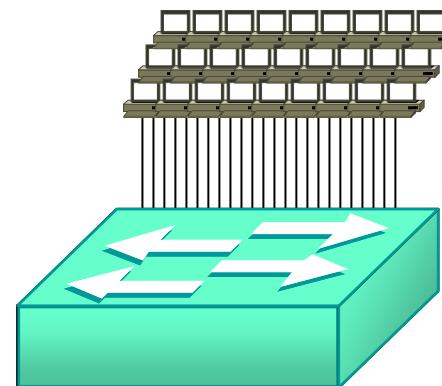
Les ports à 1 Gb/s sont appelés ‘**uplink**’ .

Ils sont reliés à d’ autres switch et permettent d’ aggréger le trafic reçu sur plusieurs 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 :

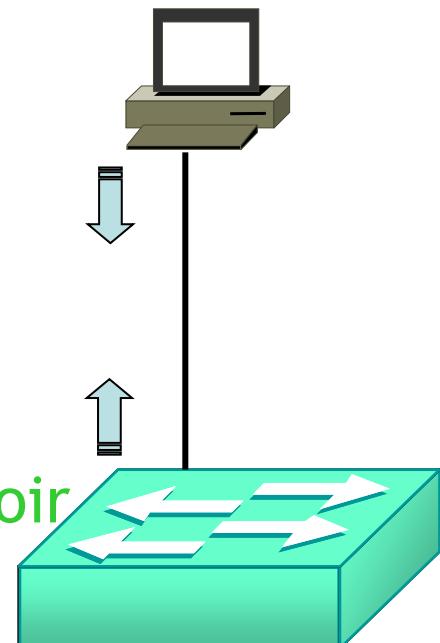


Full-duplex

- S'il n'y a que 2 équipements sur un même segment (*), alors il n'y a pas de collision :

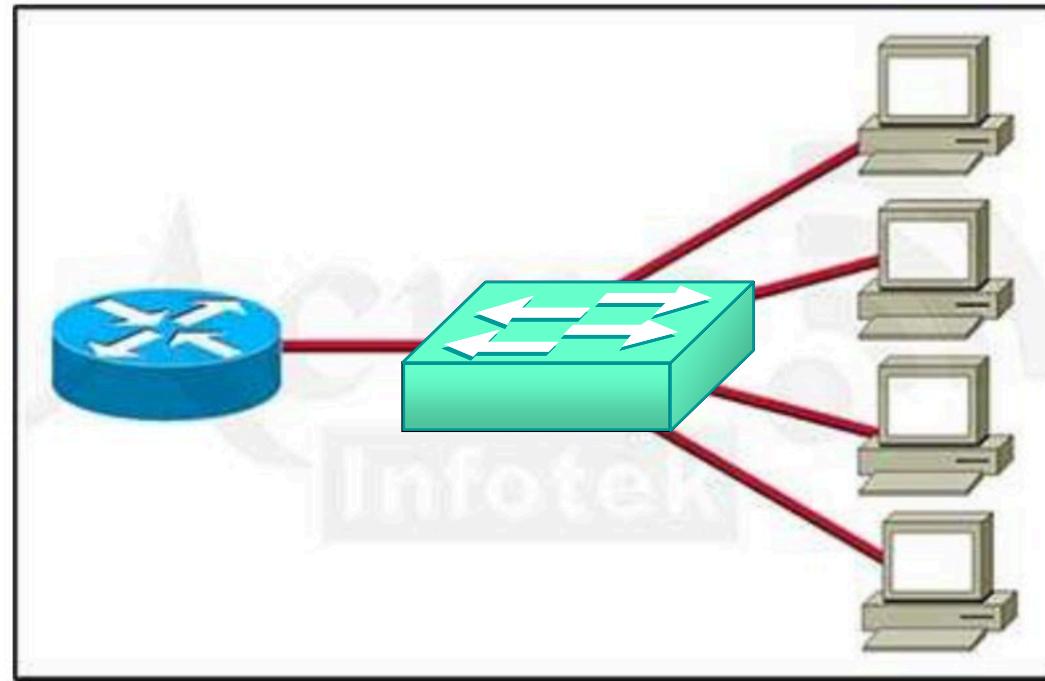
- pas de CSMA / CD

- chaque équipement peut émettre et recevoir en même temps



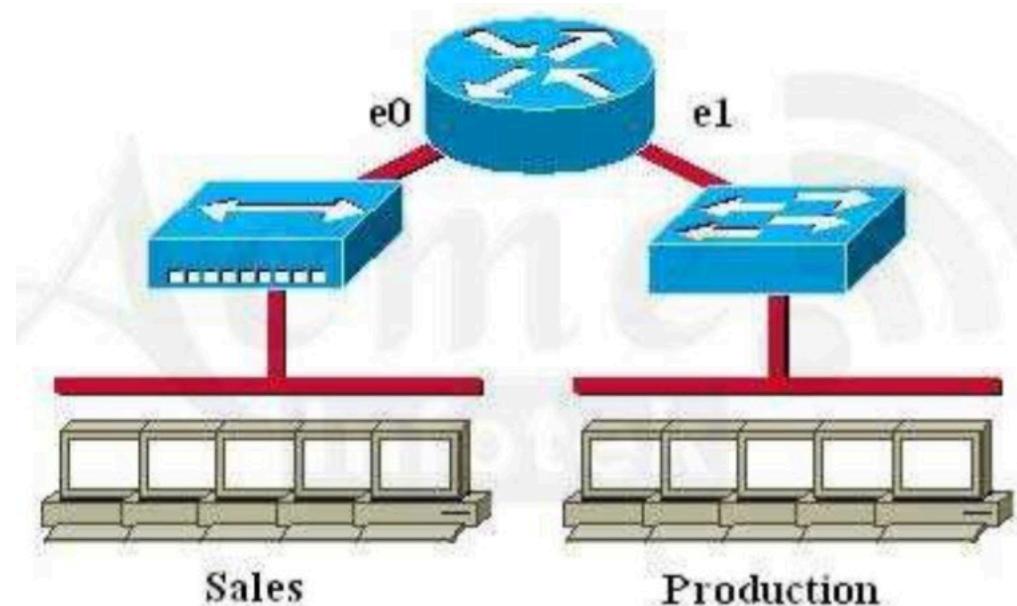
(*) et si les 2 cartes réseau savent fonctionner en full-duplex

Test



- Combien de domaines de collision ?
- Combien de domaines de broadcast ?
- 5
- 1

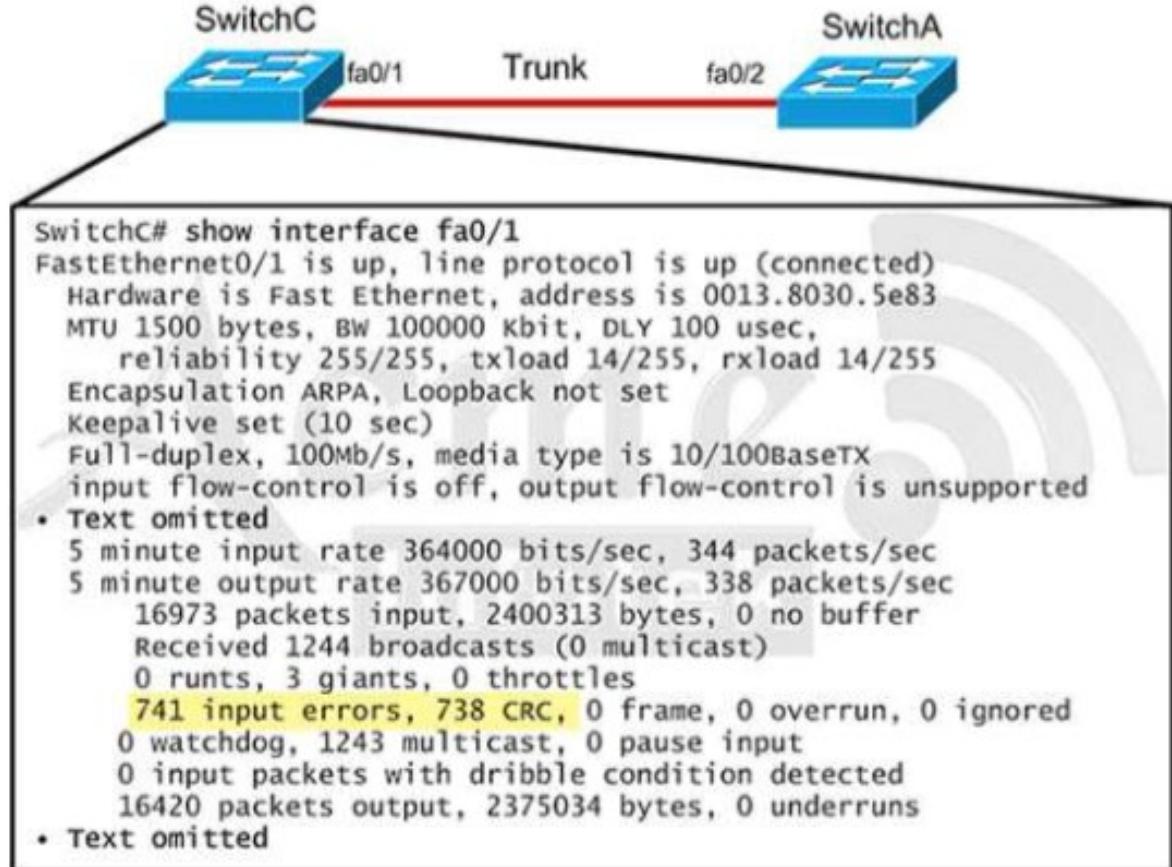
Test



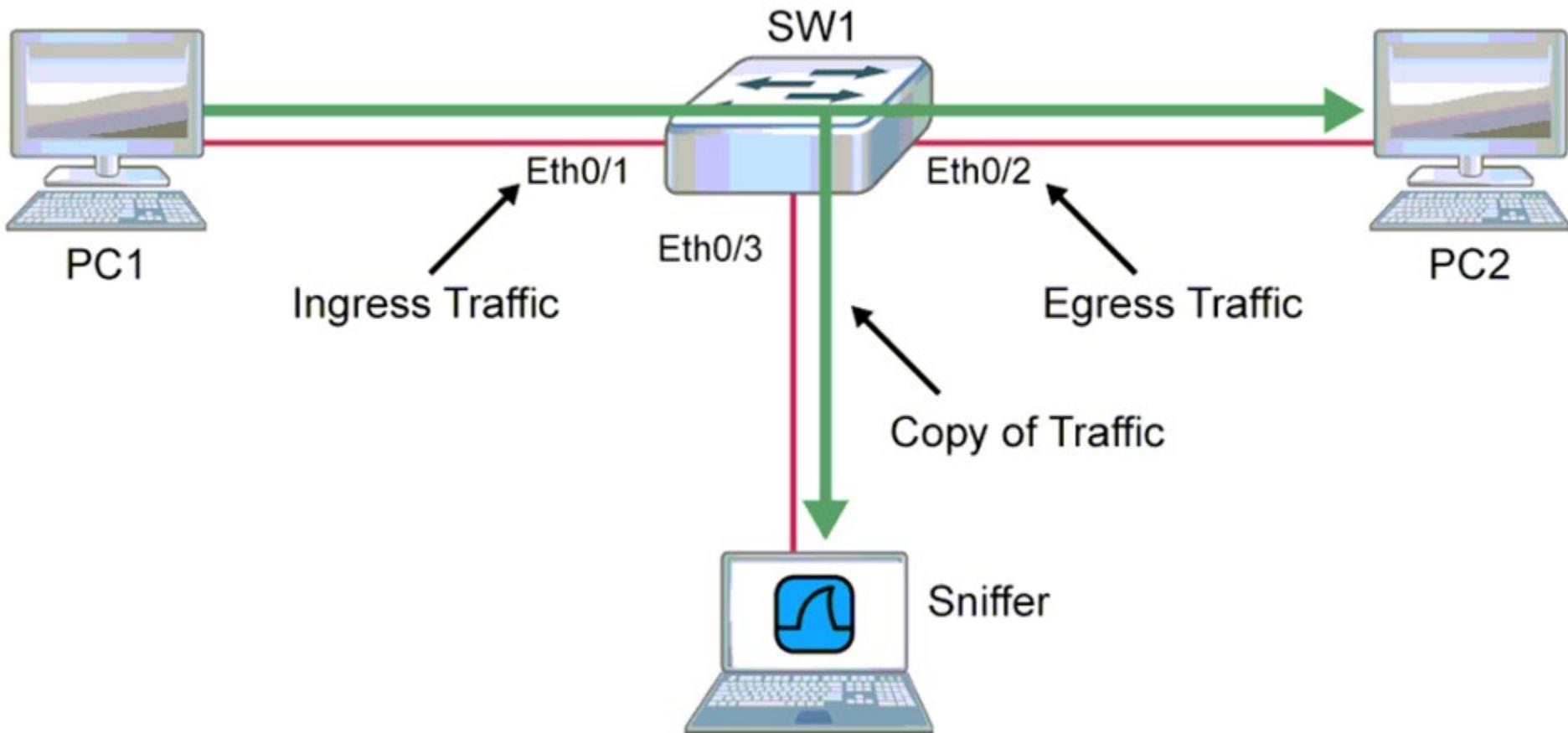
- Combien de domaines de collision ?
- Combien de domaines de broadcast ?
- 7
- 2

Duplex mismatch

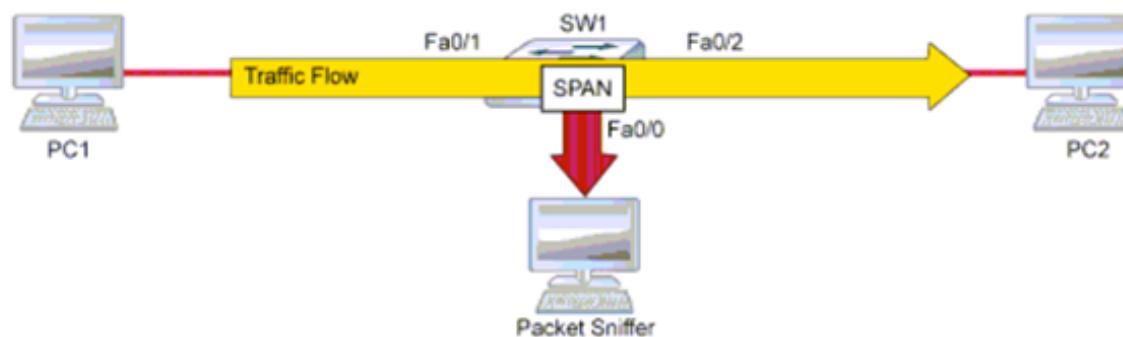
- Un côté en Full-duplex (C) - CRC
- L'autre côté en Half-duplex (A) - Late collision



Redirection de ports (Source Port Analyser)



Redirection de ports SPAN



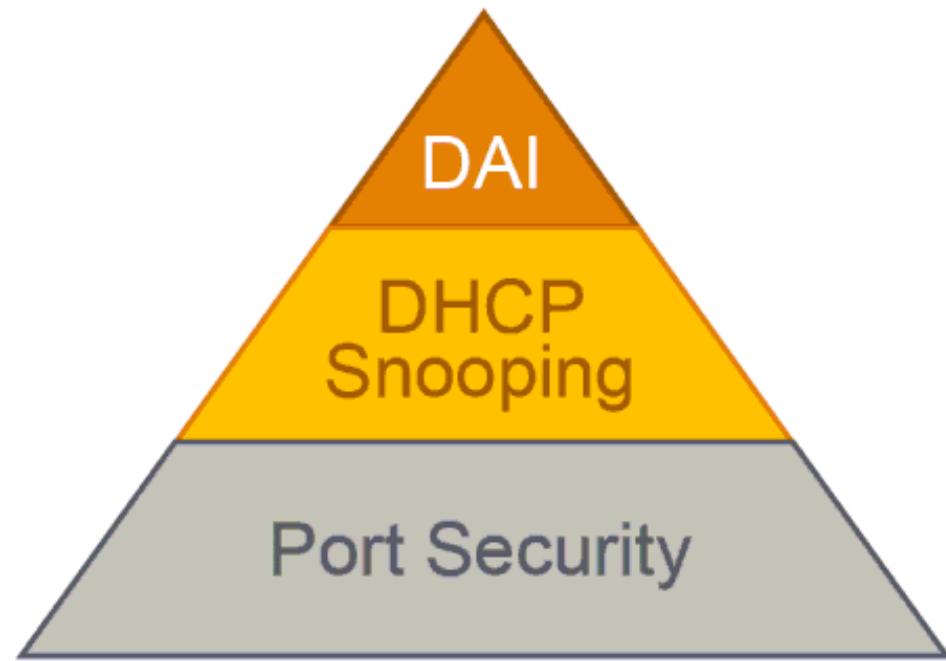
```
SW1(config)# monitor session 1 source interface FastEthernet0/2 both  
SW1(config)# monitor session 1 destination interface FastEthernet0/0
```

Sécurité des accès

Mitigating Threats at Access Layer

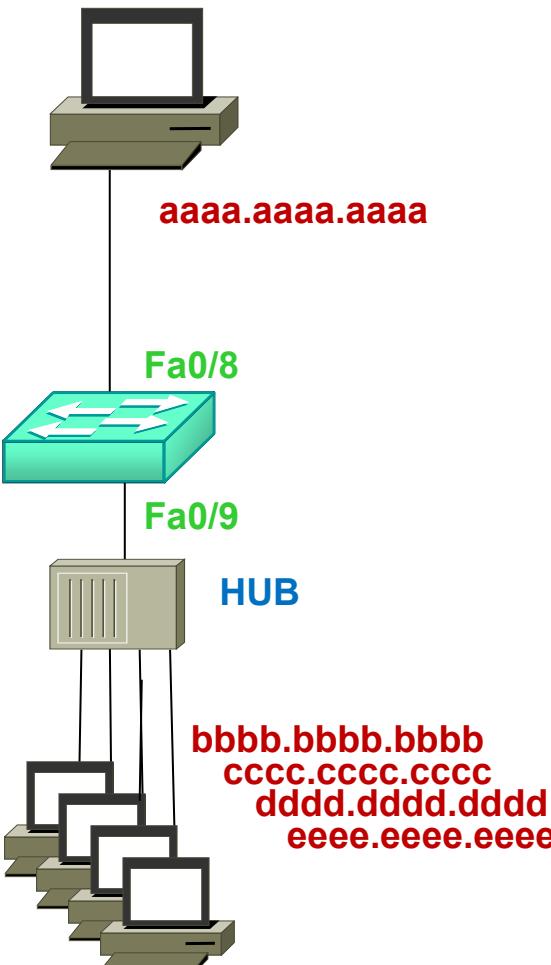
You can mitigate most access layer threats with these features:

- **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.



Identity-Based Networking

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 (agrégation 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**

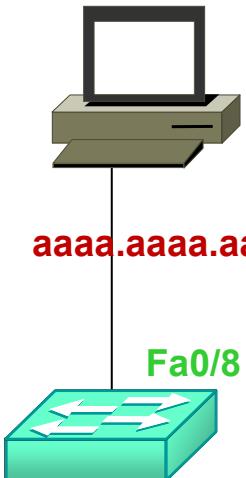
aaaa.aaaa.aaaa

→ n'autoriser que cette adresse Mac.

switchport port-security

→ activer la fonctionnalité '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

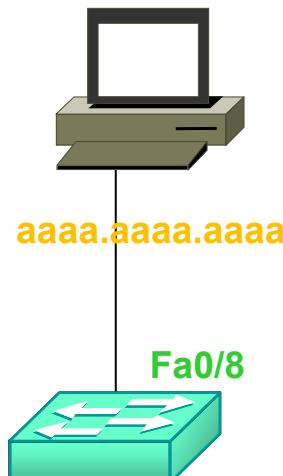
➔ activer la fonctionnalité 'port-security'

Si aucune adresse Mac n' est configurée statiquement :

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

méthode dangereuse :

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

aaaa.aaaa.aaaa → n'autoriser qu'une seule adresse Mac

switchport port-security mac-address **sticky**

→ autoriser l'adresse Mac de la 1^{ère} trame reçue

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

switchport port-security

→ activer la fonctionnalité '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 de manière 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

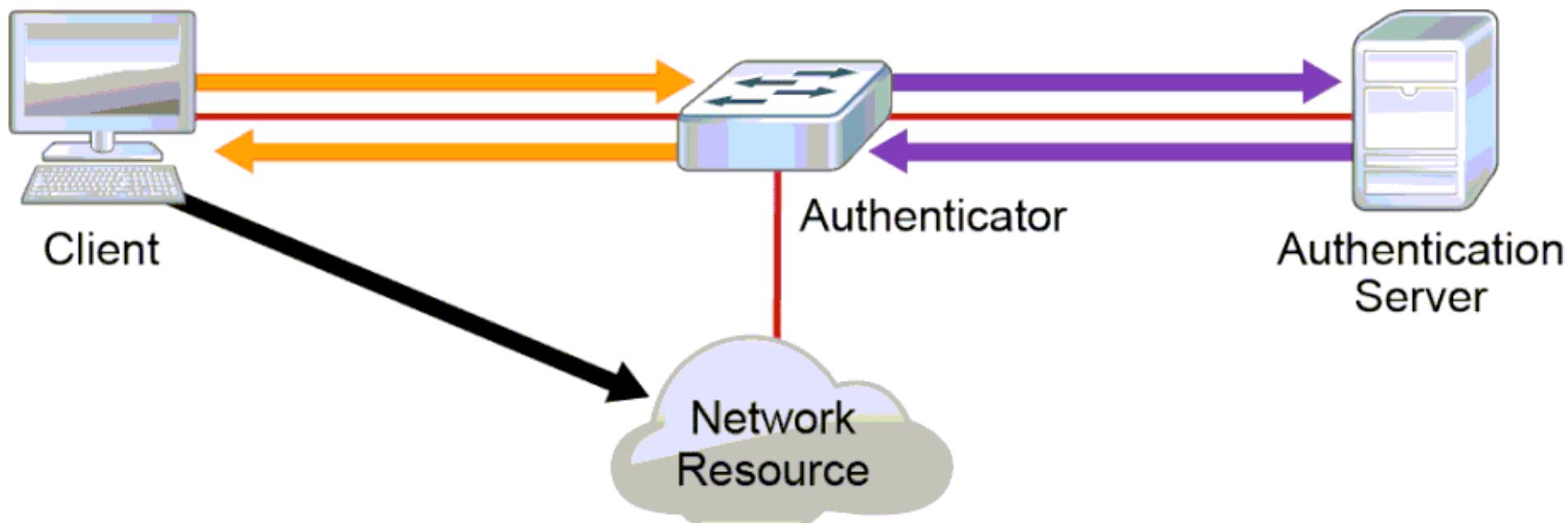
...



Identity-Based Networking

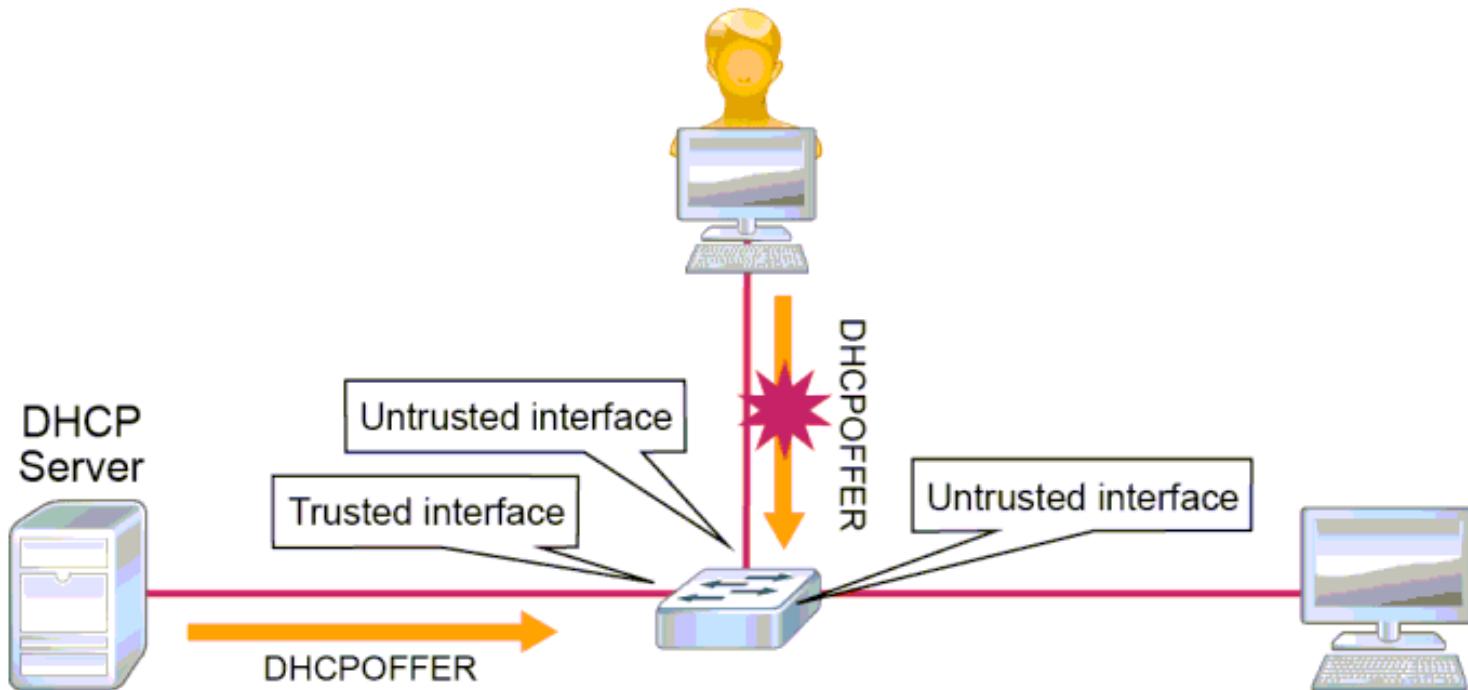
Identity-based network verifies the users when they connect regardless of their physical location.

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





DHCP Snooping and DAI



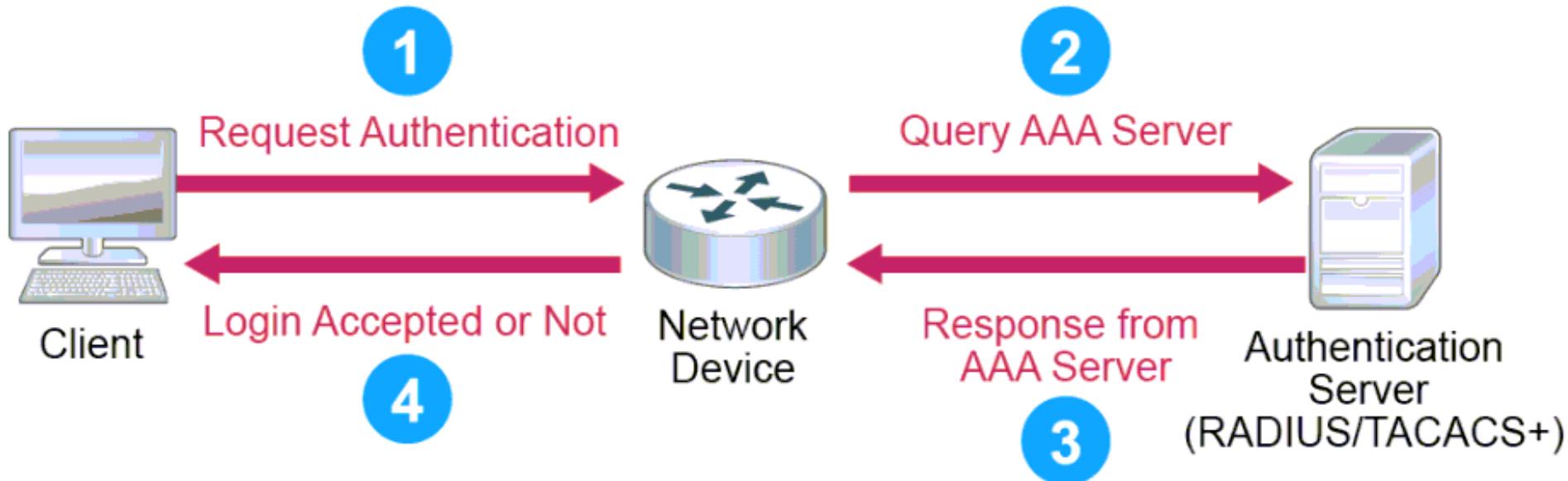
DHCP snooping is a Layer 2 security feature that validates the DHCP messages.

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



External Authentication Options

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



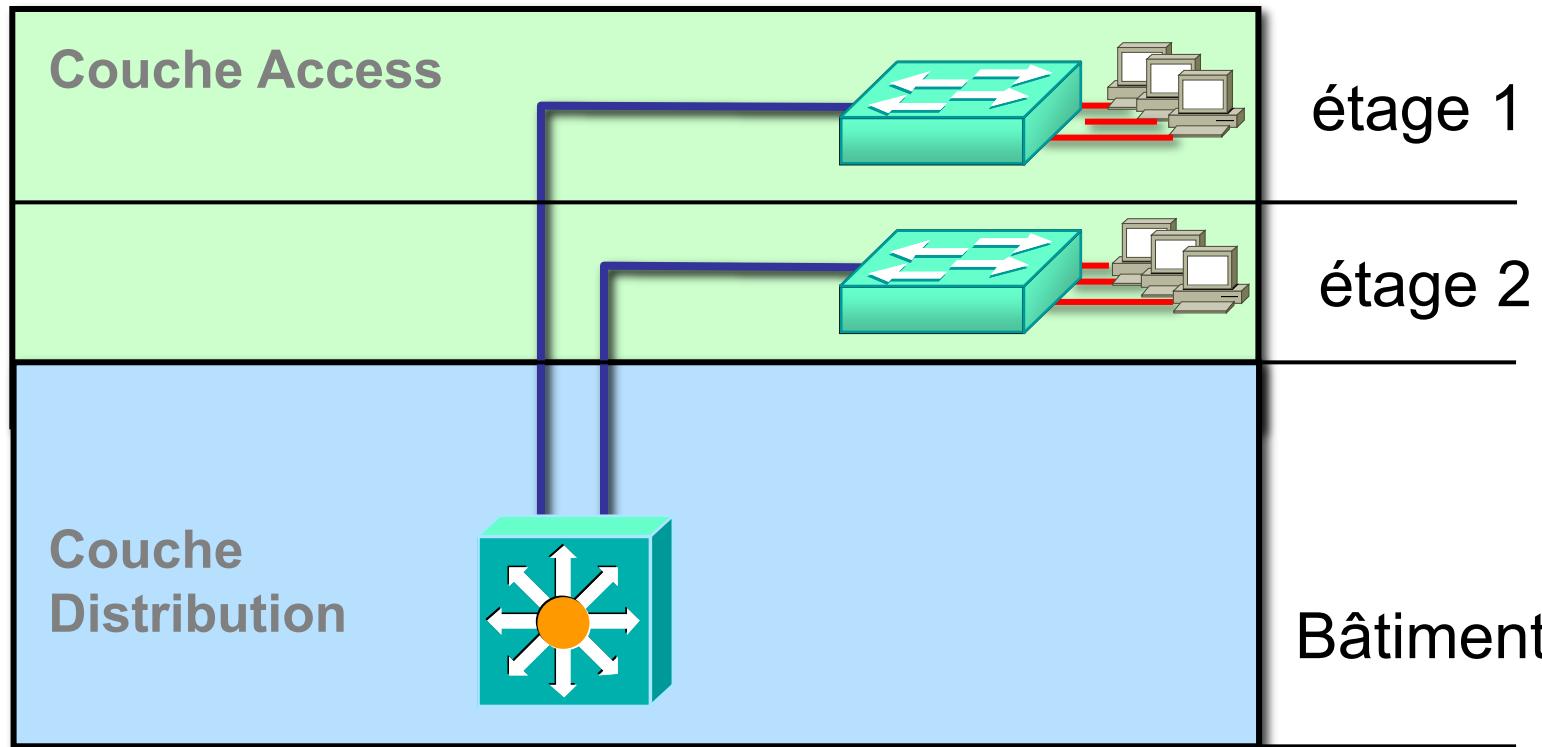
Ethernet

Le modèle hiérarchique

Conception d' un LAN

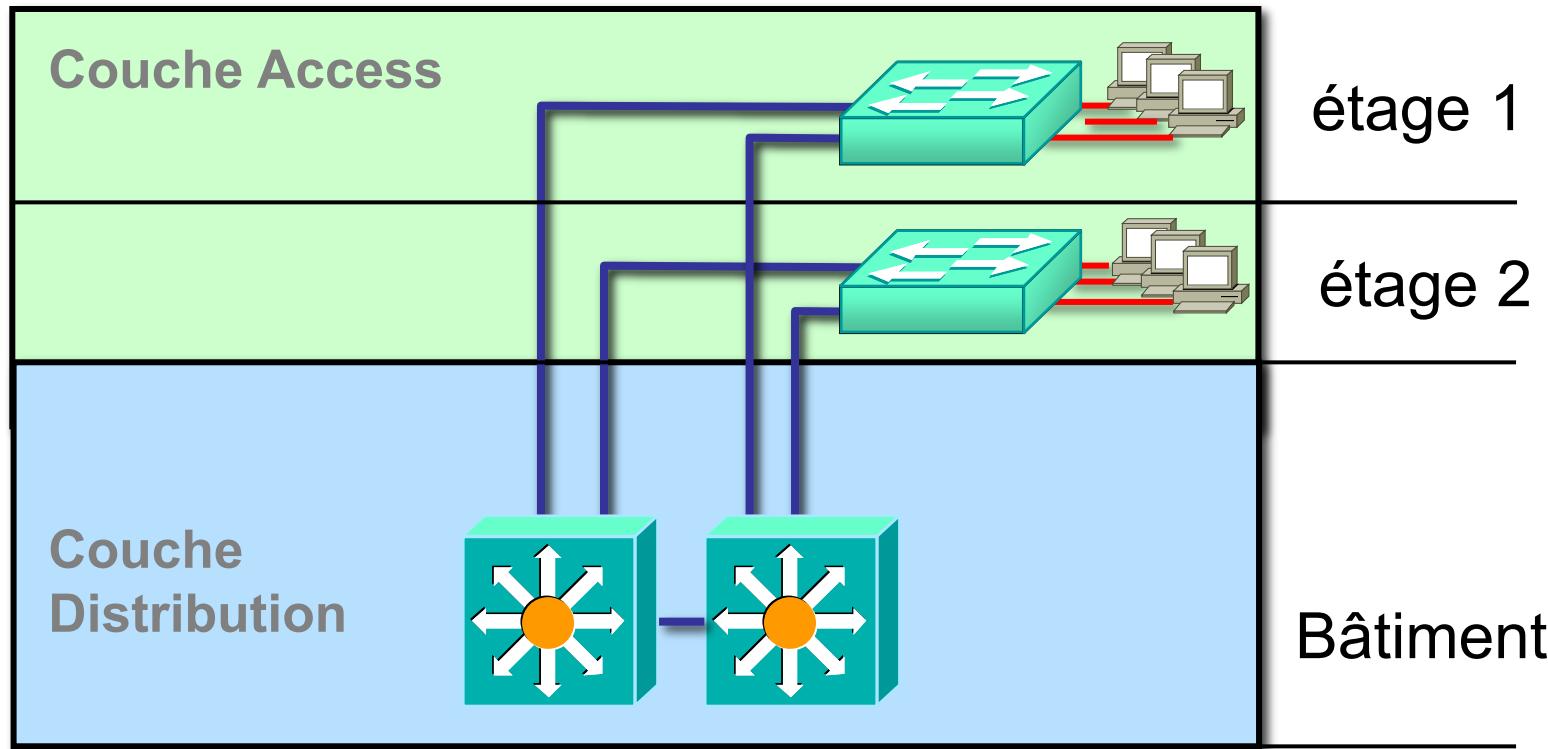
- On utilisera classiquement :
 - des switchs à chaque étage
 - nommés « **switch d' accès** »
 - directement connectés aux PCs
 - des switchs pour relier les étages entre eux
 - nommés « **switch de distribution** »
 - connectés aux switch d' accès

Exemple



Le switch de distribution est alors un point de **défaillance** du réseau

Redondance



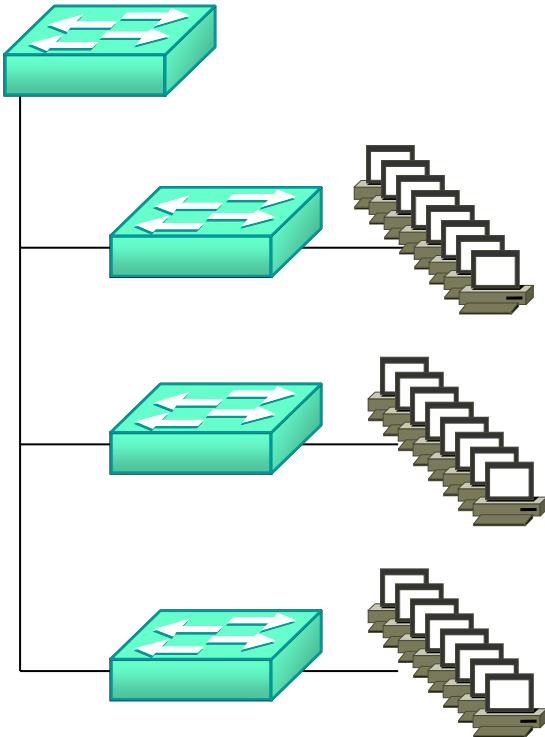
On utilisera **DEUX** switchs de distribution.

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

VLAN

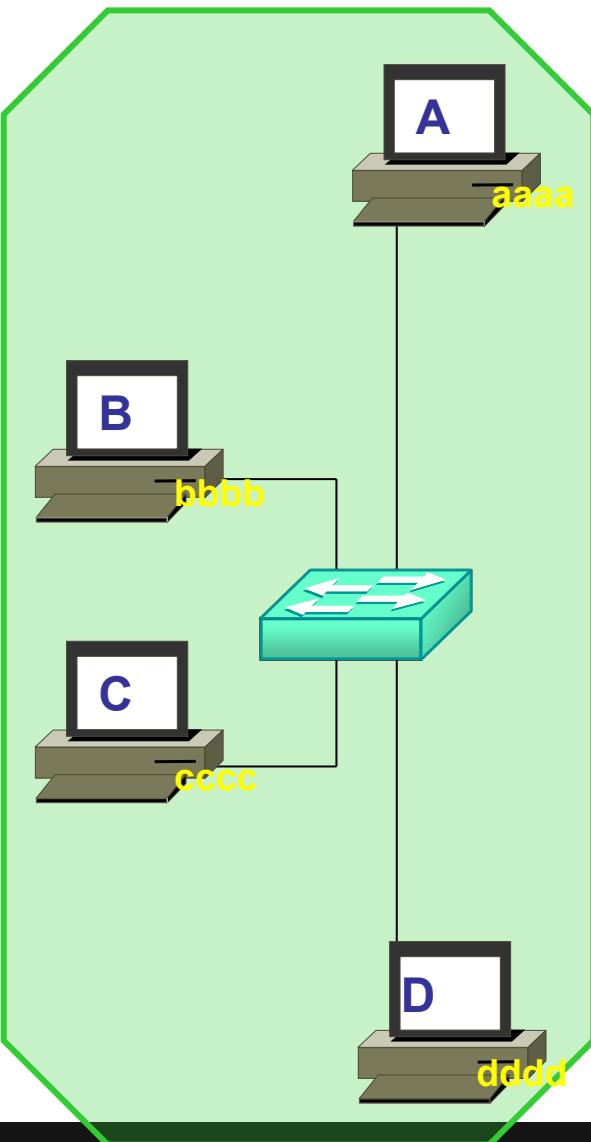
Virtual Local Area Network

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**

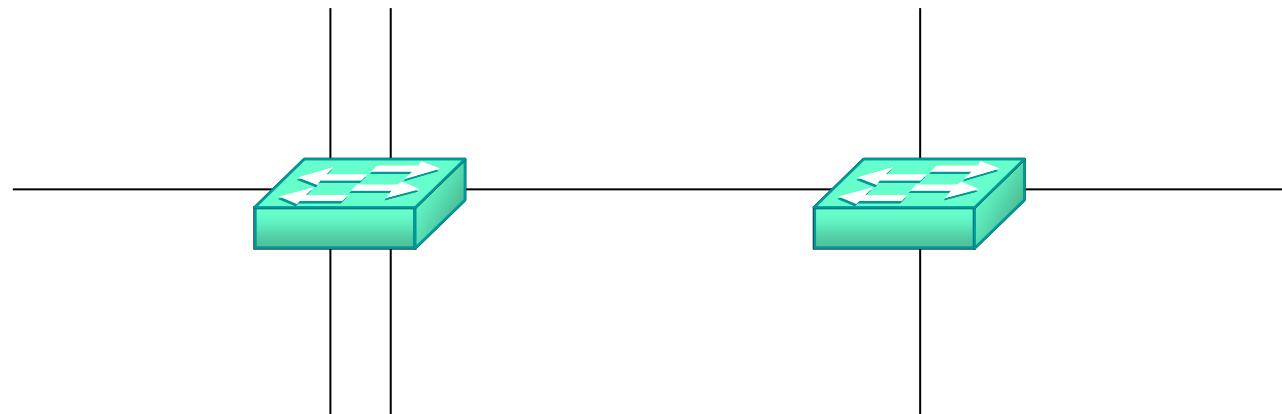
Domaine de broadcast



- 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.

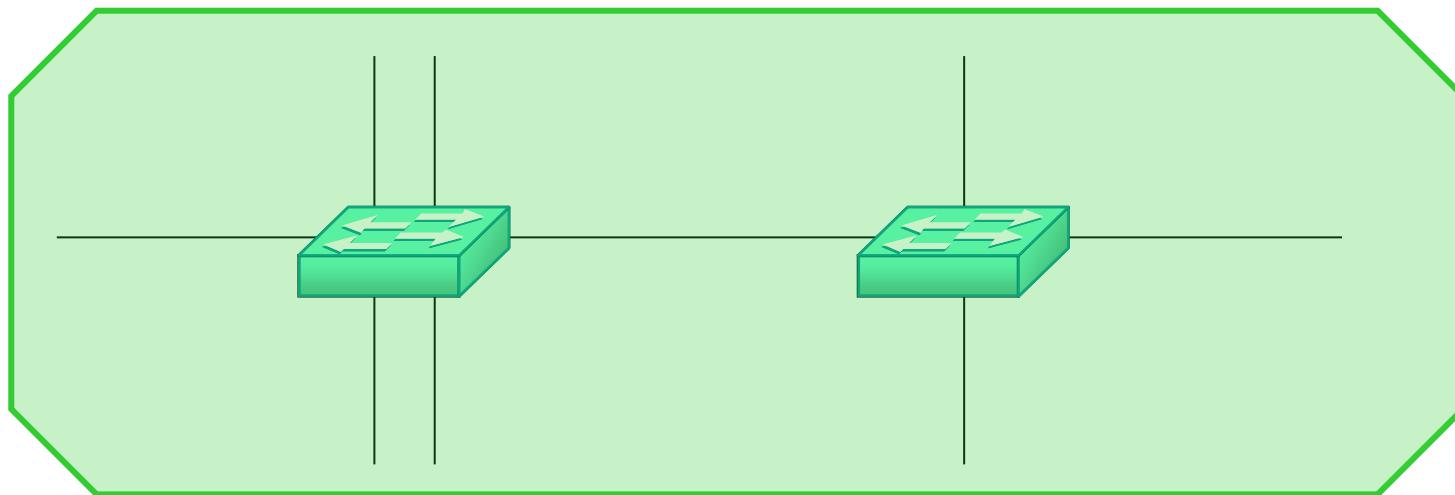
Exercice 1

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



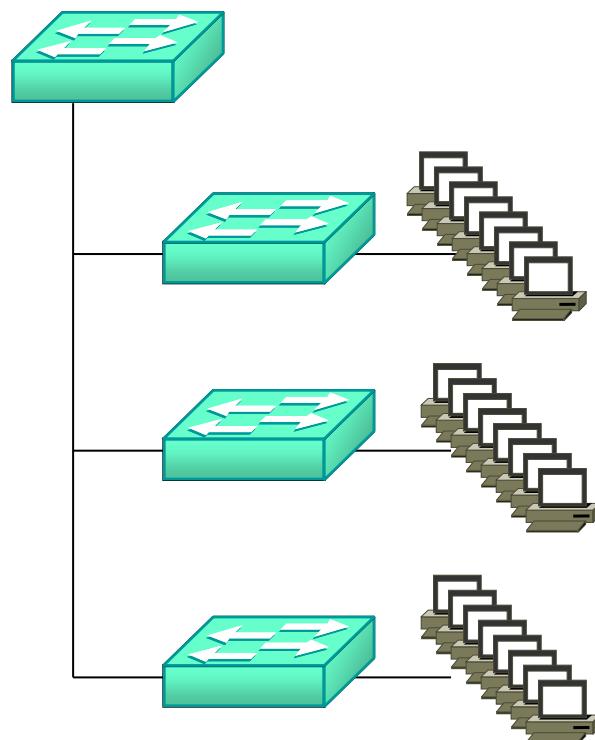
Solution 2

Un seul domaine de broadcast !



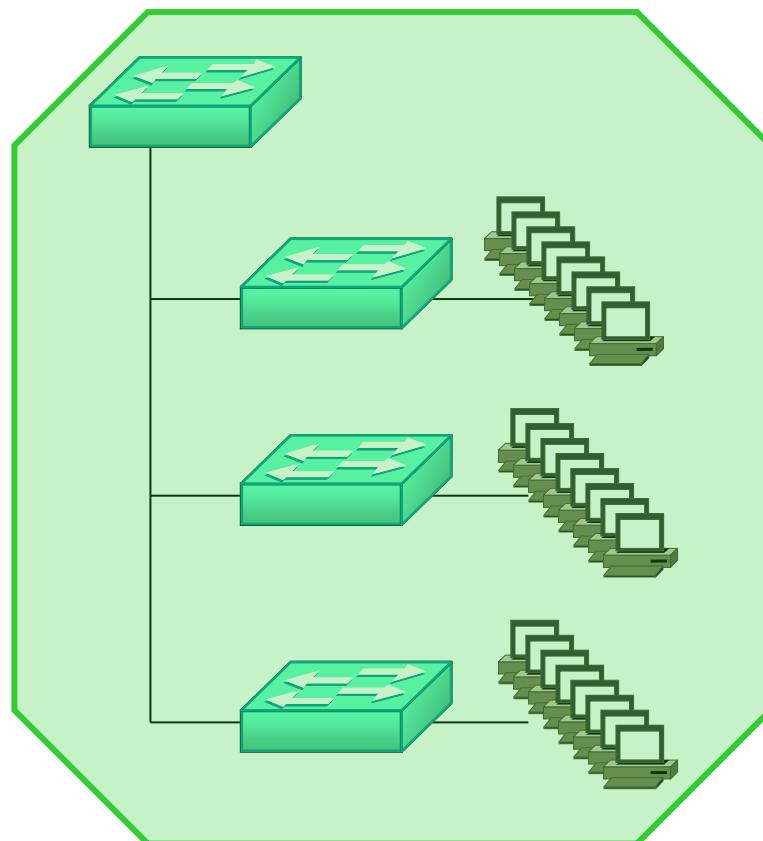
Exercice 2

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



Solution 2

Un seul domaine de broadcast !



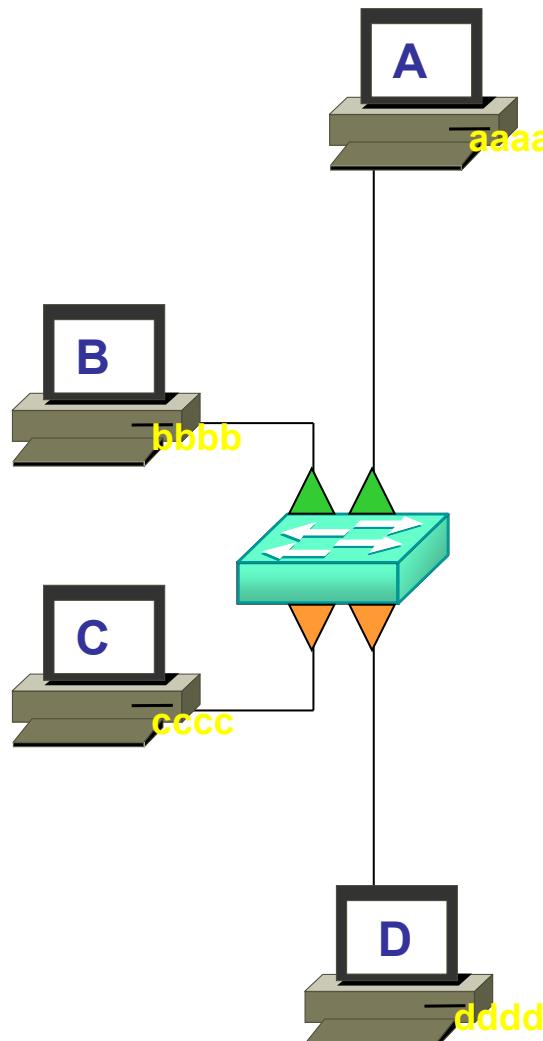
Comment limiter la diffusion des broadcast ?
des multicast ?
des unknown unicast ?

Diviser le domaine de broadcast en plusieurs domaines de broadcast

Les VLANs

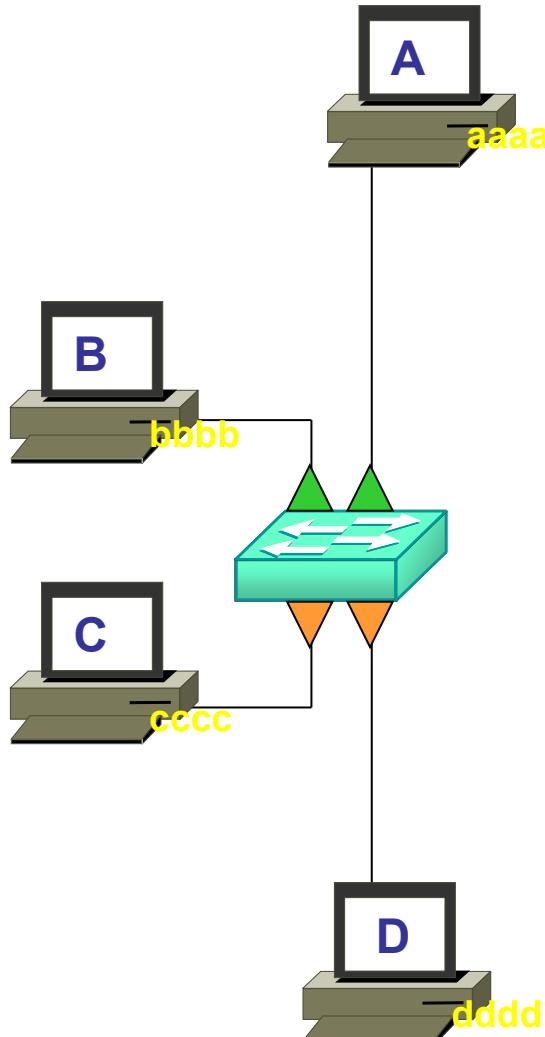
- Créer plusieurs VLANs sur le switch
- Chaque VLAN représente un domaine de broadcast :
 - **le switch ne permettra aucune communication entre 2 VLANs**
- Chaque VLAN est identifié par un **numéro entre 1 et 4096**

Exemple : 2 VLANs



- Crée 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

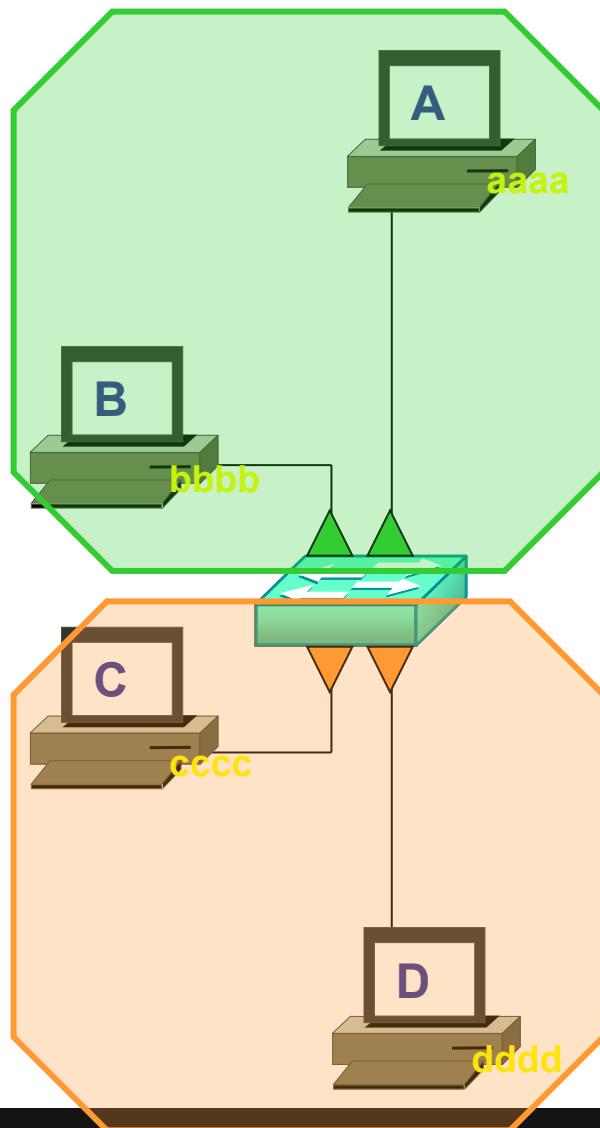


- Quel que soit le type de trame (unicast, broadcast, multicast) , seules les communications suivantes seront possibles :

- A et B
- C et D

Aucune autre communication ne sera autorisée par le switch !

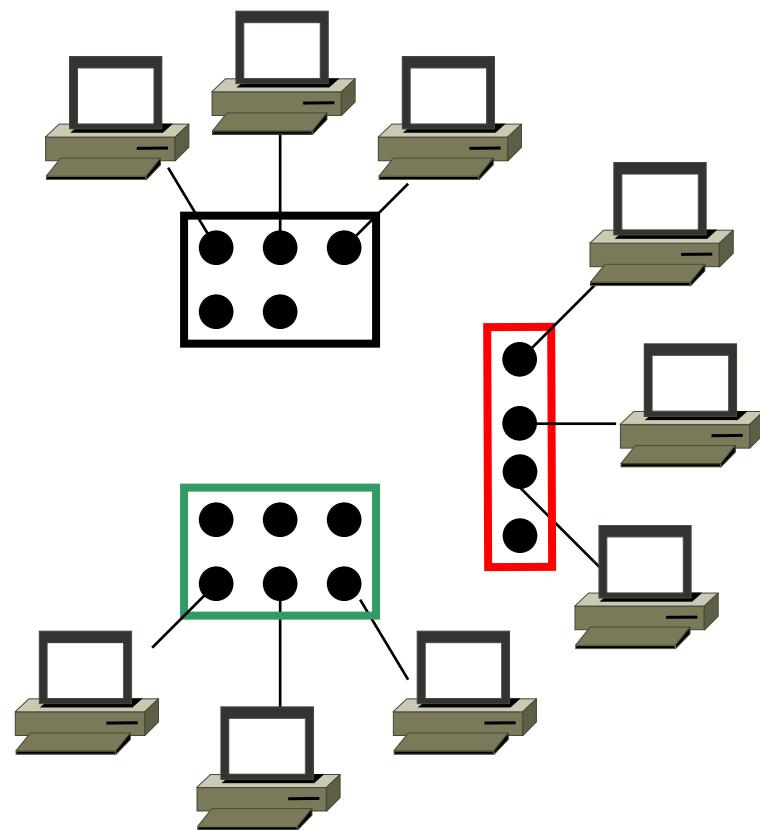
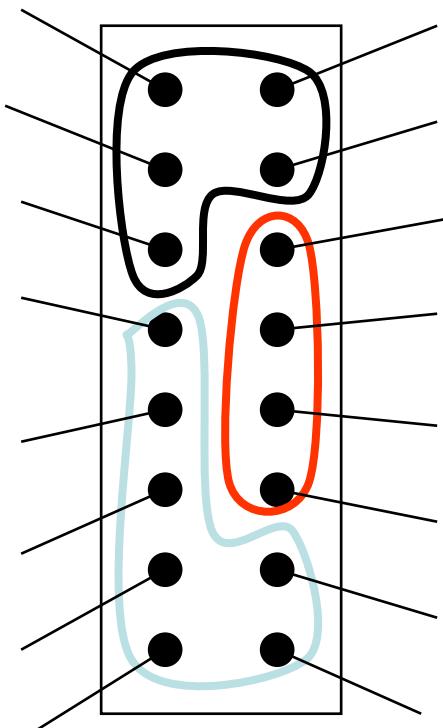
Exemple : 2 VLANs



- 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
```

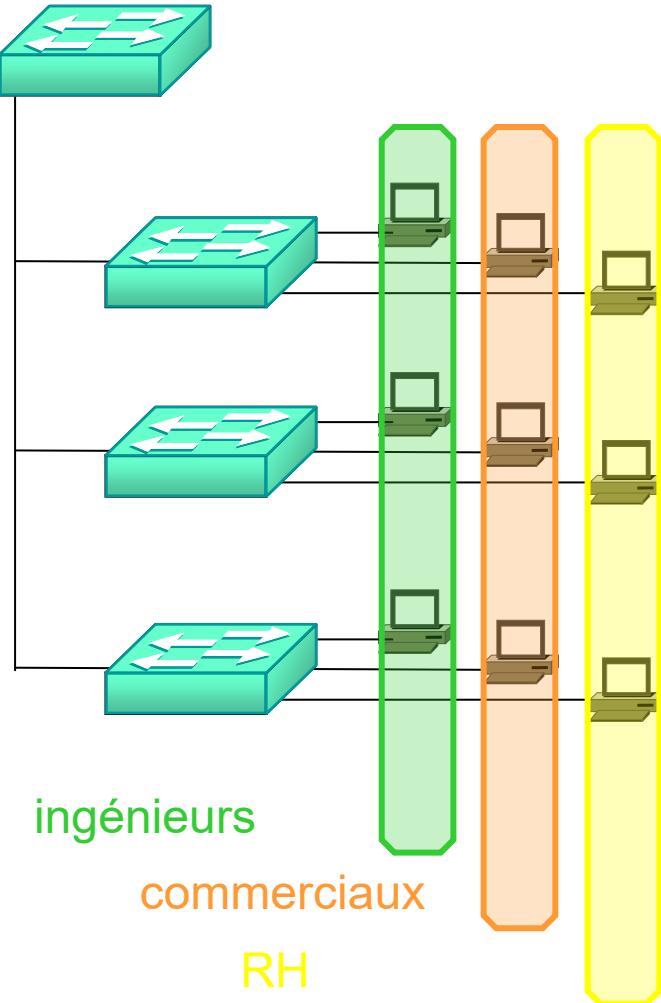
Vérifier les VLAN

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

VLAN

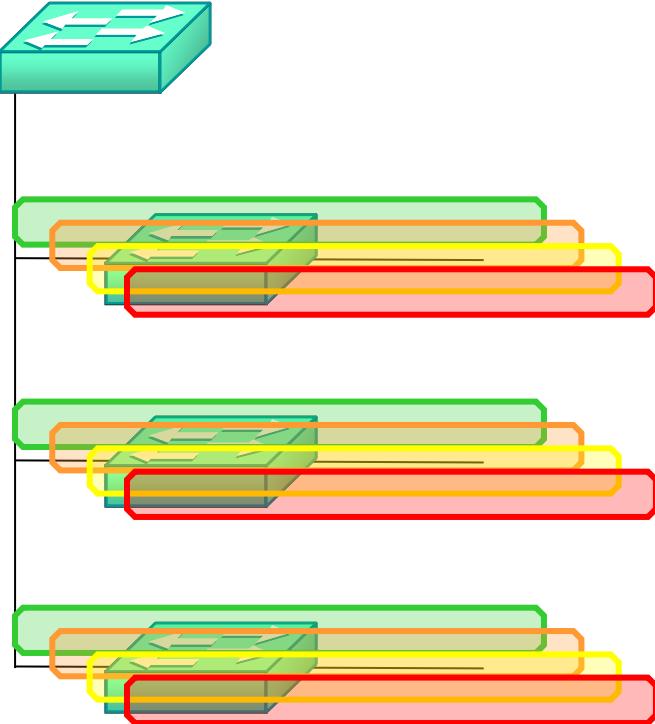
Implémentation

Implémentation n° 1



- Objectifs recherchés :
 - segmentation
 - flexibilité
 - sécurité

Implémentation n° 2

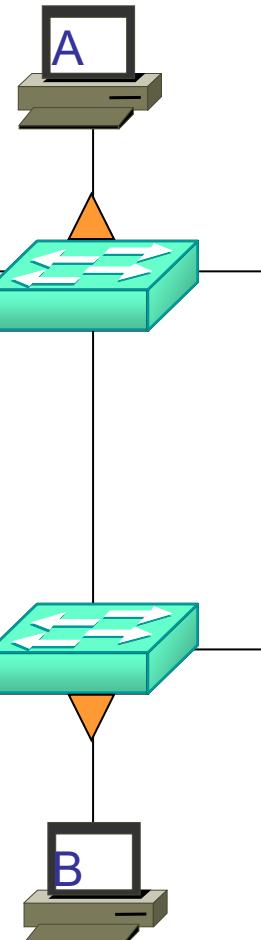


- Objectifs recherchés :
 - chaque VLAN regroupe un certain type de trafic :
 - Data
 - Management réseau
 - Voix
 - accès invités
 - Wi-Fi
 - Imprimantes

VLAN

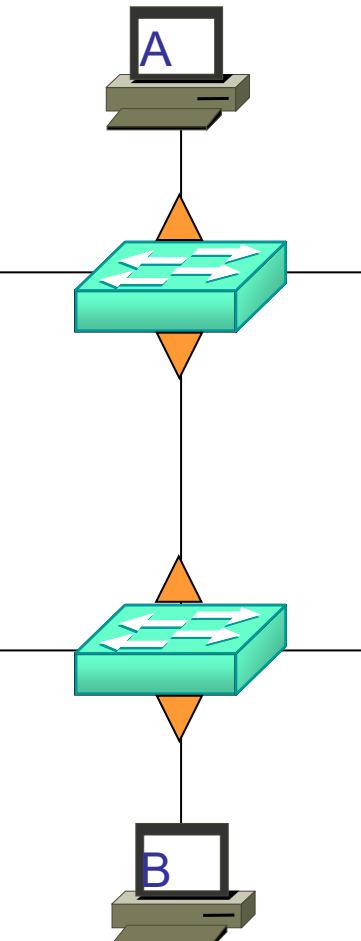
Liaisons « Trunk »

Un VLAN sur plusieurs switchs



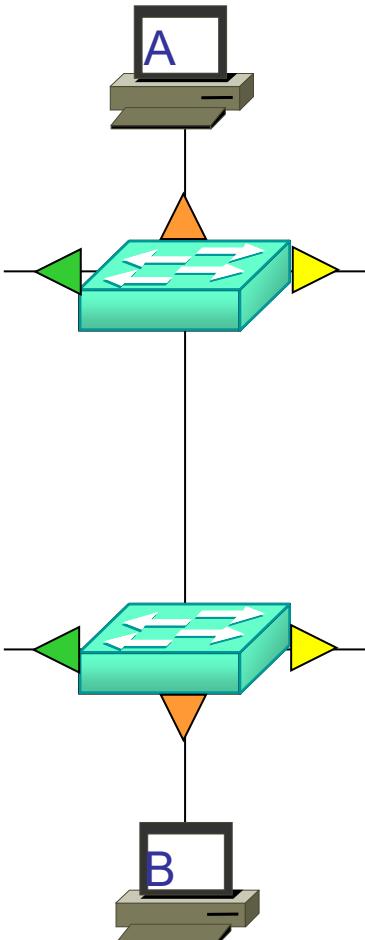
- Le VLAN **100** est utilisé sur les 2 switch.
- Comment permettre aux équipements A et B de communiquer ensemble ?

Un VLAN sur plusieurs switchs



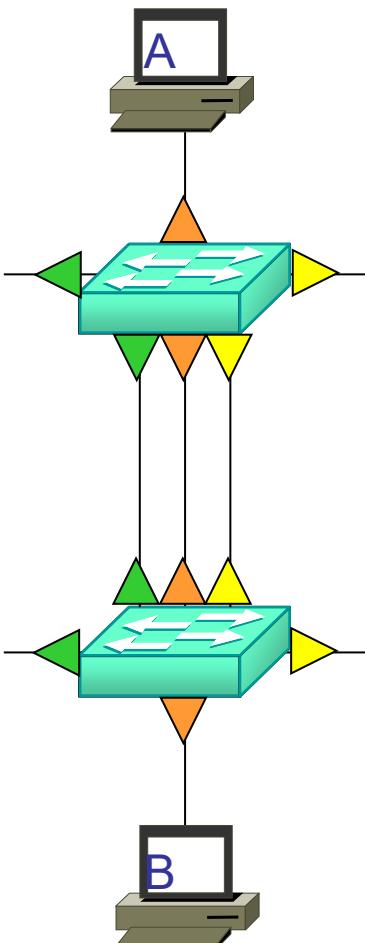
- Le VLAN **100** est utilisé sur les 2 switch.
- Affecter l' inter-switch au VLAN **100**

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 ?

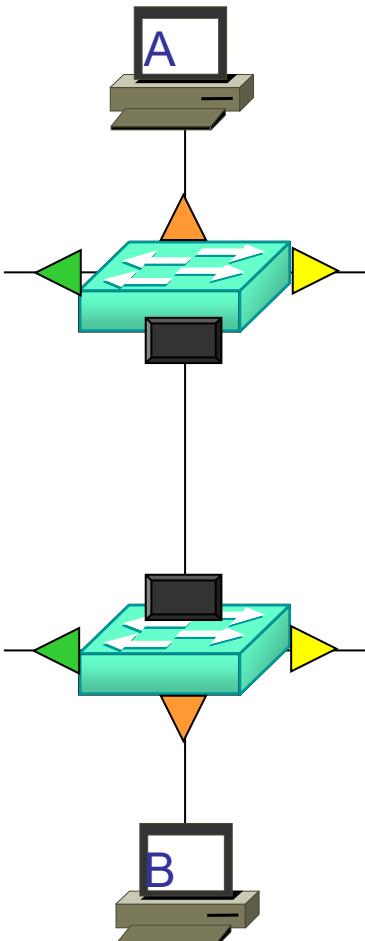
Trois VLAN sur plusieurs switchs



- 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



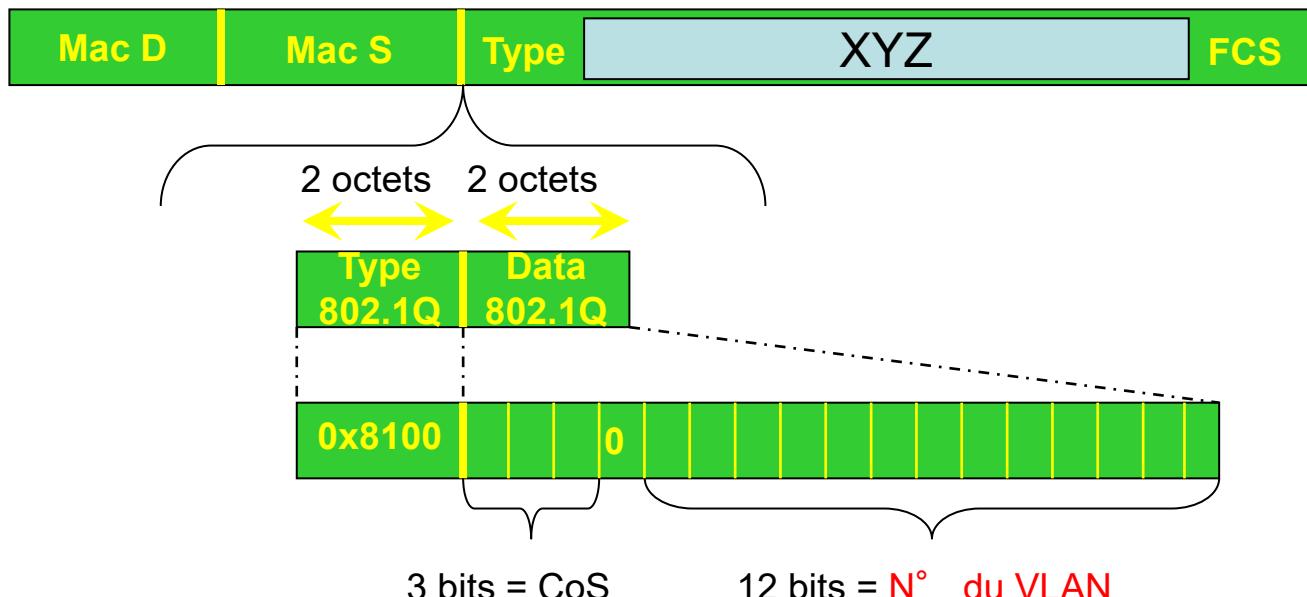
- Les VLAN 100, 200 et 300 sont utilisés sur les 2 switch.
- Configurer l' interco entre les 2 switchs en mode **TRUNK** :
 - Tous les VLANs seront **autorisés** sur l' interface trunk
 - Sur l' interface trunk, les trames seront **taggées** avec le n° du VLAN

Le TAG 802.1Q

- Trame originale, non taggée :

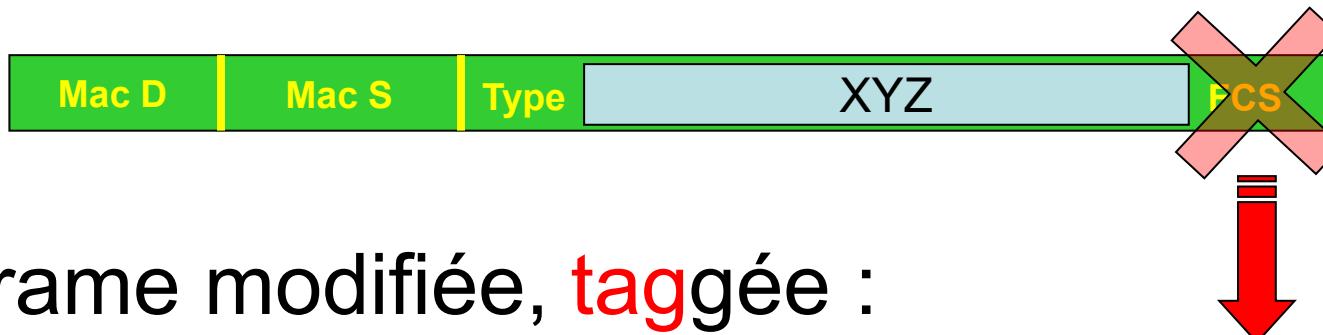


- Trame modifiée, taggée :

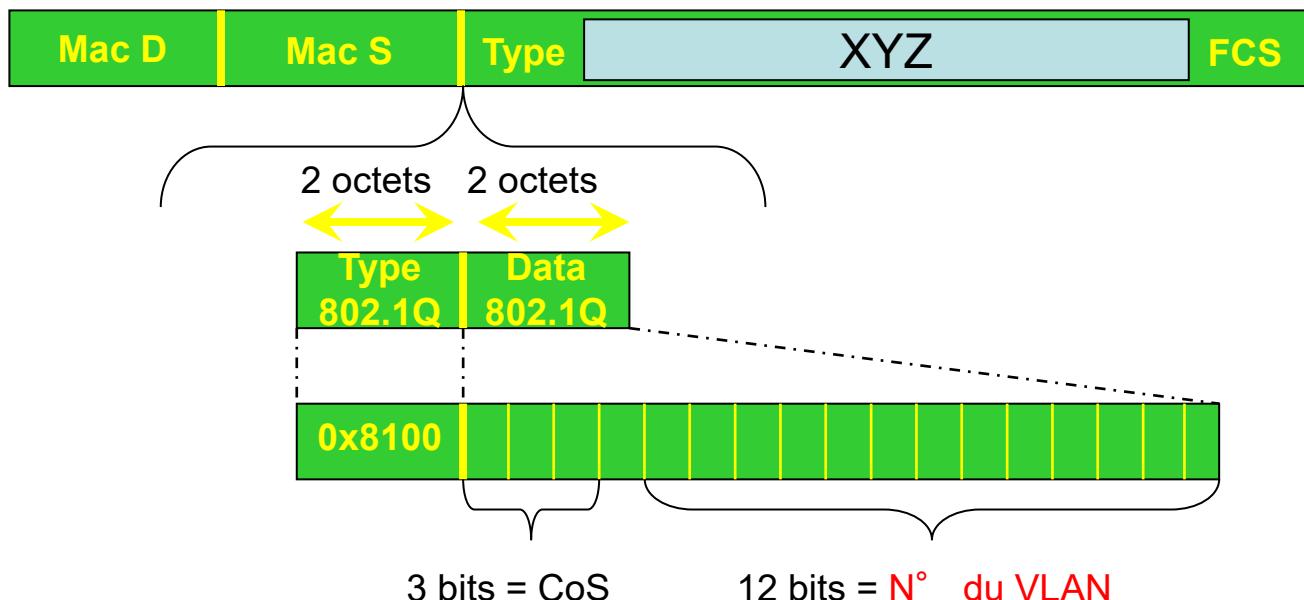


FCS recalculée !

- Trame originale, non taggée :



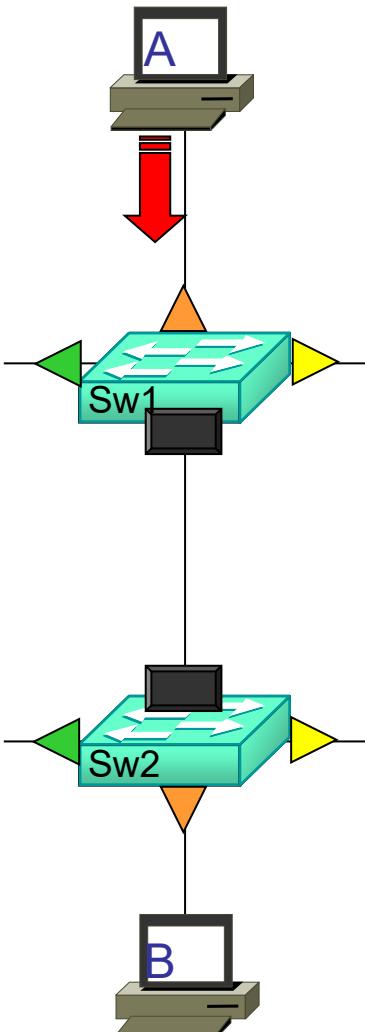
- Trame modifiée, taggée :



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.

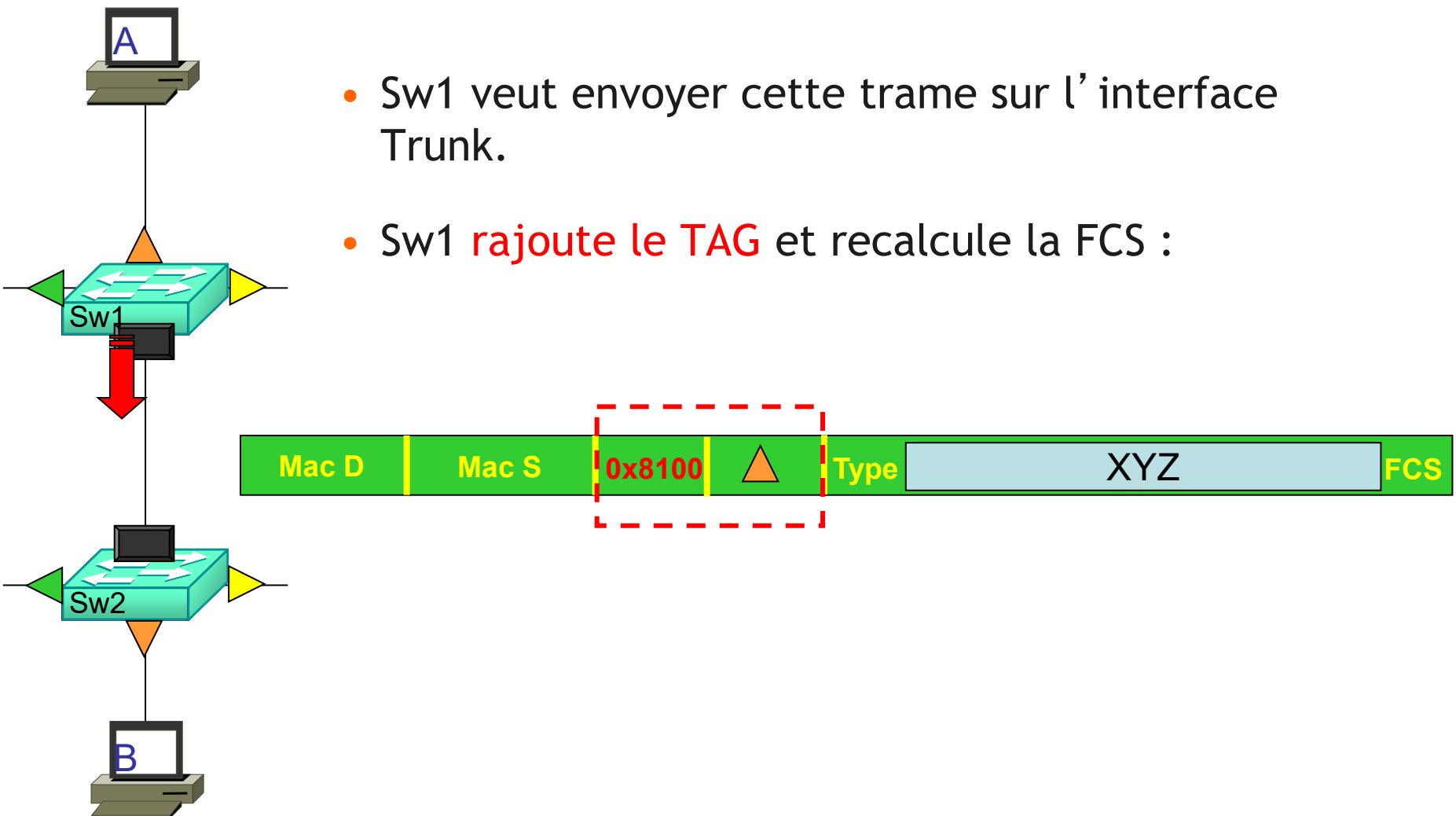
Exemple 1/3



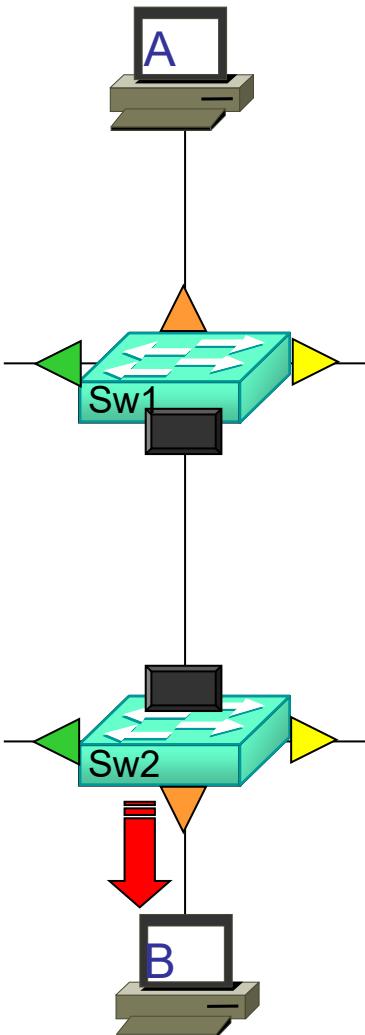
- A envoie une trame à B.
- A génère cette trame.
- Elle n'est pas taggée :



Exemple 2/3



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

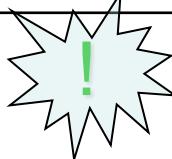
Operational Mode: trunk

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

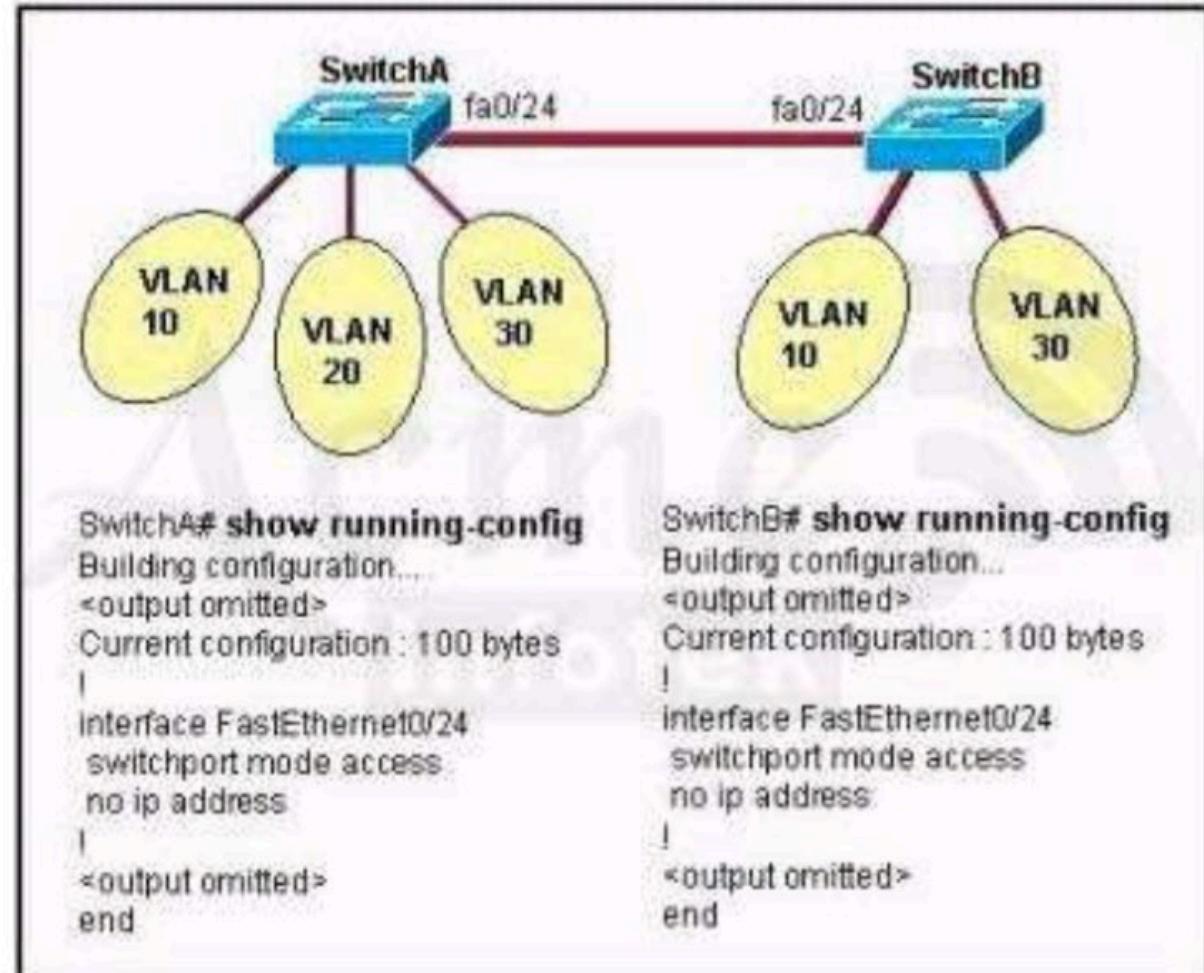
Fa0/0 1,100

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

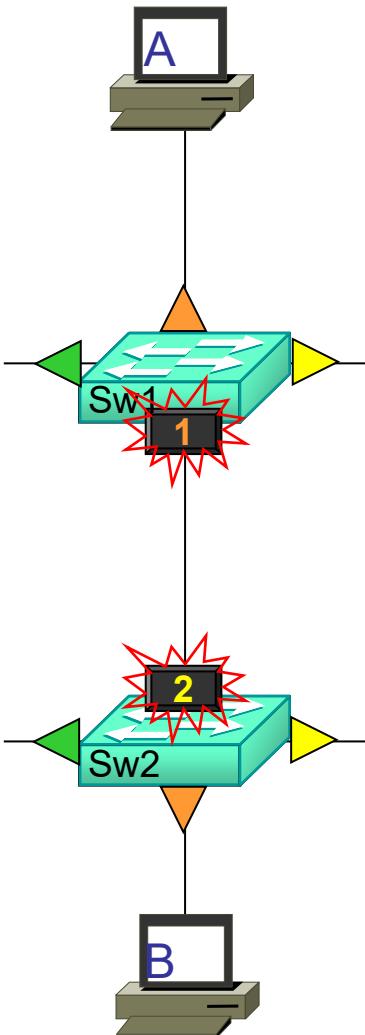
Port Vlans allowed and active in management domain

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 ?

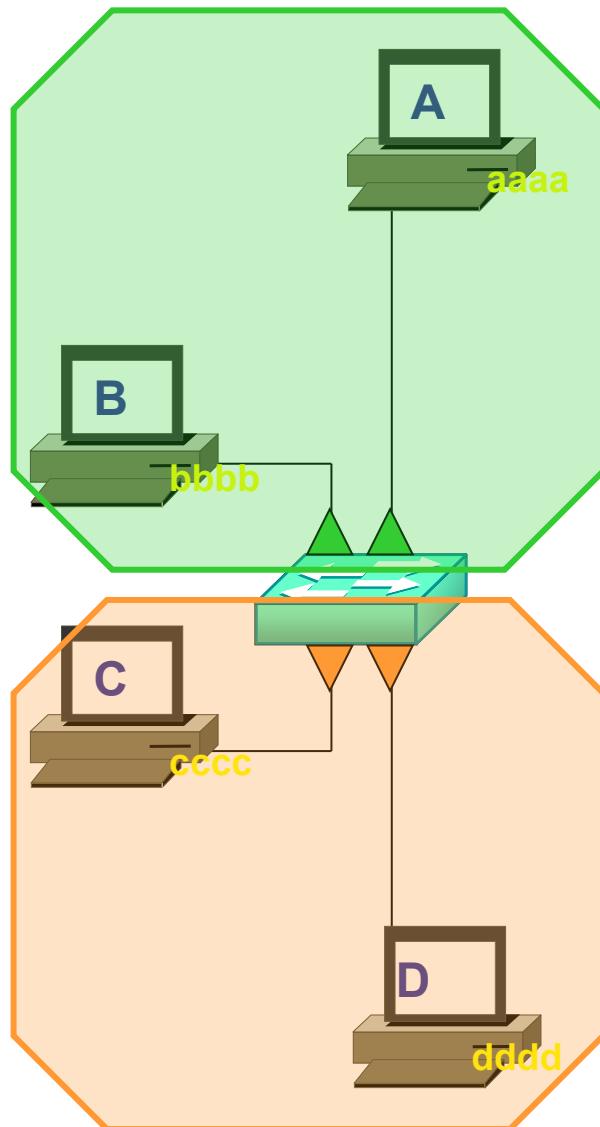
Bilan des commandes trunk

- 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 !

Router on the stick

Routage inter-VLAN

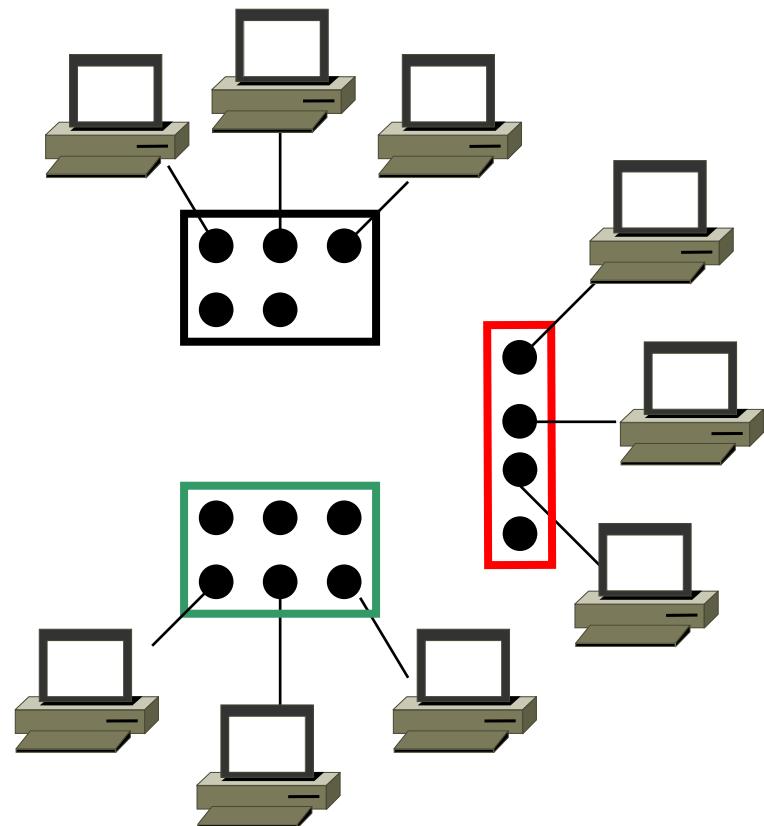
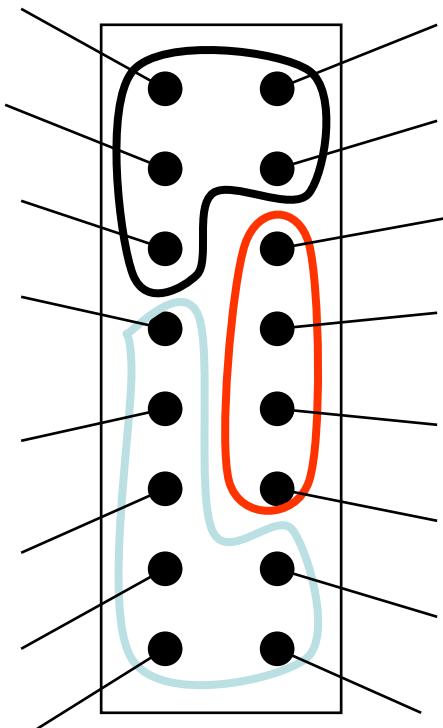
Rappel : 2 VLANs



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

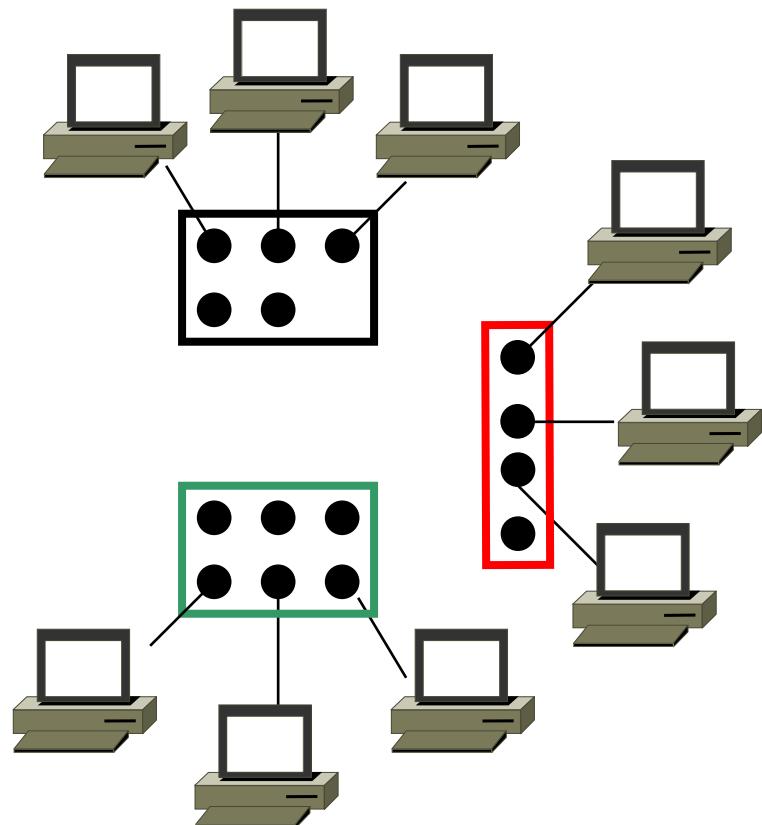
Vue logique des VLANs

- 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



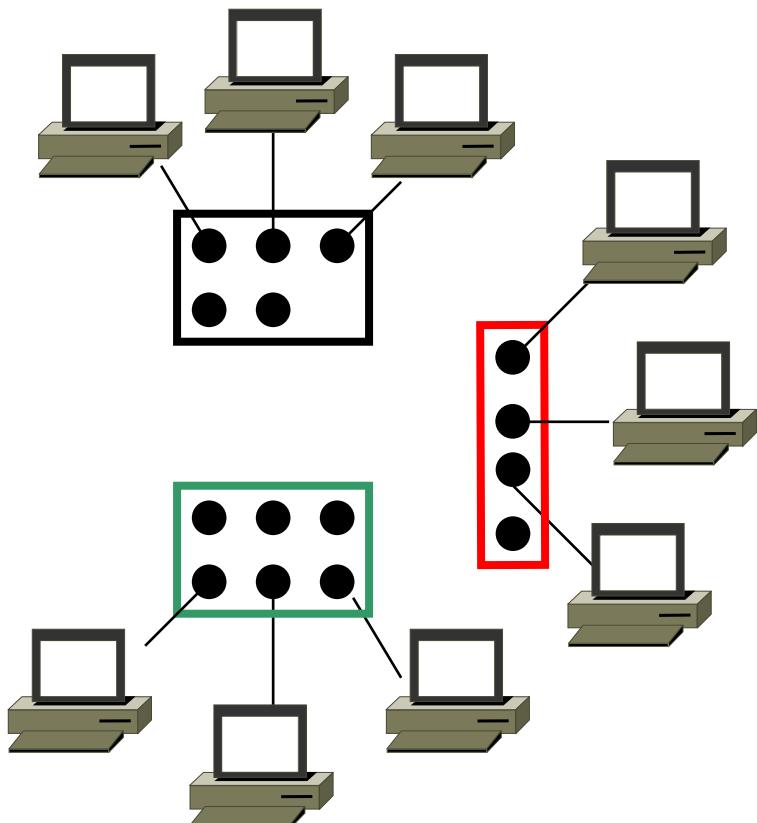
Vue logique des VLANs

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

PROBLEME :

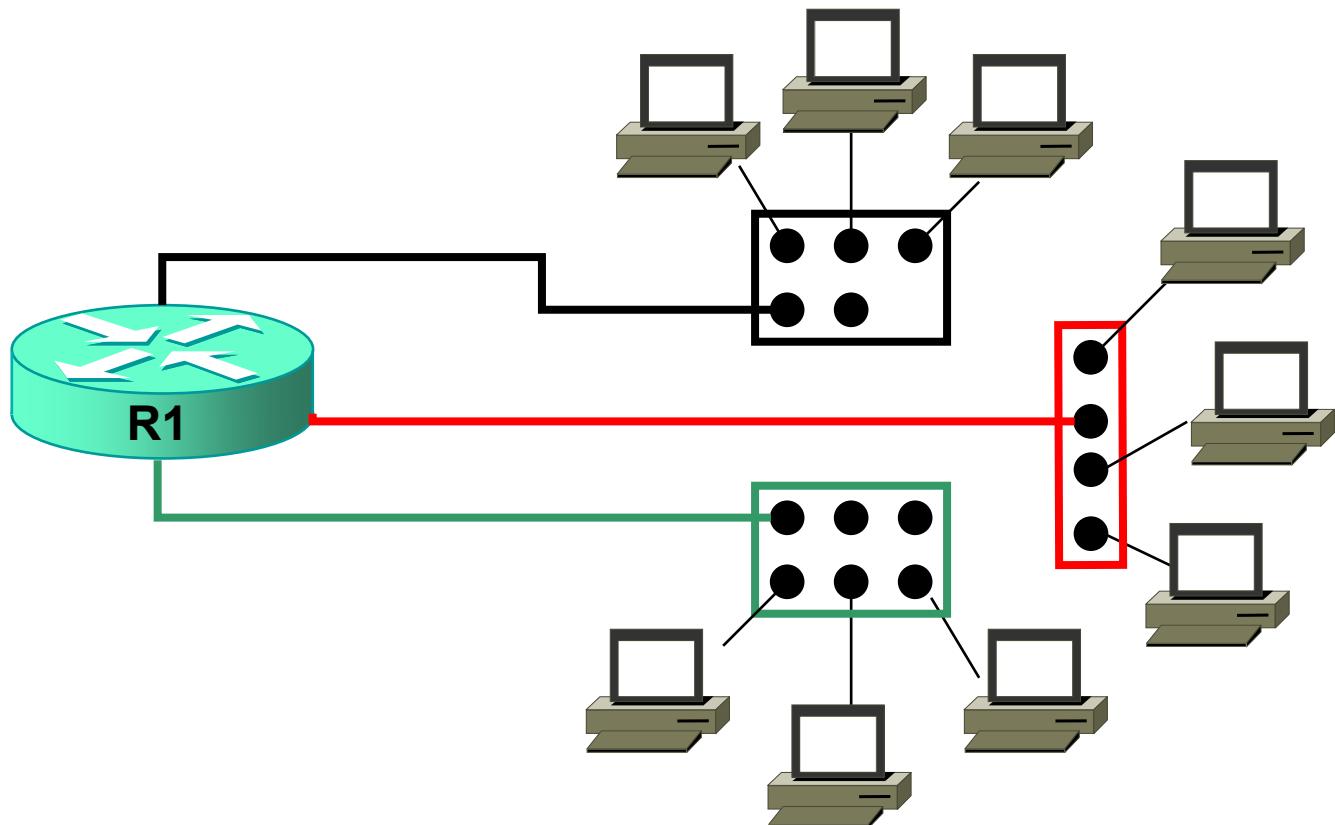
les équipements placés dans différents VLANs ne peuvent plus communiquer ensemble !

SOLUTION :
utiliser un ROUTEUR.



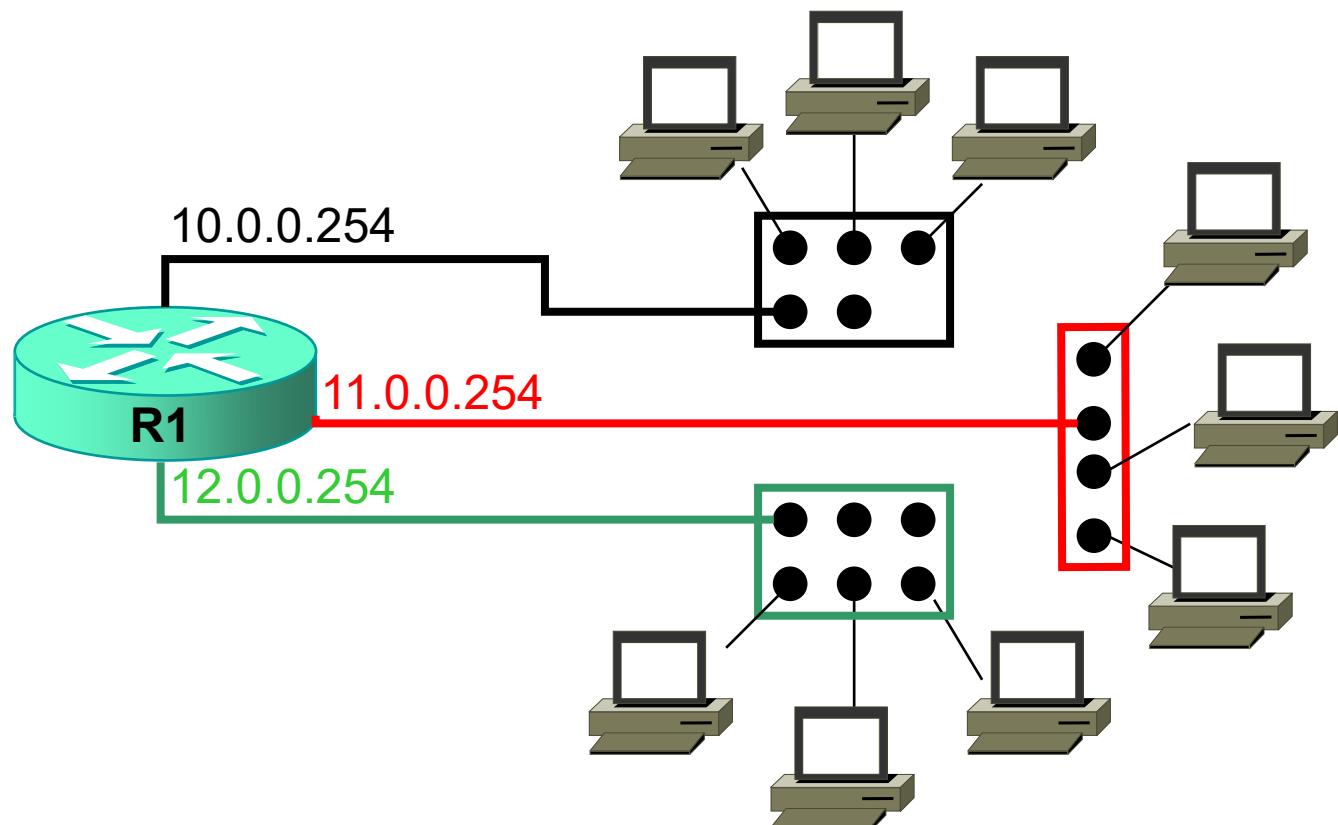
Utiliser un routeur

- Le routeur devra avoir une interface dans chaque VLAN :



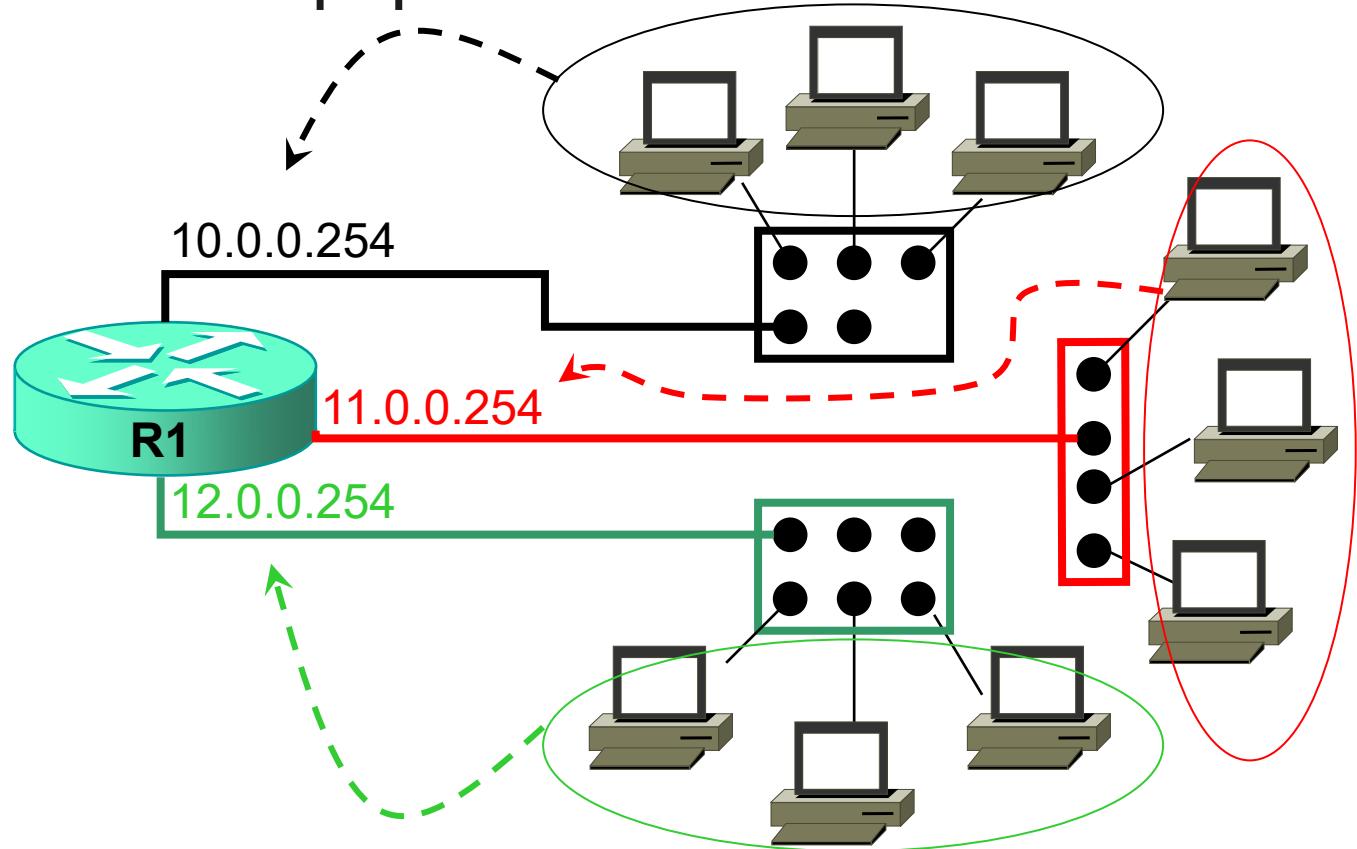
Utiliser un routeur

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



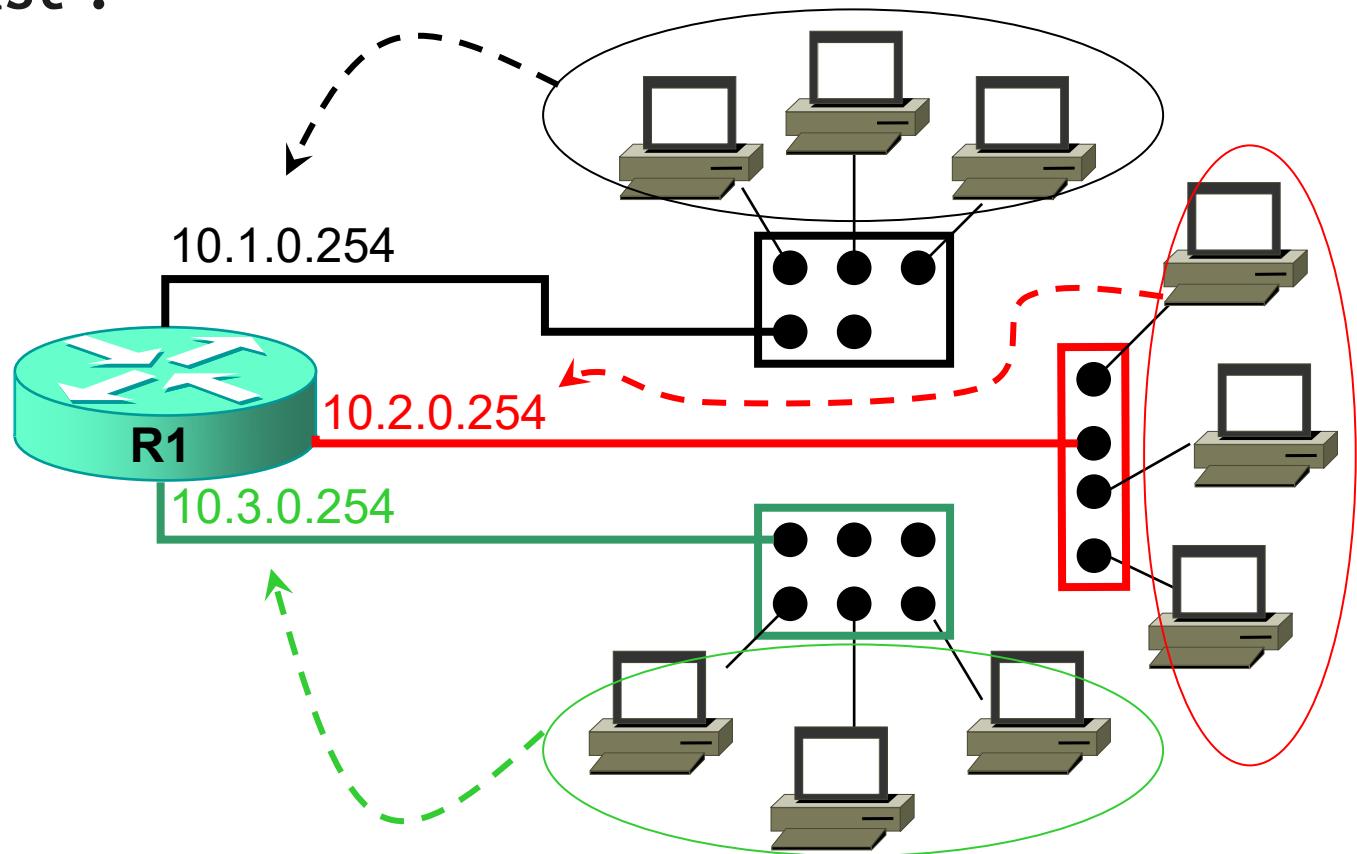
Utiliser un routeur

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



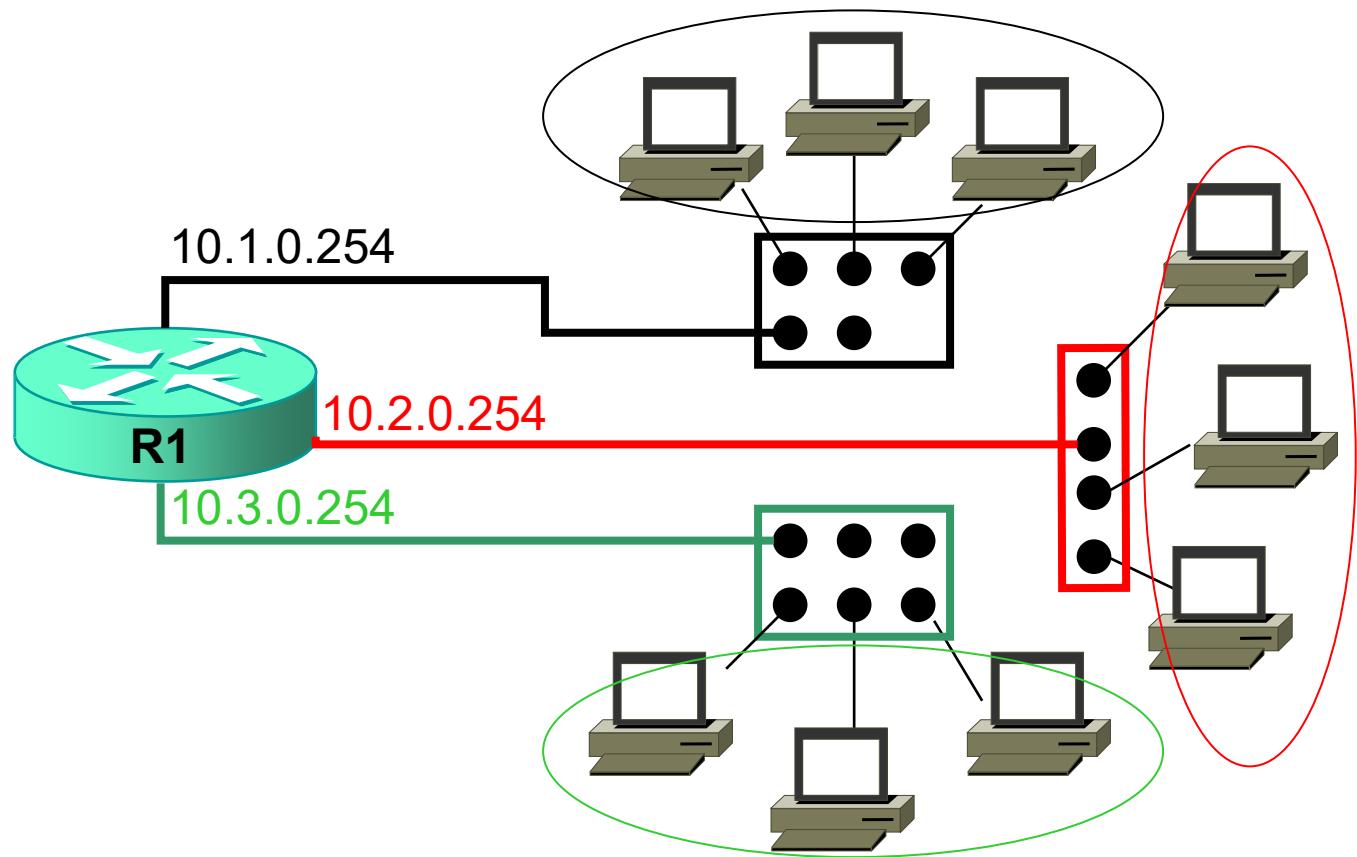
Domaine de broadcast

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



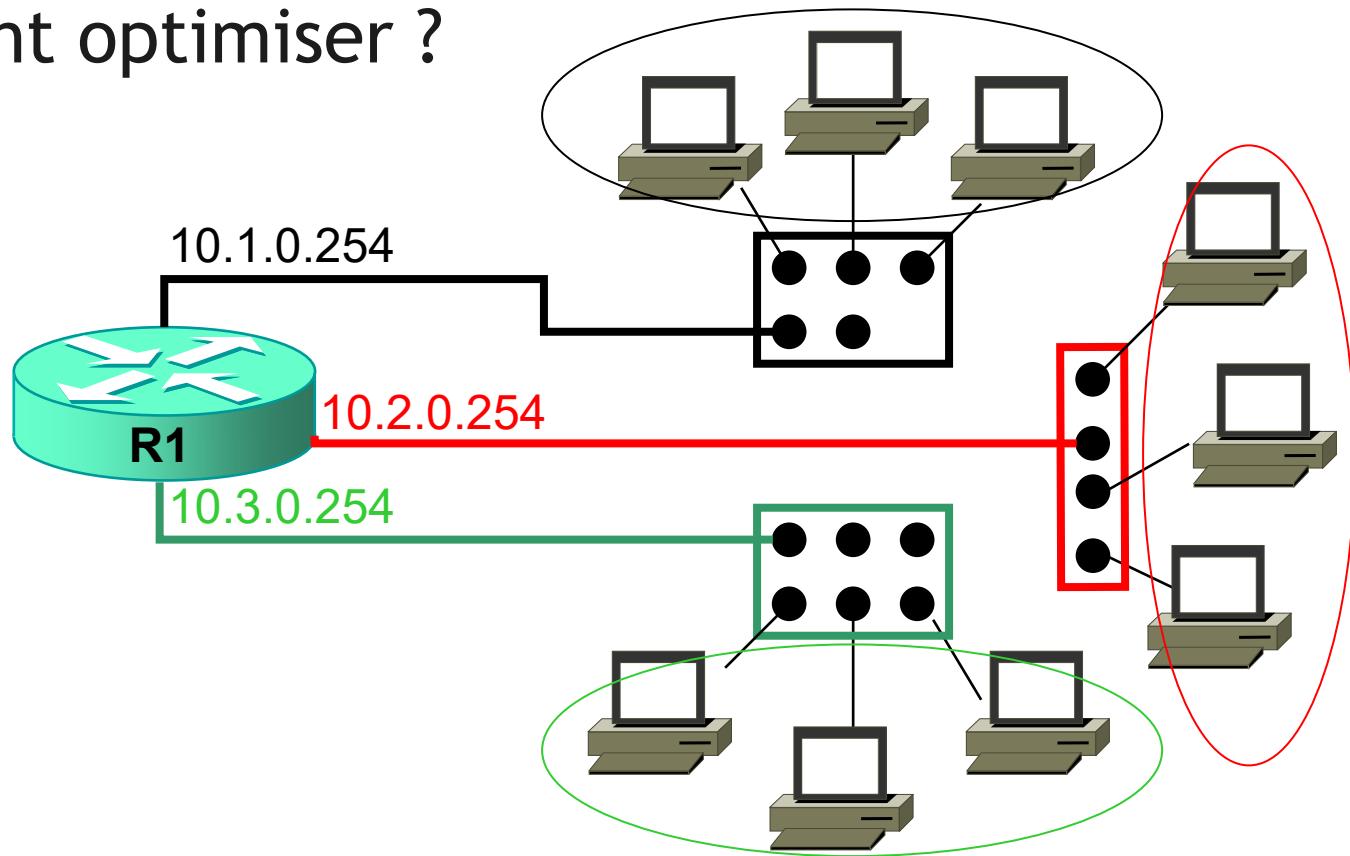
Domaine de broadcast

- Toujours TROIS !



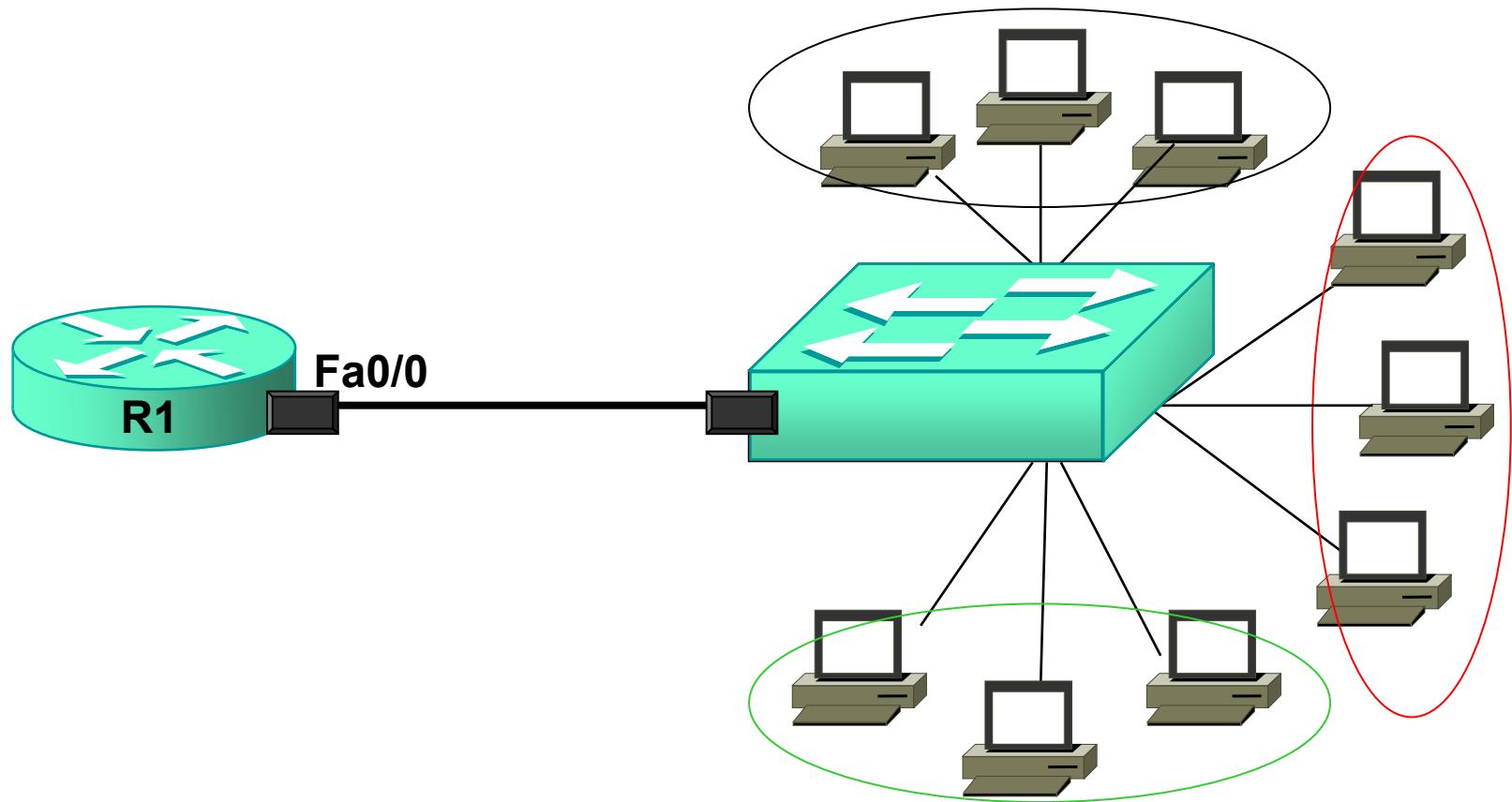
Optimiser

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

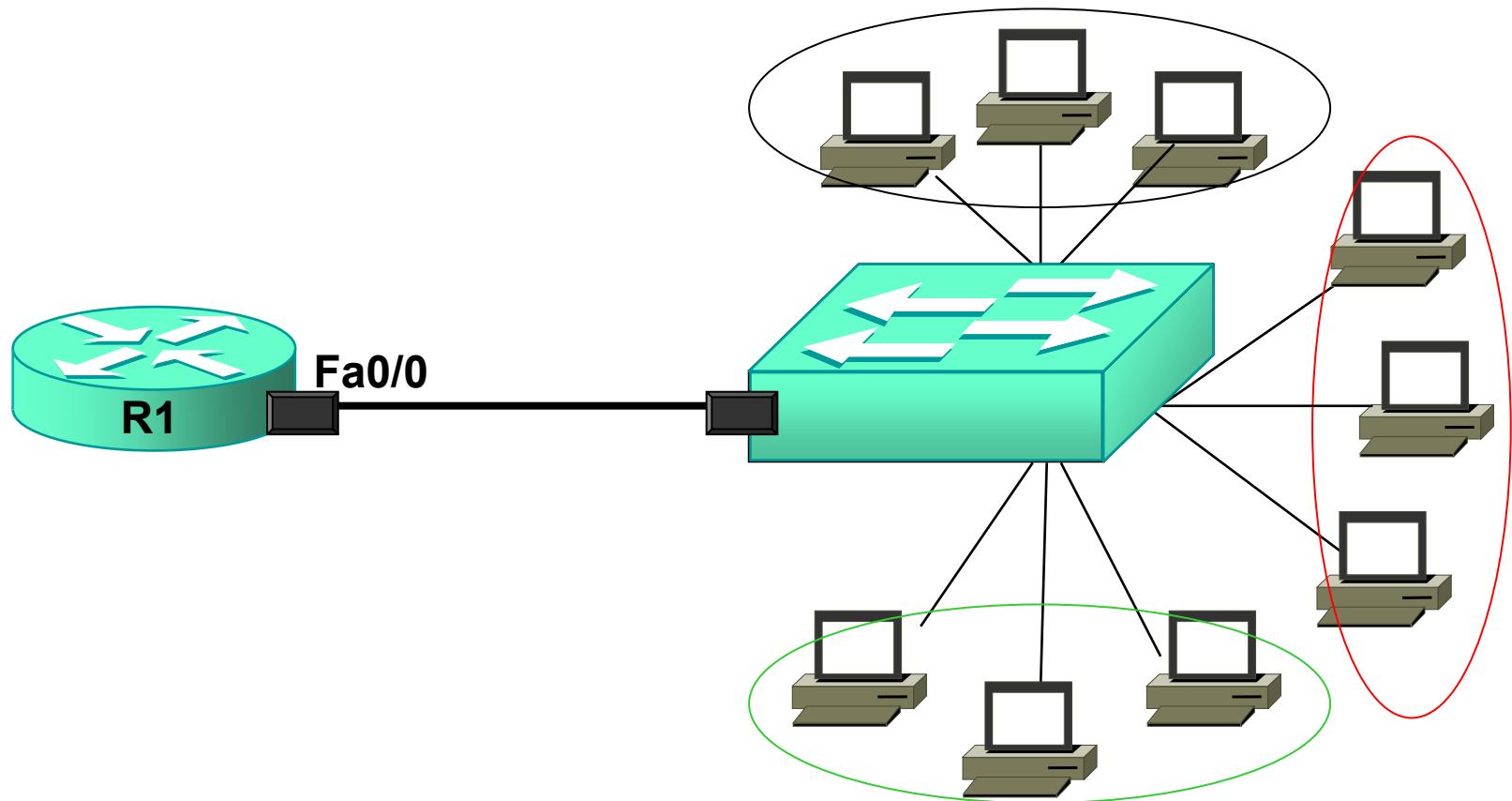


Trunk

- Utiliser une seule interface, en **trunk** !

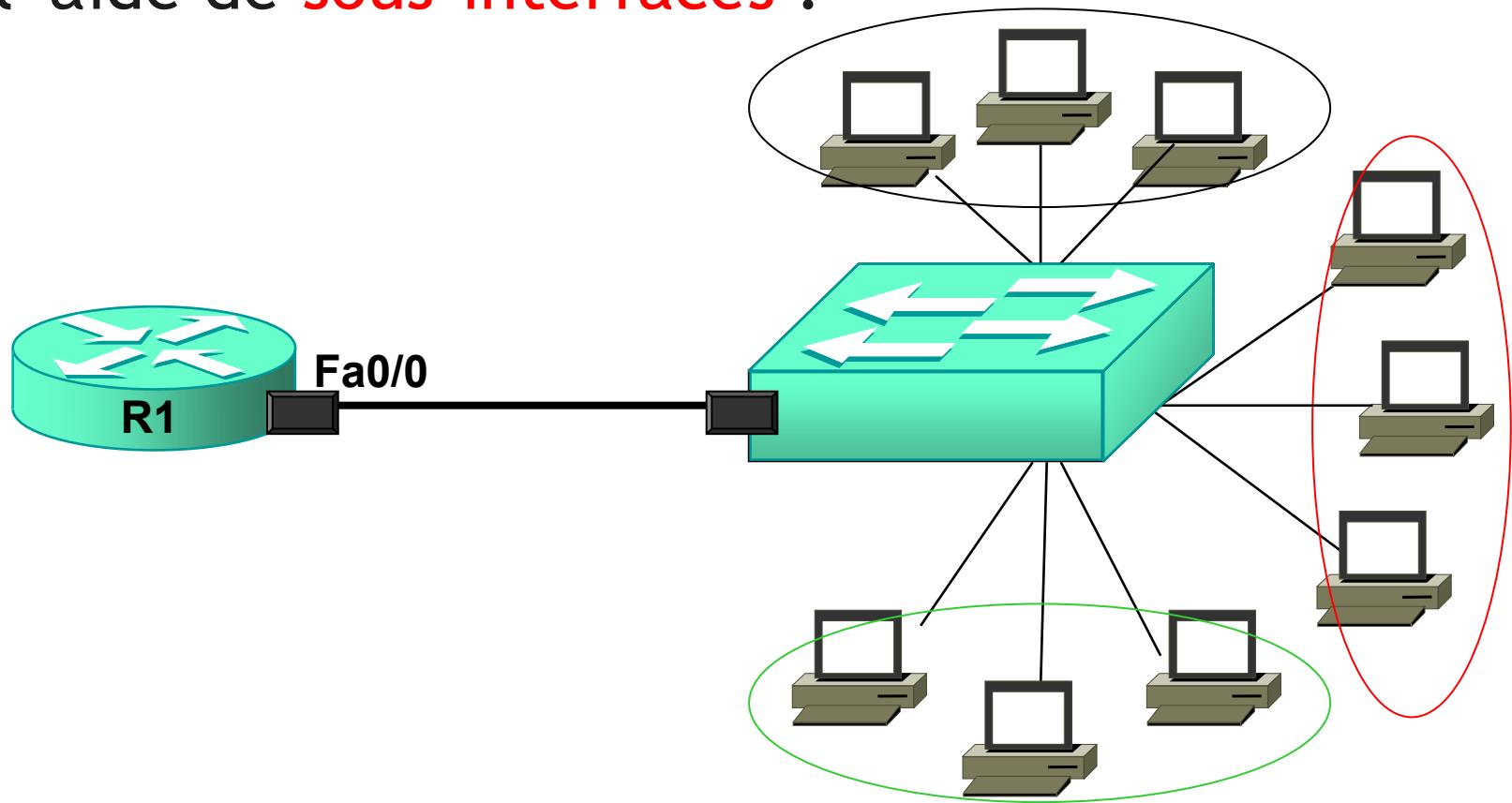


- Quelle adresse IP mettre sur le routeur ?



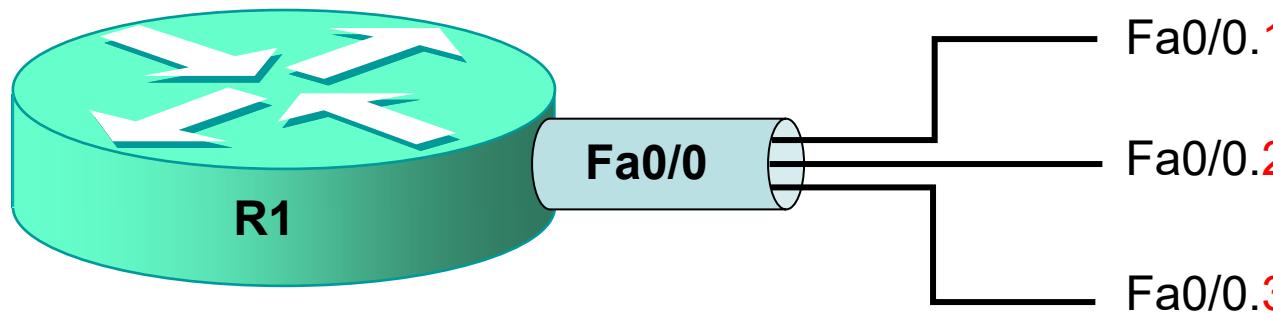
Trunk

- 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.

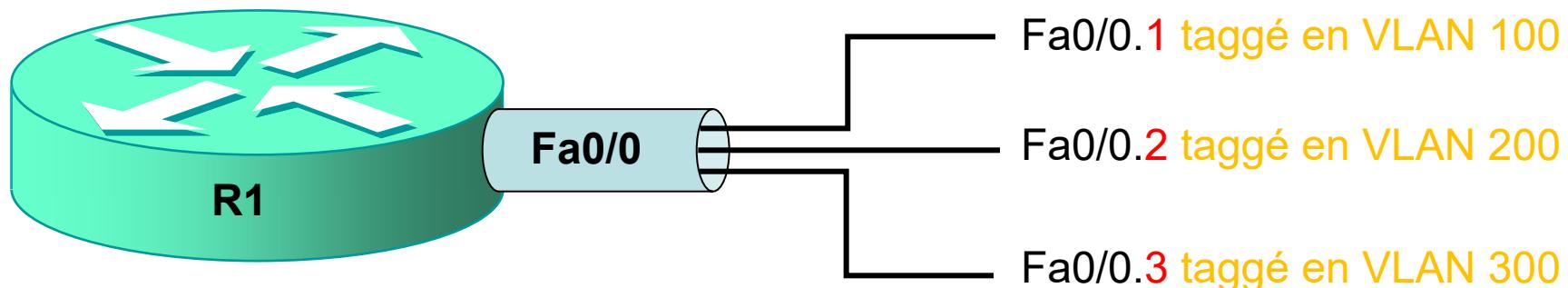


POUR CRÉER les
SOUS-INTERFACES :

{
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**



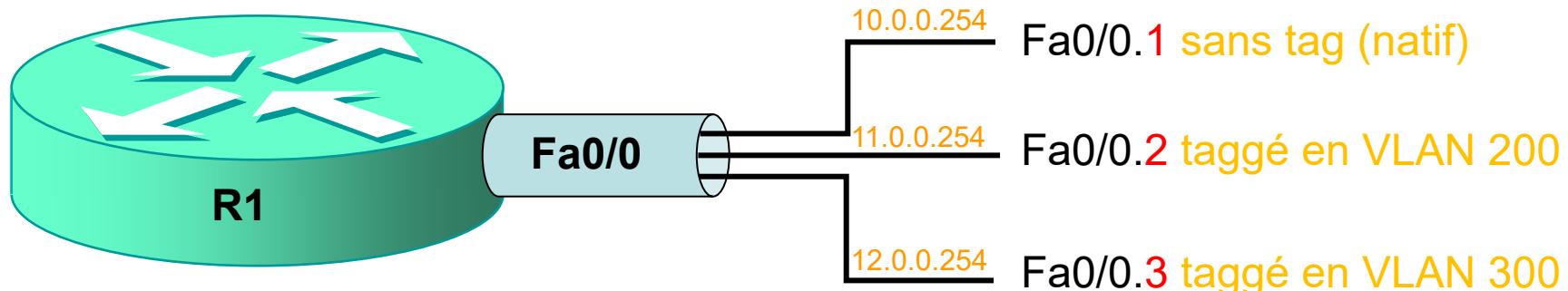
POUR ASSOCIER les
SOUS-INTERFACES à
un numéro de VLAN :

{

- 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

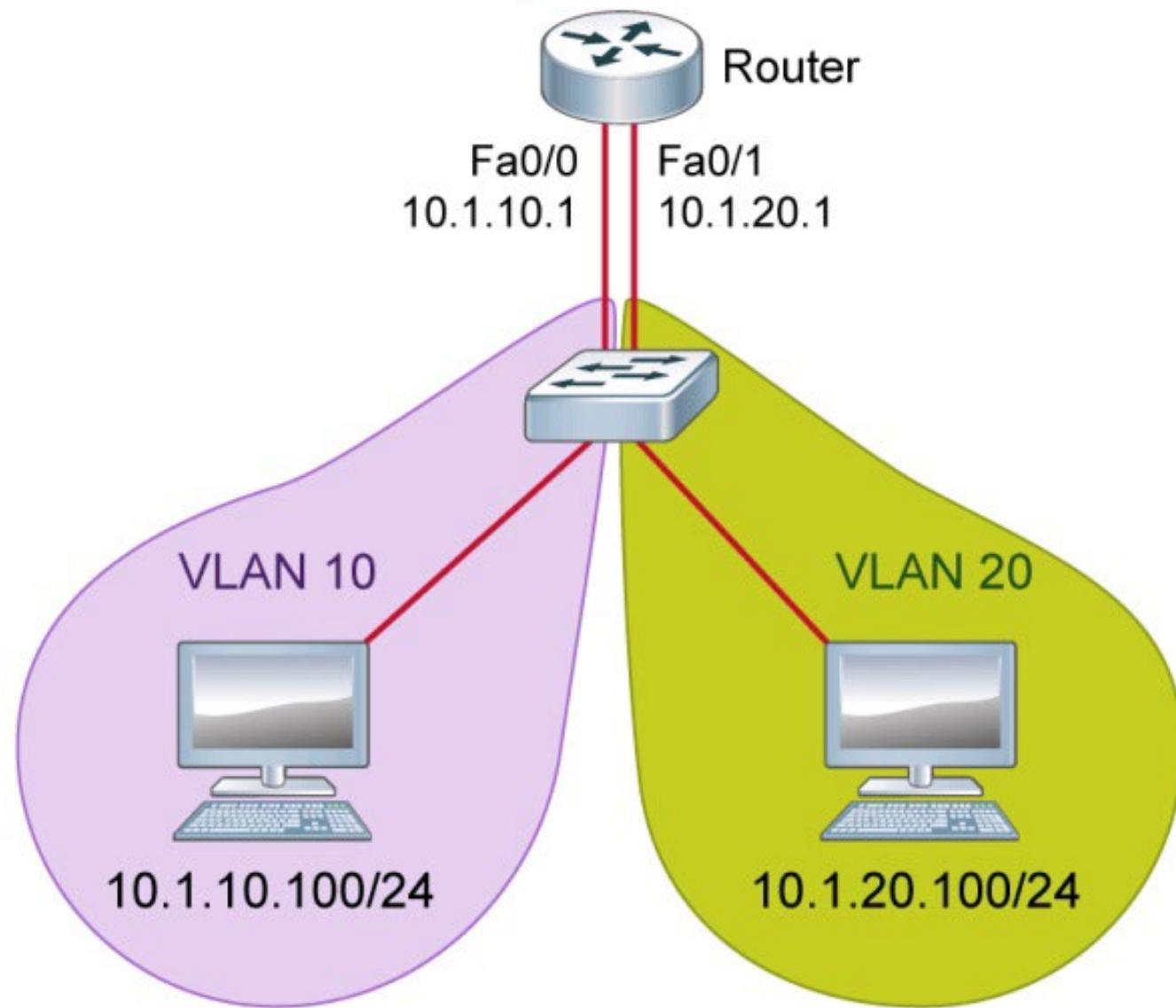
- Chaque sous-interface doit avoir une **adresse IP** : la passerelle du VLAN.



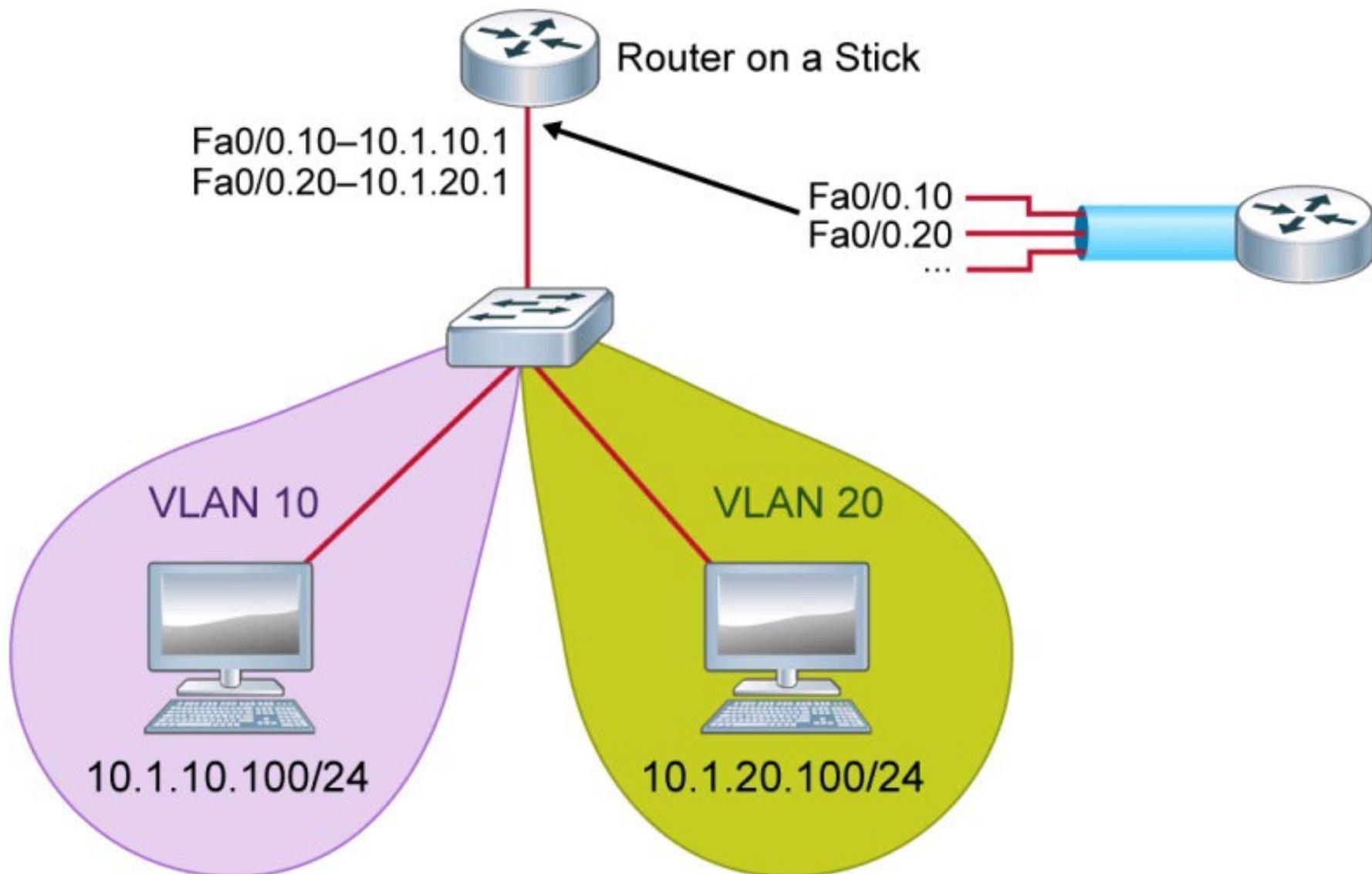
POUR CONFIGURER
une adresse IP dans
chaque SOUS-
INTERFACE :

```
{ 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
```

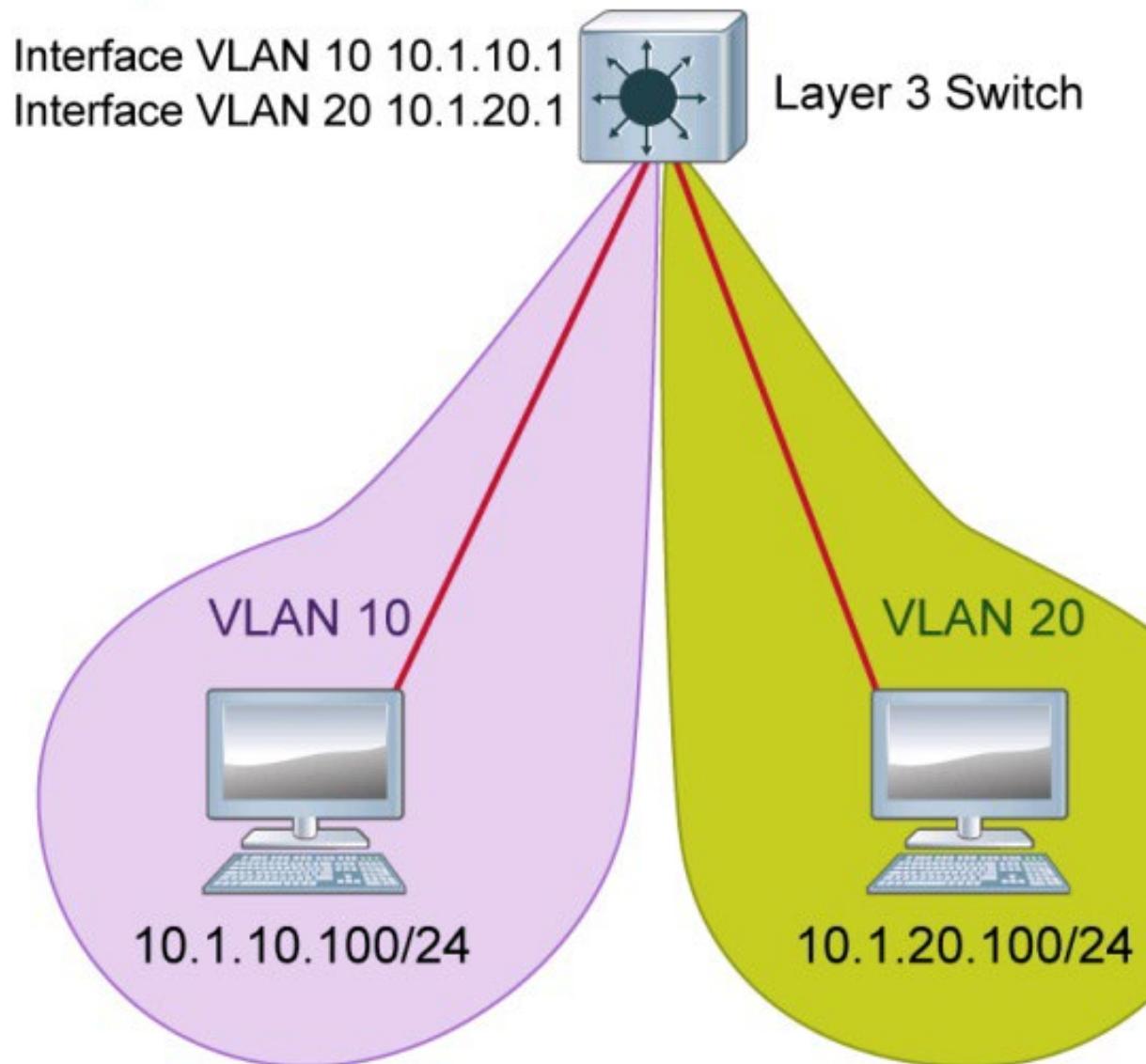
Option 1: Router with a Separate Interface in Each VLAN



Option 3: Router on a Stick



Option 2: Layer 3 Switch

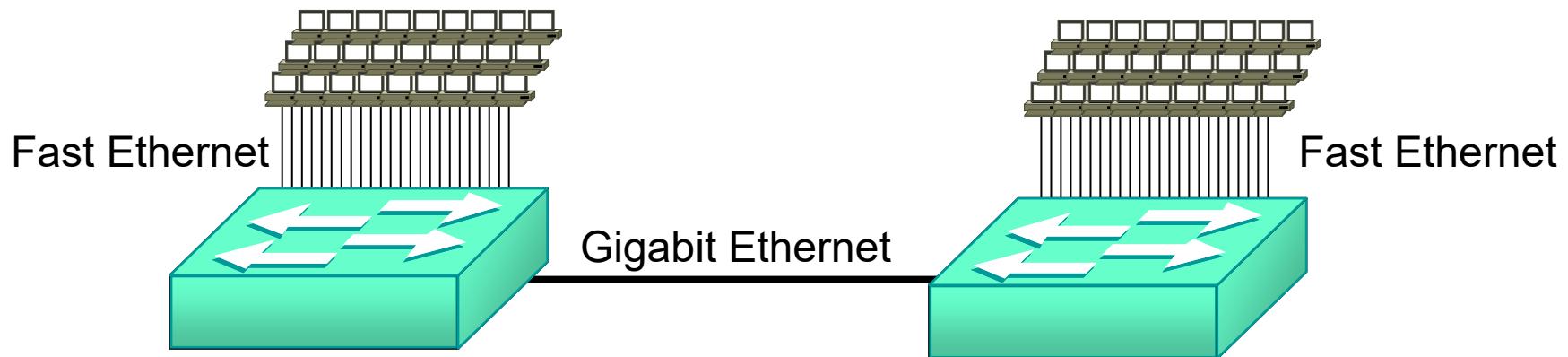


Le management du switch

Introduction

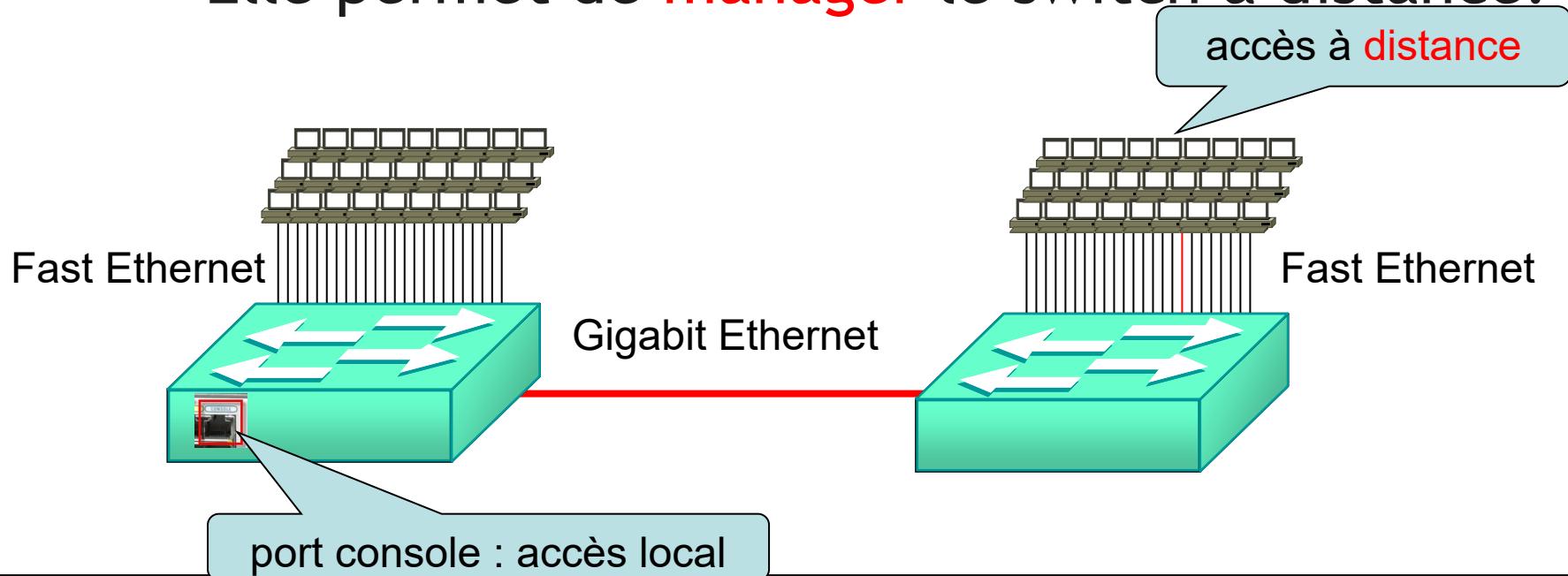
L'adresse IP d'un switch.

- 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
```

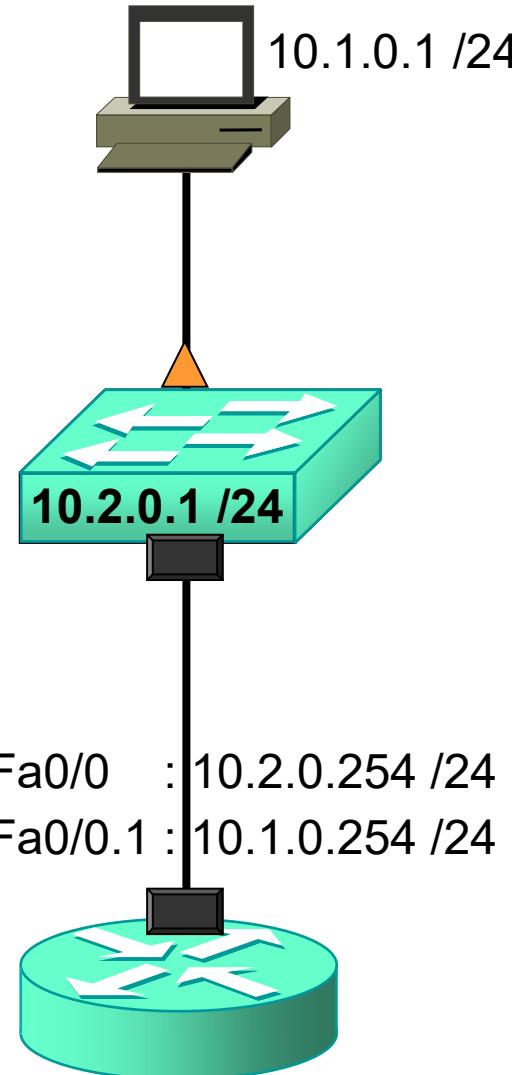
```
interface vlan 1
```

```
ip address 10.0.0.1 255.255.255.0
```

```
exit
```

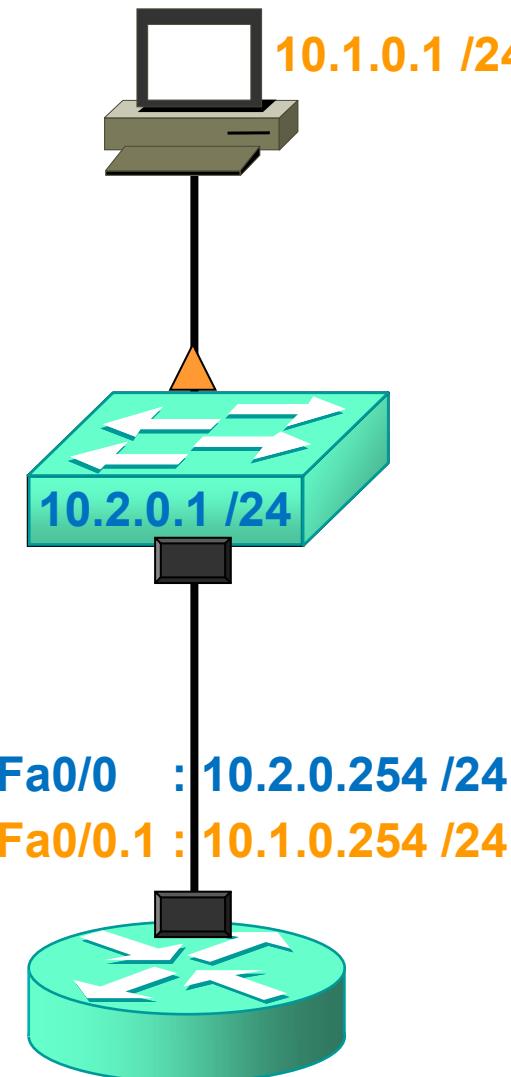
```
default-gateway 10.0.0.254
```

Exercice



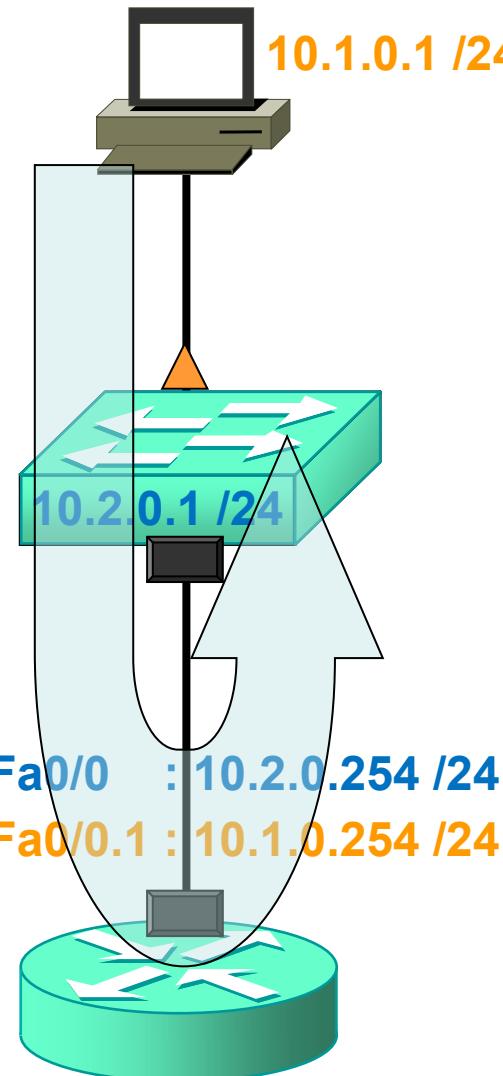
- Quelle est la passerelle par défaut du PC ?
- Quelle est la passerelle par défaut du switch ?
- Quel chemin empruntera le traffic entre le PC et le switch ?

Solution



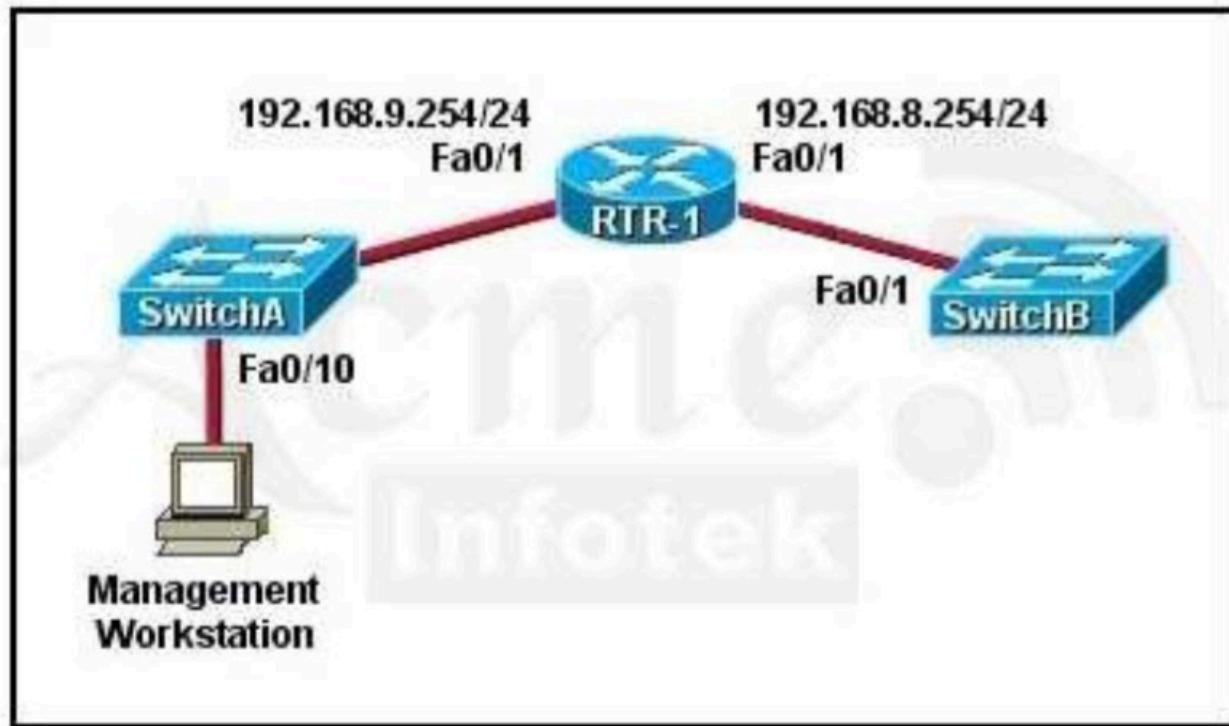
- La passerelle par défaut du PC est **10.1.0.254**
- La passerelle par défaut du switch est **10.2.0.254**.

Solution



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

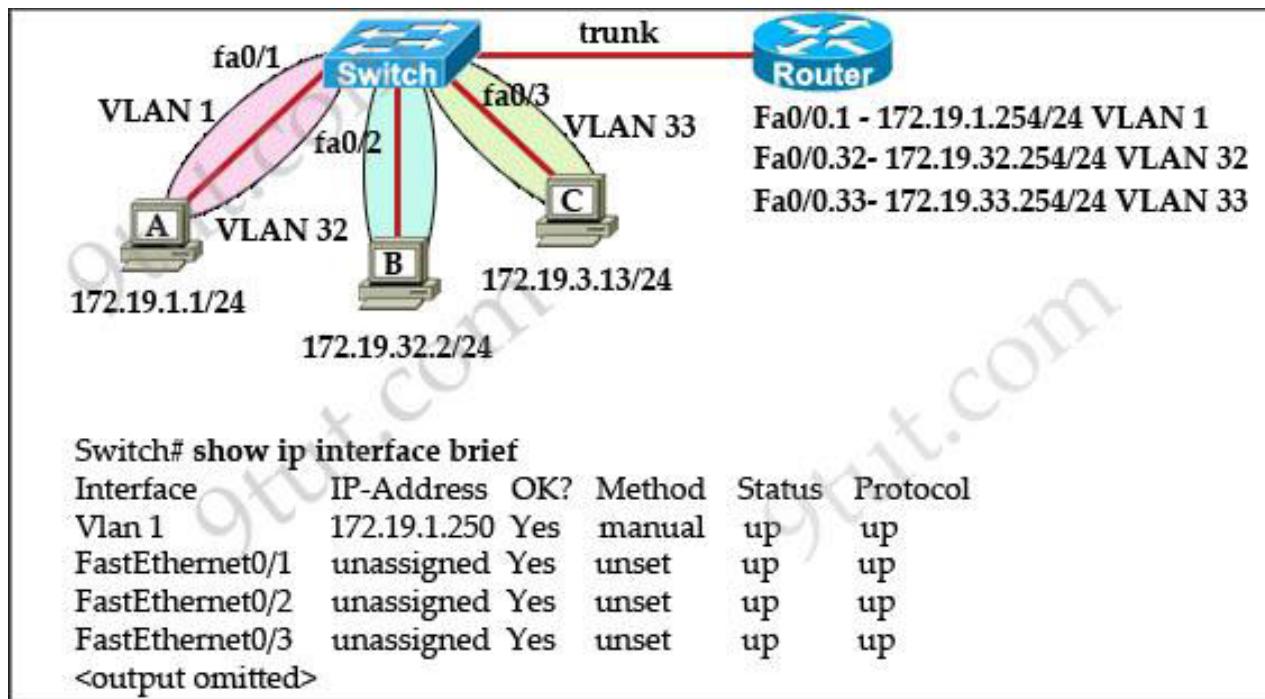
Quelle configuration permettra de manager le switch B à distance ?



```
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

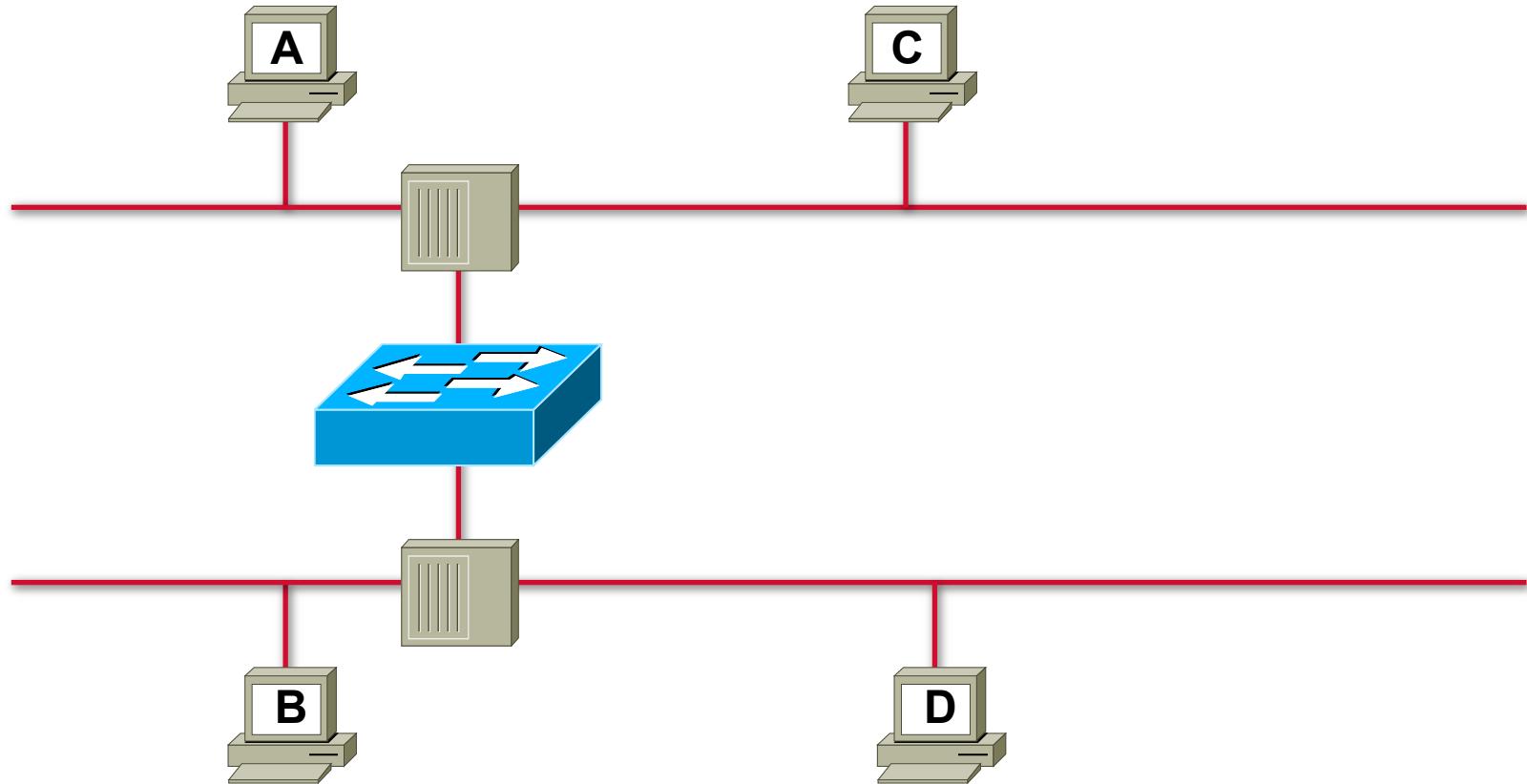
The network administrator normally establishes a Telnet session with the switch from host A. However, host A is unavailable. The administrator's attempt to telnet to the switch from host B fails, but pings to the other two hosts are successful. What is the issue?



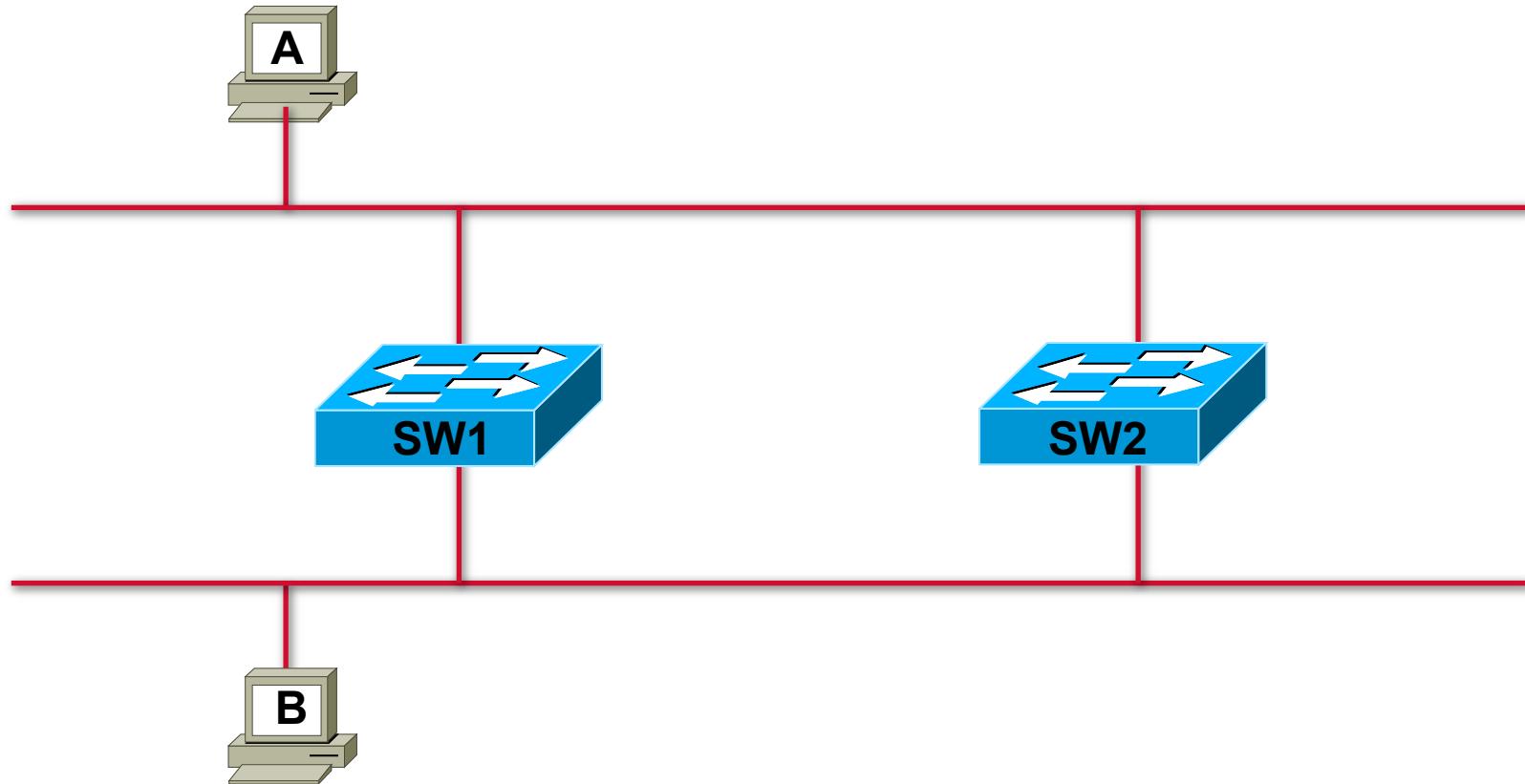
STP

Spanning-Tree Protocol

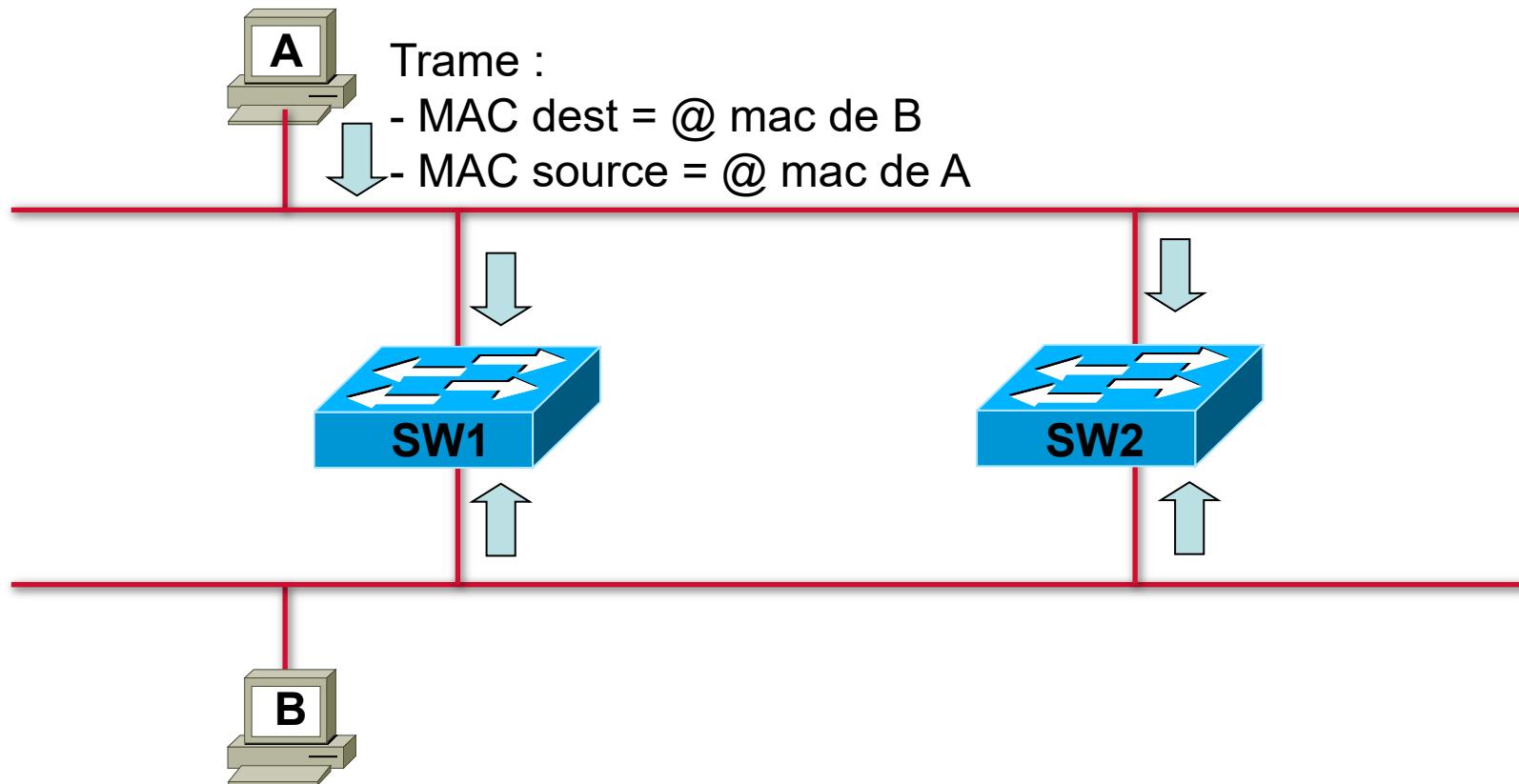
Et si le switch tombe ...



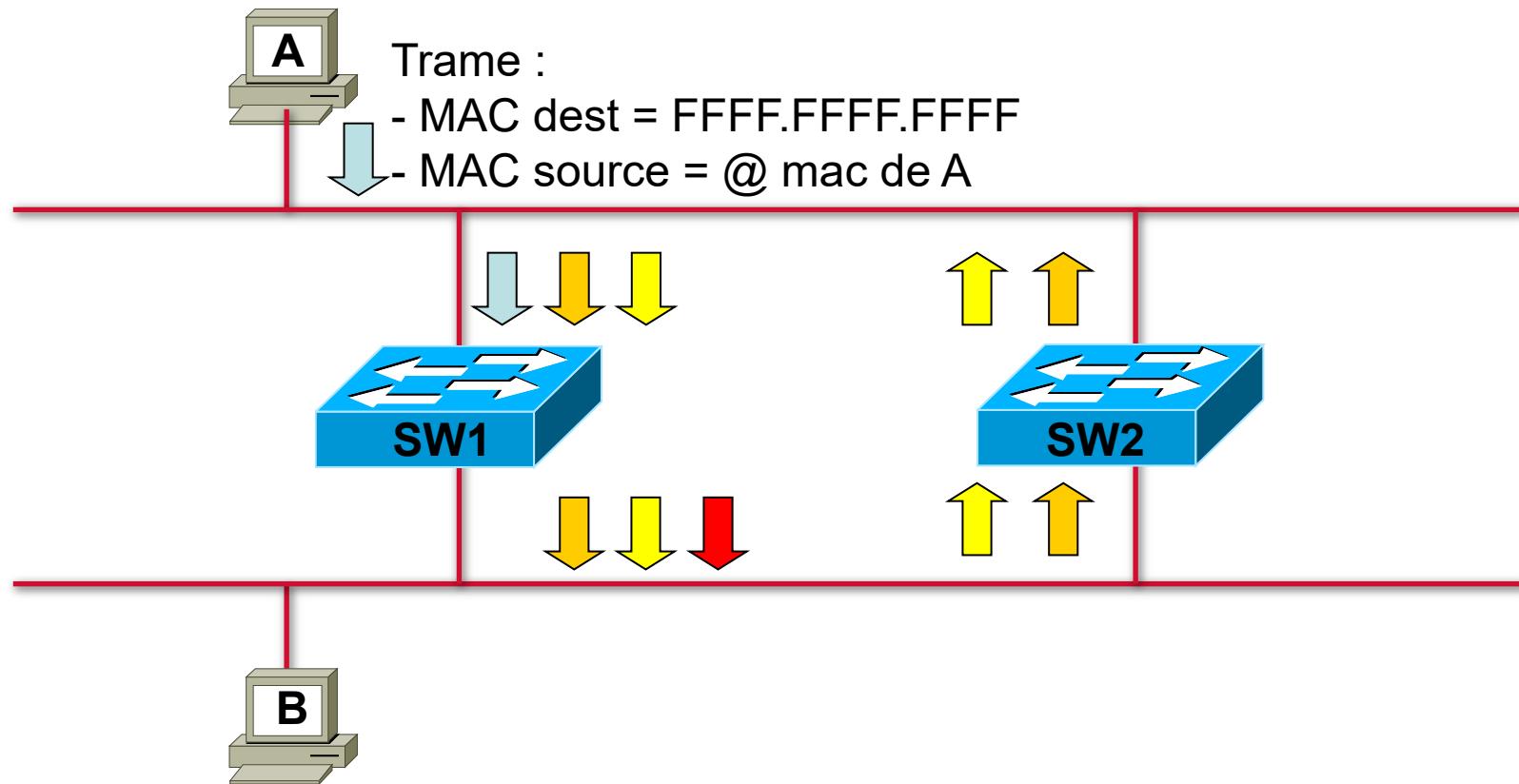
Redondance



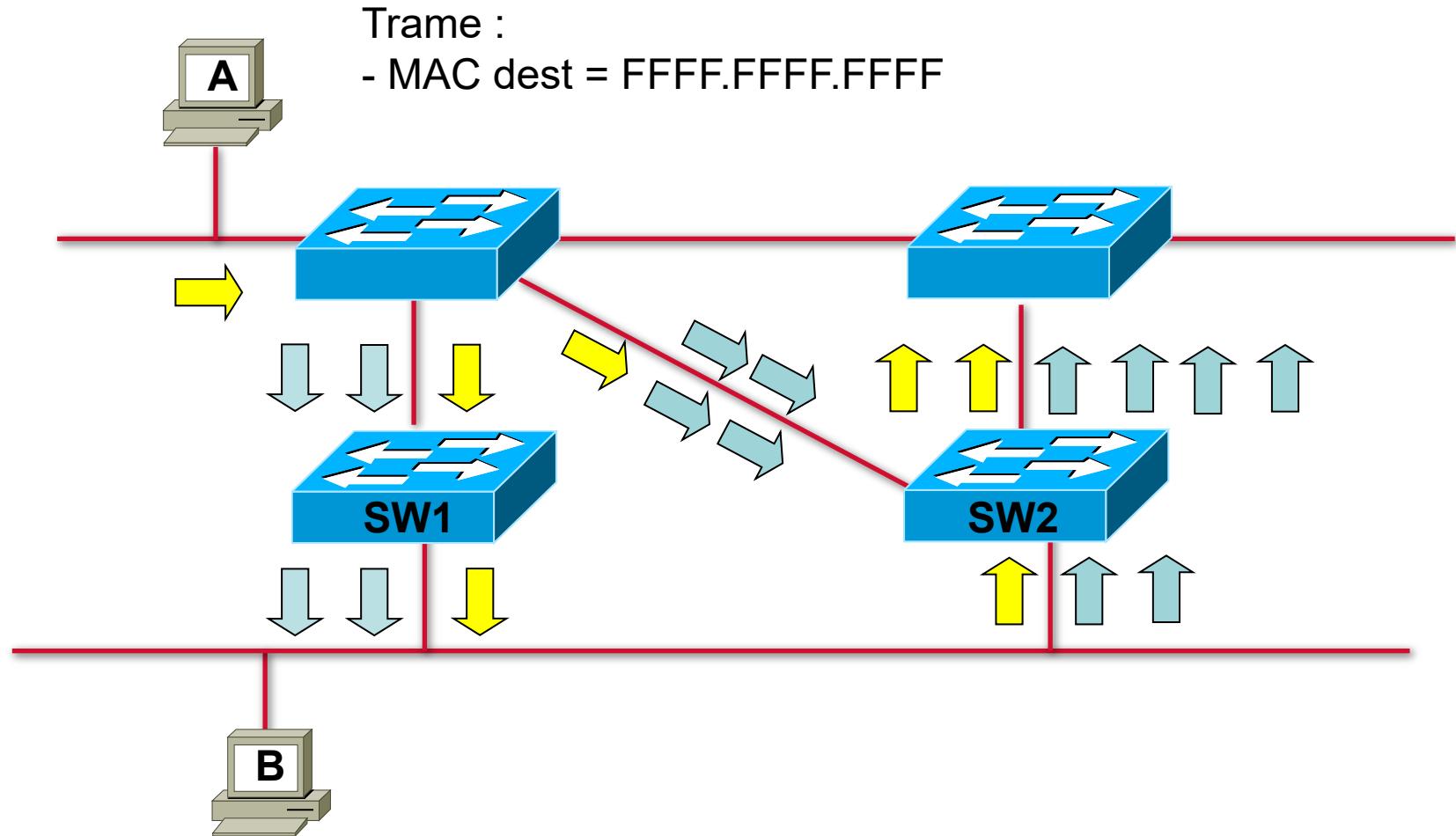
Instabilité de la table des @ MAC



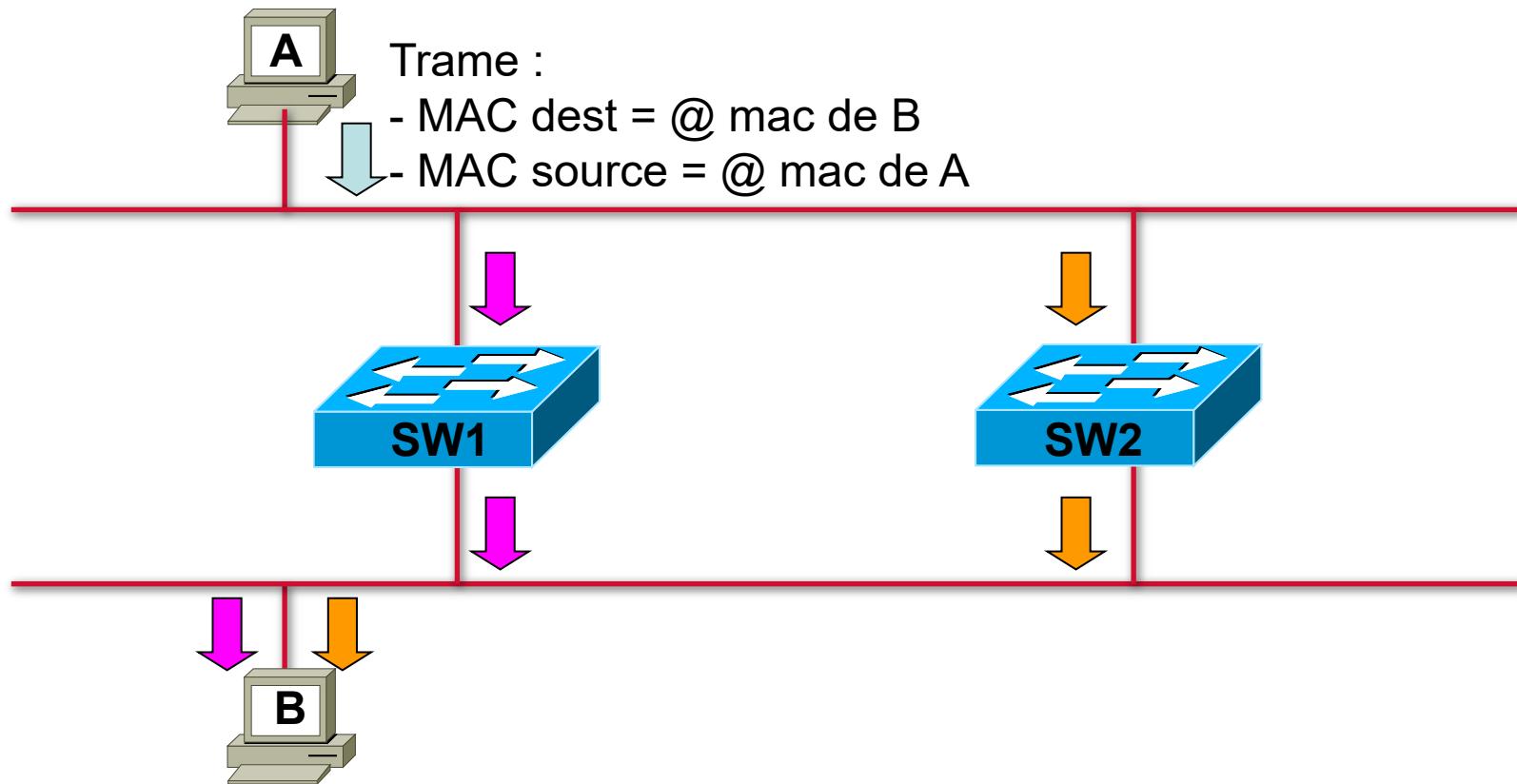
Tempête de broadcast



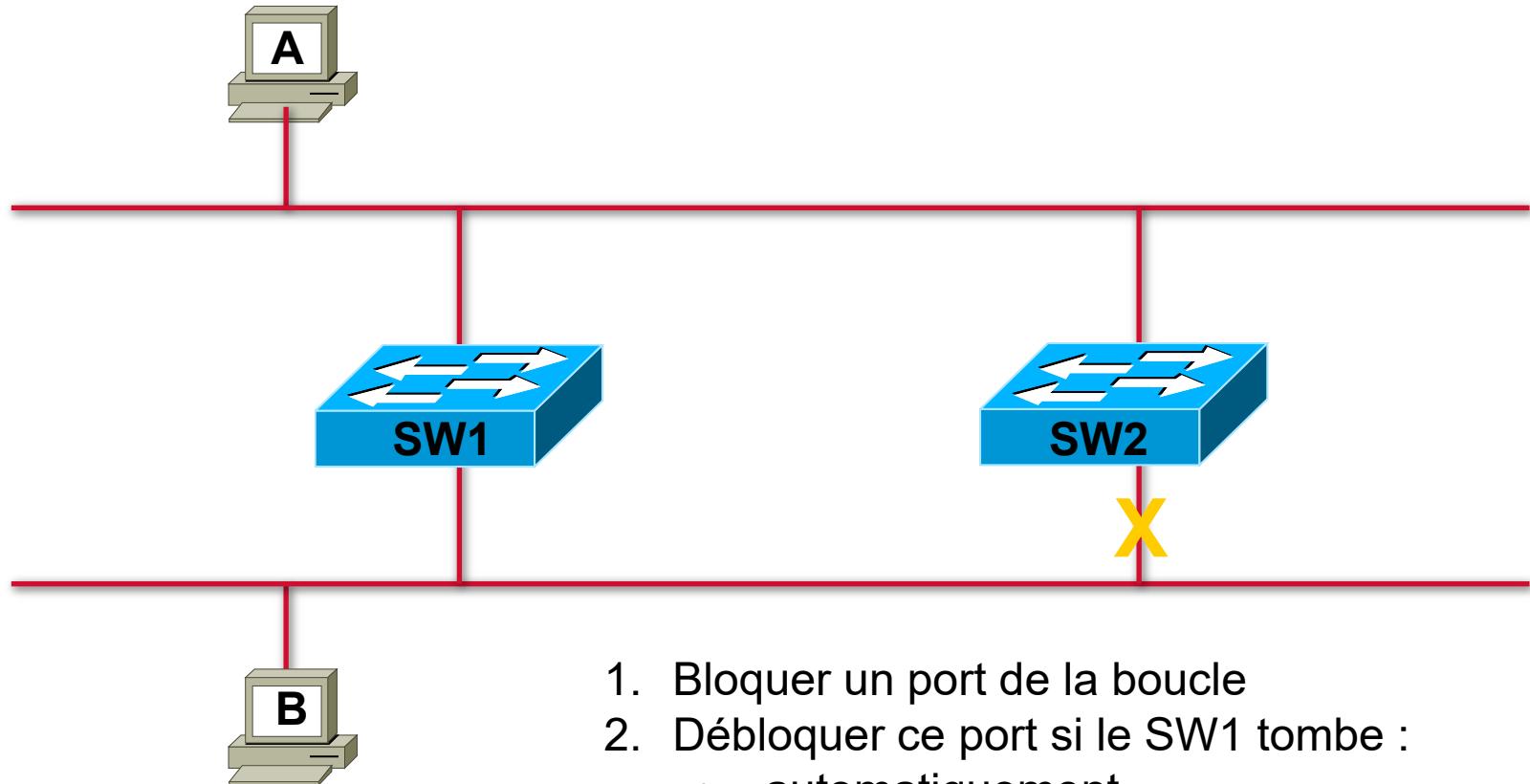
Tempête de broadcast



Duplication des trames



Solution : STP = 802.1d



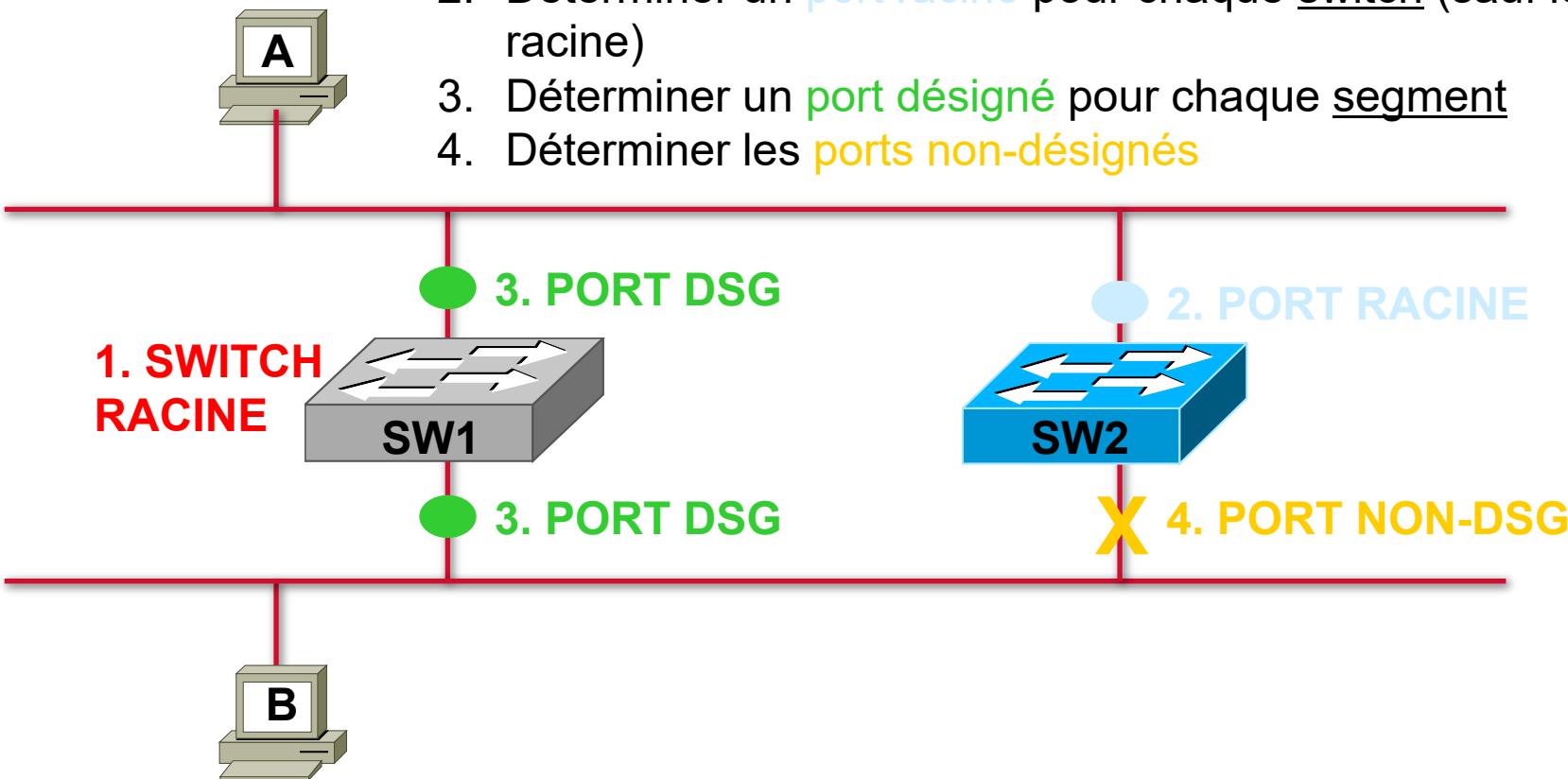
1. Bloquer un port de la boucle
2. Débloquer ce port si le SW1 tombe :
 - automatiquement
 - le plus rapidement possible

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)



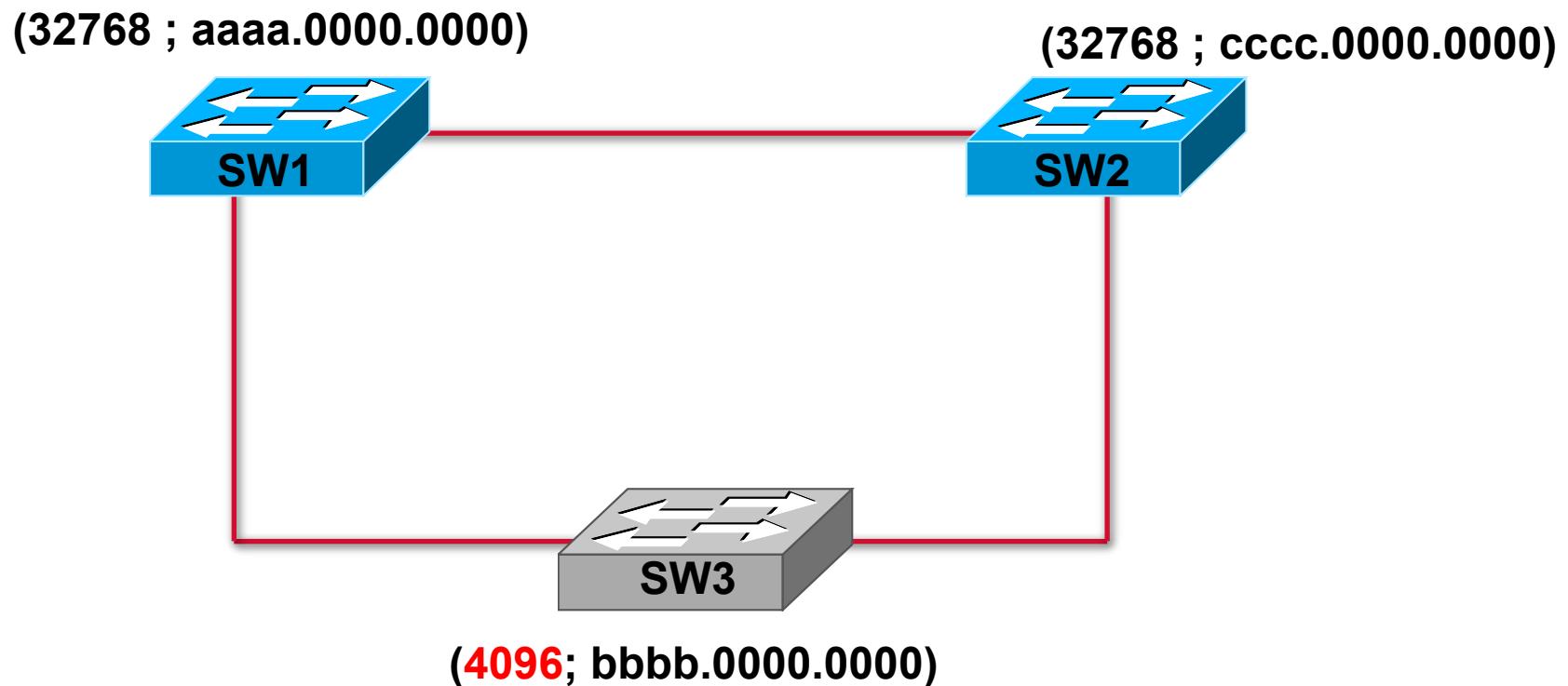
(32768 ; cccc.0000.0000)



(4096; bbbb.0000.0000)



Solution 1



Exercice 2

(32768 ; a96a.0000.0000)

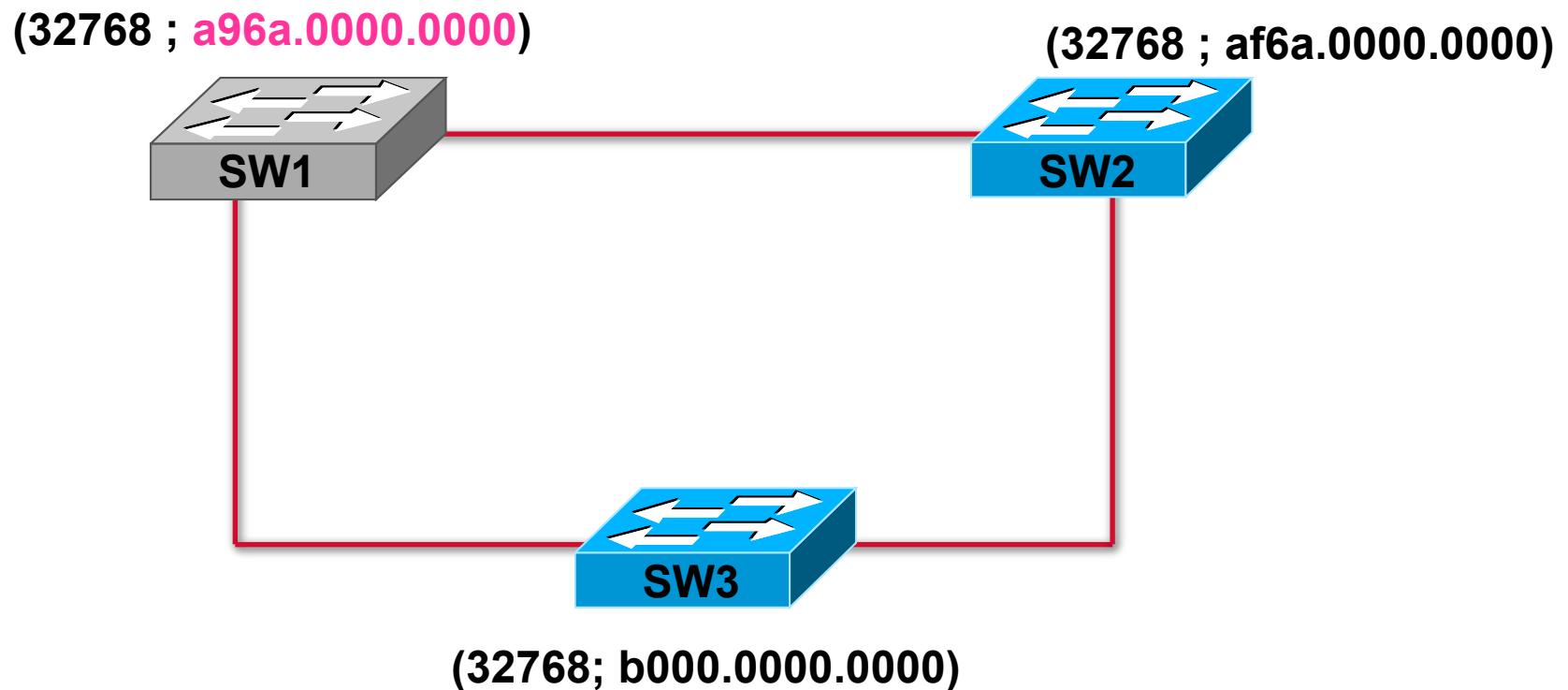


(32768 ; af6a.0000.0000)



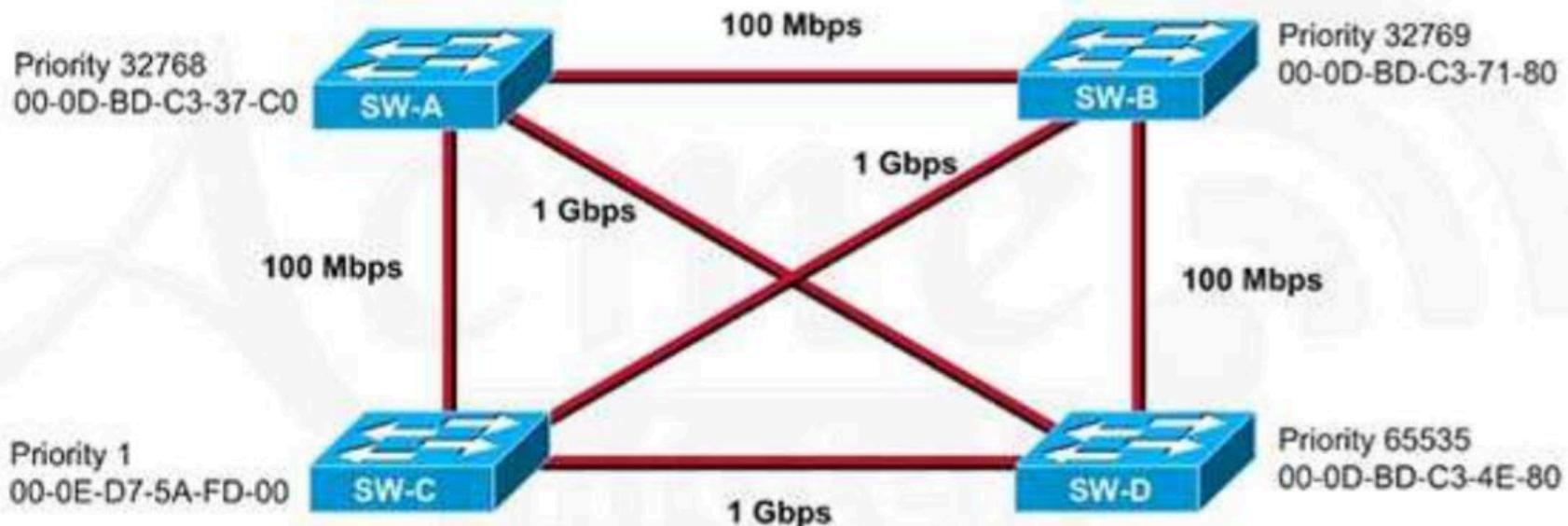
(32768; b000.0000.0000)

Solution 2



Test

- Qui sera élu switch racine ?



- 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

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

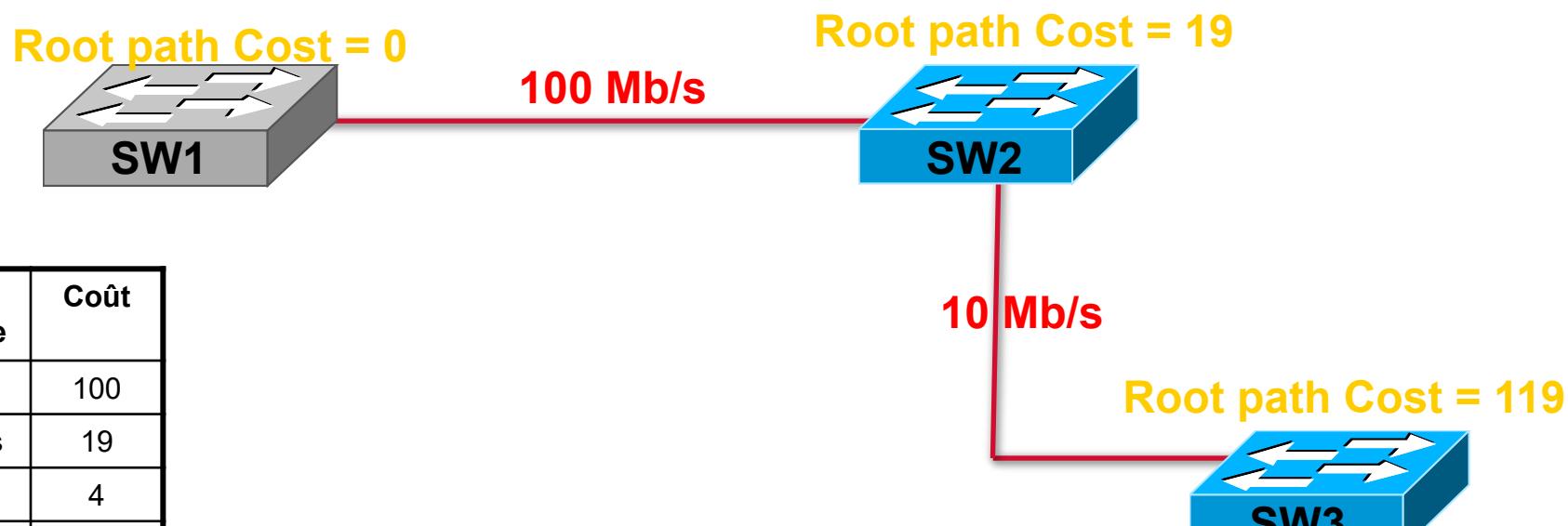
Coût de chaque liaison

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

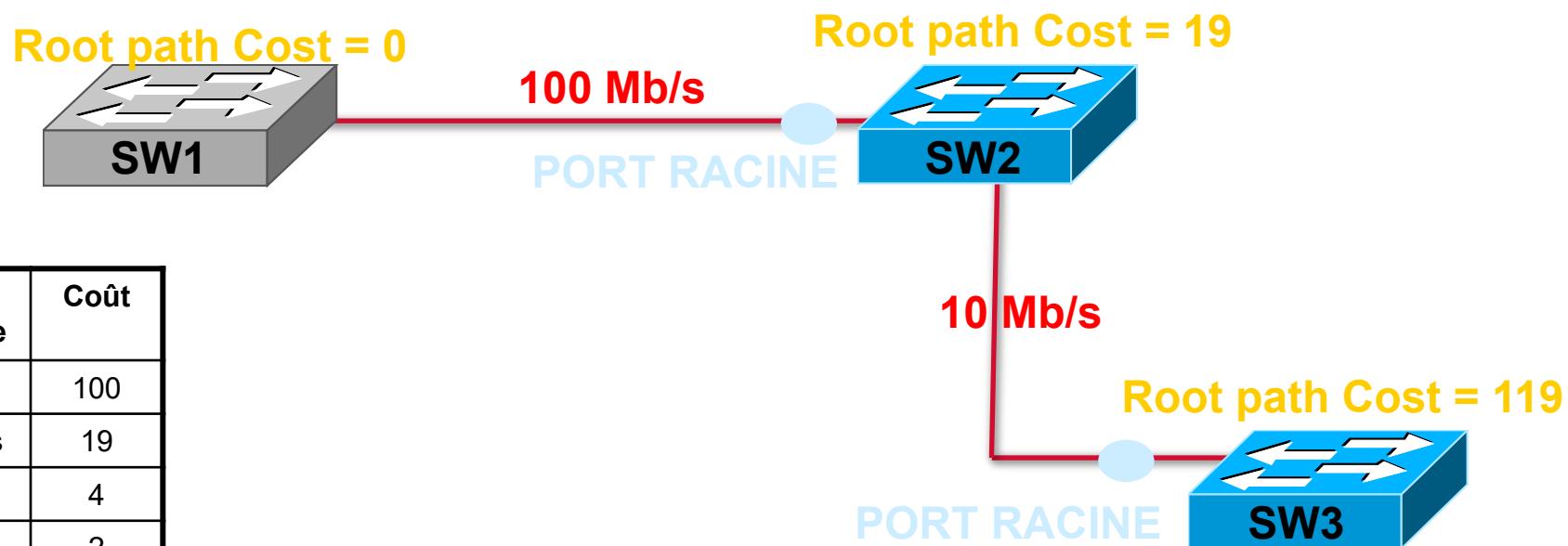
Bandé passante	Coût
10 Mb/s	100
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2
100 Gb/s	1

Root Path Cost

- Somme des coûts entre moi et le switch racine.

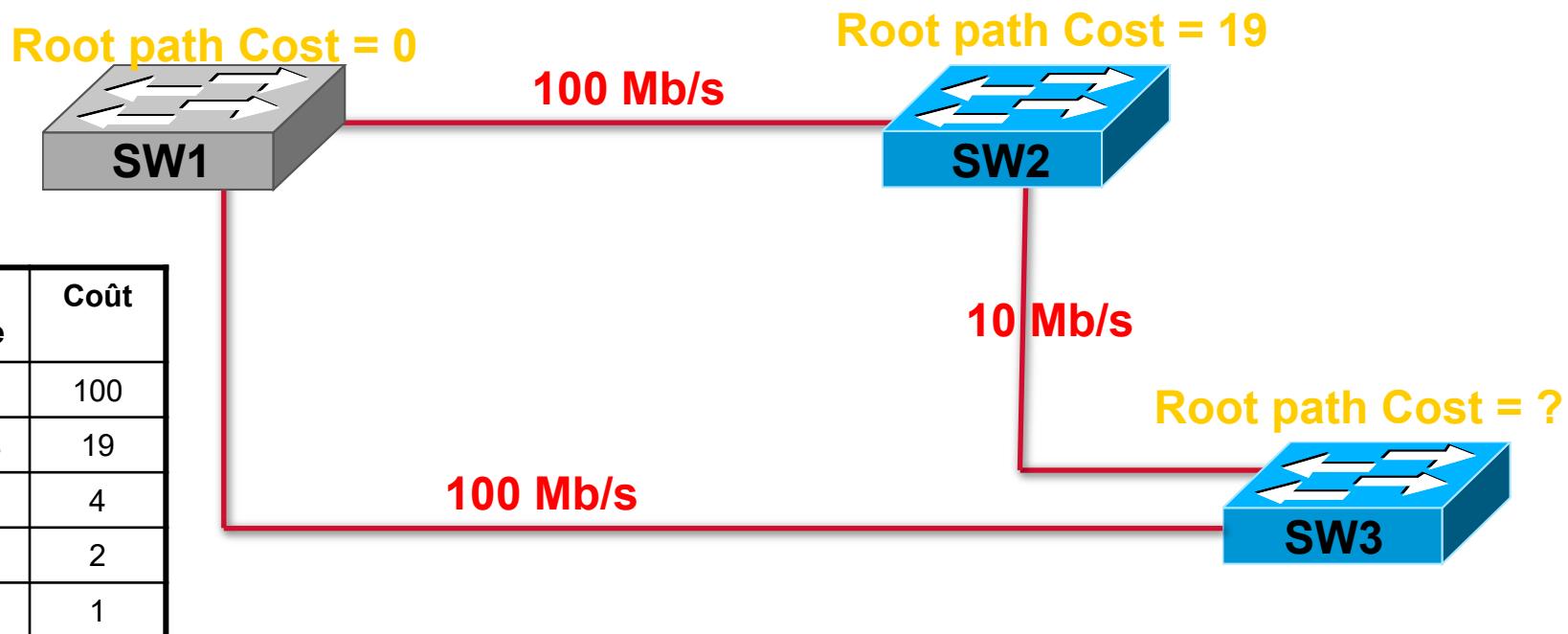


Port Racine (Root Port)



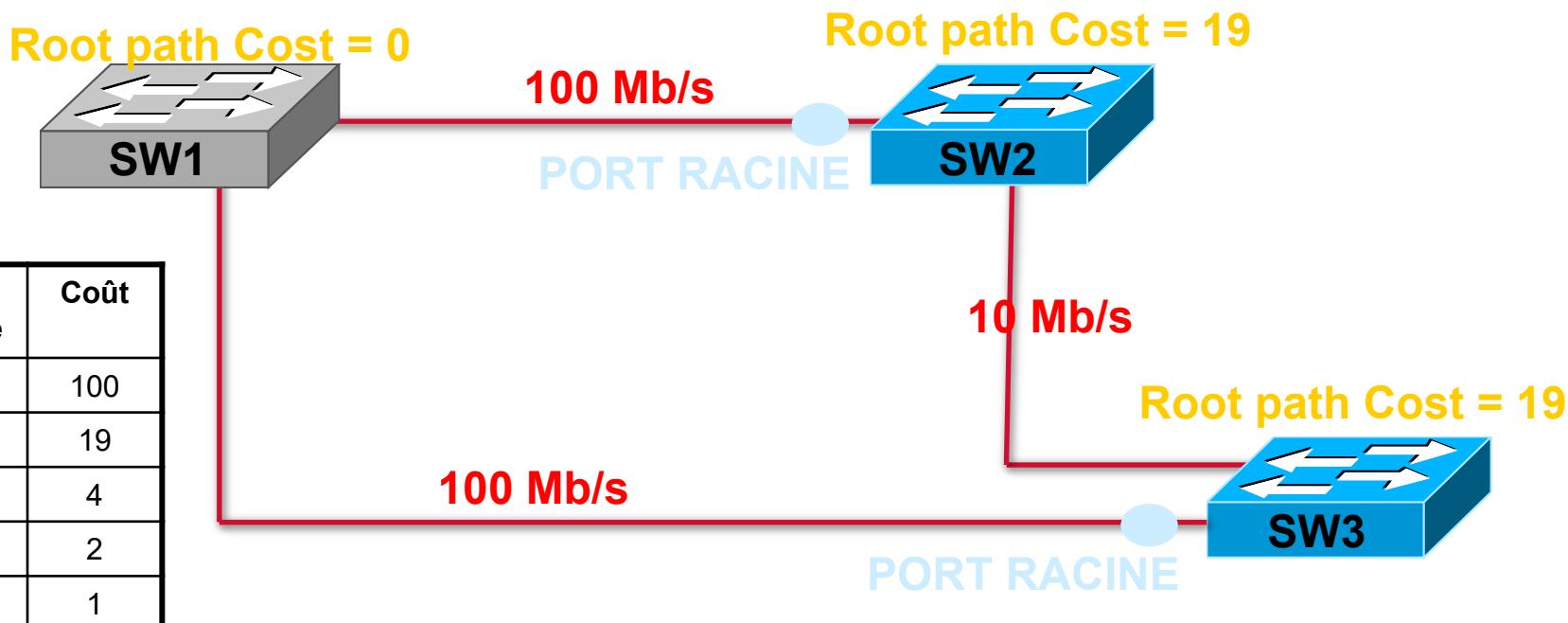
Exercice 1

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



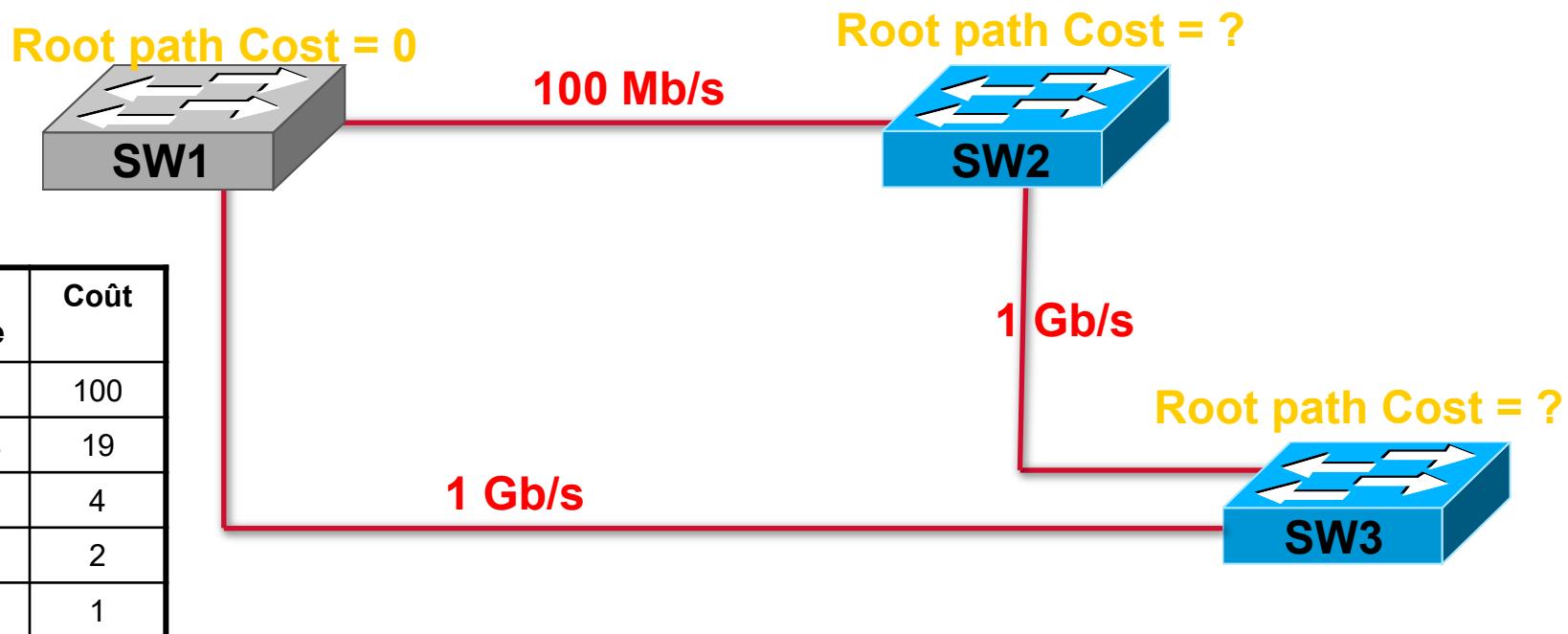
Solution

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



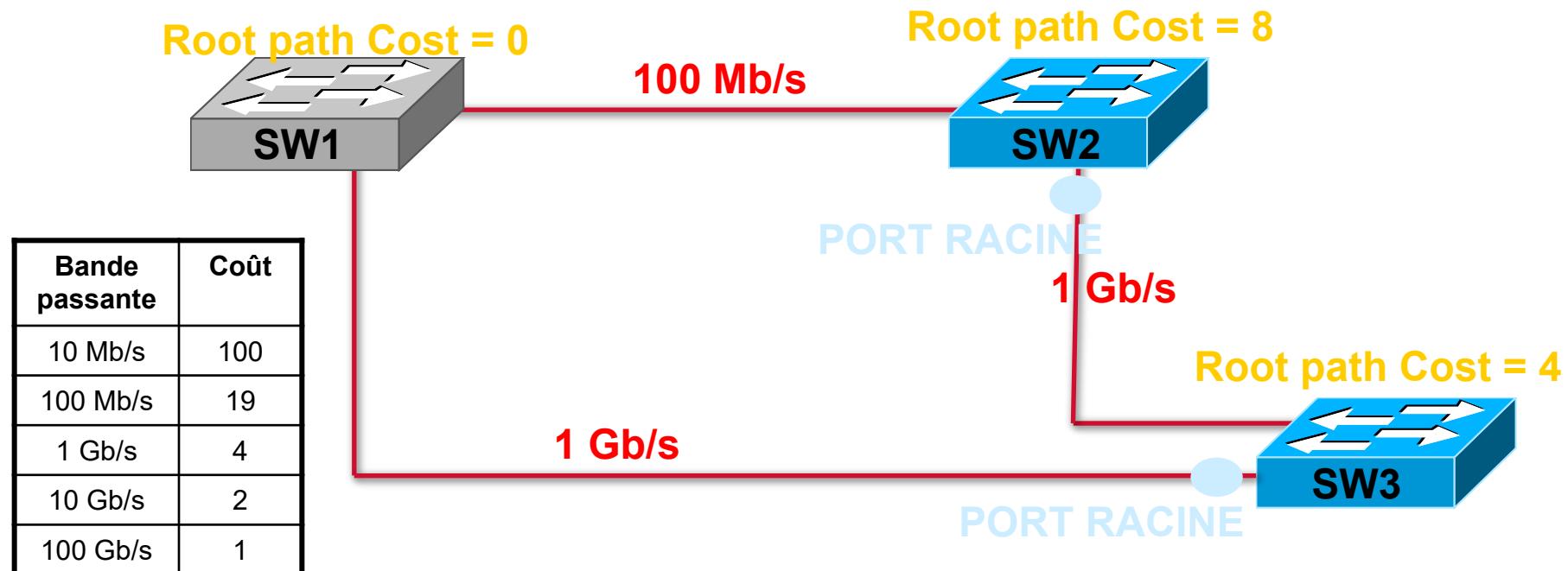
Exercice 2

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



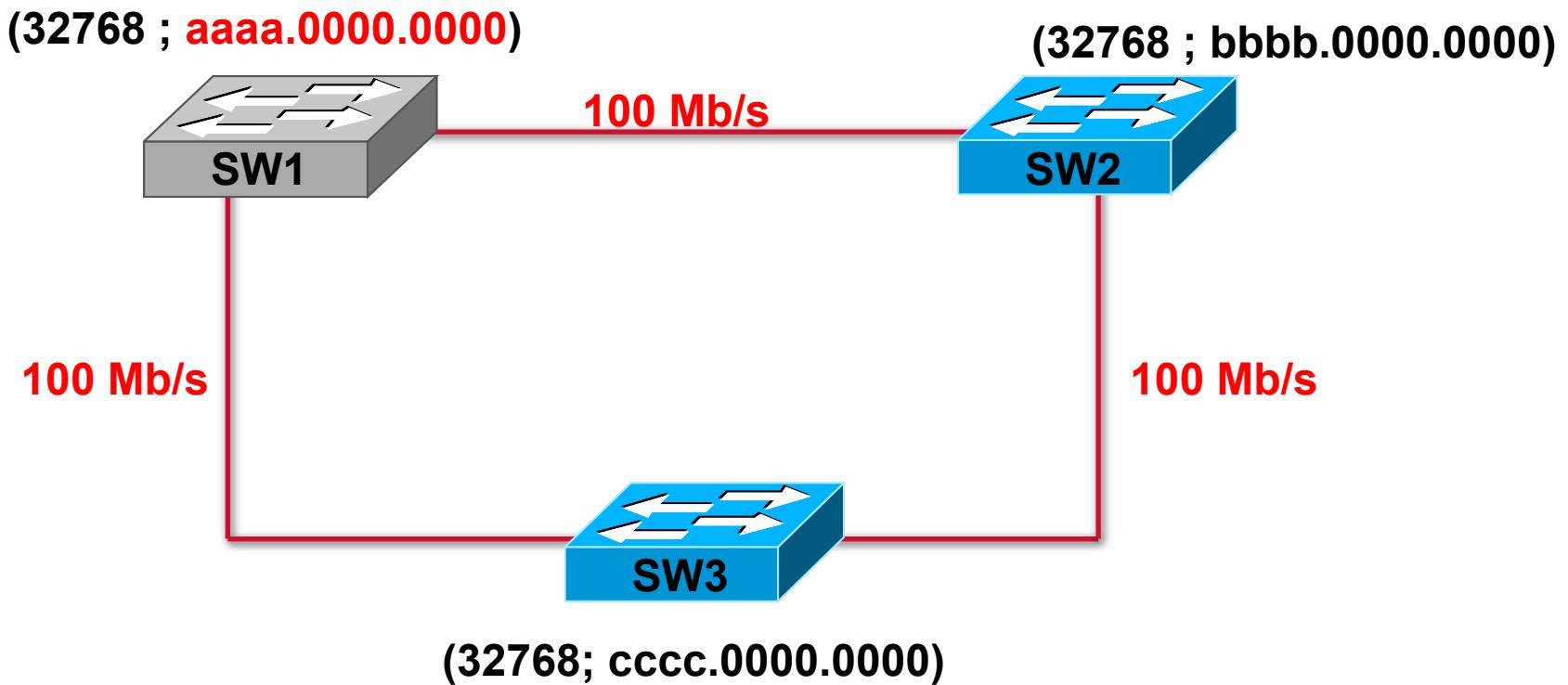
Solution

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



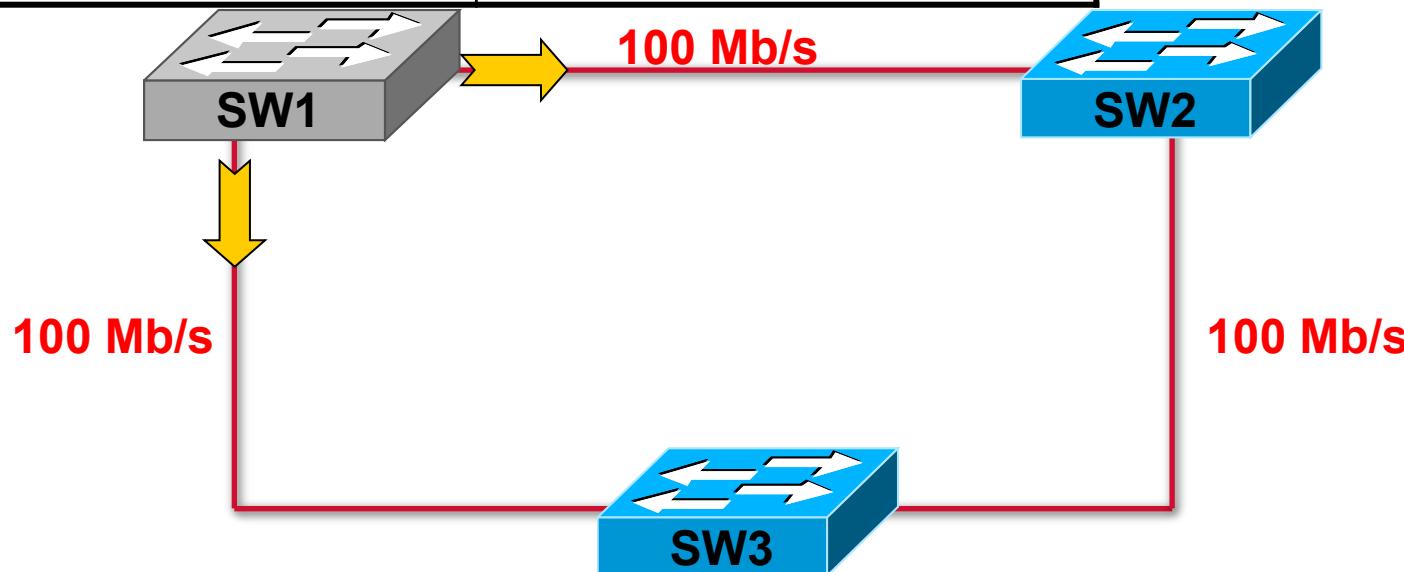
- Bridge Protocol Data Unit
- Générés par le switch racine
- Envoyé toutes les 2 secondes
- Sur toutes les interfaces
- 4 champs nous intéressent :
 - BRIDGE-ID du switch racine
 - BRIDGE-ID du switch local
 - ROOT PATH COST
 - PORT-ID

Exemple



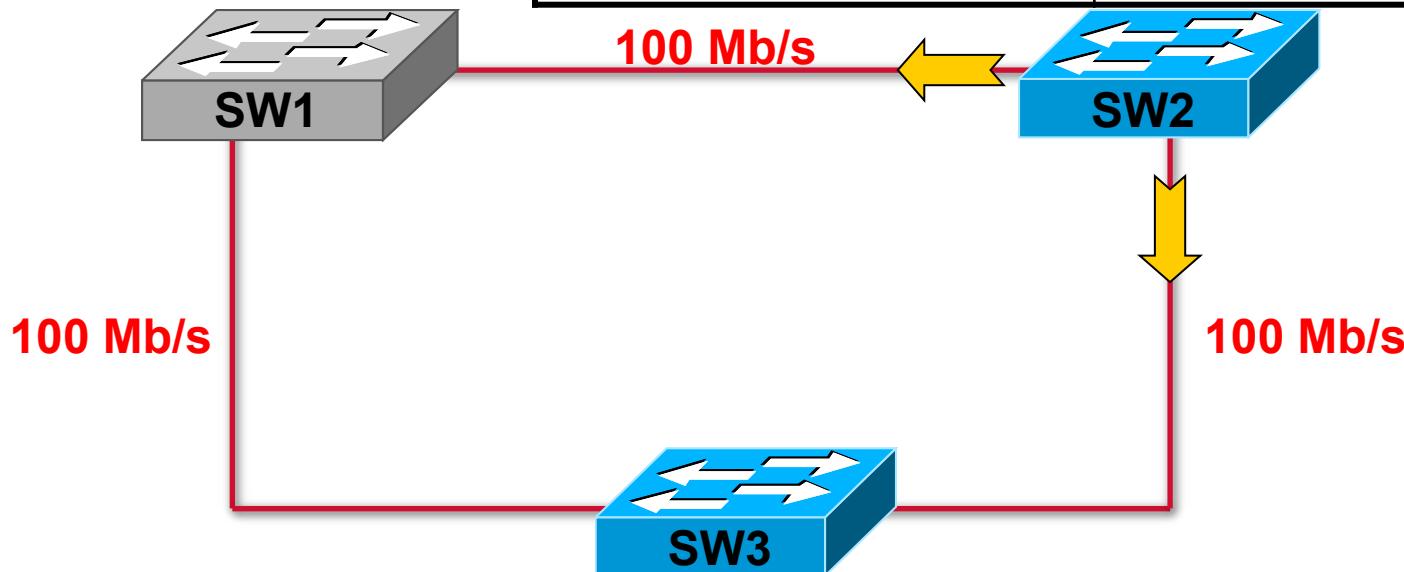
BPDUs envoyés par SW1

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

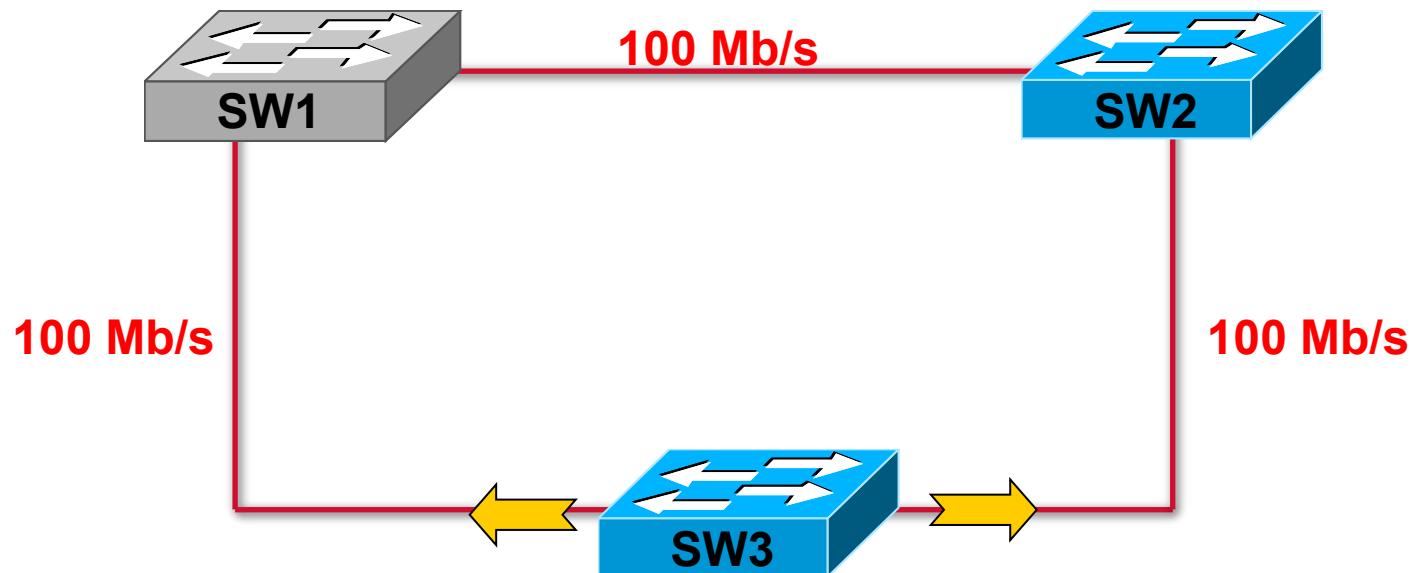


BPDU envoyés par SW2

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



BPDU envoyés par SW3

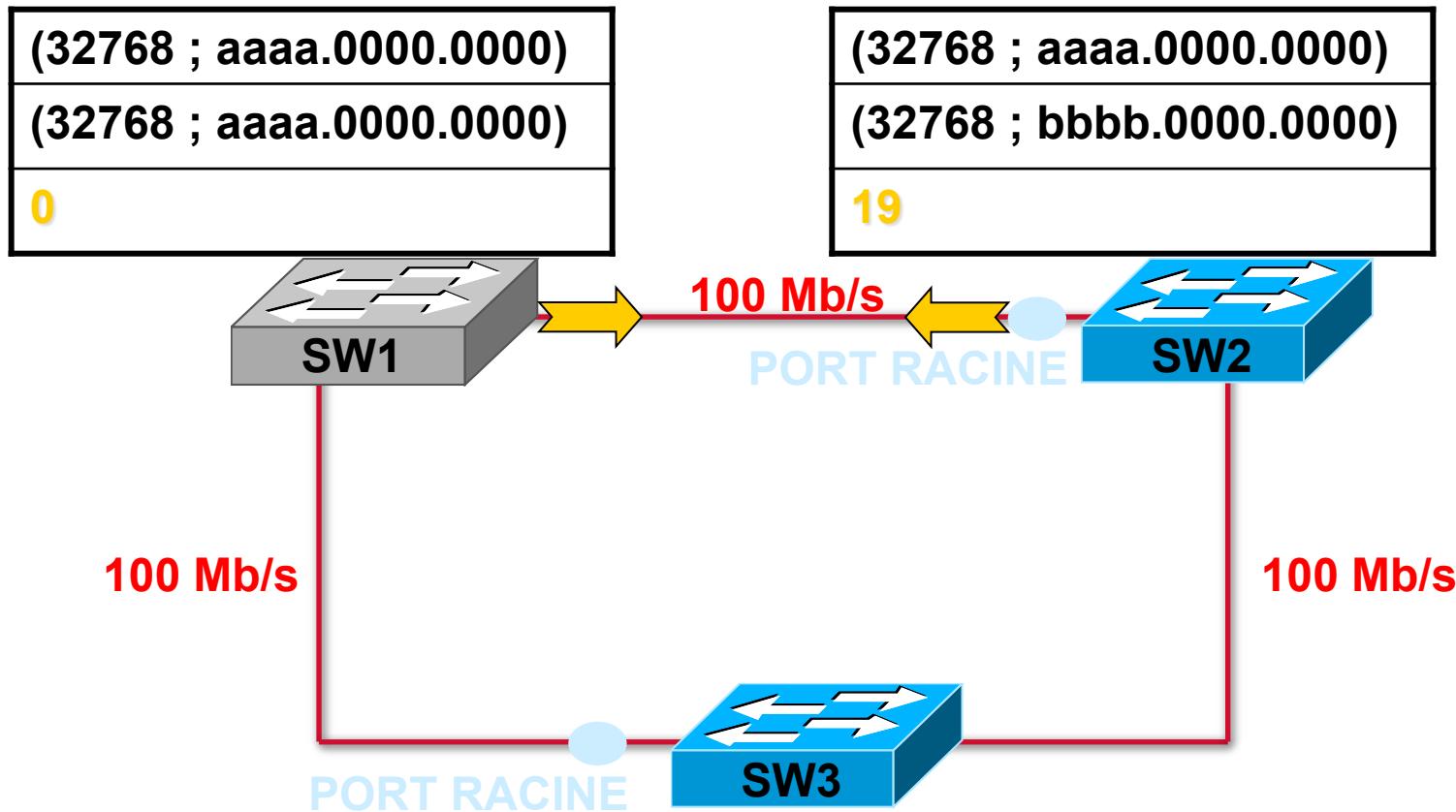


Bridge-ID du sw racine :	(32768 ; aaaa.0000.0000)
Mon Bridge-ID :	(32768 ; cccc.0000.0000)
Root Path Cost :	19

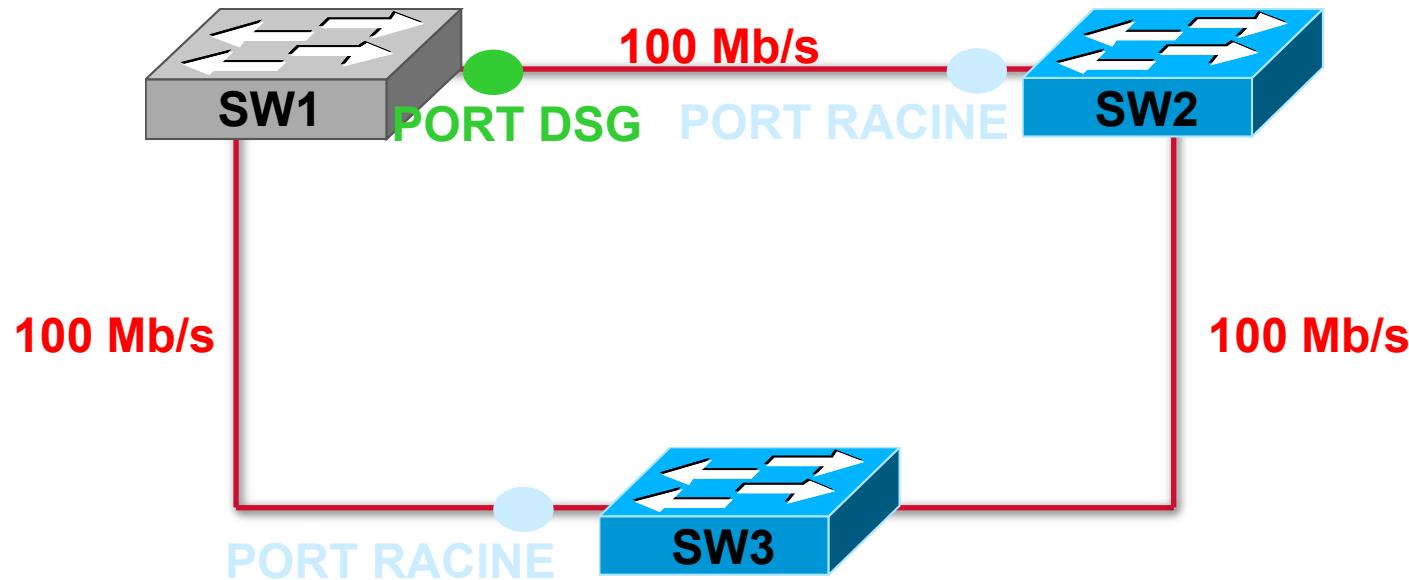
Règle de l' étape 3

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

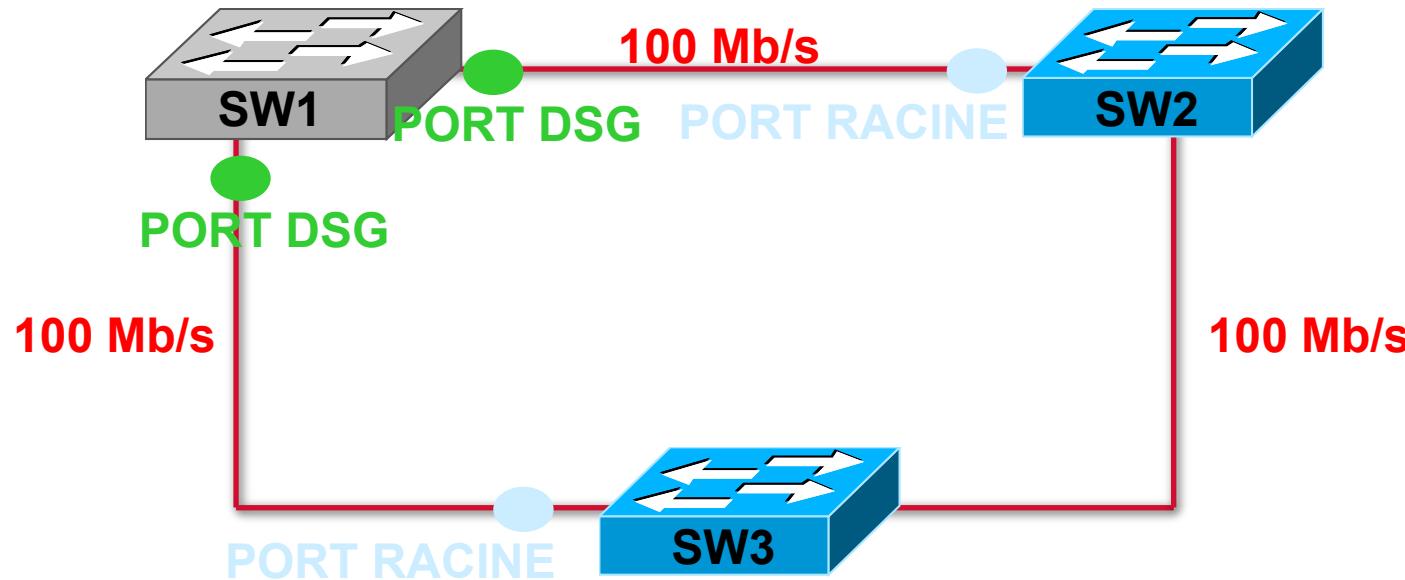
Port DSG sur segment 1-2



Port DSG sur segment 1-2

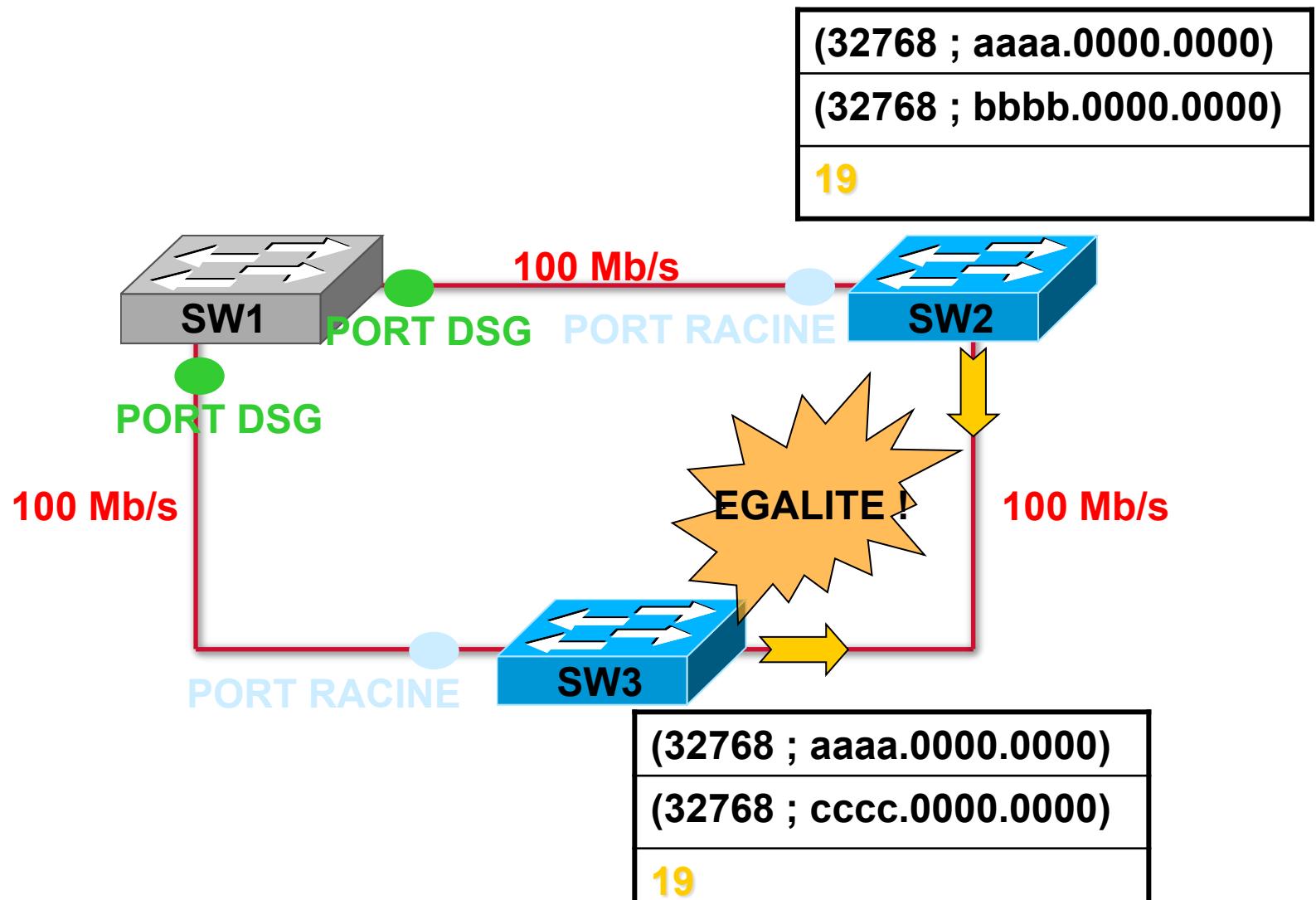


Port DSG sur segment 1-3



TOUS les ports du switch RACINE sont des ports DESIGNES

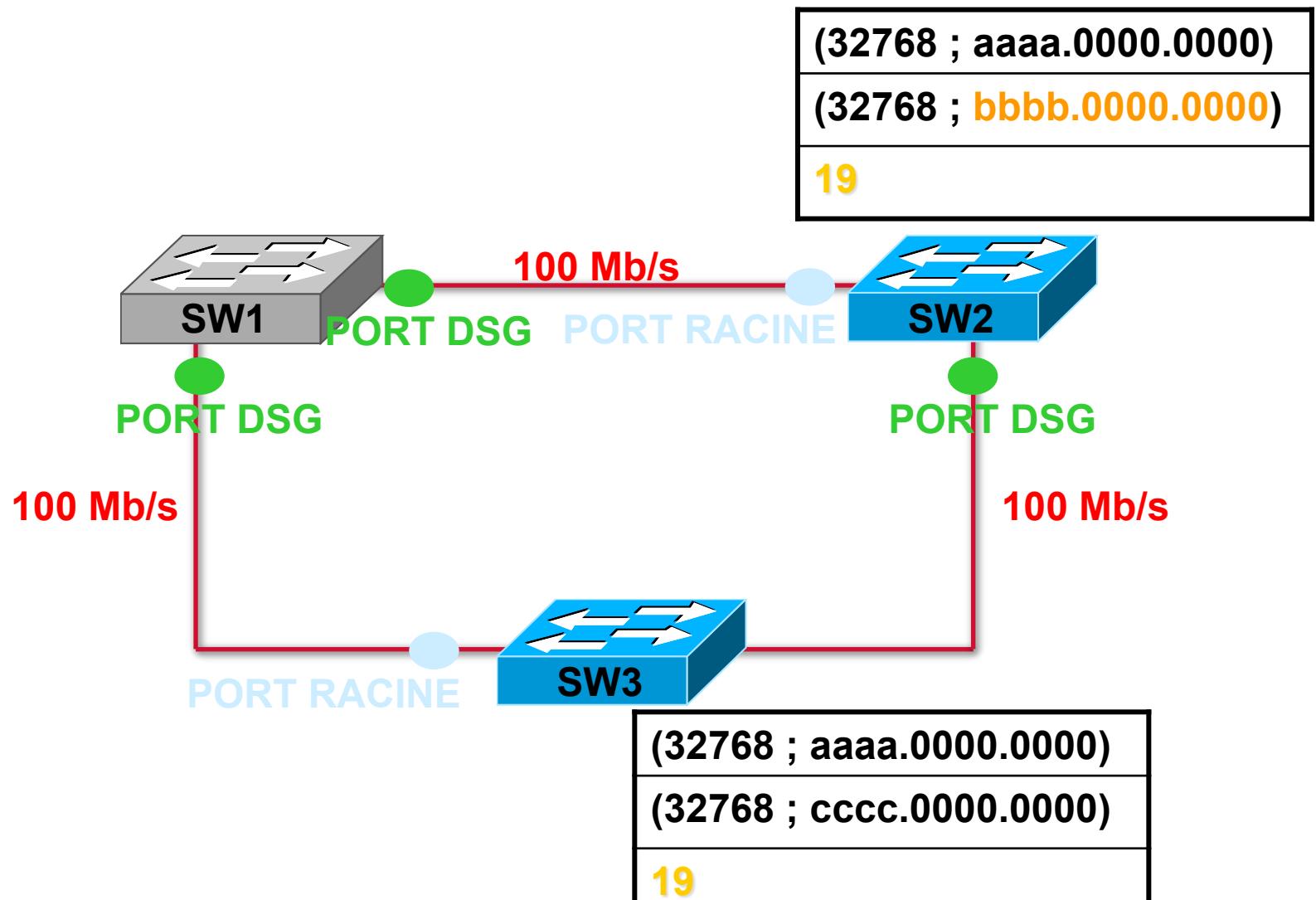
Port DSG sur segment 2-3



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.

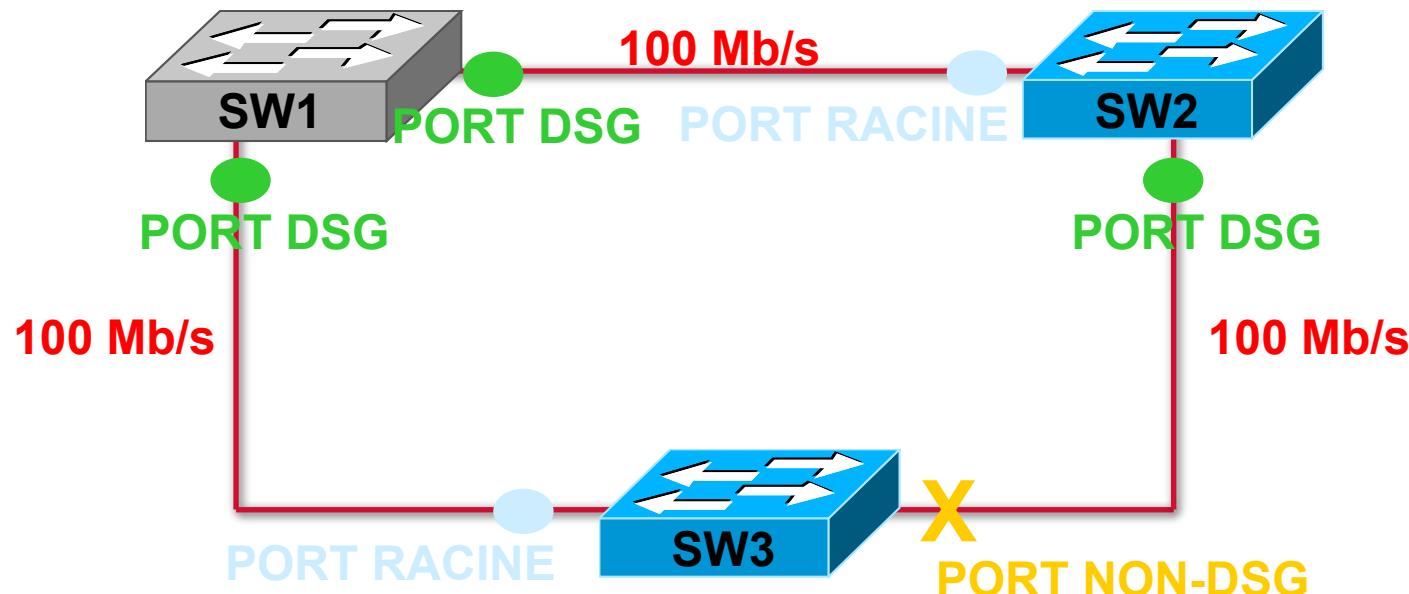
Port DSG sur segment 2-3



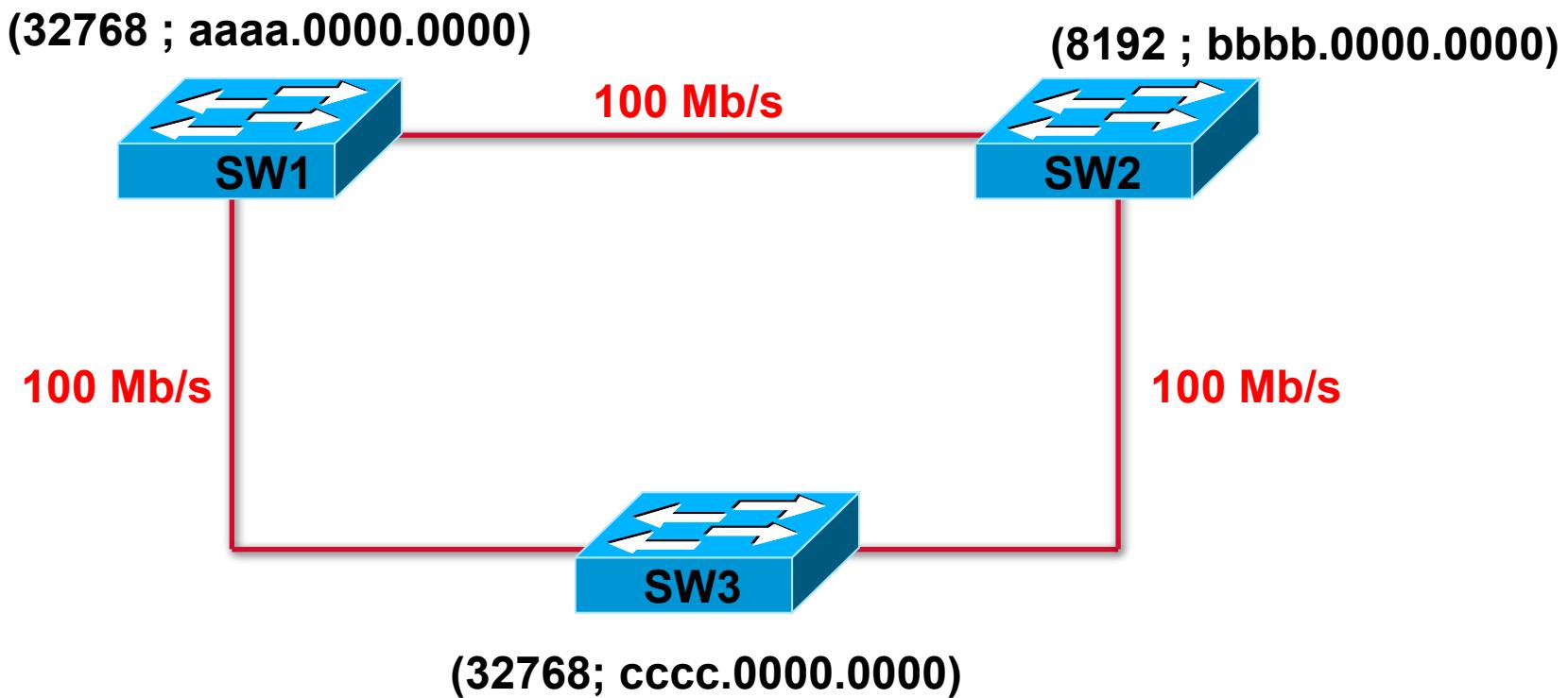
Règle de l' étape 4

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 DESIGNÉ

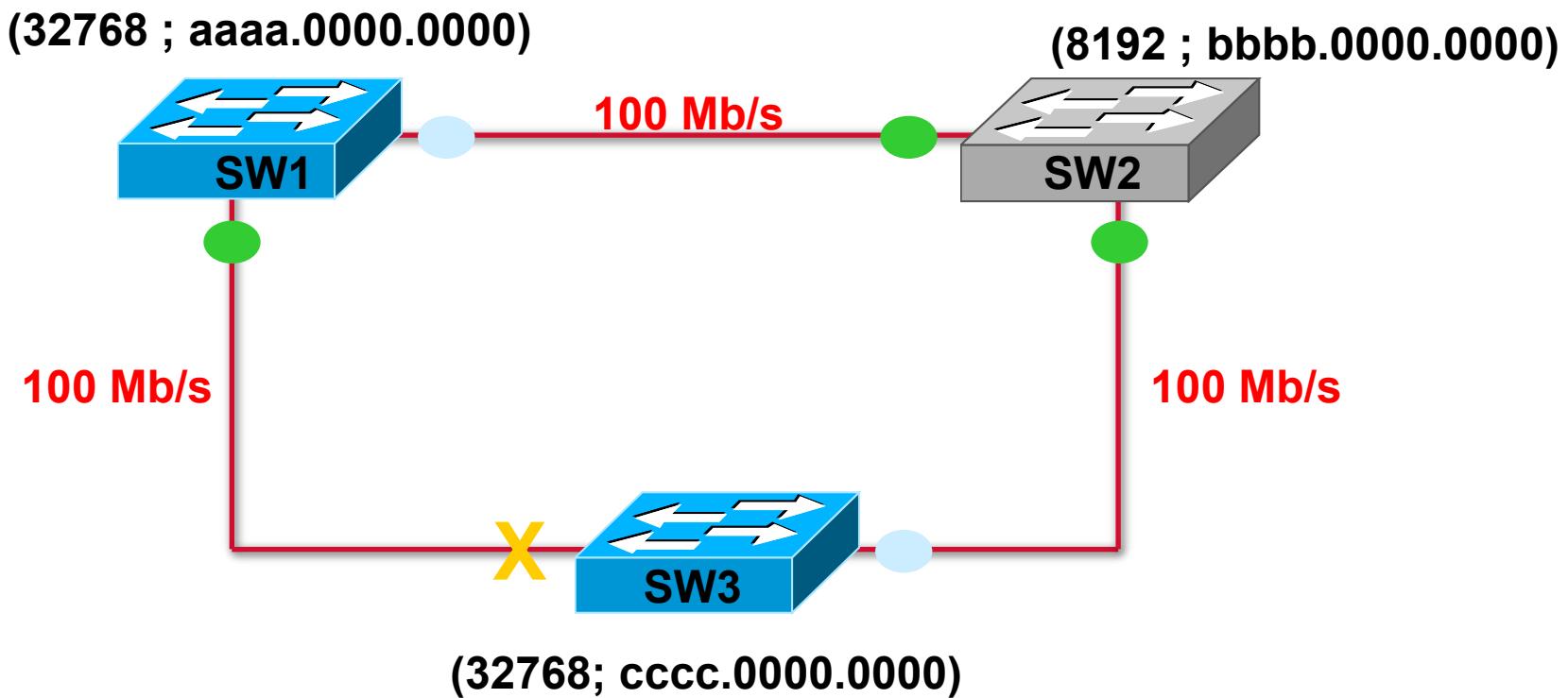
Port non désigné



Exercice 1

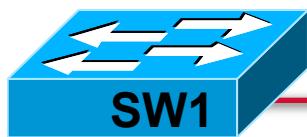


Solution 1



Exercice 2

(32768 ; aaaa.0000.0000)



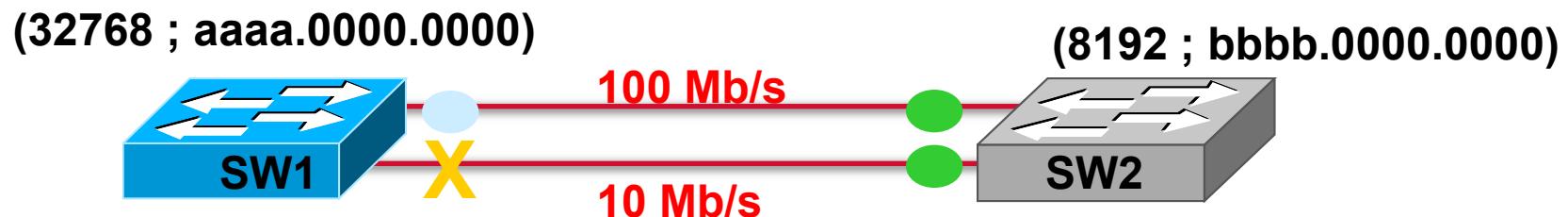
100 Mb/s

(8192 ; bbbb.0000.0000)



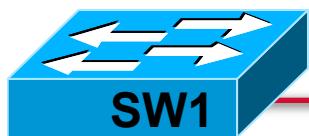
10 Mb/s

Solution 2



Exercice 3

(32768 ; aaaa.0000.0000)



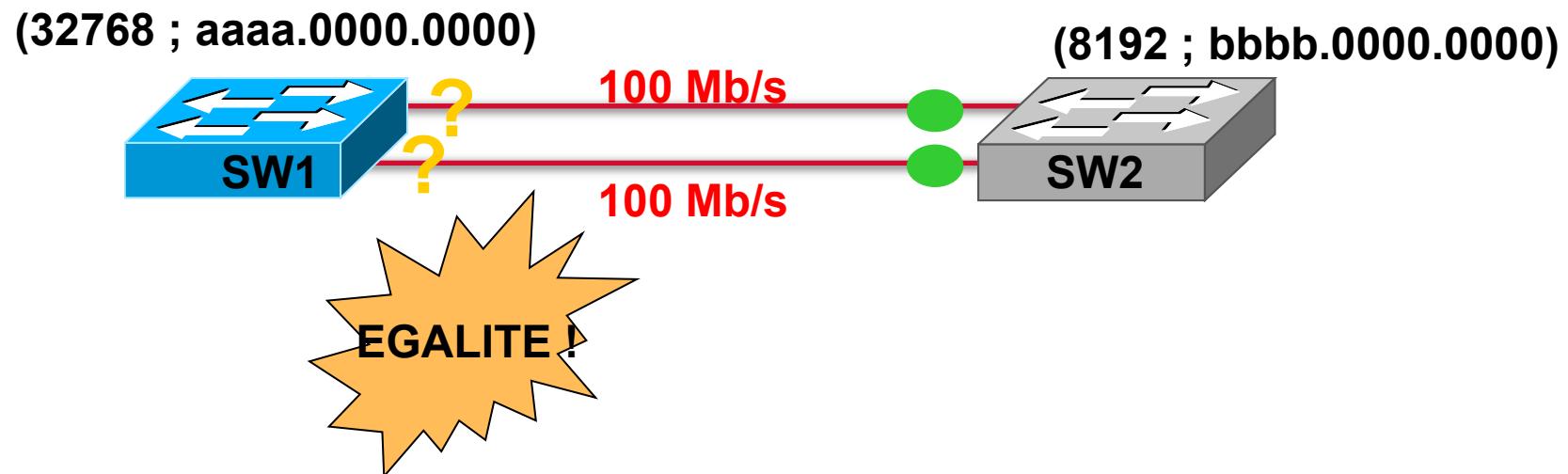
100 Mb/s

(8192 ; bbbb.0000.0000)



100 Mb/s

Solution partielle 3



Le PORT-ID

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

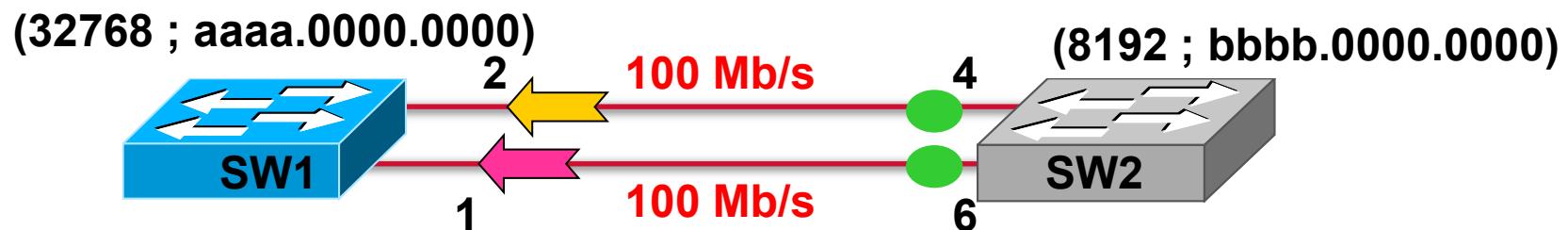
- Port PRIORITY :
 - entre 1 et 256
 - par défaut 128

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

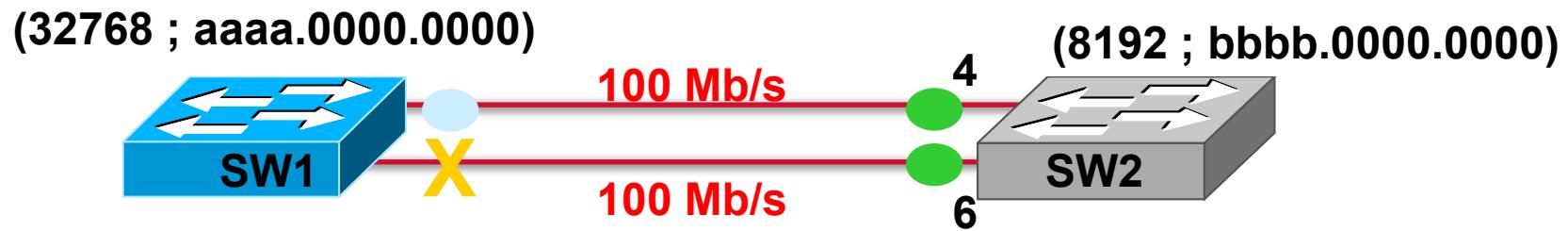
Quels Port-ID sont envoyés ?

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



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

Solution 3



Etats d'un port

- Racine FORWARDING
- Désigné FORWARDING
- Non désigné BLOCKING

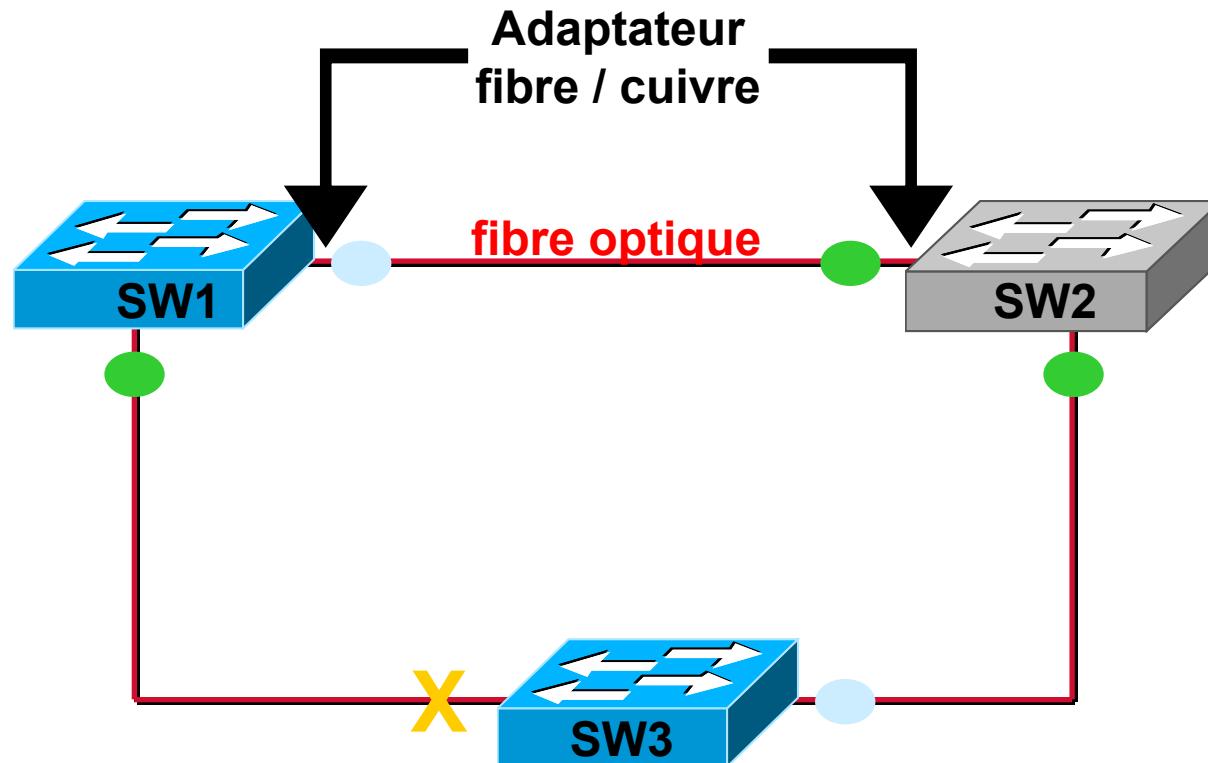
Passage en Forwarding

- 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

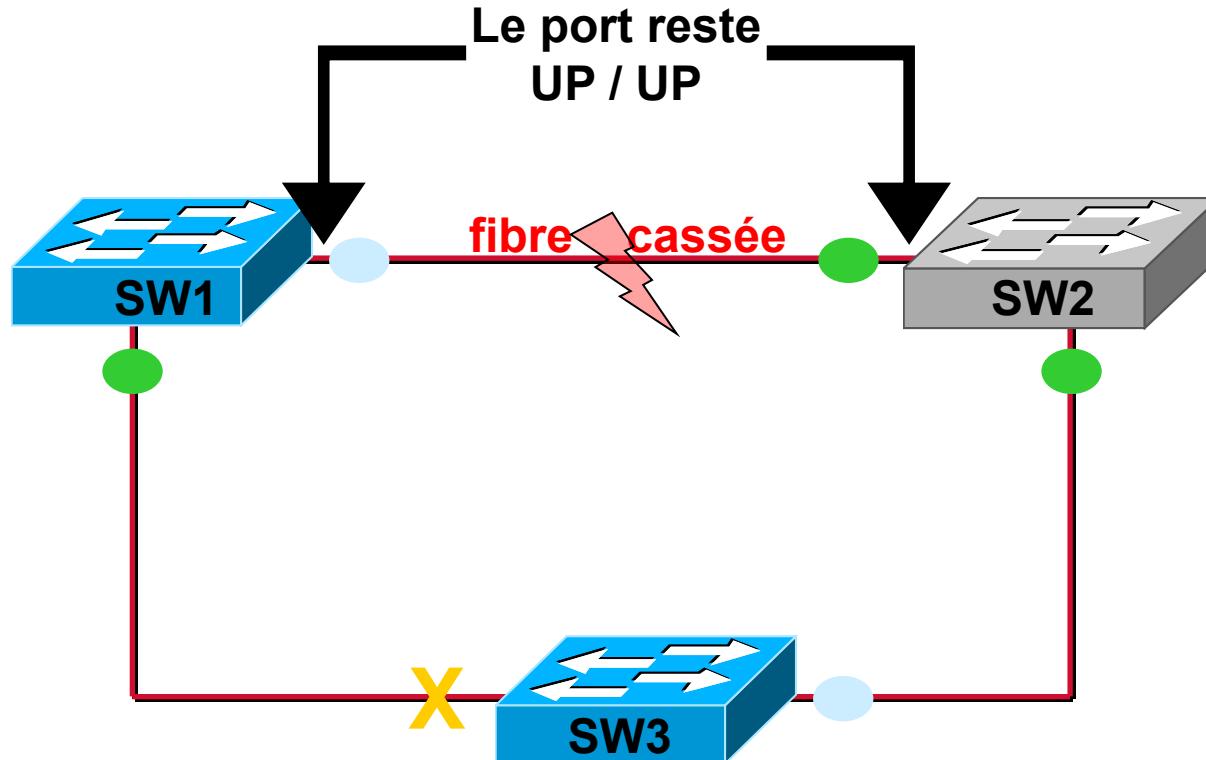
Timers STP

- 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

Name	Port	ID	Prio	Designated				Port ID
				Cost	Sts	Cost	Bridge 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 précédente
 - 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

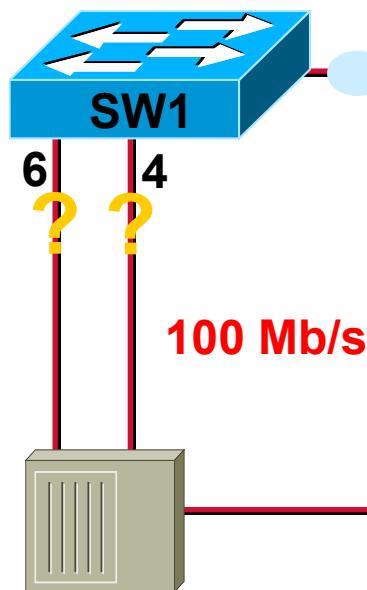
- `conf t`
- `spanning-tree mode rapid-pvst`
- Compatible avec STP.
- Les BPDU sont générés par **chaque switch** (et pas seulement par le switch racine).
 - Je n'attends plus 20 secondes pour réagir.
 - Je réagis dès que 3 BPDU ne sont pas arrivés

Rôles d' un port

- Racine 
- Désigné 
- Non désigné : 
 - 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’

(32768 ; aaaa.0000.0000)

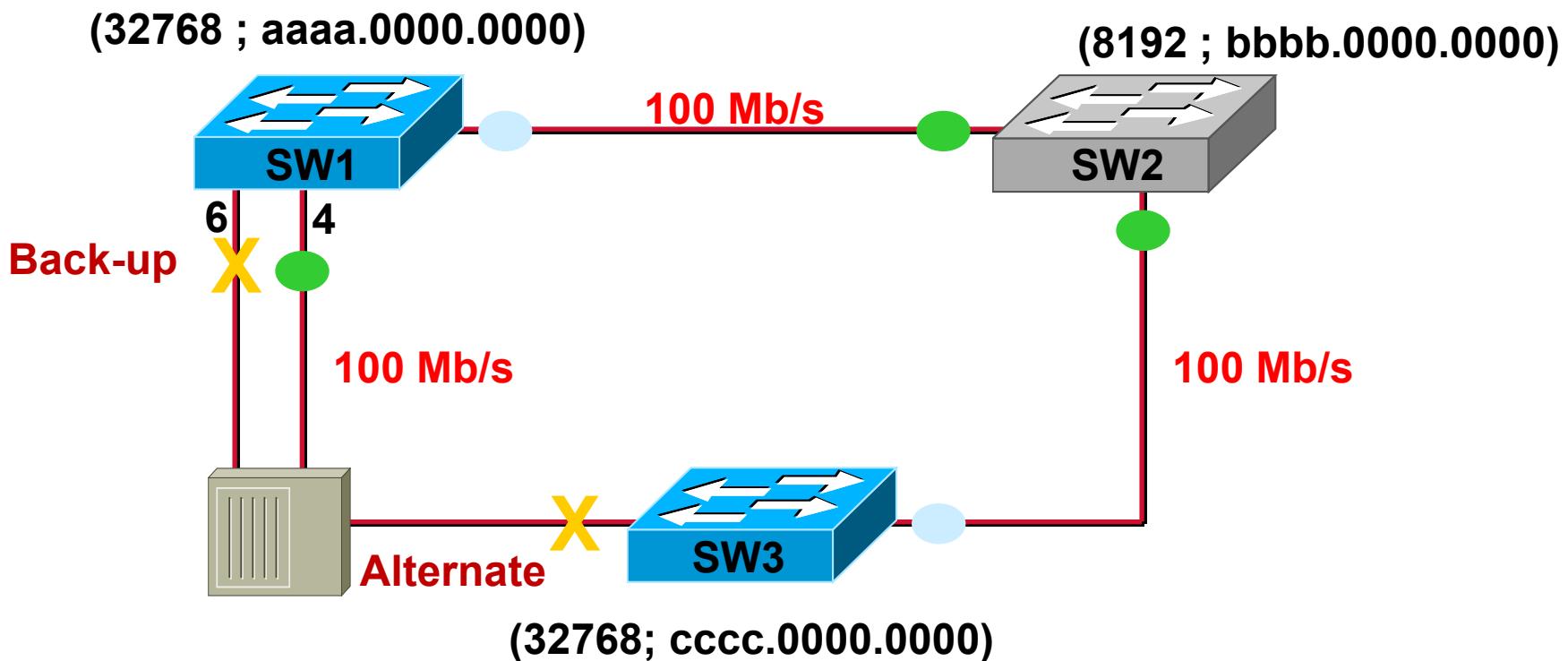


(8192 ; bbbb.0000.0000)

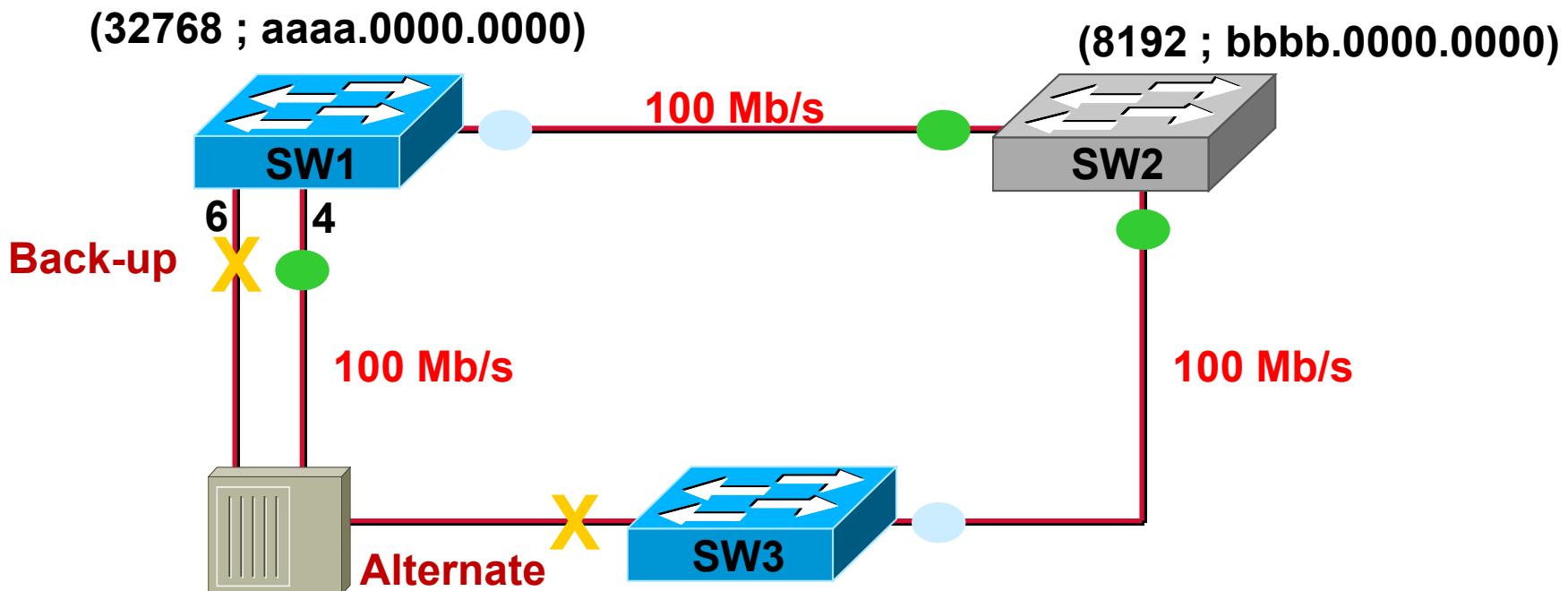
Quels sont les rôles
de chaque port de ce
segment ?

(32768; cccc.0000.0000)

Exemple pour ‘alternate / backup’



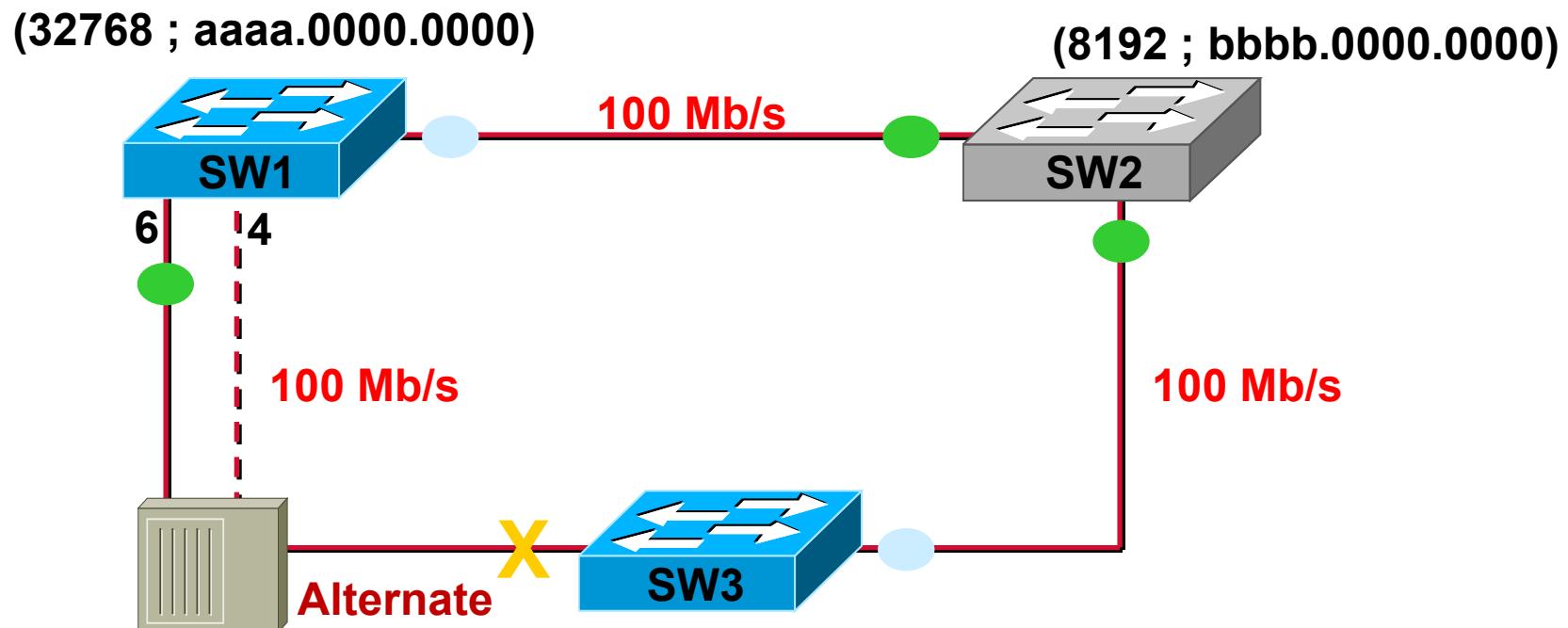
Exemple pour ‘alternate / backup’



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

(32768; cccc.0000.0000)

Exemple pour ‘alternate / backup’



Le Back-up prend la
relève.

(32768; cccc.0000.0000)

RSTP : 3 types des ports

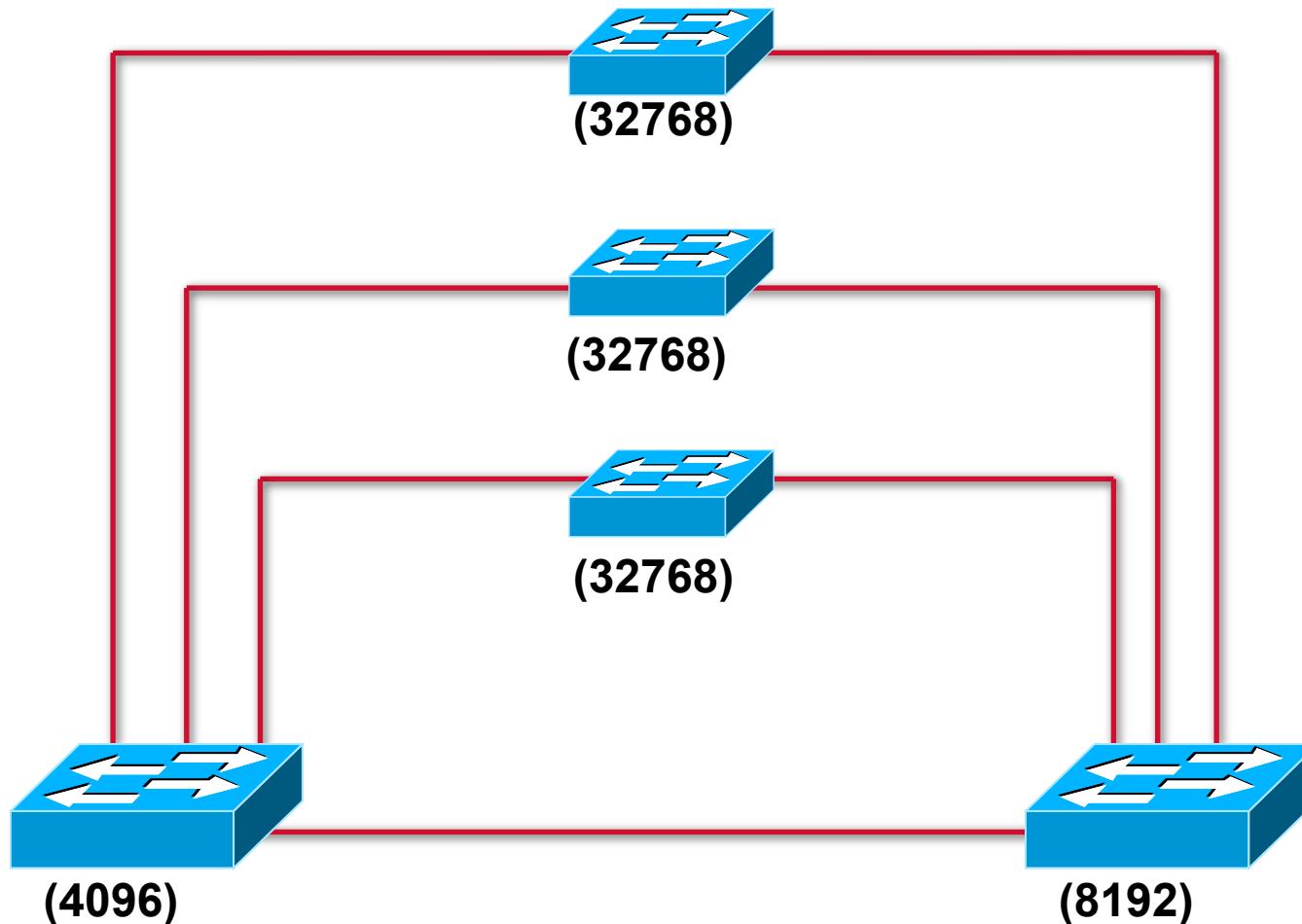
- « Point-to-Point »
 - Switch en full duplex
 - Convergence plus rapide avec RSTP
- « Shared »
 - Hub (half duplex)
- « Edge »
 - Connecté à un host
 - Configuré via PortFast

PVST+

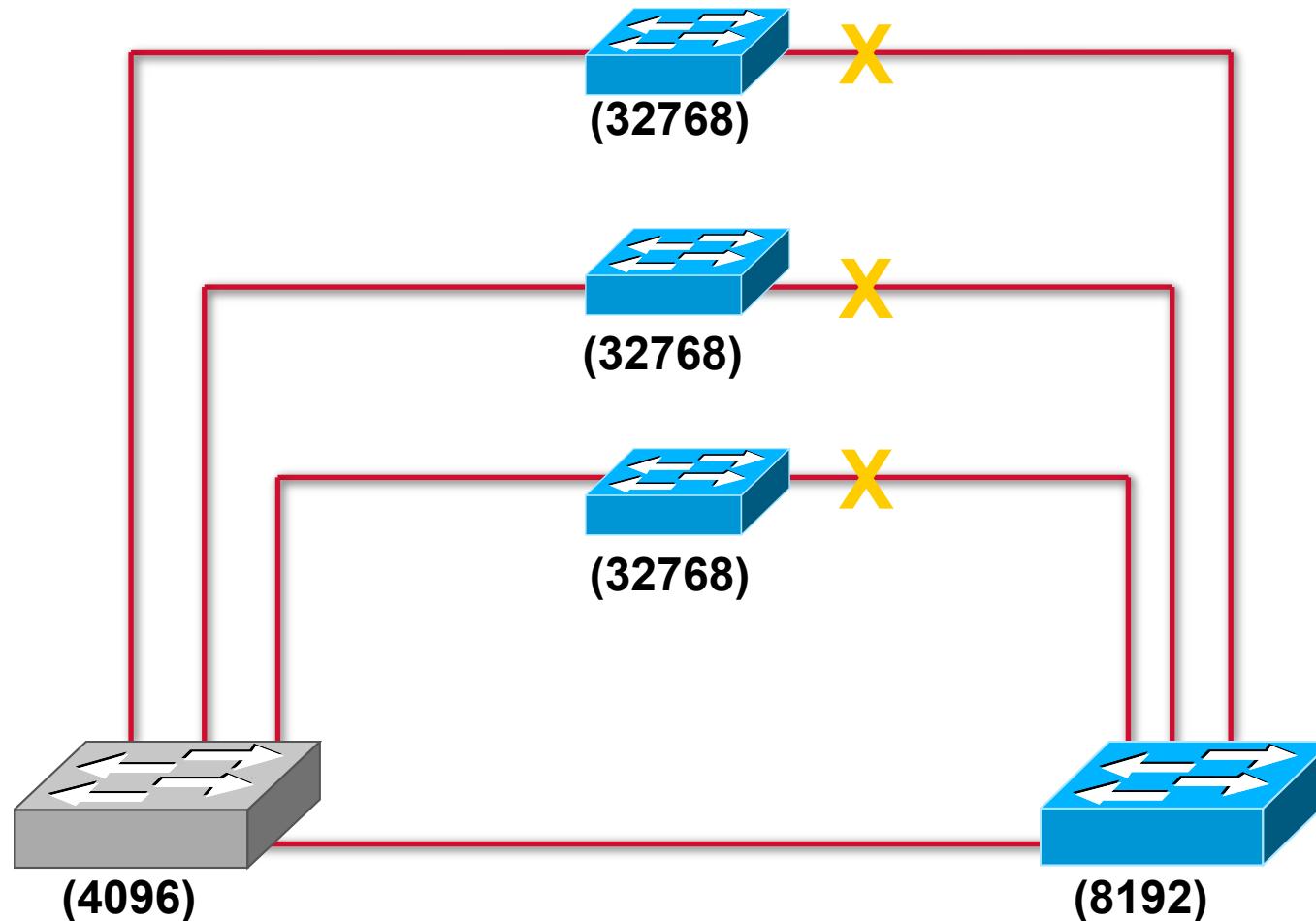
- Per VLAN Spanning-Tree
- Un arbre de recouvrement pour CHAQUE vlan.
- Compatible avec Rapid-STP.

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

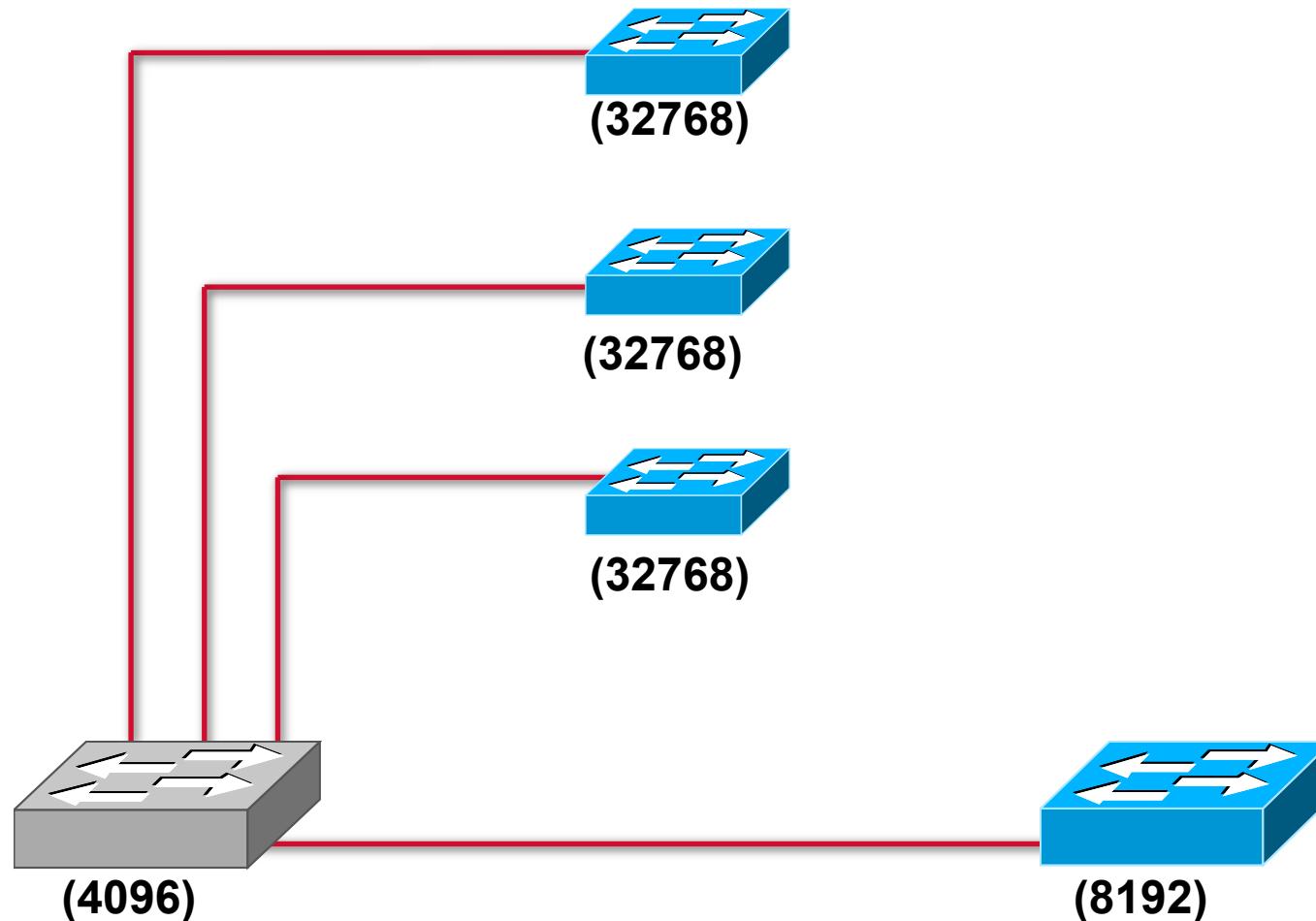
Batiment avec 3 étages



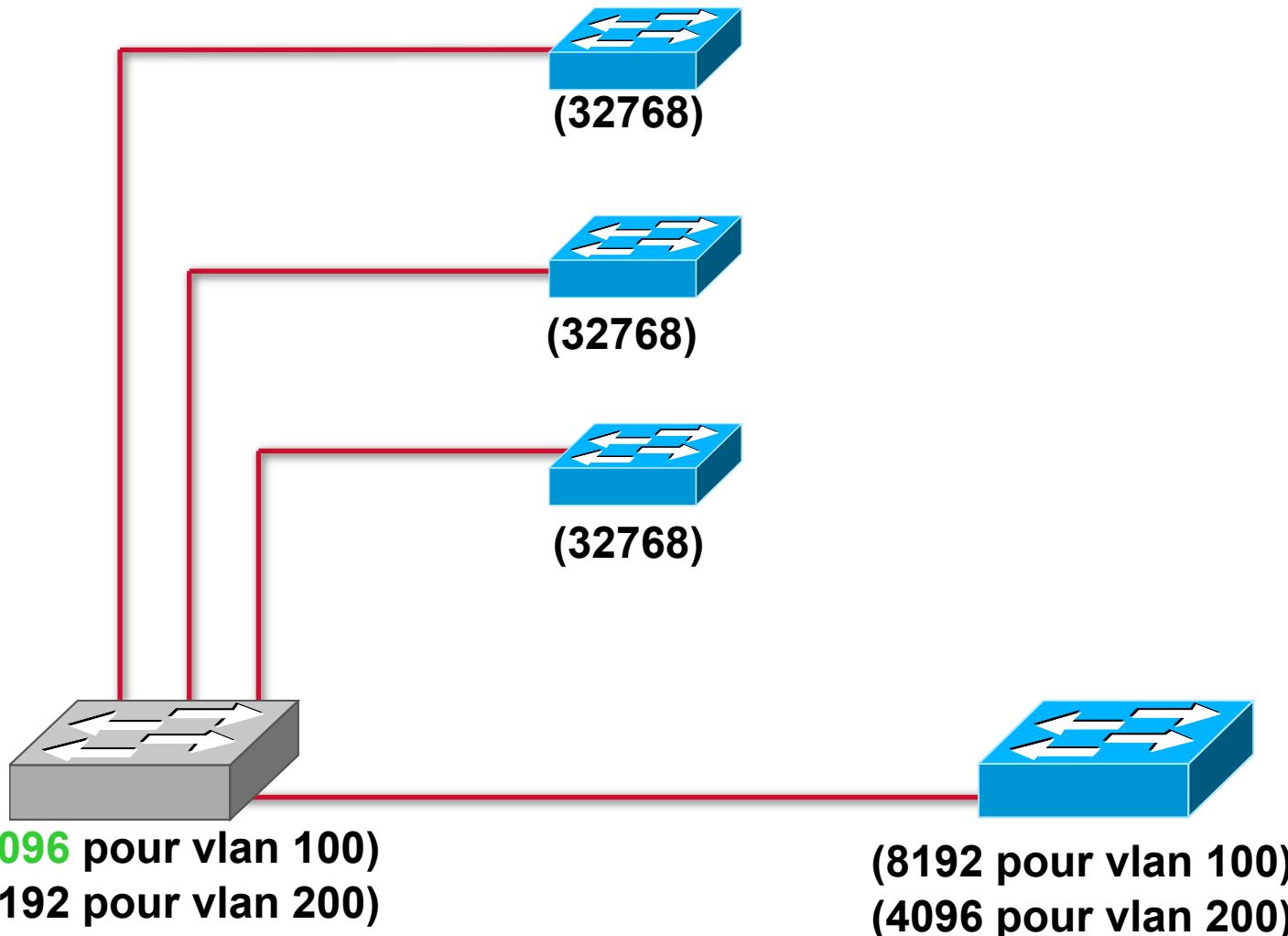
1 STP pour tous les VLANs



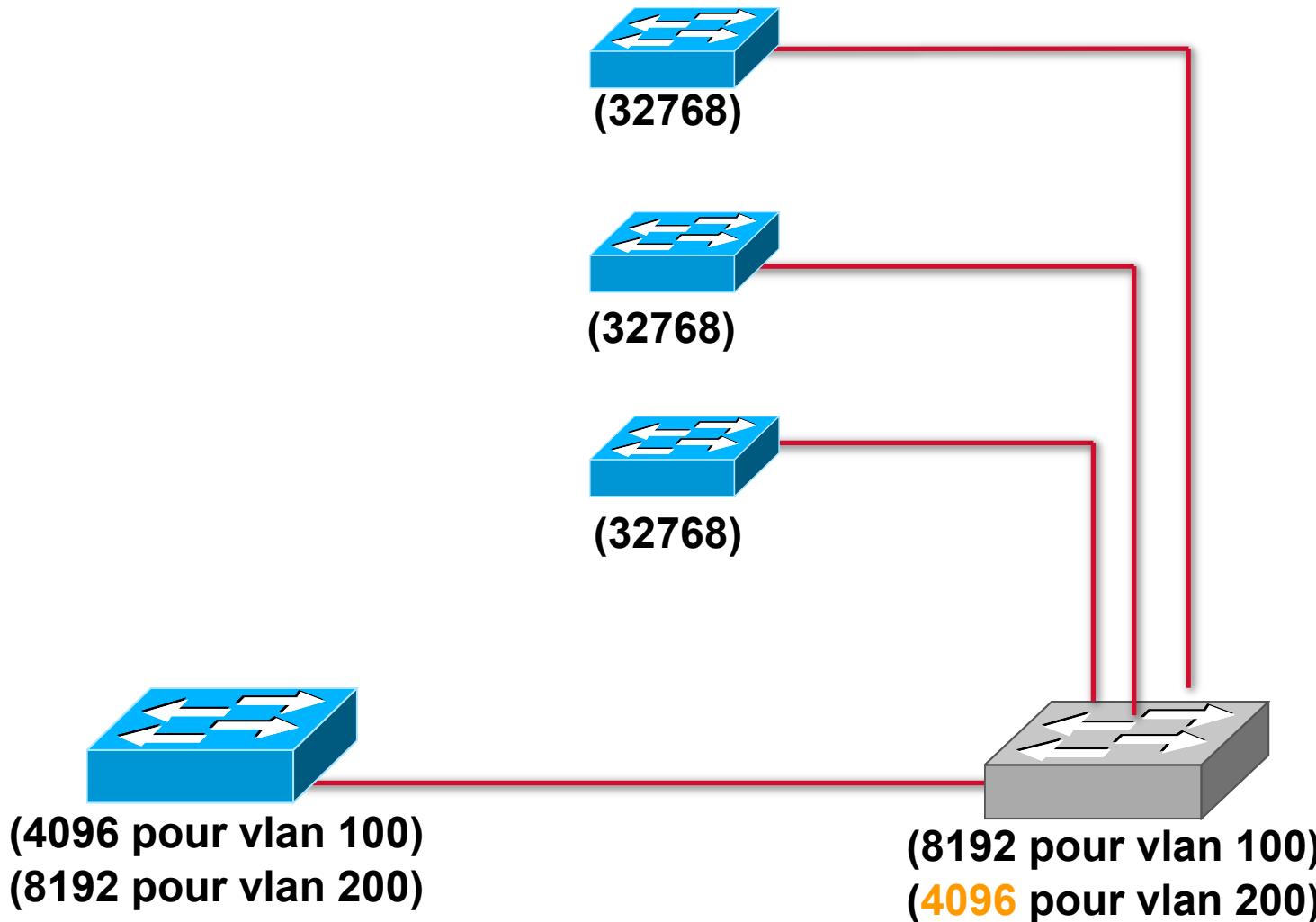
TOUT le trafic passe par ici...



PVSTP : trafic du VLAN 100



PVSTP : trafic du VLAN 200



Positionner le sw racine

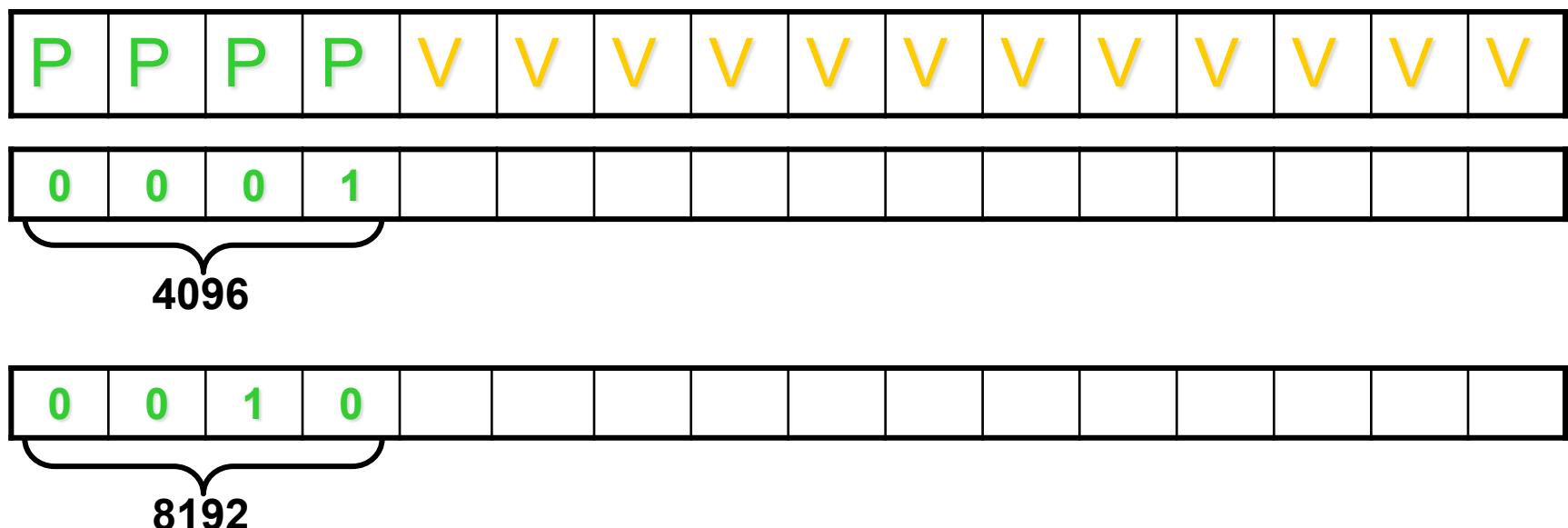
- Diminuer sa priorité.
- Par défaut, Bridge PRIORITY = 32768
- Pour diminuer :
 - conf t
 - spanning-tree vlan 100 priority 8192
 - obligatoirement un multiple de 4096

Le CHAMP bridge priority

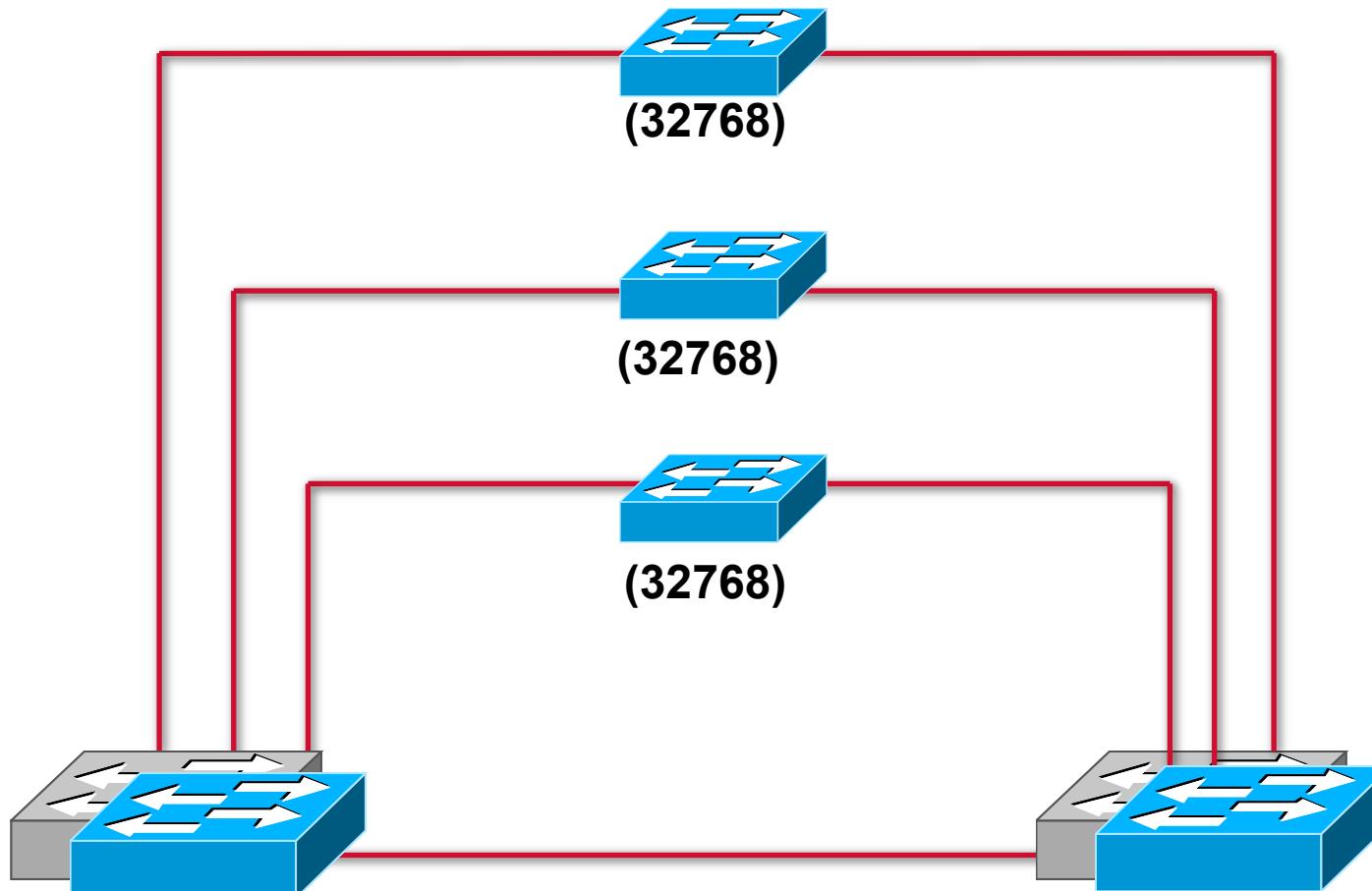
Entre 0 et 65535 = 16 bits

Utilisé pour coder à la fois :

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



Configuration PVSTP

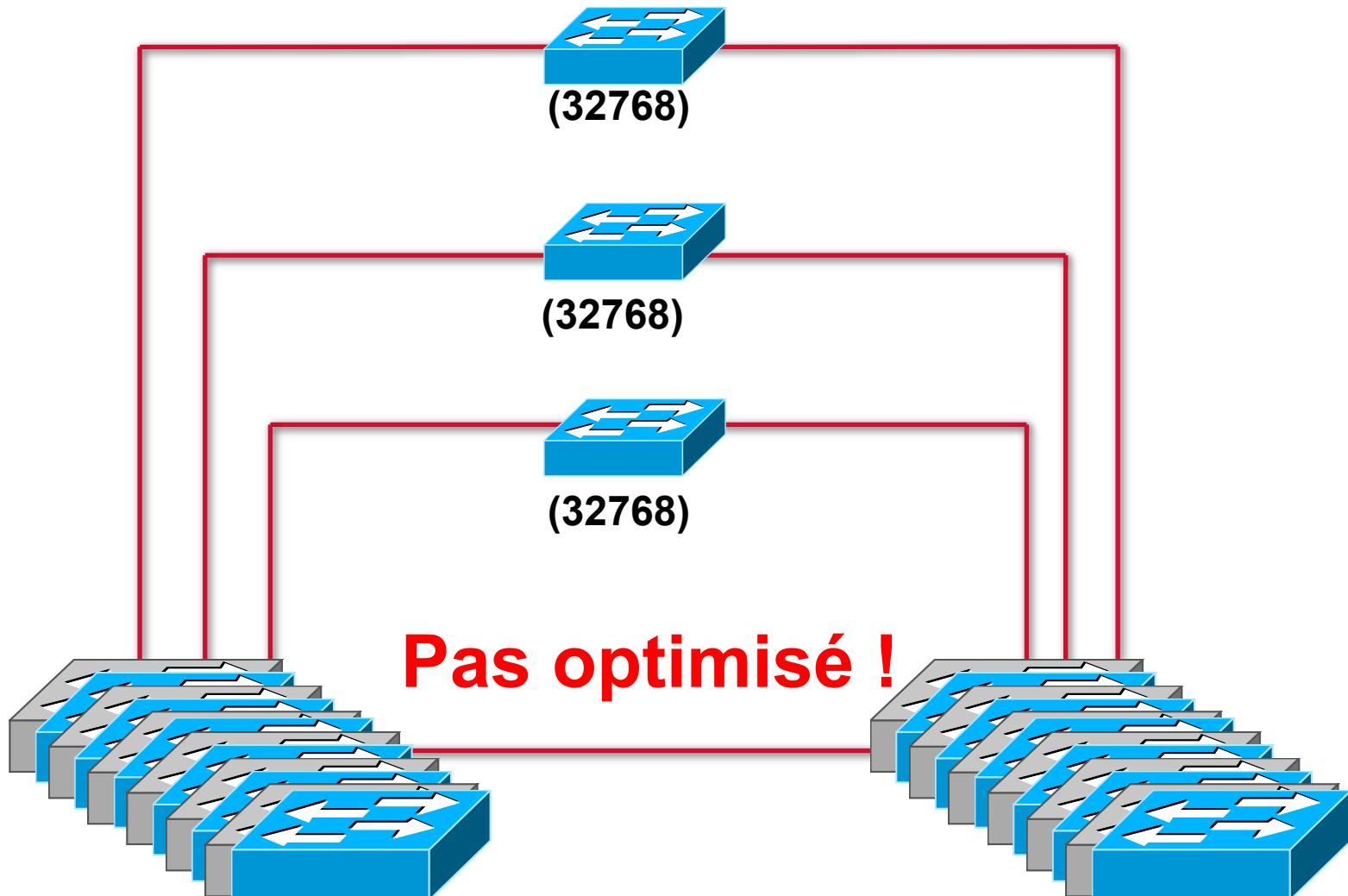


spanning-tree vlan 100 priority **4096**
spanning-tree vlan 200 priority 8192

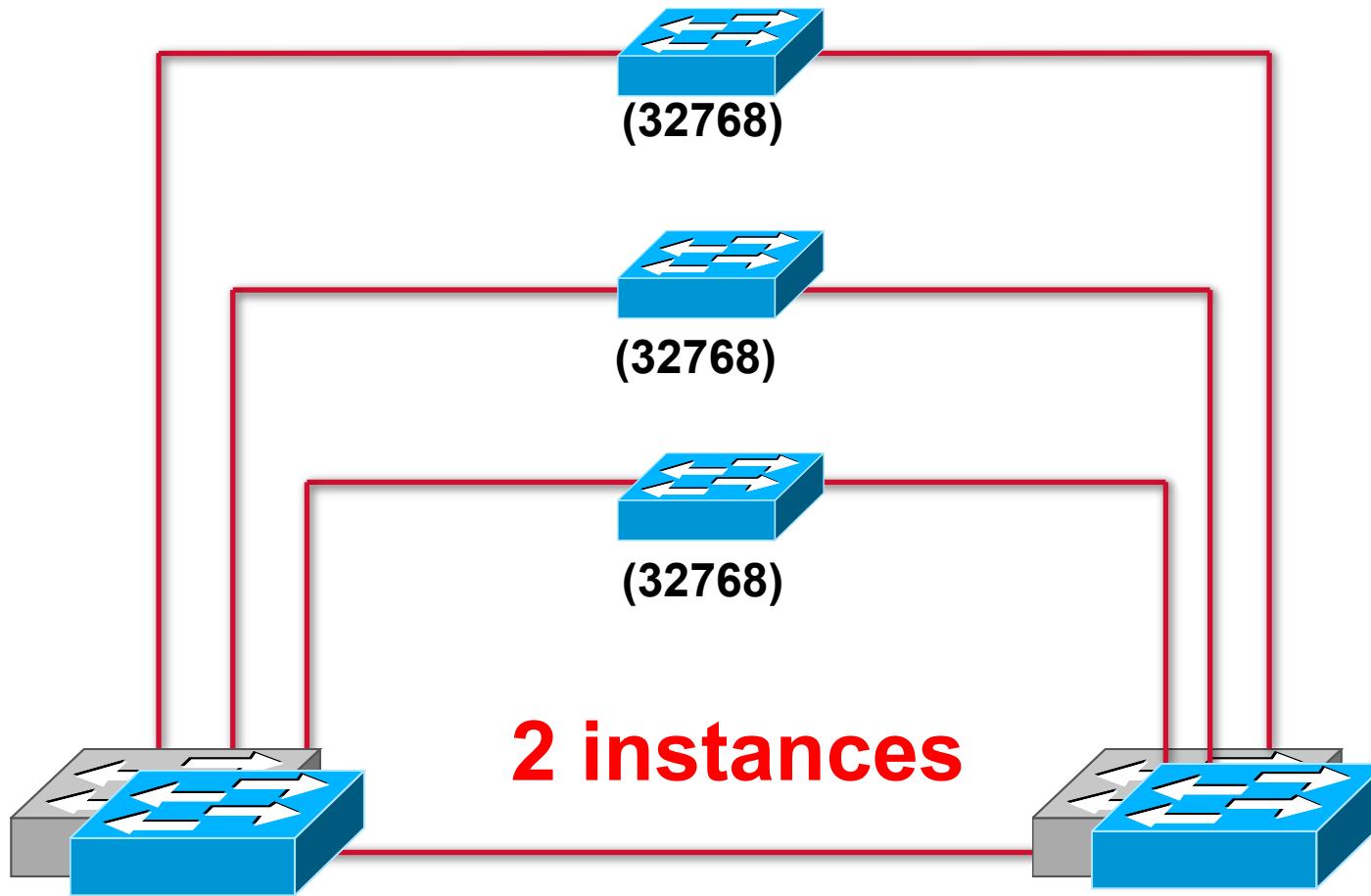
spanning-tree vlan 100 priority 8192
spanning-tree vlan 200 priority **4096**

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

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

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

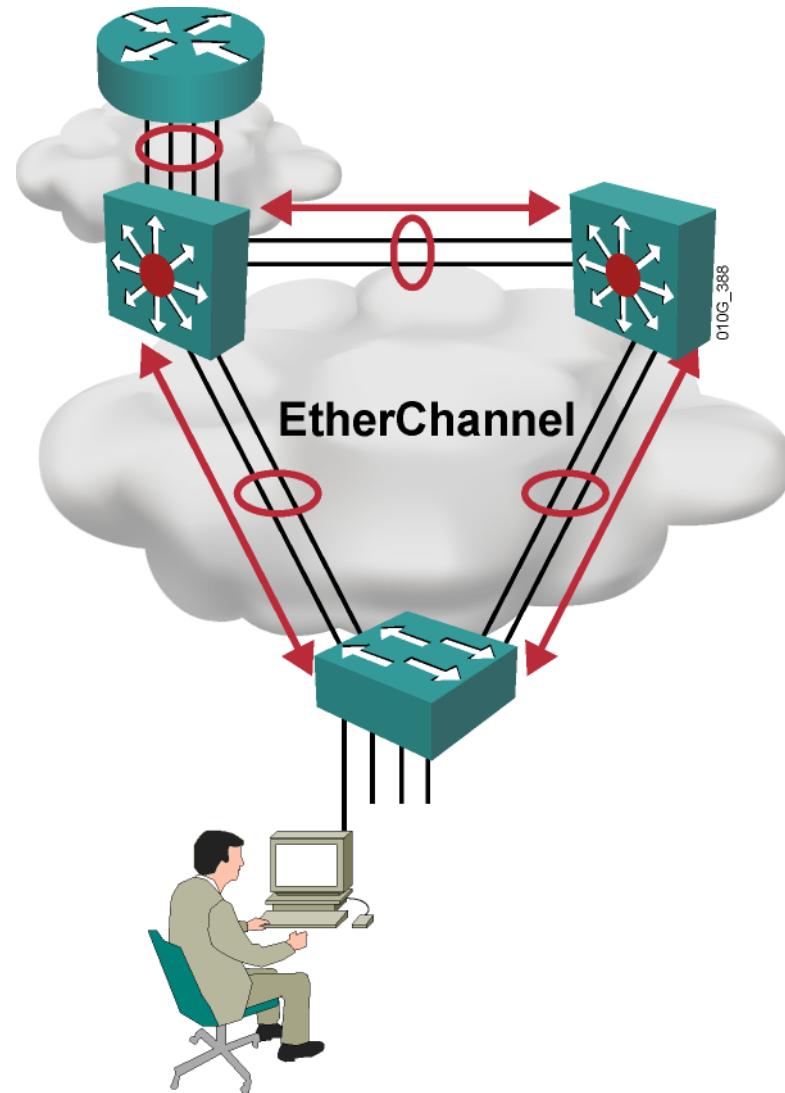
Correct Answer: A

Etherchannel

Aggrégation de liens

EtherChannel

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



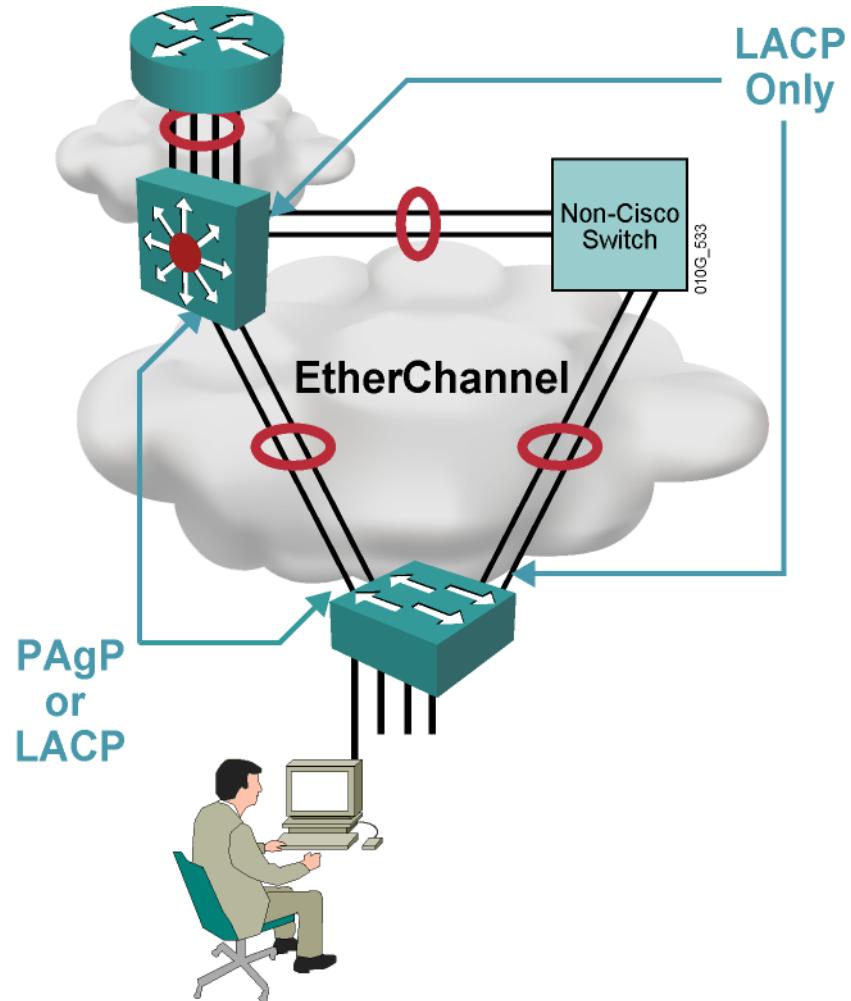
Protocoles de négociation dynamique

PAgP

- Propriétaire Cisco

LACP

- Standard IEEE 802.3ad



Terminologie de négociation

LACP		PAgP		Static Persistance
	Active	Passive		
Active	Yes	Yes	Desirable	Auto
Passive	Yes	No	Auto	Yes
				On
				On

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

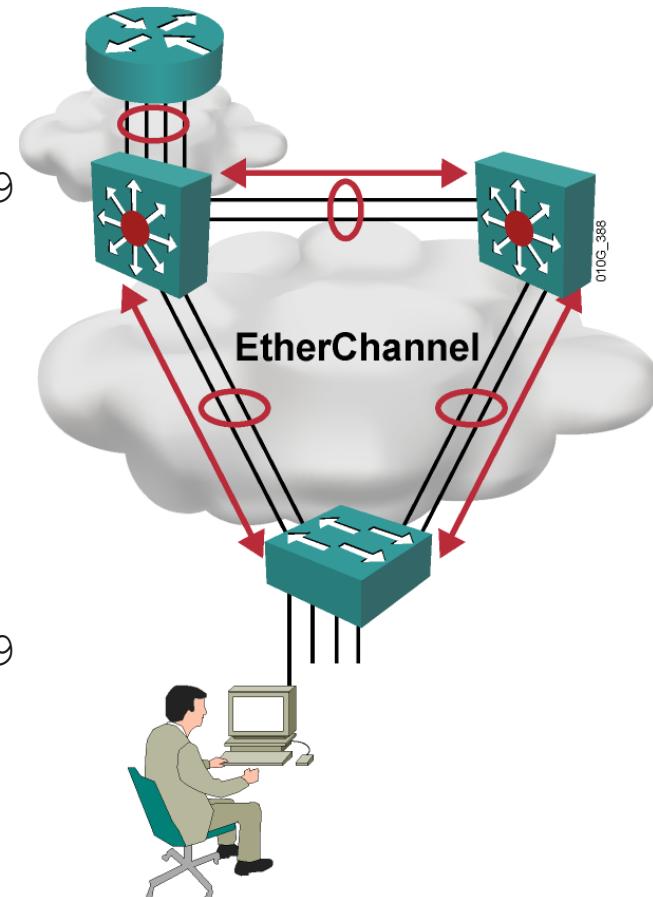
```
interface FastEthernet0/9
description DSW121 0/9-10 - DSW122 0/9
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,21-28
switchport mode trunk
```

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

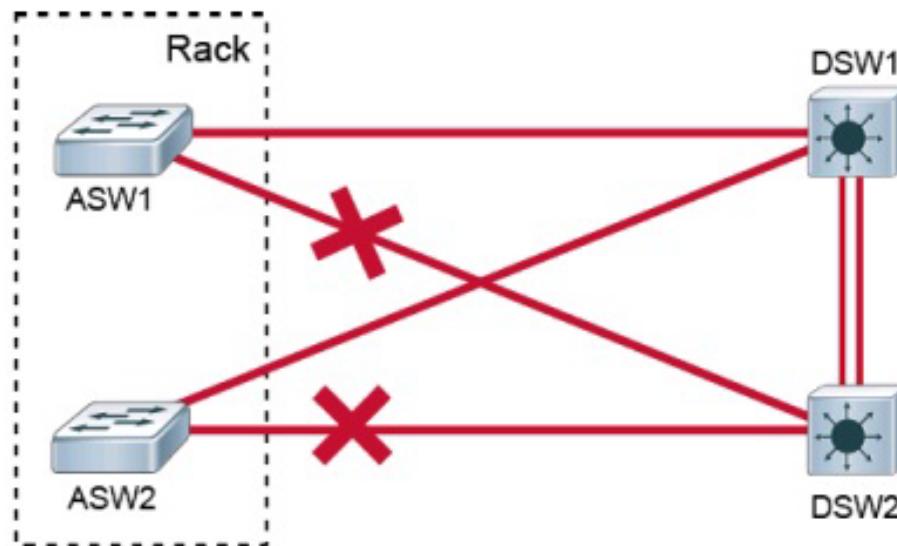


Switch Stacking



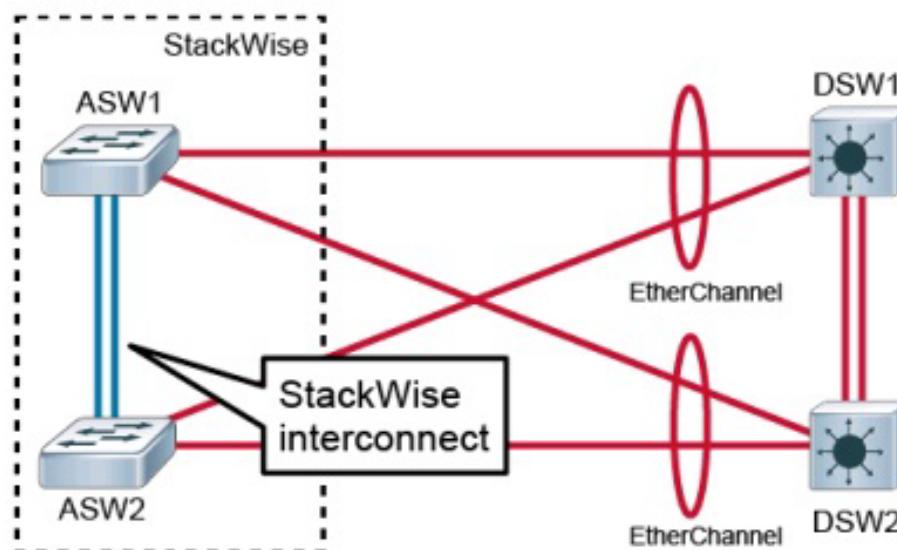
- StackWise provides a method to join multiple physical switches into a single logical switching unit.
- Switches are united by special interconnect cables.
- The master switch is elected.
- The stack is managed as a single object and has a single management IP address.

Switch Stacking (Cont.)



Typical switch topology:

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



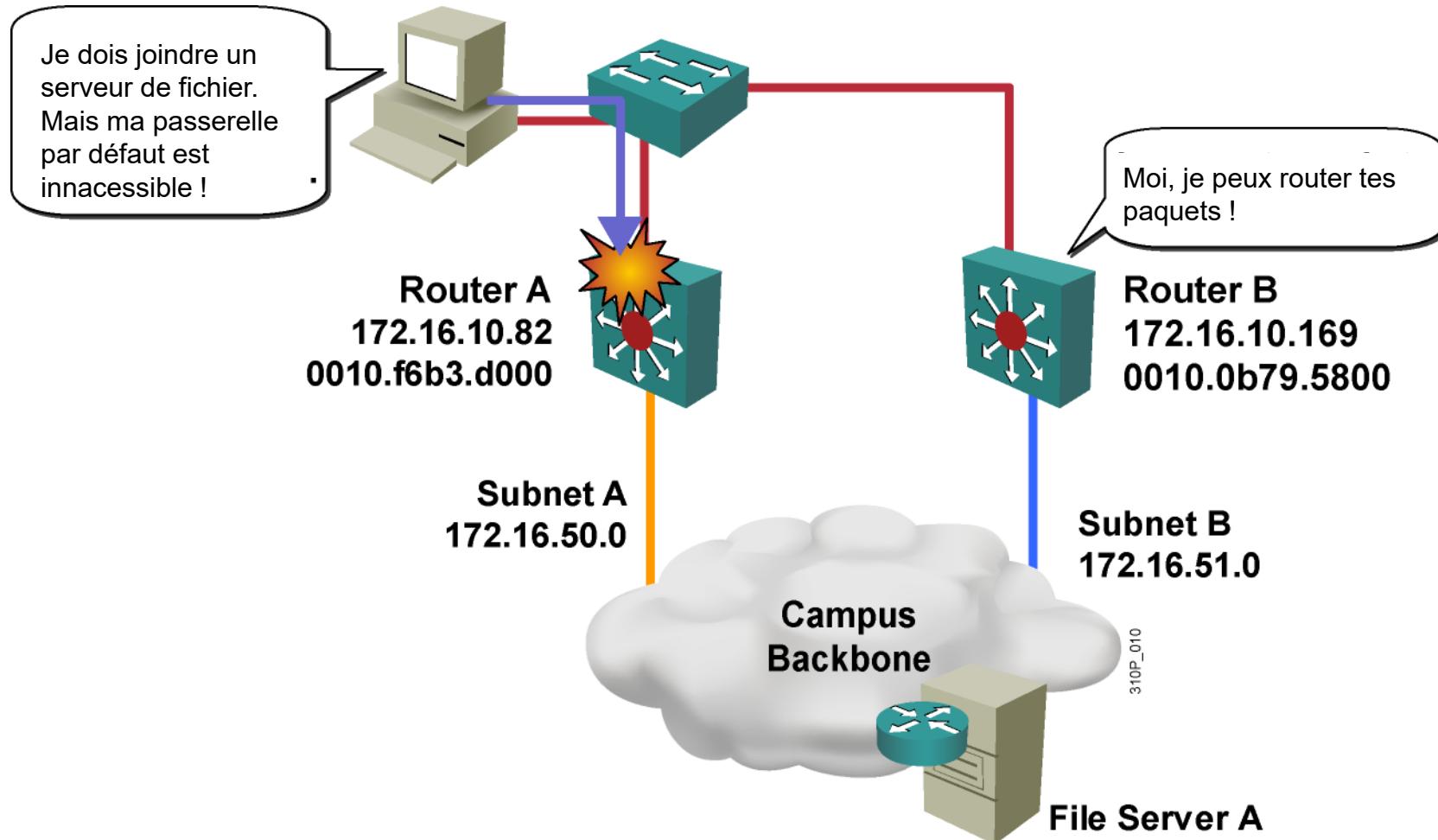
Topology using StackWise:

- 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

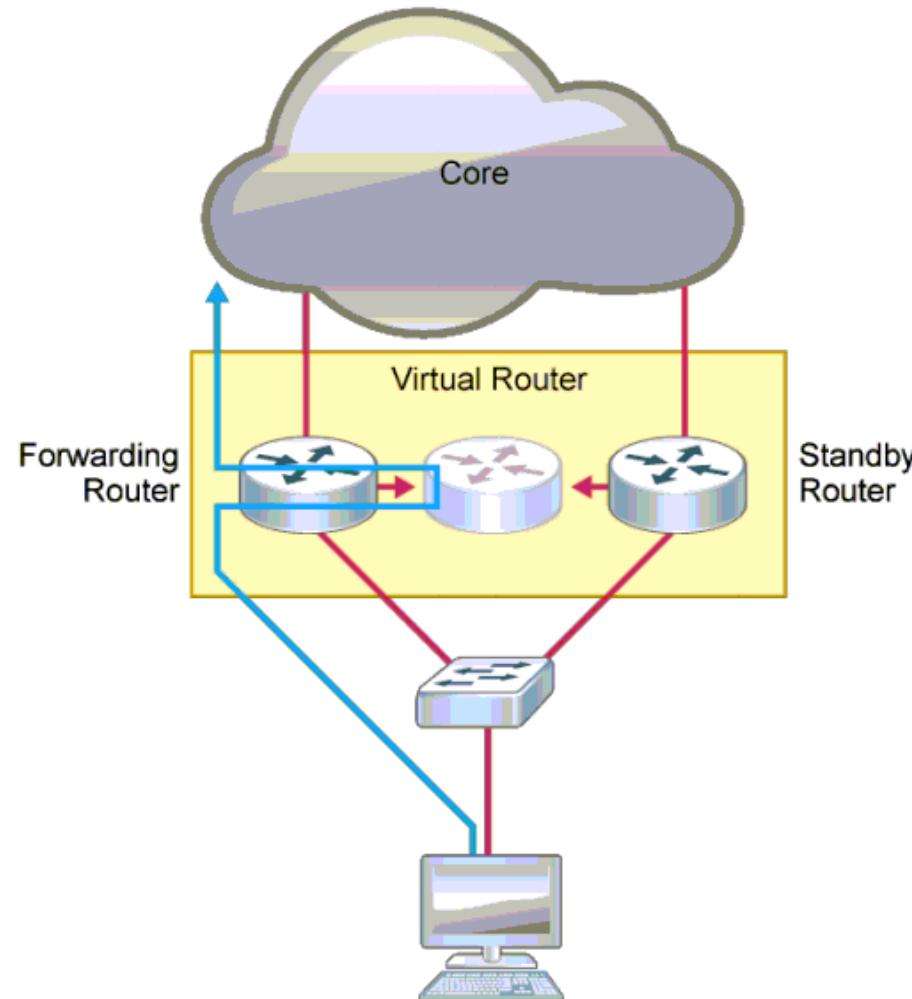
Configurer la redondance de la passerelle par défaut avec HSRP

Indisponibilité de la passerelle par défaut

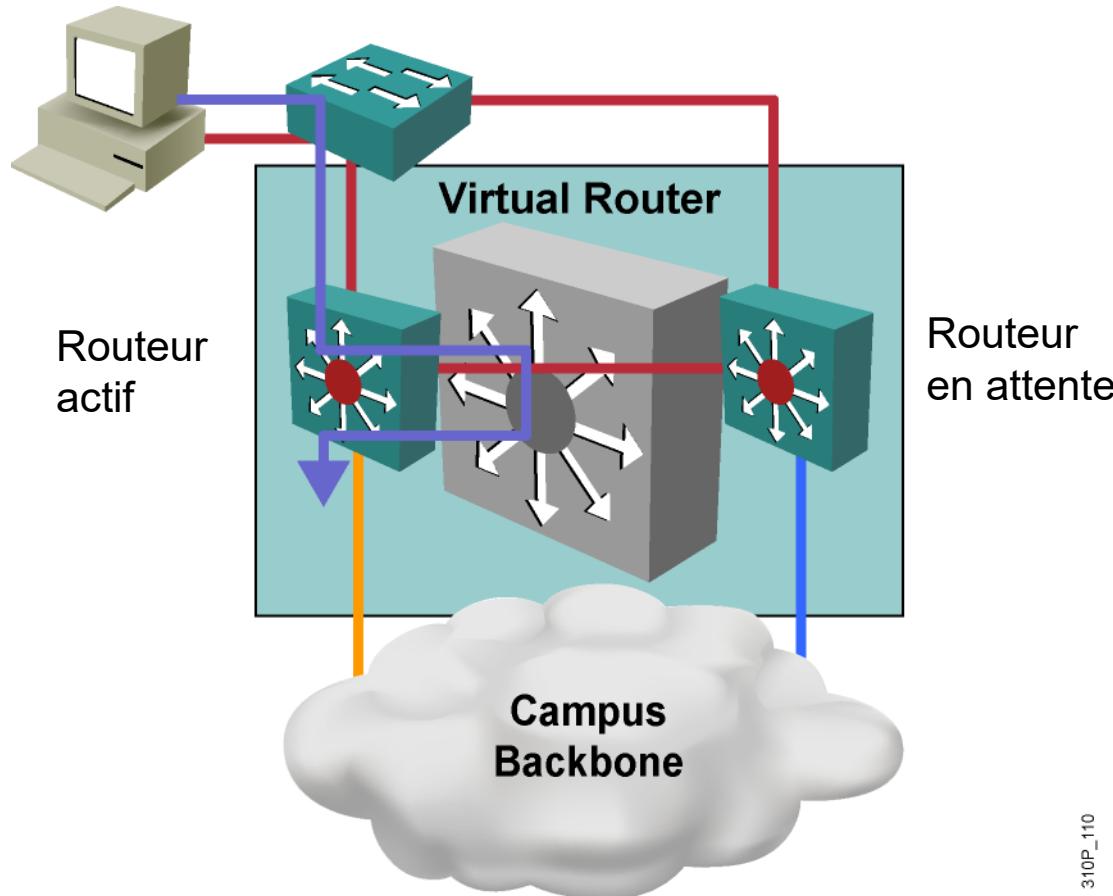


First Hop Redundancy Protocol

Understanding FHRP



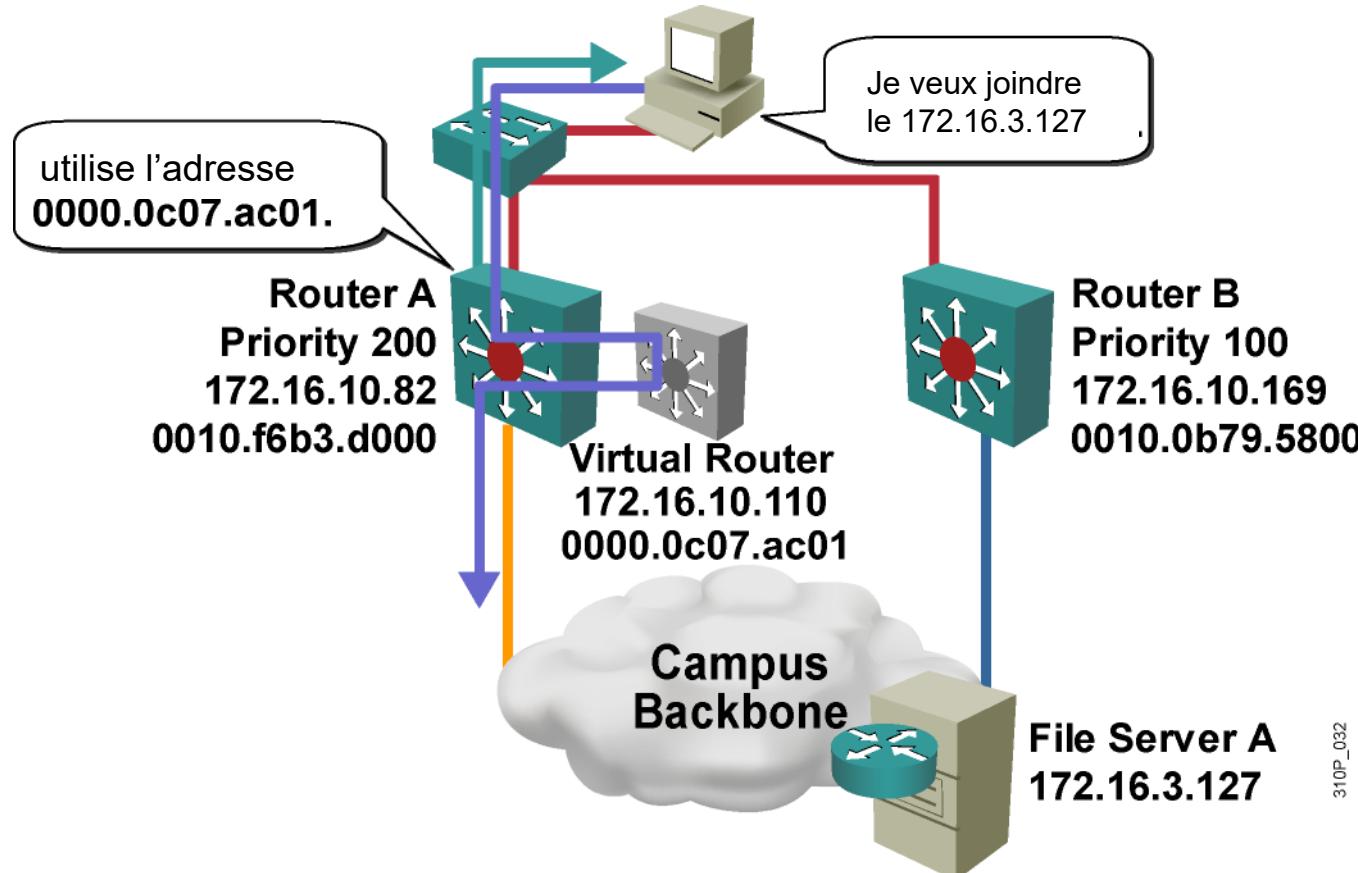
Cisco HSRP (Hot Standby Routing Protocol)



310P_110

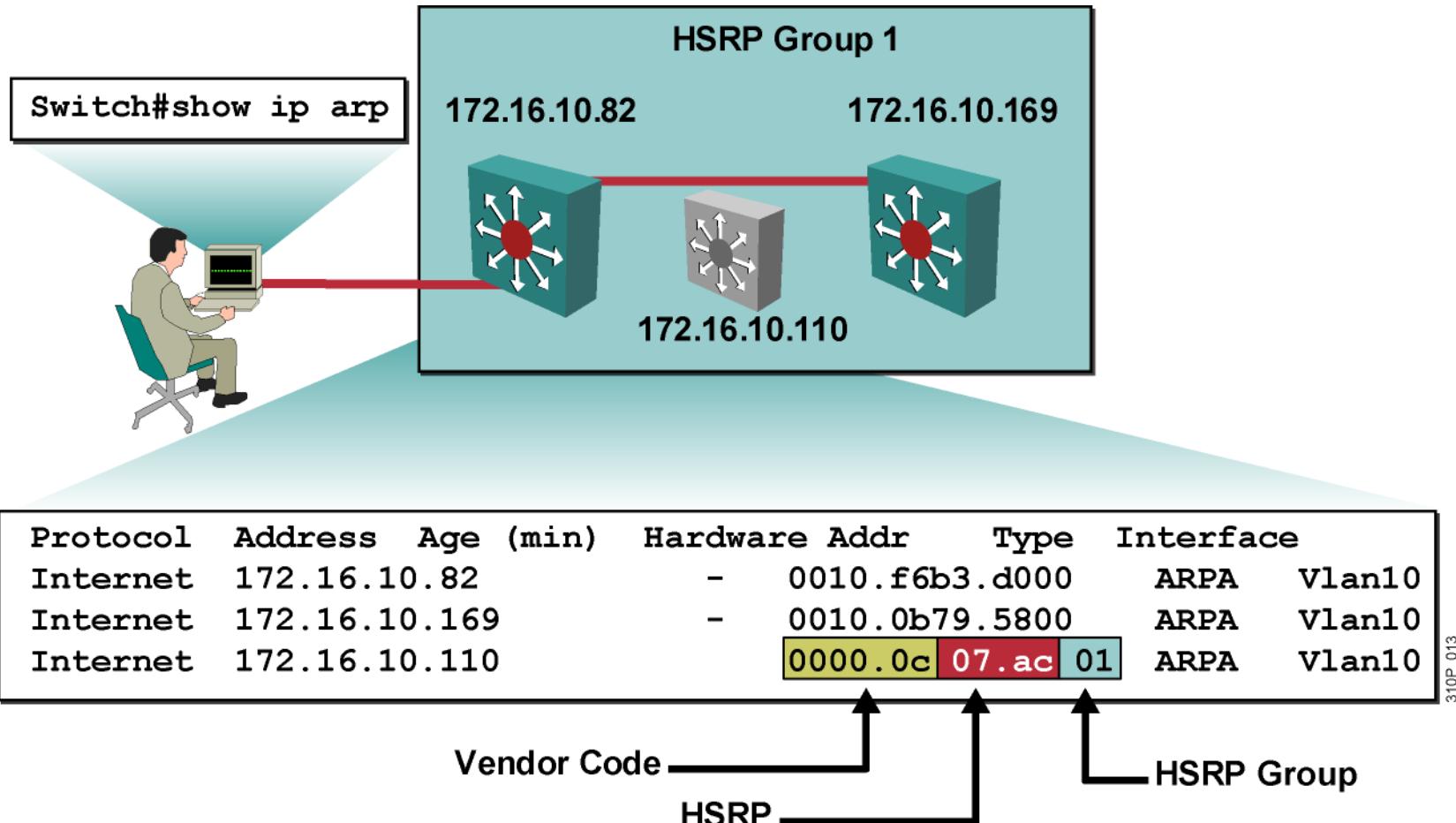
Un ensemble de routeurs, en secours d'un routeur actif, est appelé groupe HSRP

Le routeur Actif

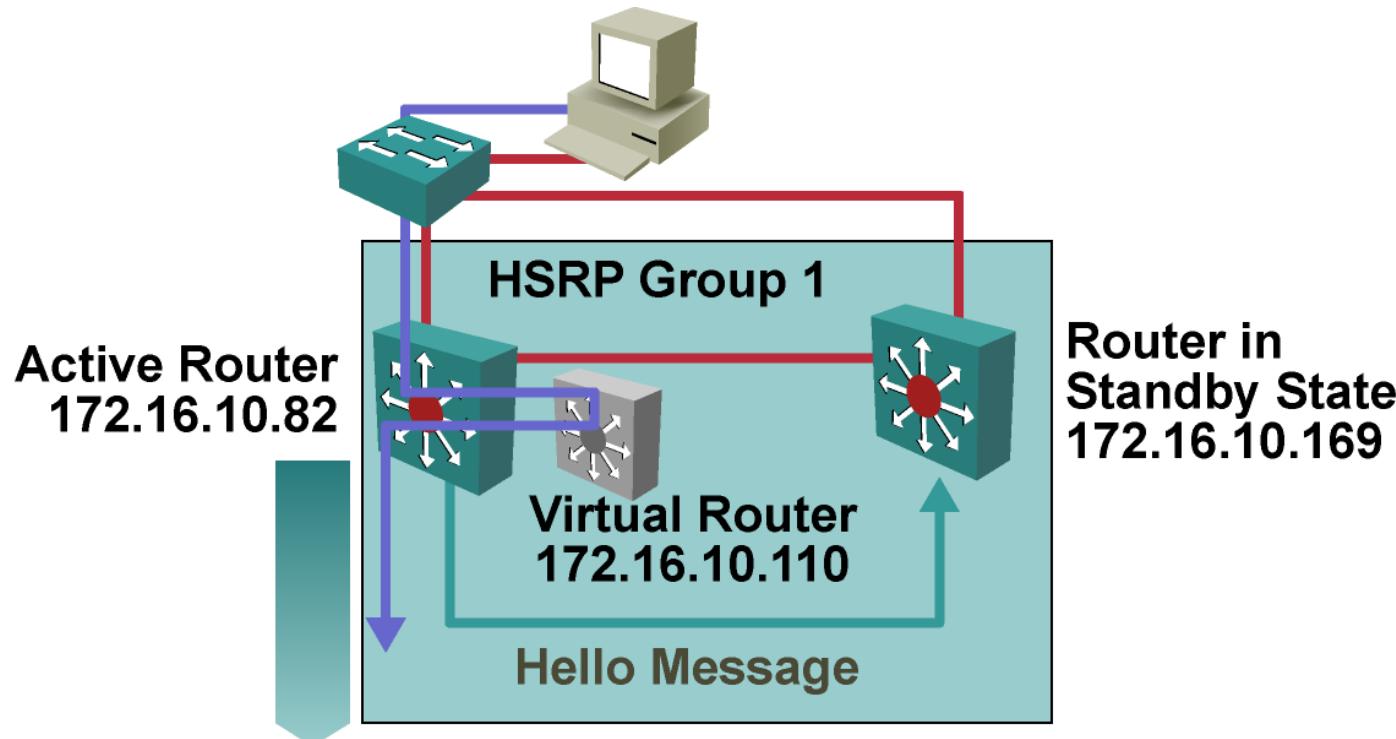


Le routeur actif répond aux requêtes ARP avec l'adresse MAC virtuelle du routeur virtuel

Adresse MAC virtuelle



Le routeur Standby

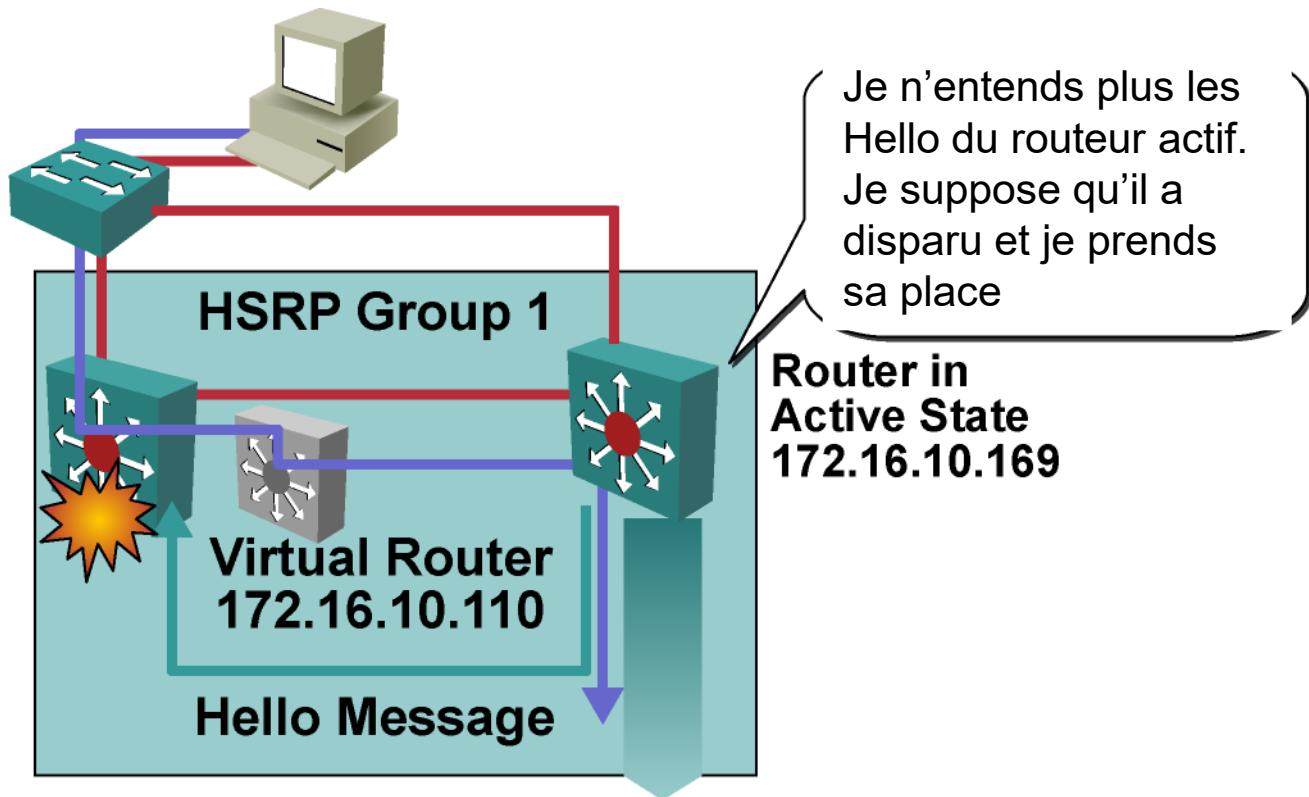


```
1d23h : SB1:Vlan10 Hello out 172.16.10.82 Active pri 200 hel 3 hol 10 ip 172.16 .10.110
```

310P_033

Le routeur Standby écoute les hellos périodiques sur 224.0.0.2.

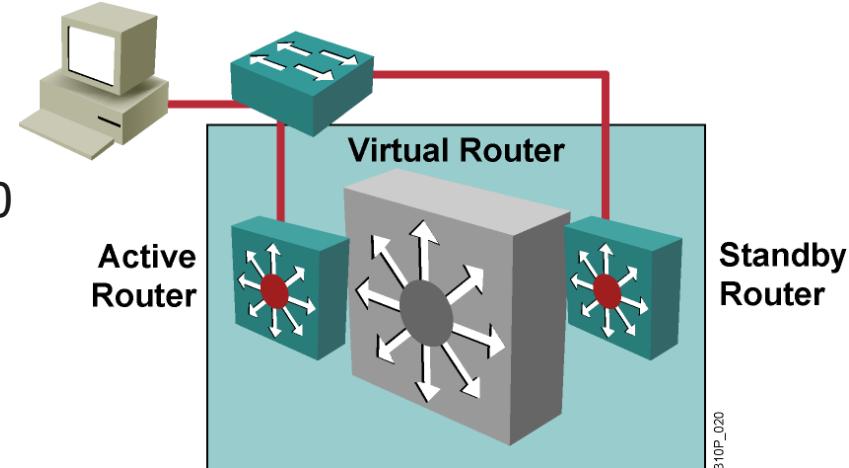
Si le routeur actif n'entend plus le Stanby



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

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
V111       10  110   Active     local           172.16.10.169  172.16.10.110
```

Configuration des priorités HSRP

```
Switch#show standby vlan 10
interface Vlan10
  ip address 172.16.10.82 255.255.255.0
  no ip redirects

  standby 1 priority 150
  standby 1 ip 172.16.10.110
```

Assigned Priority
Standby Group Number

```
Switch (config-if) #standby 1 priority 150
```



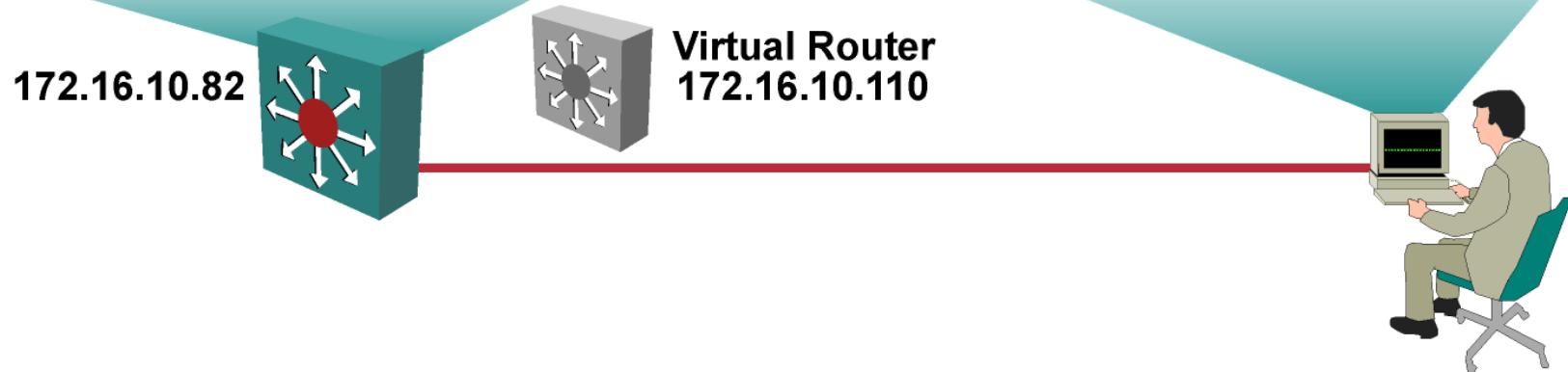
- C'est le routeur qui a la plus grande priorité qui devient actif
- La priorité par défaut est 100
- En cas d'égalité, c'est le routeur avec la plus grande adresse IP qui devient actif.

Configuration HSRP de la préemption

```
Switch#show standby vlan 10
interface Vlan10
 ip address 172.16.10.82 255.255.255.0
 no ip redirects
 standby 1 priority 150
standby 1 preempt
standby 1 ip 172.16.10.110
```

Assigned Preempt
Standby Group Number

```
Switch(config-if)#standby 1 preempt
```



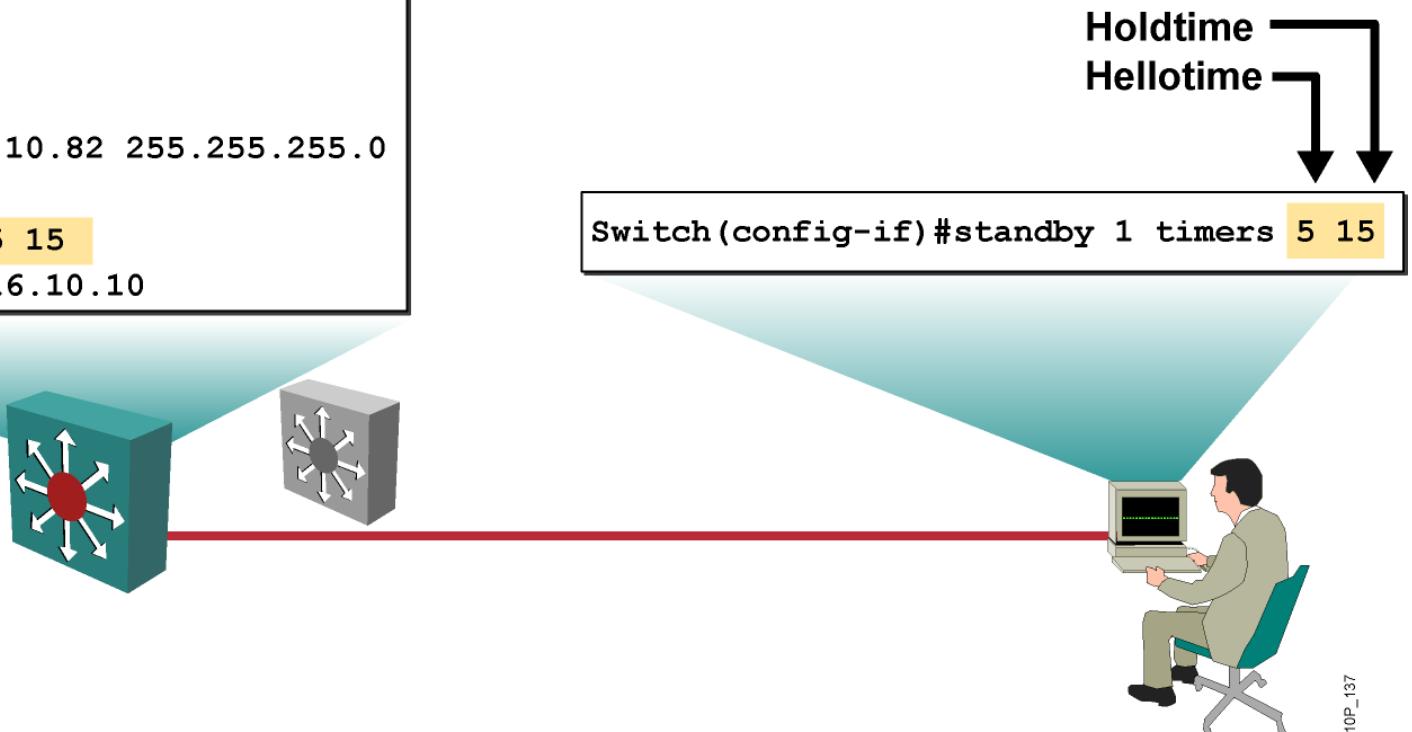
La préemption permet au routeur actif de reprendre la main lorsqu'il reprend du service

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
```

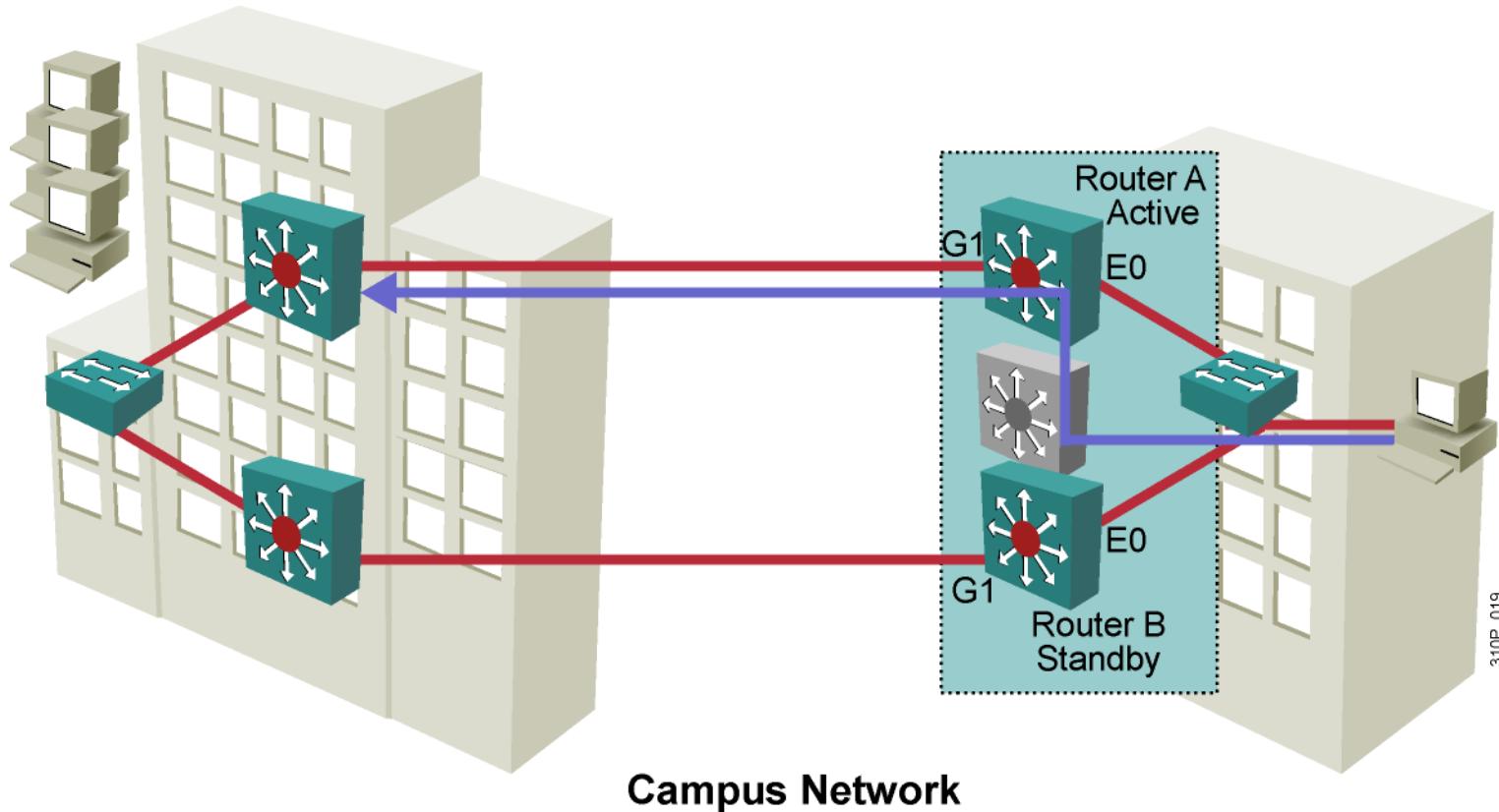


```
Switch(config-if)#standby 1 timers 5 15
```

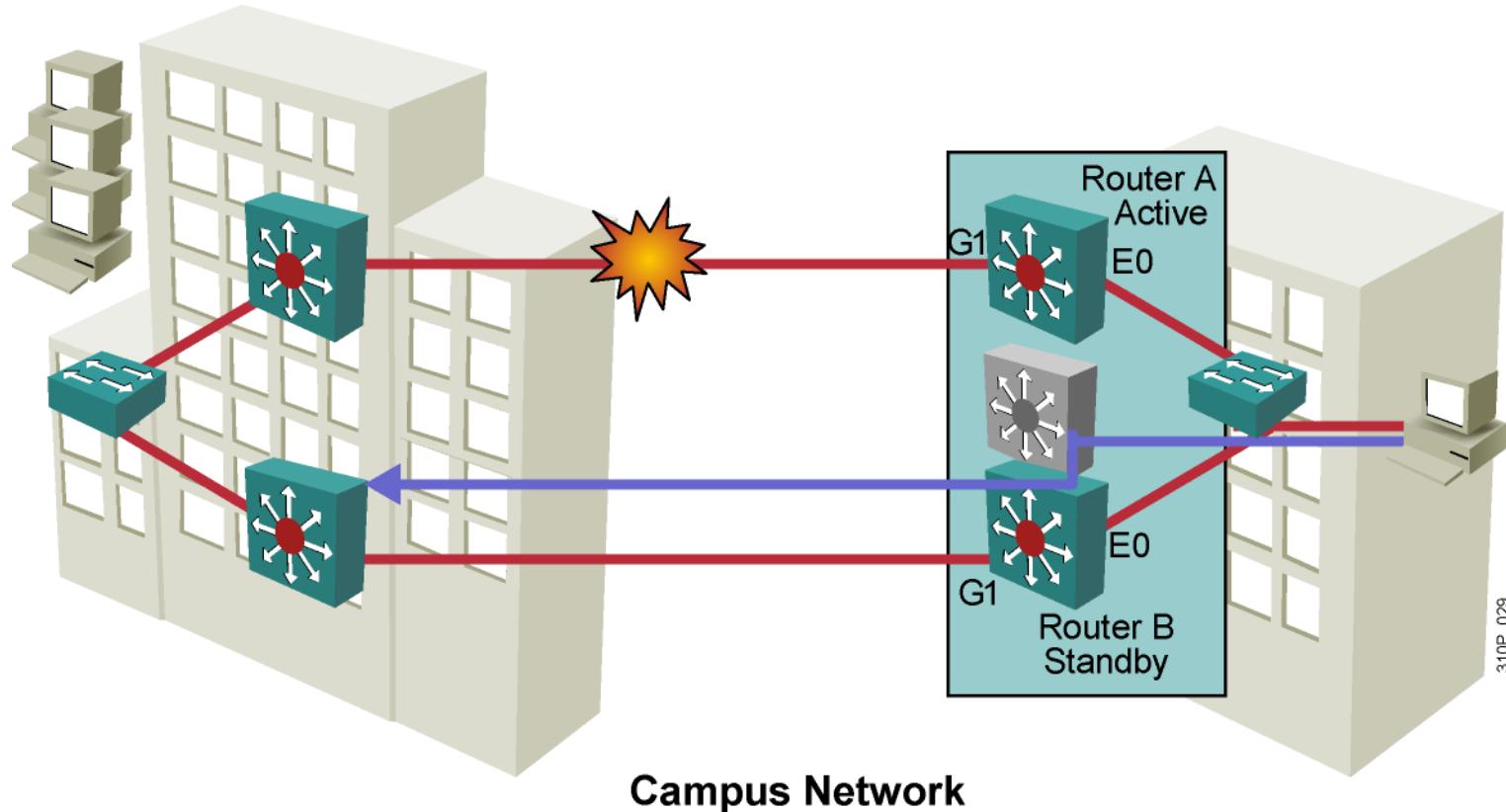
310P_137

Le Holdtime doit être supérieur à 3 fois le Hello

Supervision du lien



Un lien tombe et le trafic bascule



310P_029

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

ACL

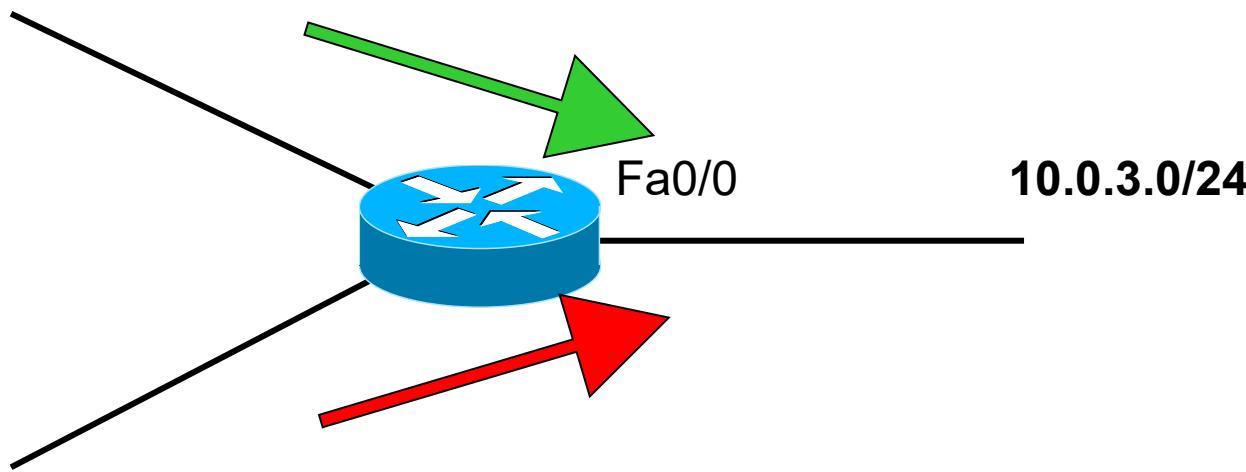
Access-List

Objectif

10.0.1.0/24

10.0.2.0/24

10.0.3.0/24

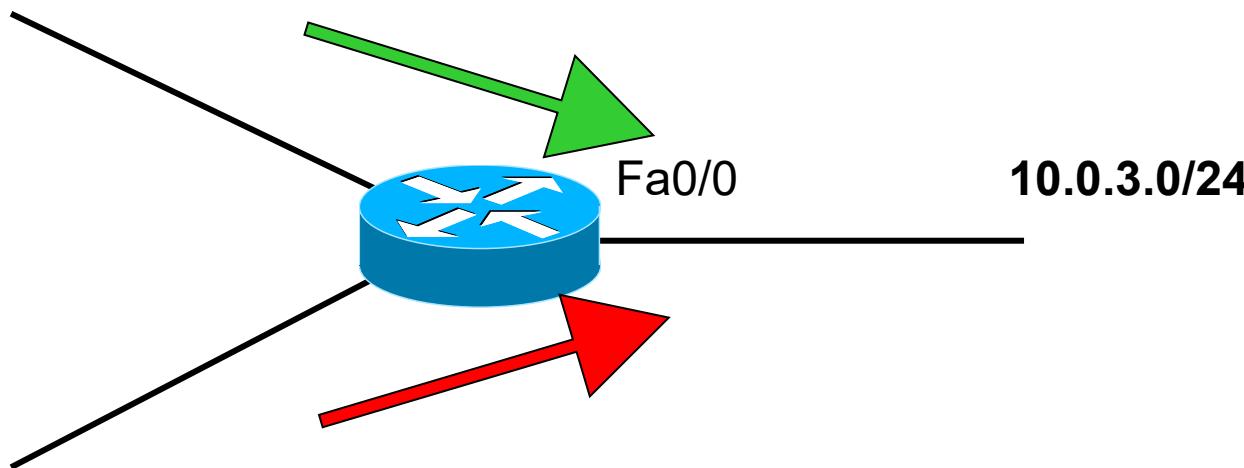


Objectif

10.0.1.0/24

10.0.2.0/24

10.0.3.0/24



- 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 adresse :

- 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'adresse :

- Exemple : autoriser toute address
- access-list 1 permit 0.0.0.0 **255.255.255.255**
- access-list 1 permit **any**

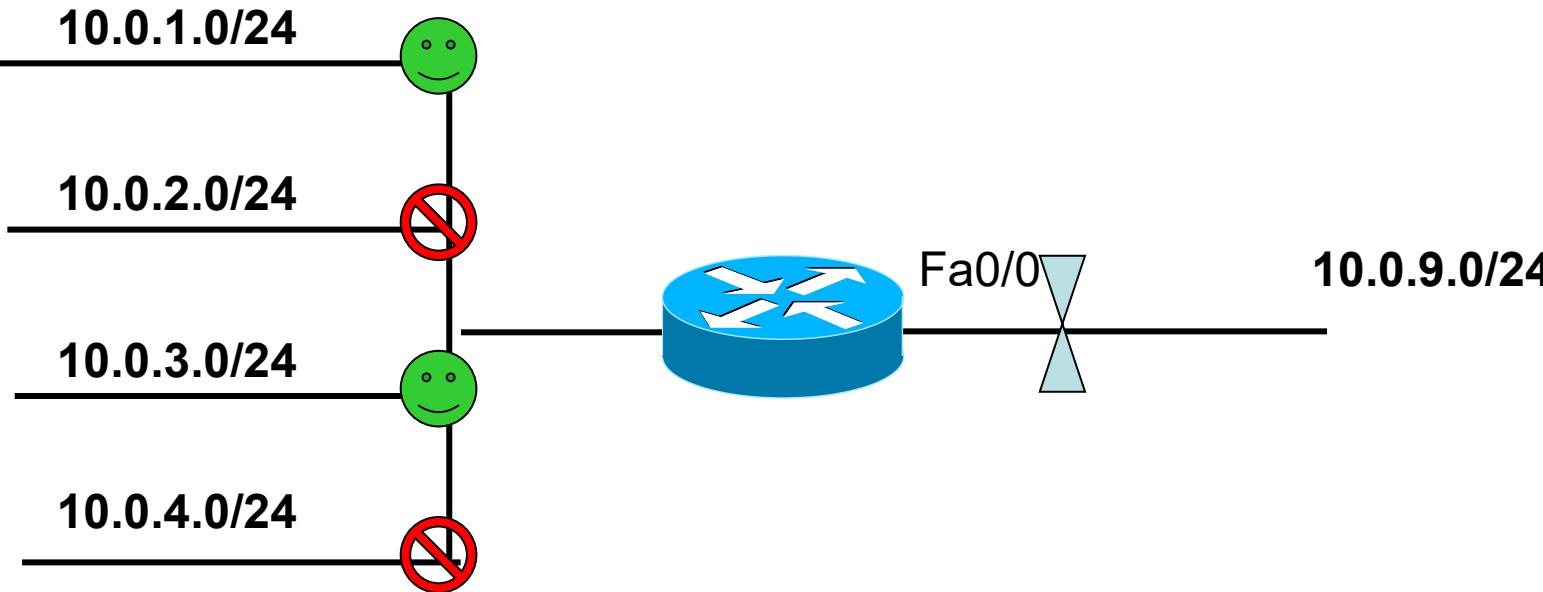
Dernière ligne implicite

- 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

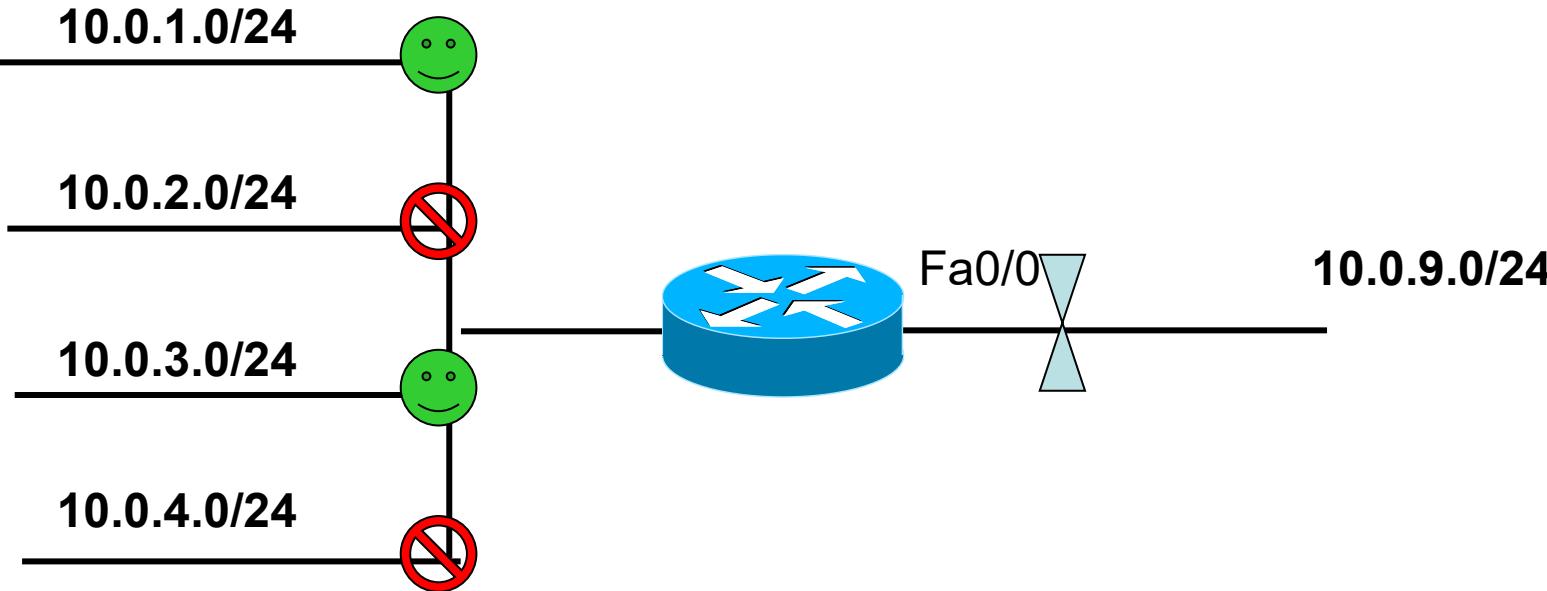
deny any (implicite, non écrit)

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

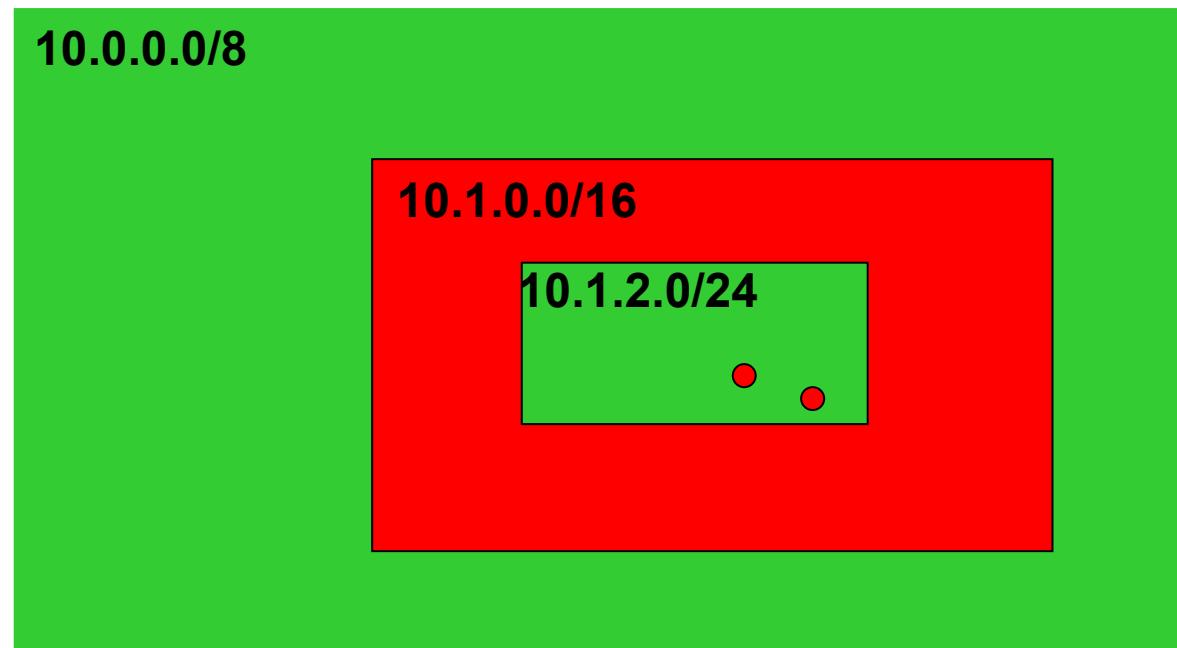
Exemple 1 Optimisation



- 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
- 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

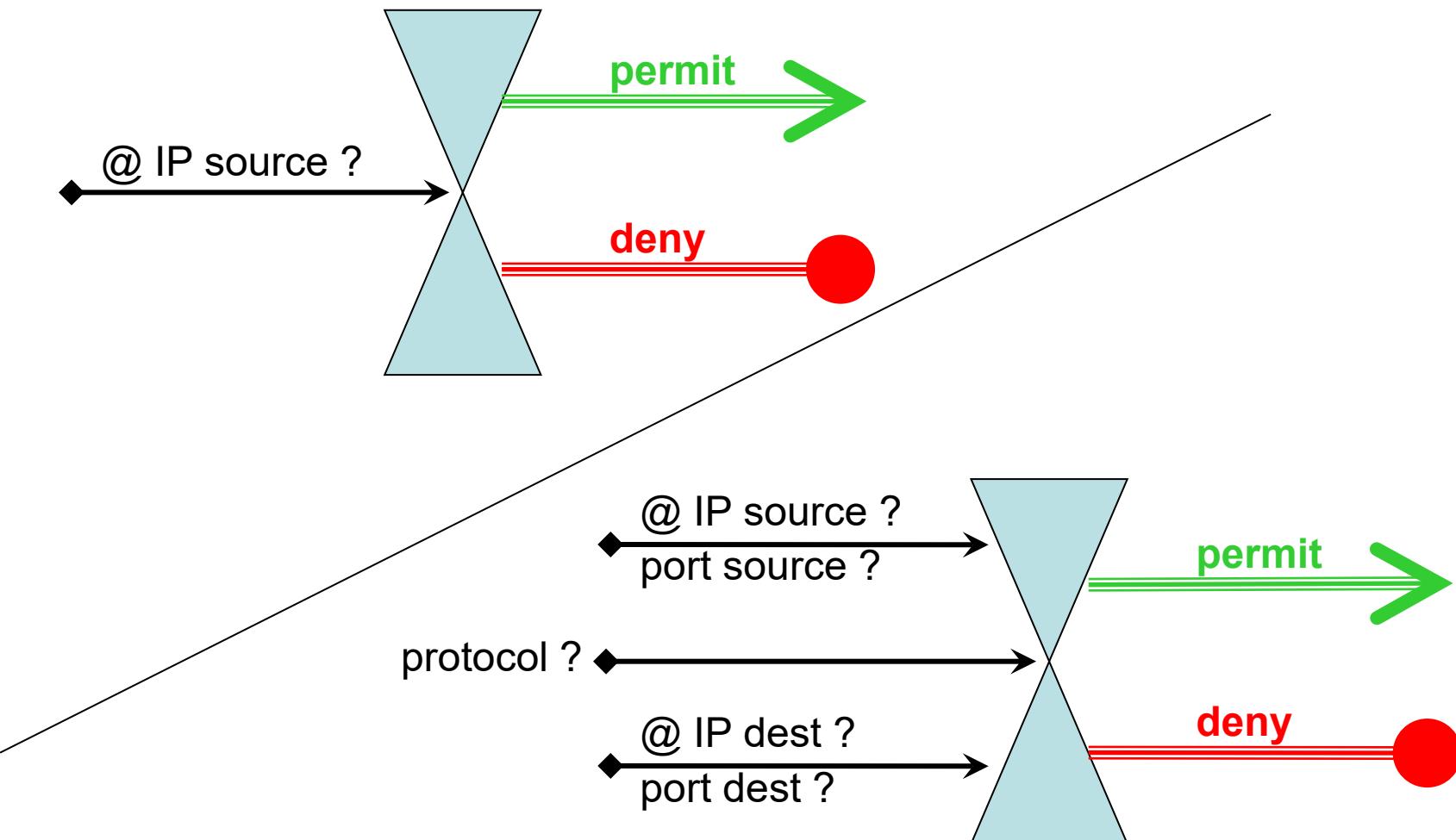
- Vérifier les ACL configurées :
 - Show access-lists

- Vérifier où sont appliquées les ACL :
 - Show ip interface

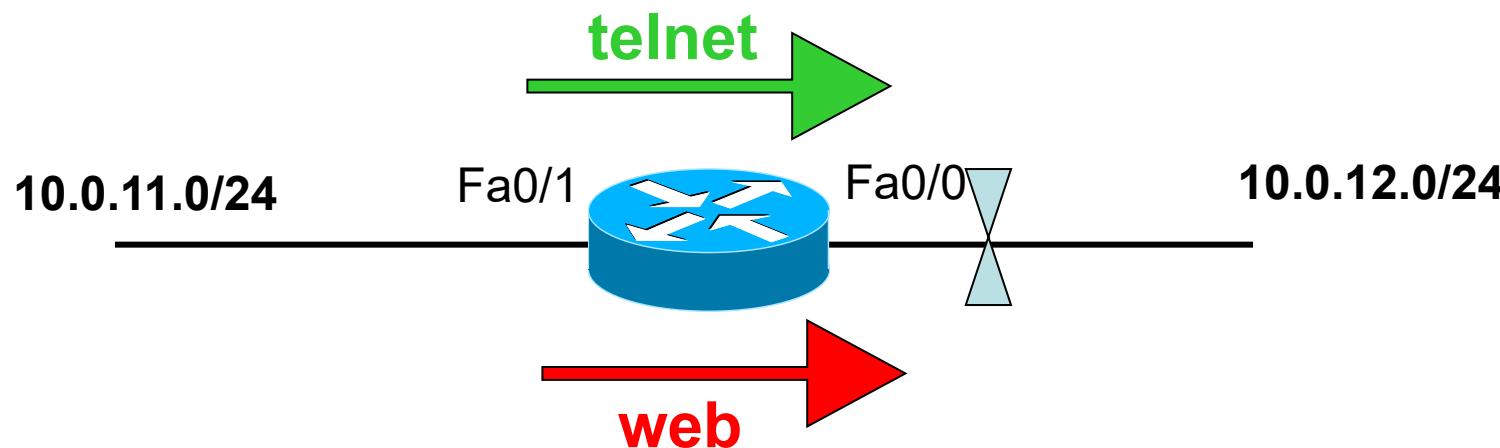
ACL étendues

- 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

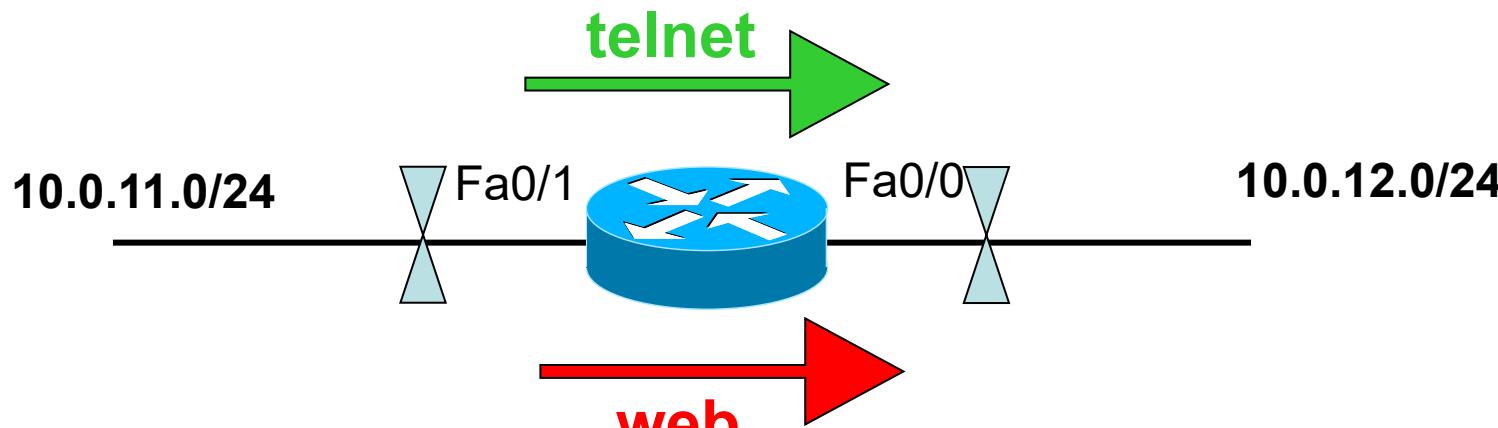


Utilité d'une ACL étendue



- 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	Identifiant	permit ou deny	Protocole	@ 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 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

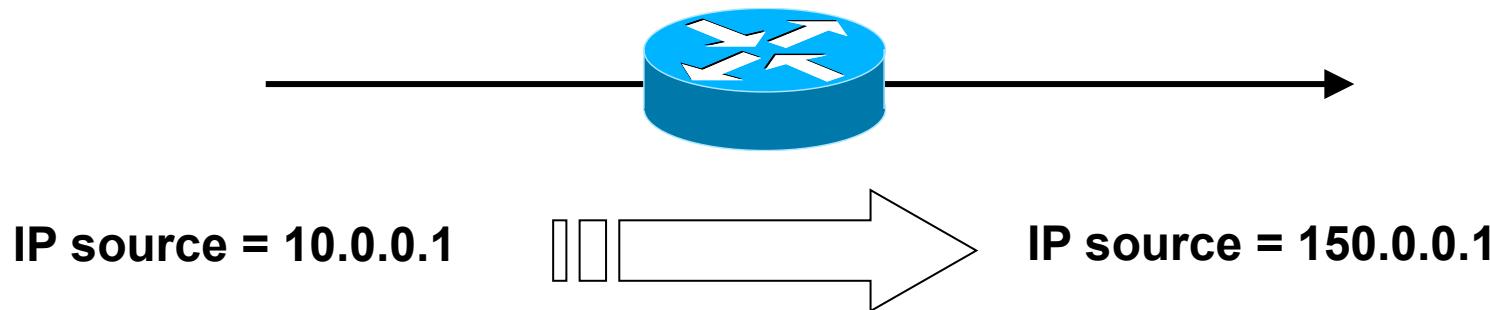
Solution

- 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



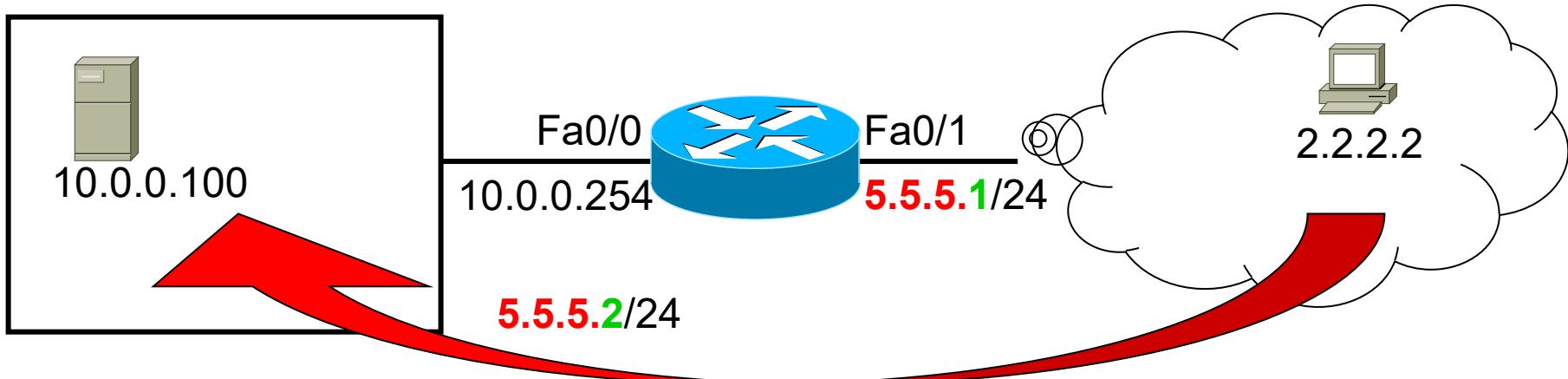
- Le routeur a modifié l'@ IP source du paquet avant de le transmettre.

Quel peut être l'intérêt ?

Quatre possibilités

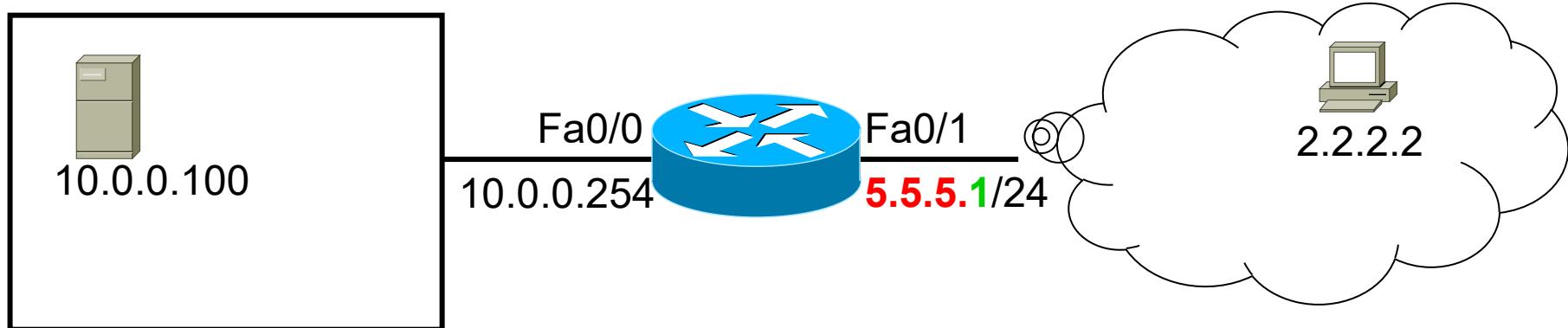
- NAT Statique
- PAT Statique
- NAT Dynamique
- PAT Dynamique

NAT Statique



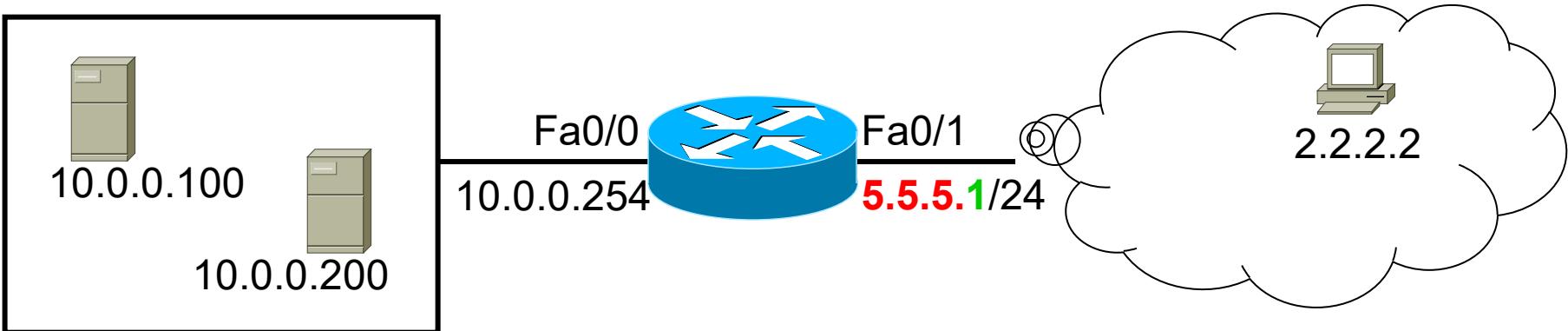
- Objectif :
 - permettre aux clients d'accéder à mon serveur web
- Problème :
 - 10.0.0.100 est interdit sur internet
- Solution :
 1. prétendre que mon serveur web est accessible sur **5.5.5.2**
 2. translater 5.5.5.2 en 10.0.0.100

NAT Statique



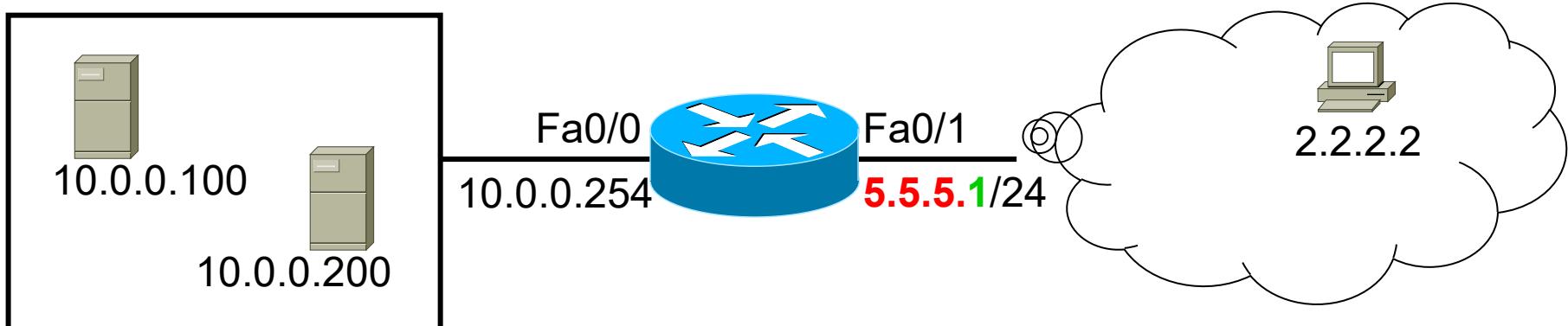
- conf t
- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- ip nat inside source static 10.0.0.100 5.5.5.2

NAT Statique

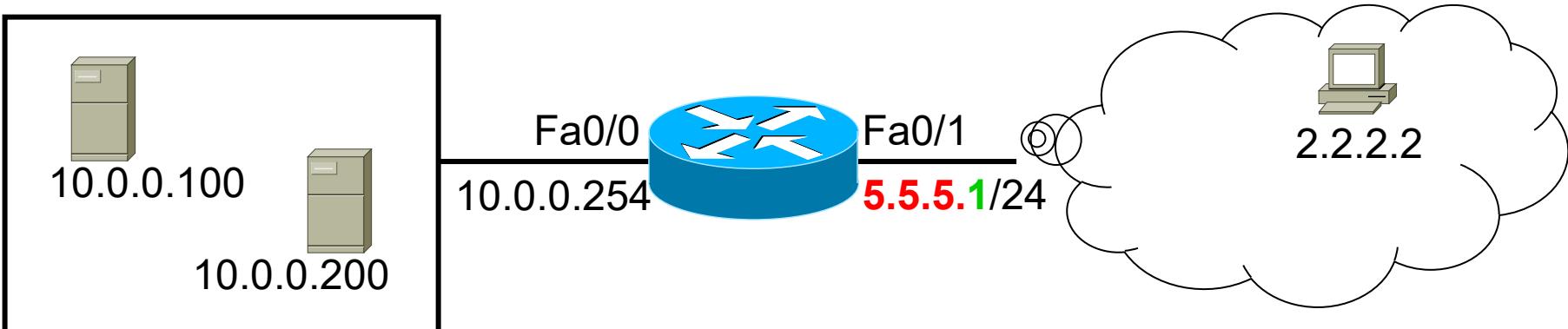


- Objectif :
 - permettre aux clients d'accéder à mes 2 serveurs (web, smtp)
- Solution n° 1:
 - prétendre que mon serveur web est accessible sur 5.5.5.2 + translater 5.5.5.2 en 10.0.0.100
 - prétendre que mon serveur smtp est accessible sur 5.5.5.3 + translater 5.5.5.3 en 10.0.0.200

NAT Statique

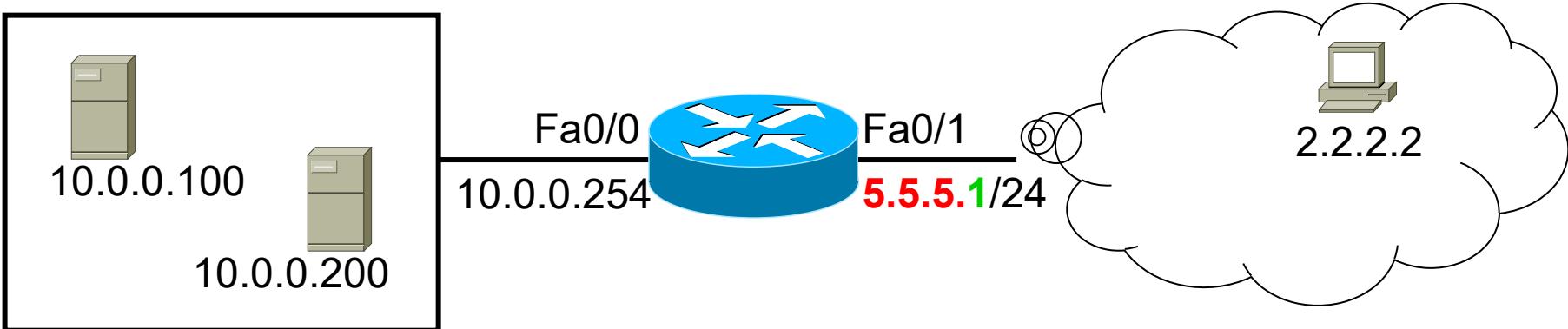


- conf t
- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- ip nat inside source static 10.0.0.100 5.5.5.2
- ip nat inside source static 10.0.0.200 5.5.5.3



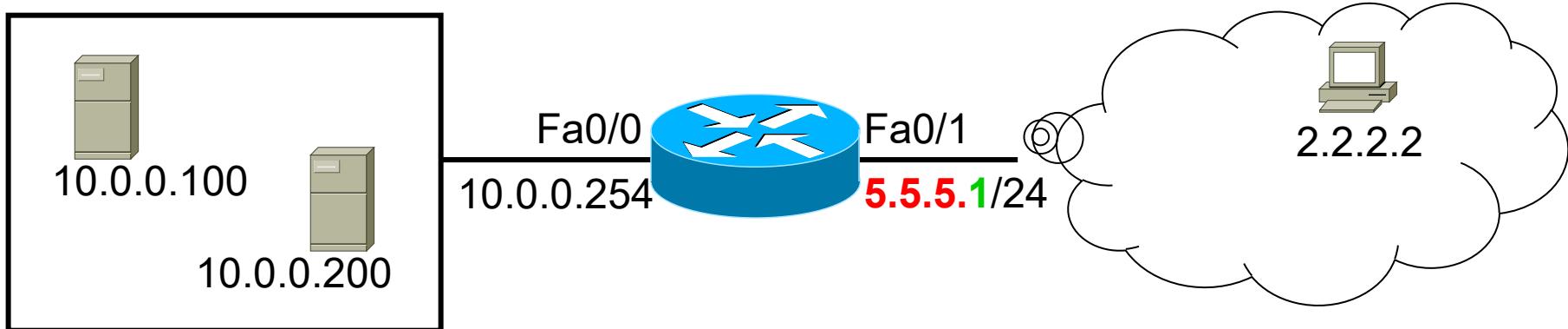
- Objectif :
 - permettre aux clients d'accéder à mes 2 serveurs web
 - utiliser **une seule adresse publique** pour accéder aux 2 serveurs
- Solution n° 2:
 - prétendre que mon serveur web est accessible sur **le port 80** de **5.5.5.2** + translater **5.5.5.2** en **10.0.0.100**
 - prétendre que mon 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



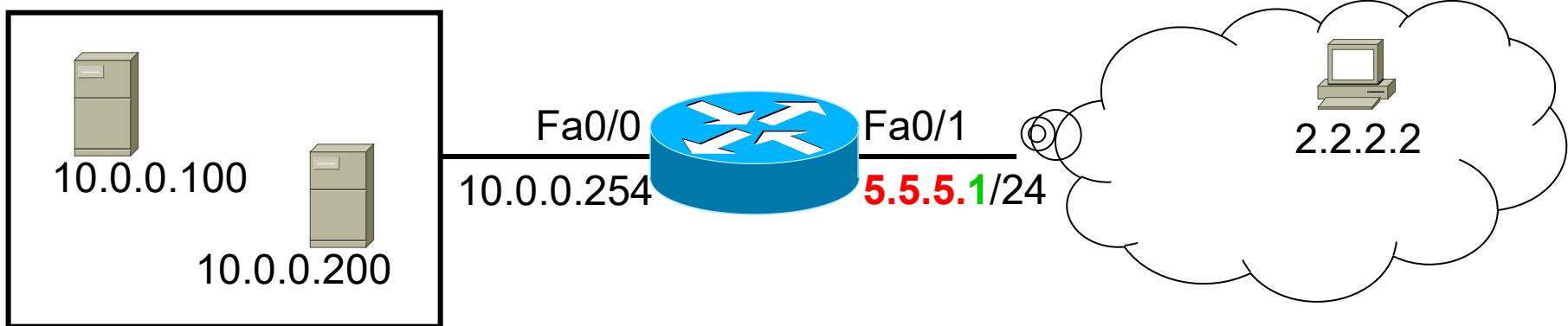
- Objectif WEB1 :
 - mon serveur web en 10.0.0.100 répond sur le port **80**
 - les clients doivent attaquer mon serveur web en allant sur 5.5.5.2 port **80**.
- Objectif WEB2:
 - mon serveur smtp 10.0.0.200 répond sur le port **80**
 - les clients doivent attaquer mon serveur smtp en allant sur 5.5.5.2 port **8080**.

PAT Statique



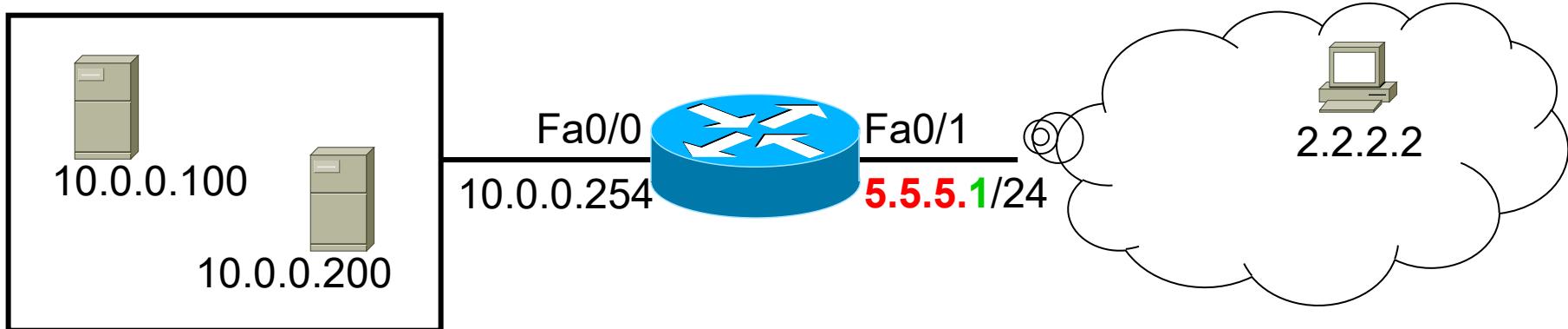
- conf t
- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- ip nat inside source static **tcp** 10.0.0.100 **80** 5.5.5.2 **80**
- ip nat inside source static **tcp** 10.0.0.200 **80** 5.5.5.2 **8080**

Exercice



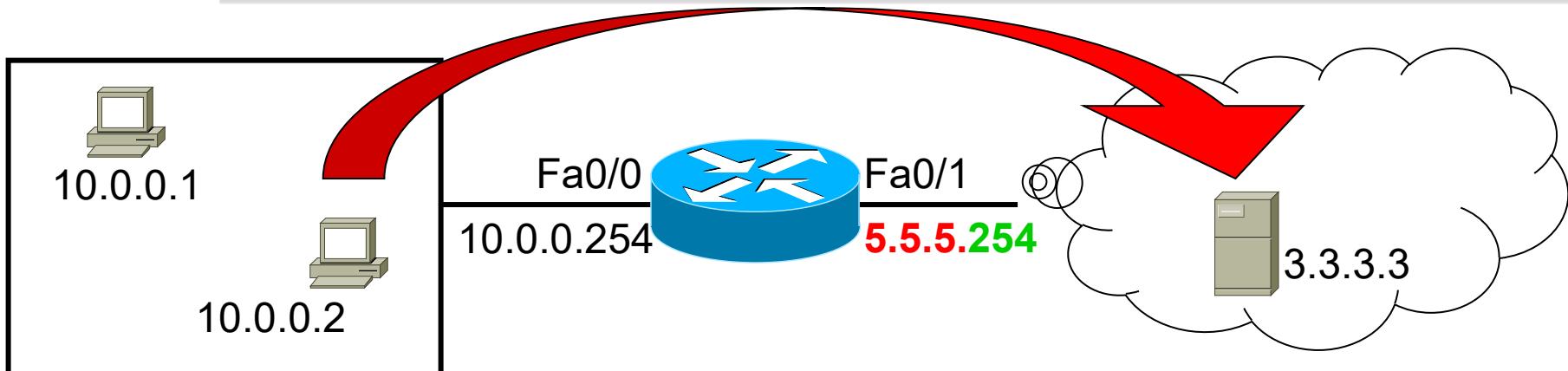
- Objectif WEB :
 - mon serveur web en 10.0.0.100 répond sur le port **80**
 - les clients doivent attaquer mon serveur web en allant sur 5.5.5.2 port **8080**.
- Objectif WEB2:
 - mon serveur telnet 10.0.0.200 répond sur le port **80**
 - les clients doivent attaquer mon serveur telnet en allant sur 5.5.5.2 port **8081**.

Solution



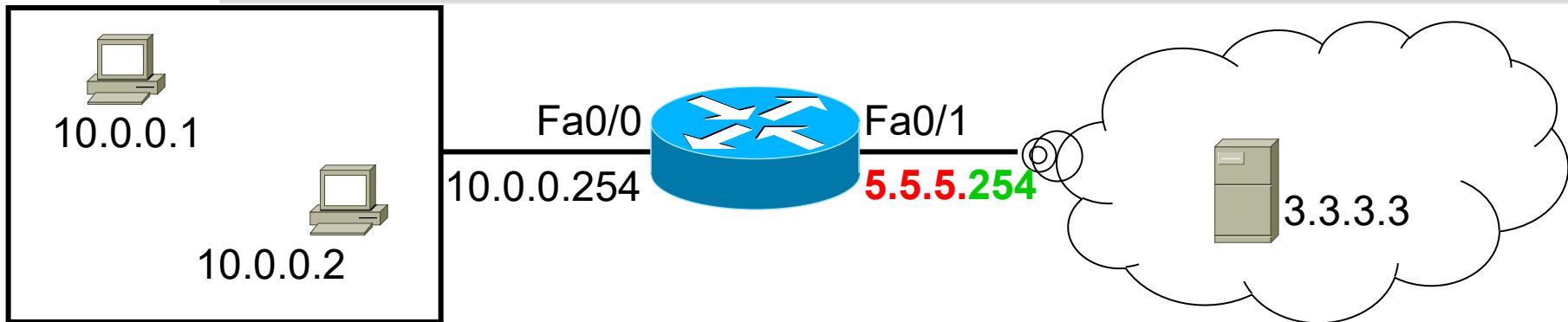
- conf t
- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- ip nat inside source static tcp 10.0.0.100 **80** 5.5.5.2 **8080**
- ip nat inside source static tcp 10.0.0.200 **80** 5.5.5.2 **8081**

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



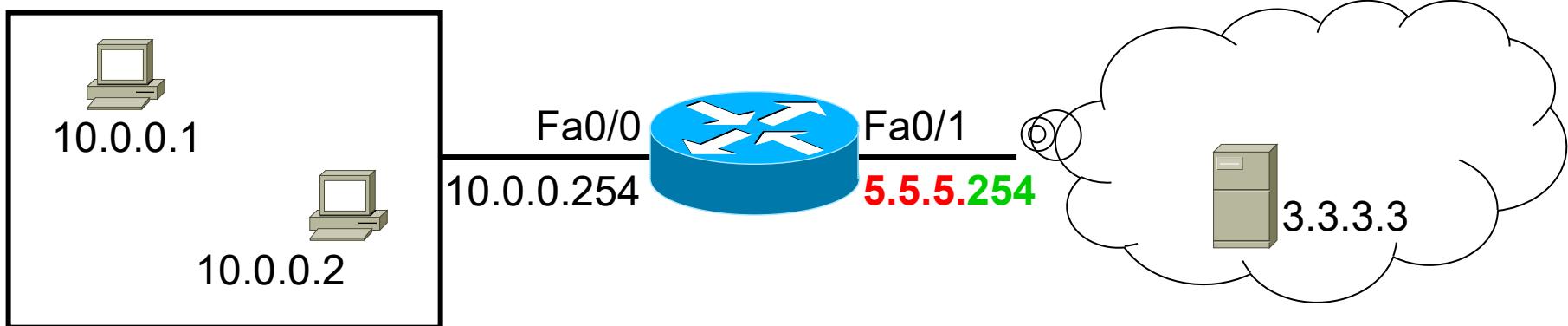
- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- ip nat pool TOTO 5.5.5.1 5.5.5.253 netmask 255.255.255.0
 - ce sont les adresses fictives qui seront attribuées aux adresses translatées
- access-list 1 permit 10.0.0.0 0.0.0.255
 - ce sont les adresses qui seront translatées
- ip nat inside 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

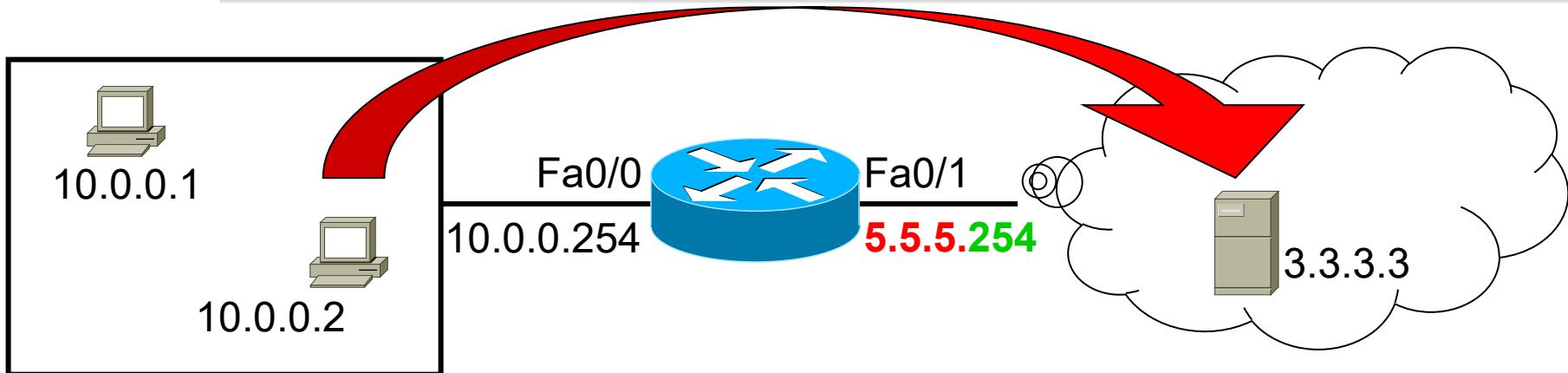


- int fa0/0
 - ip nat inside
- int fa0/1
 - ip nat outside
- access-list 1 permit 10.0.0.0 0.0.0.255
 - ce sont les adresses qui seront traduites
- ip nat inside source list 1 interface fa0/1 **overload**
 - toutes les adresses nattées se verront attribuées l'adresse IP de l'interface fa0/1 i.e. 5.5.5.254

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 traduit en 5.5.5.1
- 10.0.0.2 est traduit en 5.5.5.2

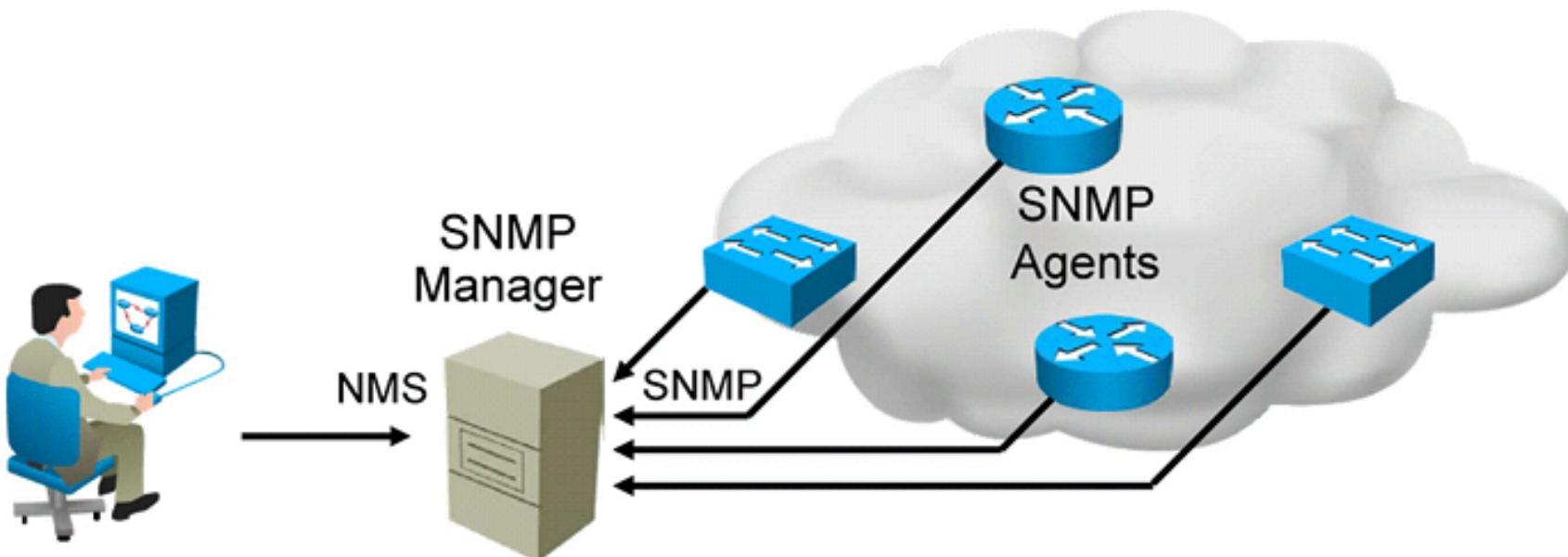
Inside Global	Inside Local	Outside Local	Outside Global
5.5.5.1	10.0.0.1	3.3.3.3	3.3.3.3
5.5.5.2	10.0.0.2	3.3.3.3	3.3.3.3

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

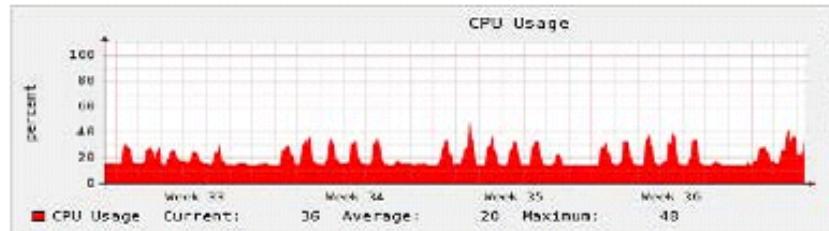
SNMP Version	Security	Bulk Retrieval Mechanism
SNMPv1	Plaintext authentication with community strings	No
SNMPv2c	Plaintext authentication with community strings	Yes
SNMPv3	Strong authentication, confidentiality, and integrity	Yes

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

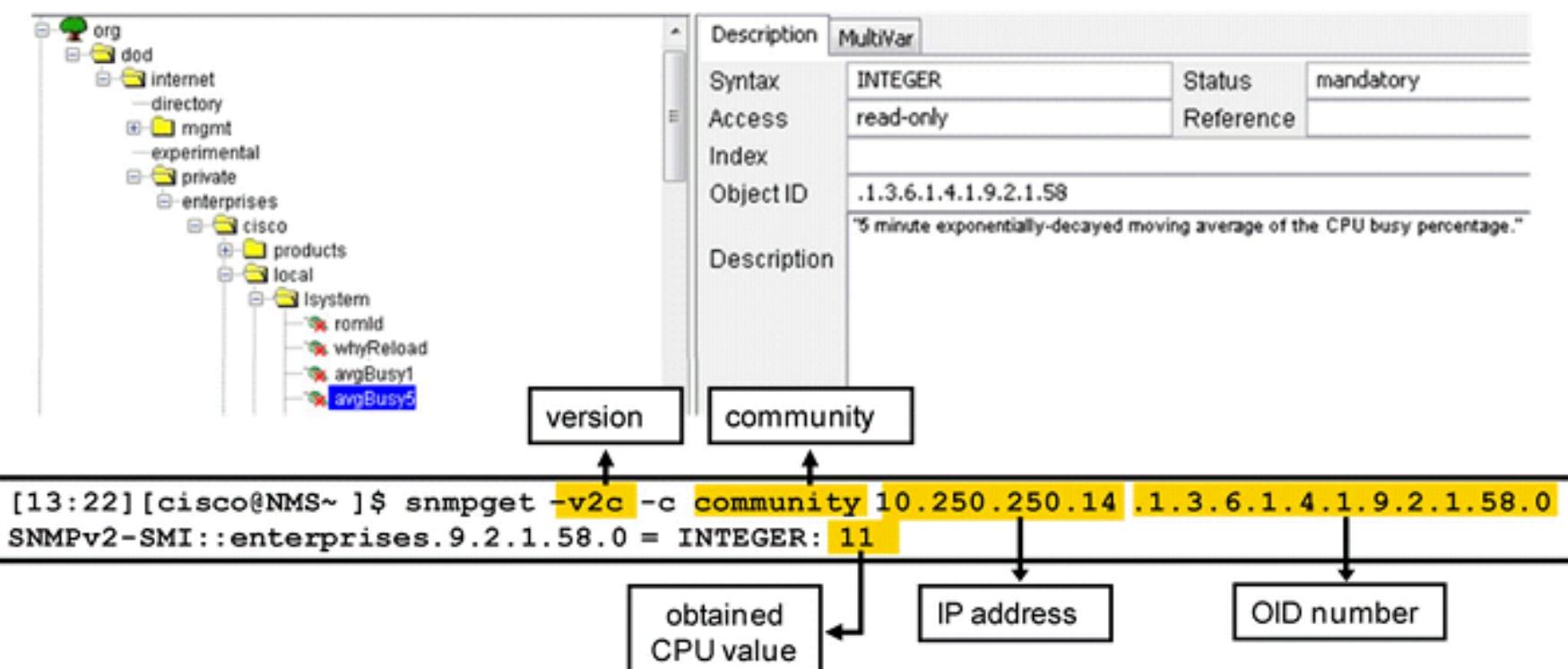
Obtaining Data from an SNMP Agent

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

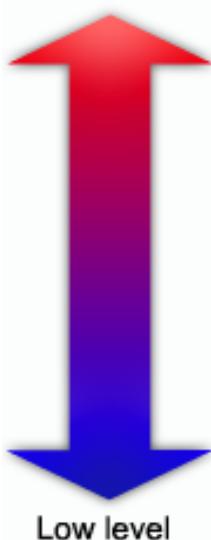
Syslog

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严重性

High level



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*]

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 mssec
 - E. logging host 10.2.0.21
-
- Réponse : D

NetFlow

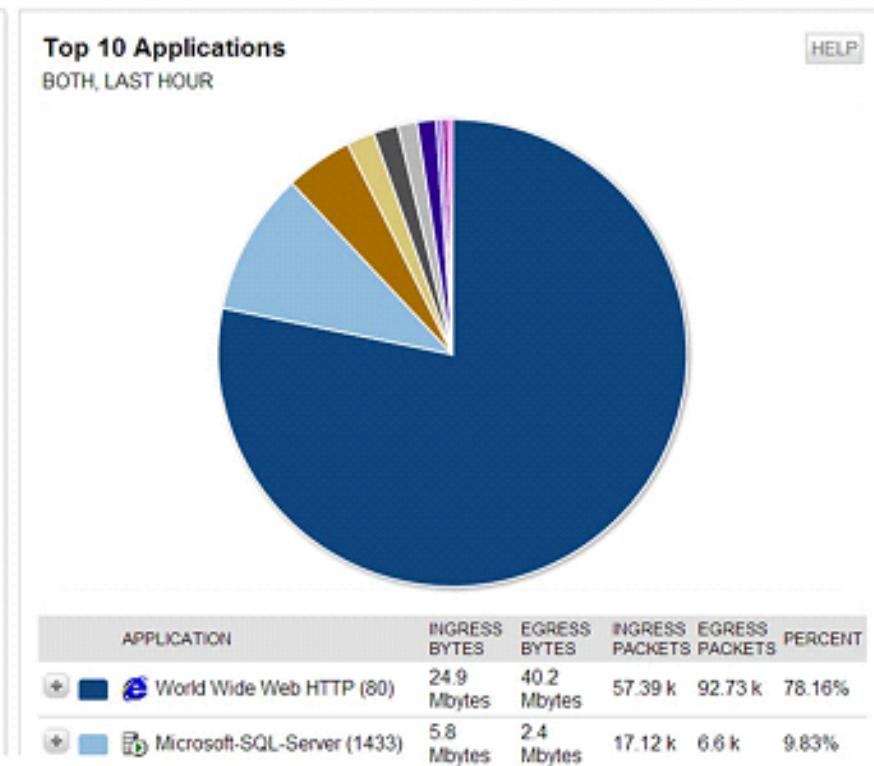
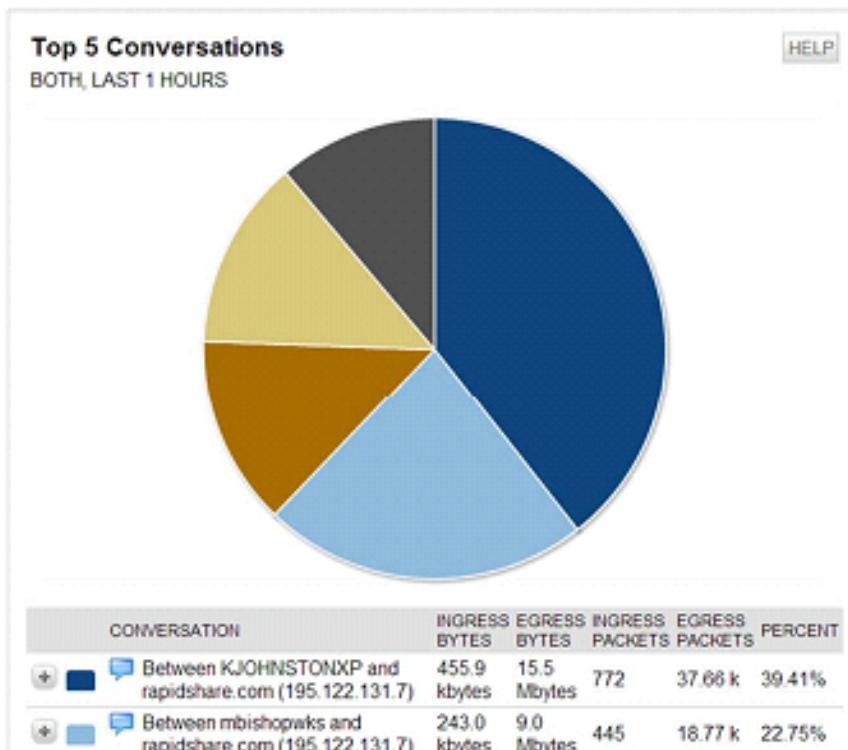
NetFlow Overview

- 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:

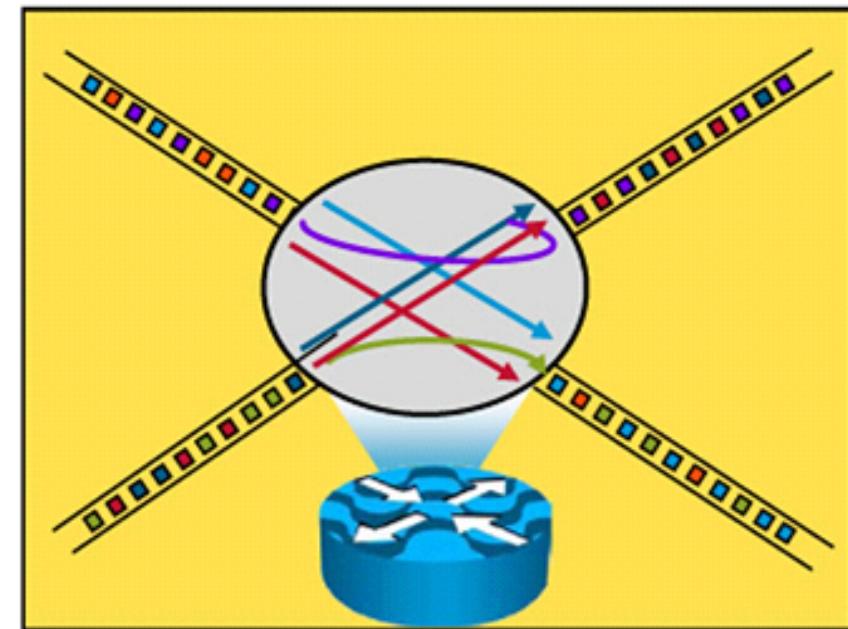
- Shows the top talkers, top listeners, top protocols, and more.



NetFlow Overview (Cont.)

Cisco defines a flow as a unidirectional sequence of packets with seven common values:

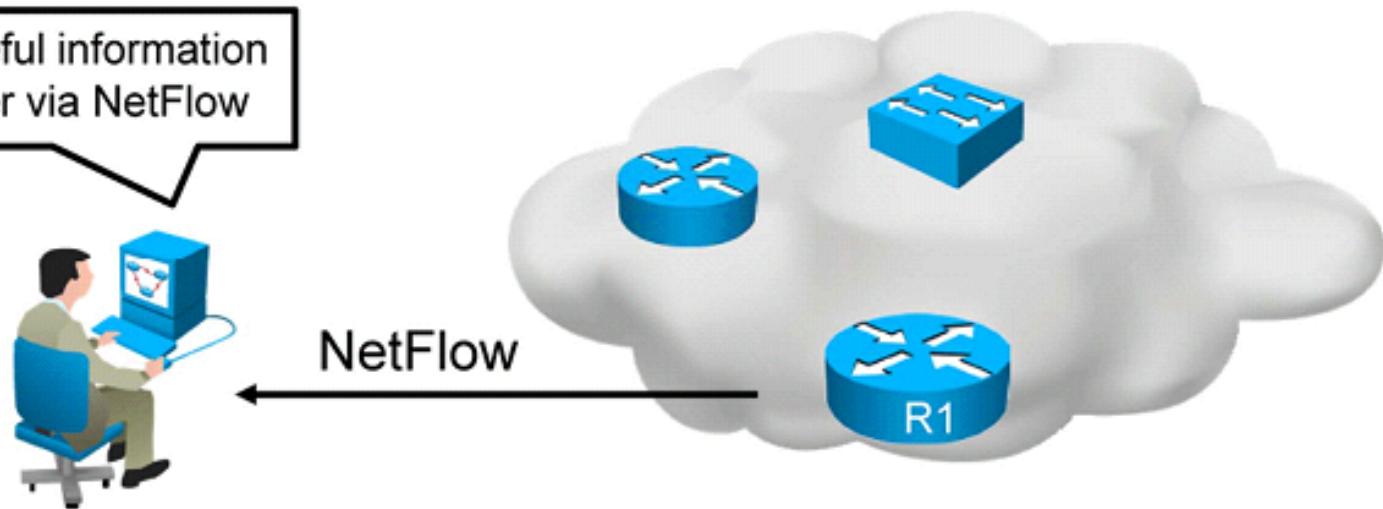
- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- ToS
- Input logical interface



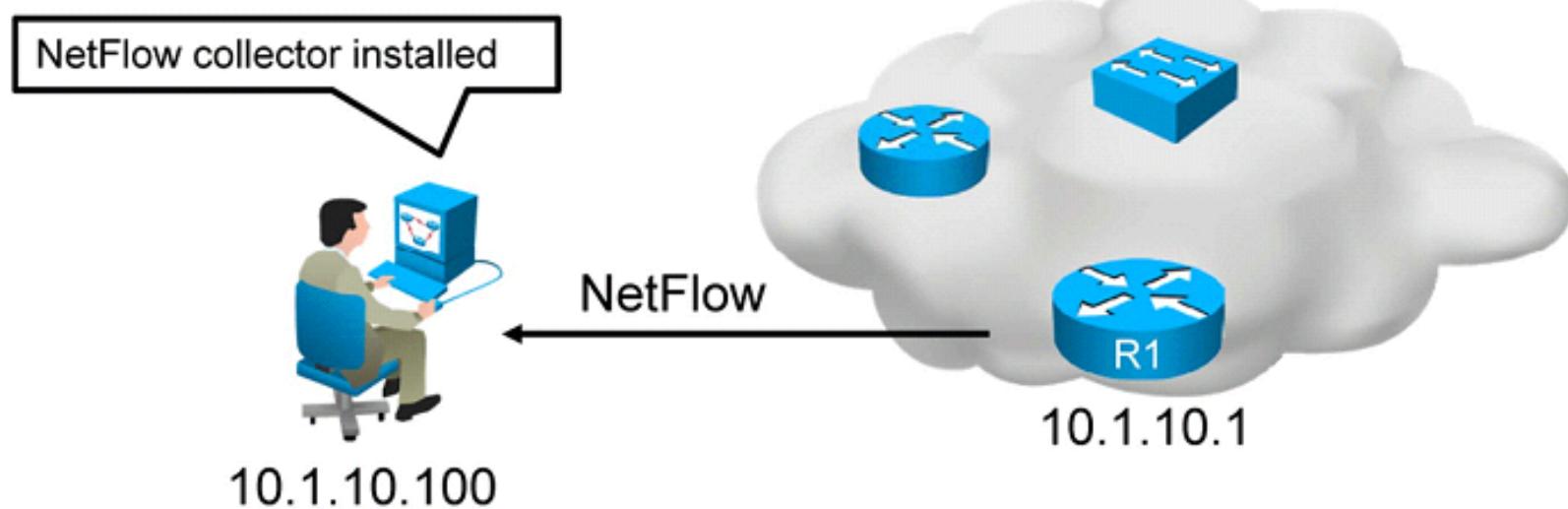
NetFlow Configuration

- Configure NetFlow data capture
- Configure NetFlow data export
- Configure NetFlow data export version
- Verify NetFlow, its operation, and statistics

Get some useful information from the router via NetFlow



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

CCNA

SWITCHING & ROUTING

2ème semaine

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
3. **Routage :**
 - Subnetting, statique, dynamique, DV, LS, RIP

Seconde
semaine

4. **Sécurité & administration :**
 - ACL, NAT, SNMP, Logging, NetFlow
5. **Routage : OSPF & EIGRP**
6. **IPv6 : adressage & routage**
7. **Etherchannels & FHRP (HSRP)**
8. **Architectures LAN et WAN (VPN)**
9. **Réseaux intelligents**
10. **Divers:**
 - Wi-Fi, QoS,

ROUTAGE

La Table de Routage

Introduction

Contenu de la table de routage

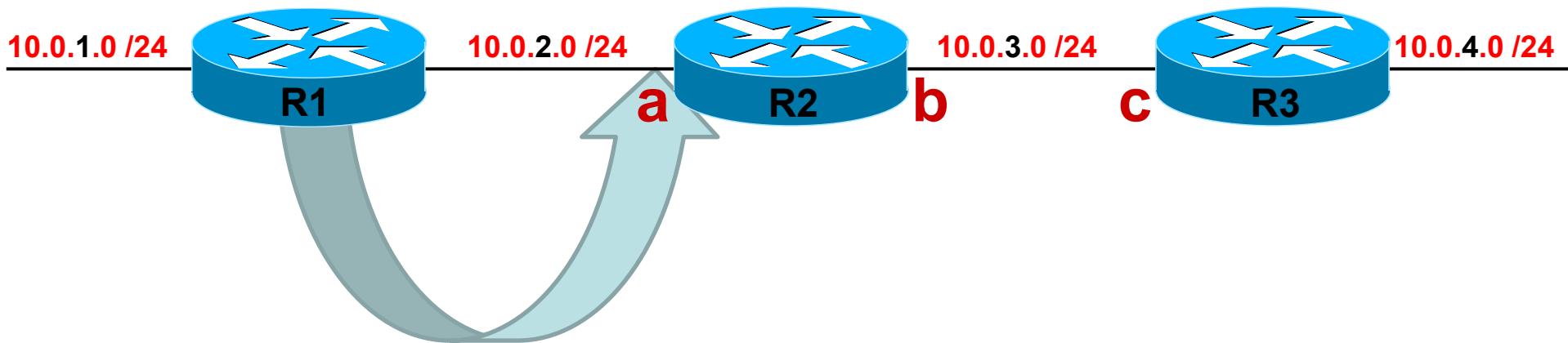
La table de routage indique **comment** acheminer les paquets :

1. Le routeur examine le champ « Adresse IP destination ».
2. Puis il cherche cette adresse dans sa Table.
3. La Table lui indique :
 - **L'interface** de sortie à utiliser
 - **Le NEXT HOP** à utiliser.

Le Next HOP est l'adresse IP du prochain saut.

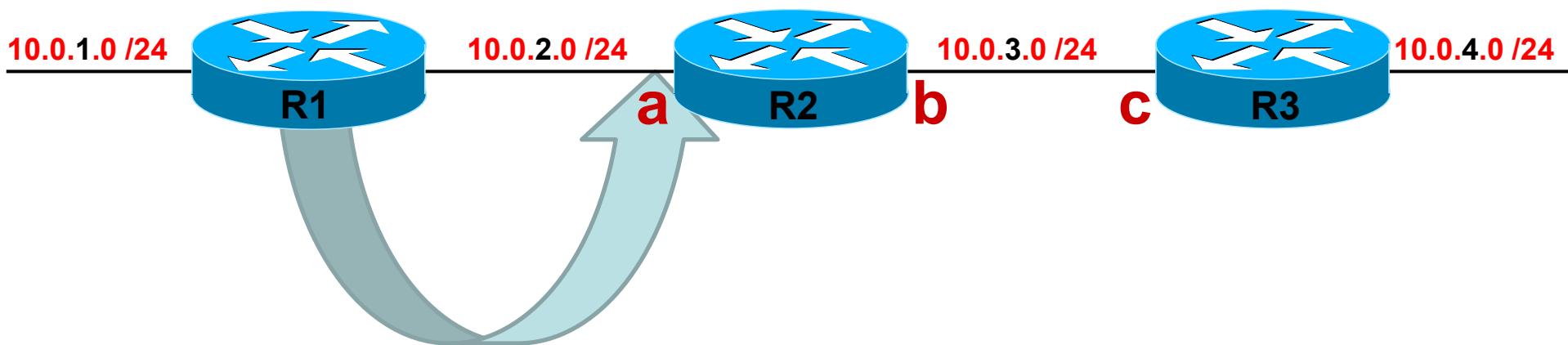
Le NEXT HOP : Exercice 1

Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.3.0 /24** ?

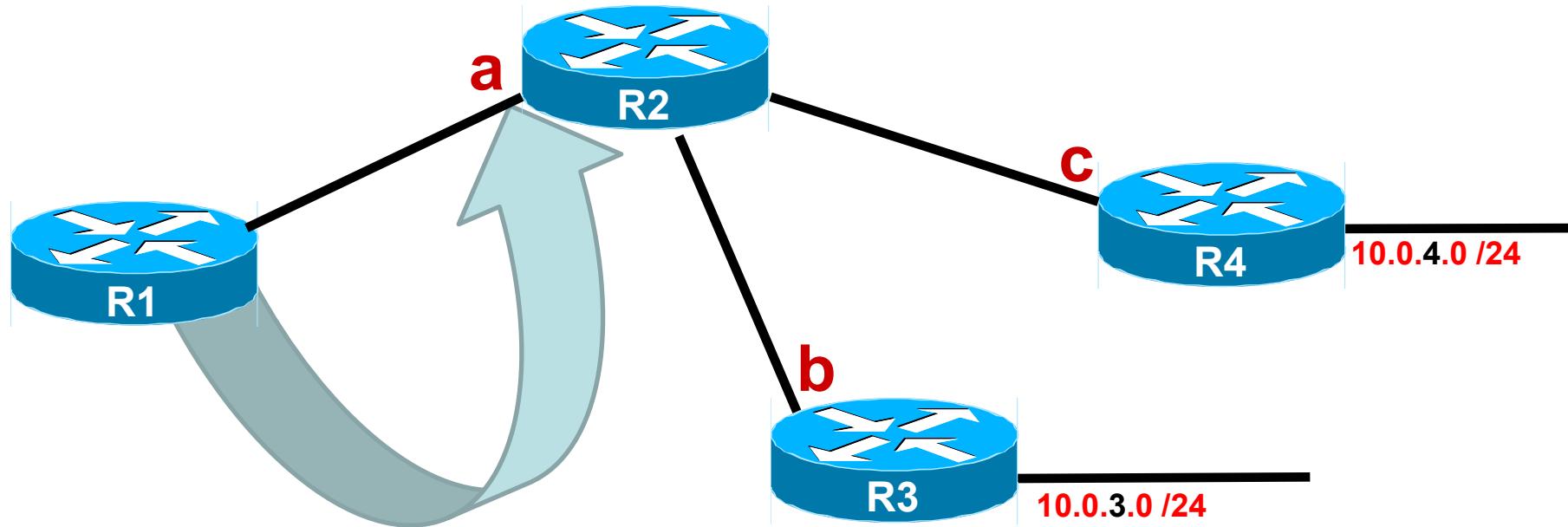


Le NEXT HOP : Exercice 2

Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.4.0 /24** ?

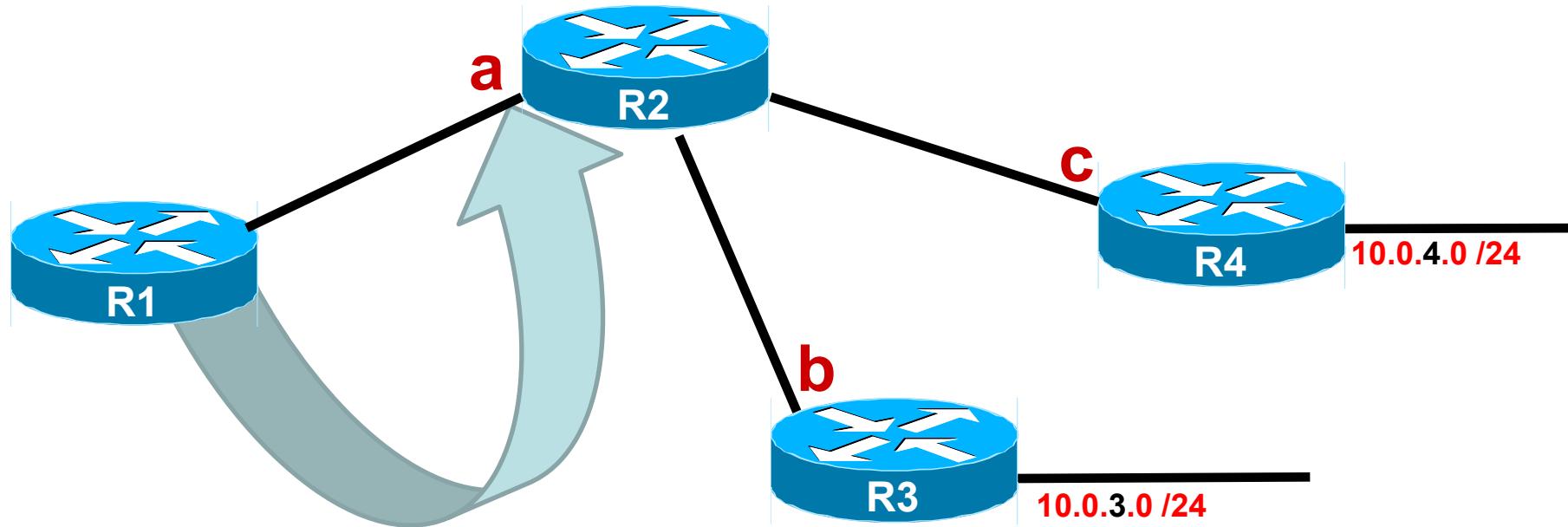


Le NEXT HOP : Exercice 3



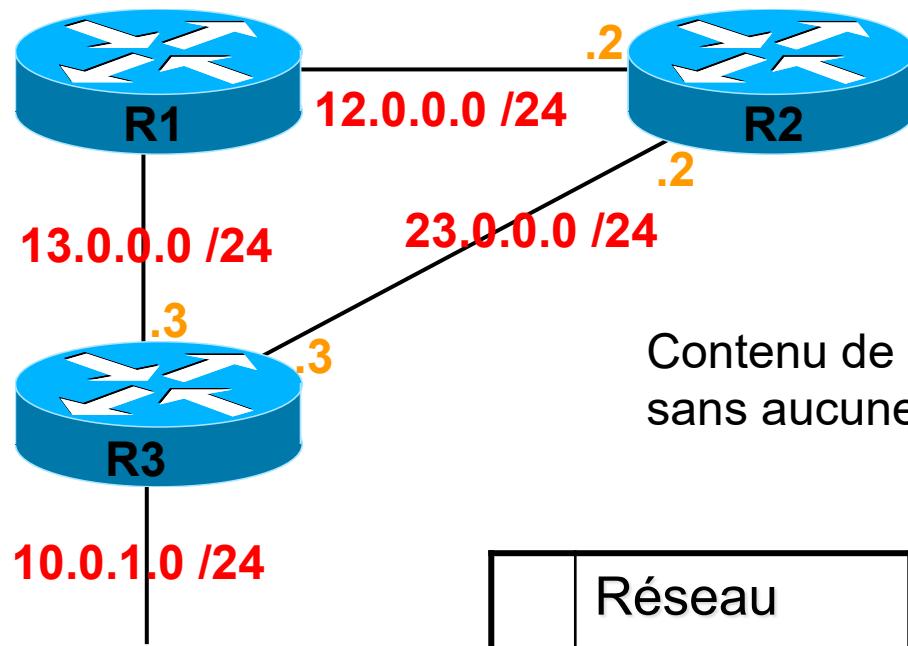
Quel NEXT HOP doit utiliser R1 pour joindre le réseau 10.0.3.0 /24 ?

Le NEXT HOP : Exercice 4



Quel NEXT HOP doit utiliser R1 pour joindre le réseau **10.0.4.0 /24** ?

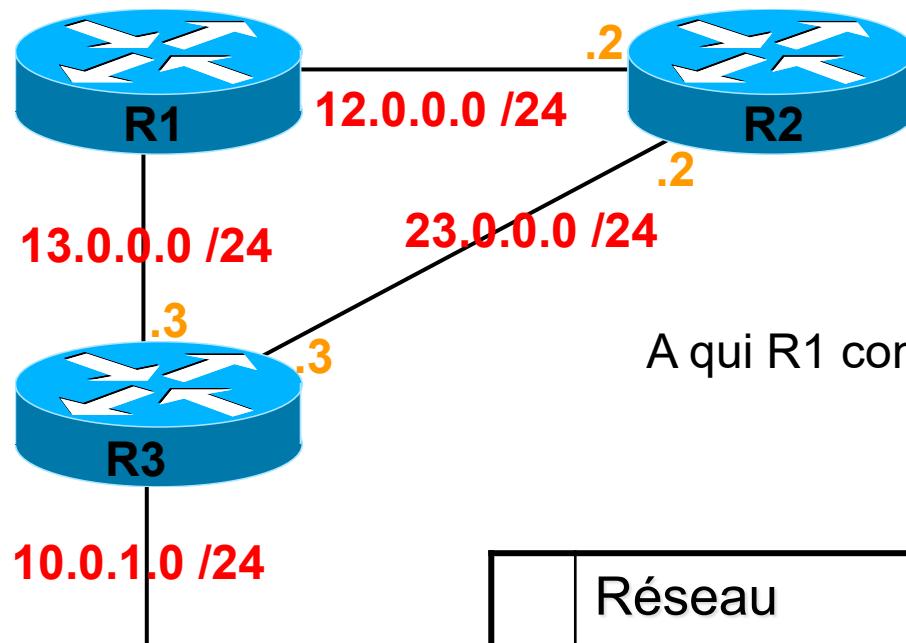
SHOW IP ROUTE



Contenu de la TABLE de ROUTAGE de R1
sans aucune route statique ni dynamique ;

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

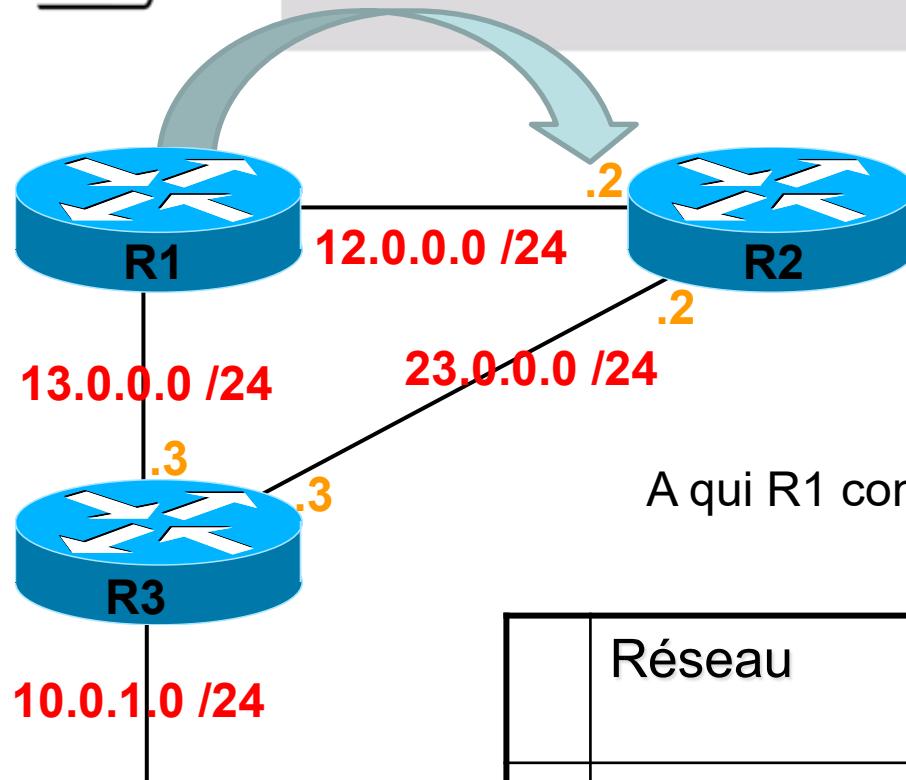
SHOW IP ROUTE : Exercice 1



A qui R1 confie les paquets à destination de 10.0.1.99 ?

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

SHOW IP ROUTE : Exercice 2



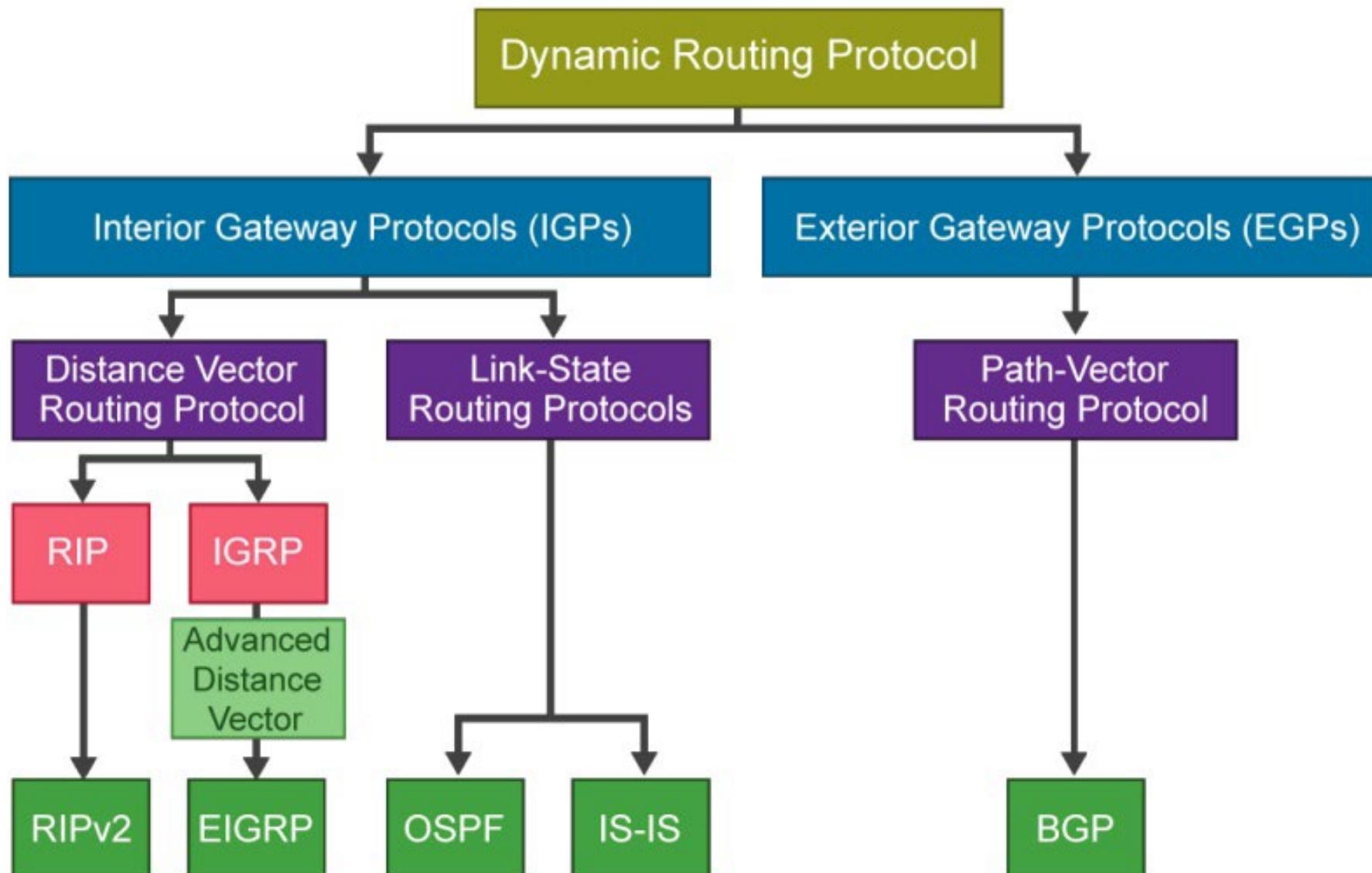
A qui R1 confie les paquets à destination de 10.0.1.99 ?

	Réseau	Masque	Next-Hop	Interface
C	12.0.0.0	/24		Fa0/2
C	13.0.0.0	/24		Fa0/0
O	10.0.1.0	/24	12.0.0.2	

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

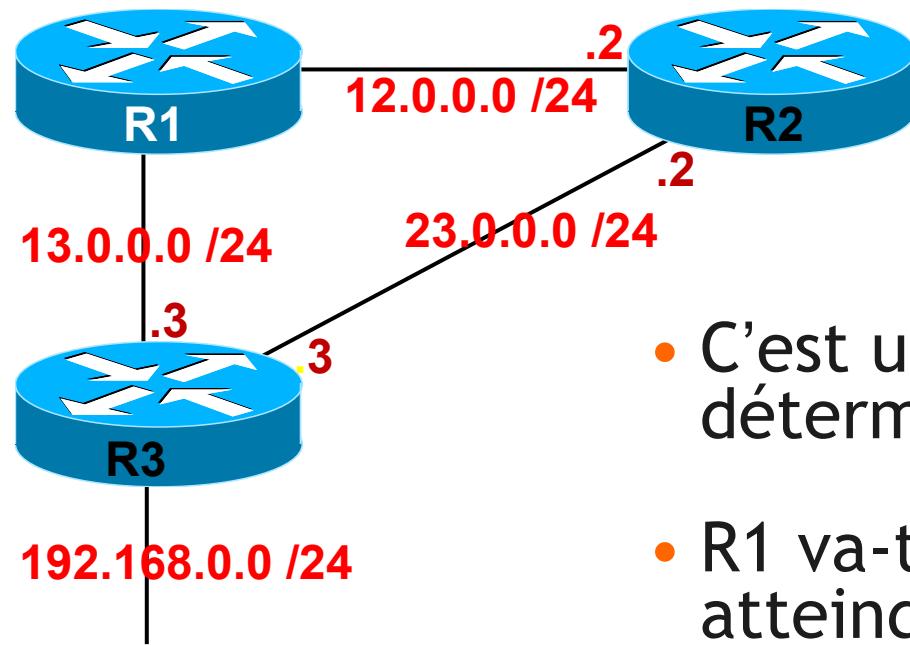
Distance Vector and Link-State Routing Protocols



2 types de protocoles de routage

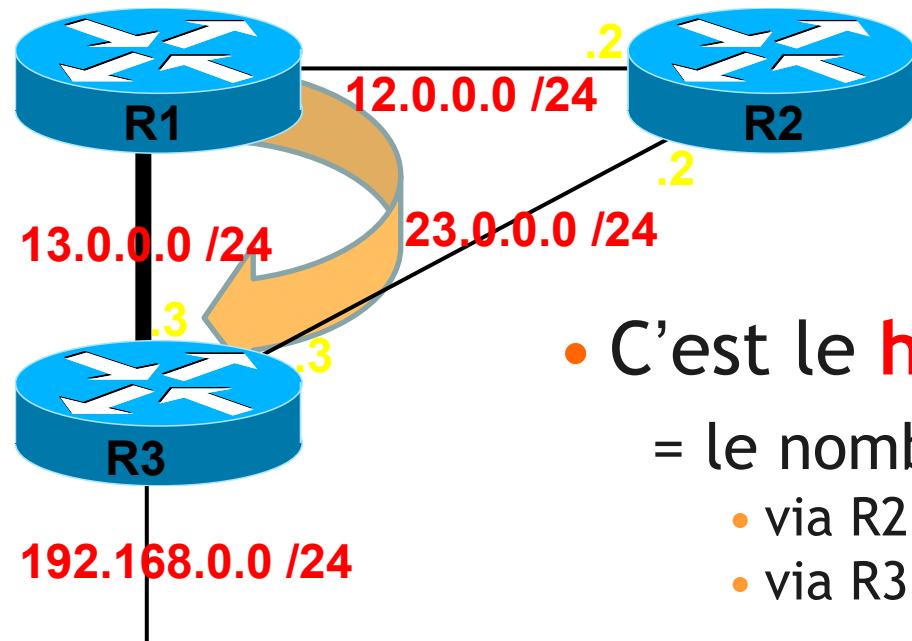
- Les protocoles à **vecteur de distance** :
 - Routage par « rumeur »
 - Le routeur envoie à son voisin une copie de sa table de routage.
 - Exemple : RIP (Routing Information Protocol)
- Les protocoles à **état de lien** :
 - Cartographie du réseau
 - Le routeur fait suivre à son voisin les informations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

La métrique



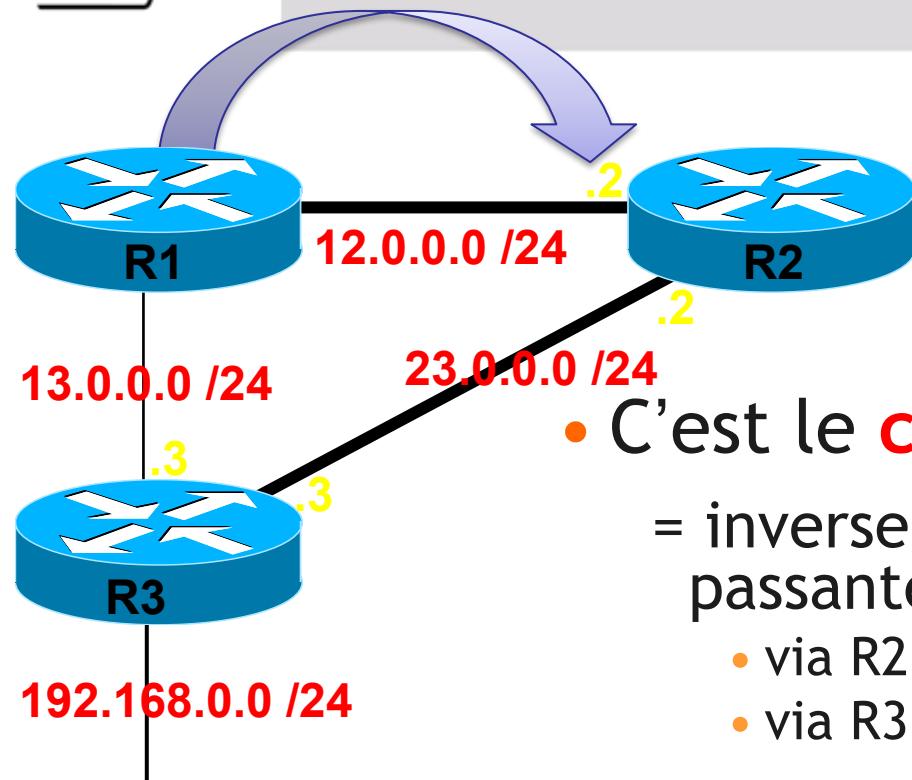
- C'est un critère utilisé pour déterminer le 'meilleur' chemin.
- R1 va-t-il passer par R2 ou R3 pour atteindre le réseau 192.168.0.0/24 ?
- R1 prendra le chemin dont la métrique est la plus **petite**.

La métrique de RIP



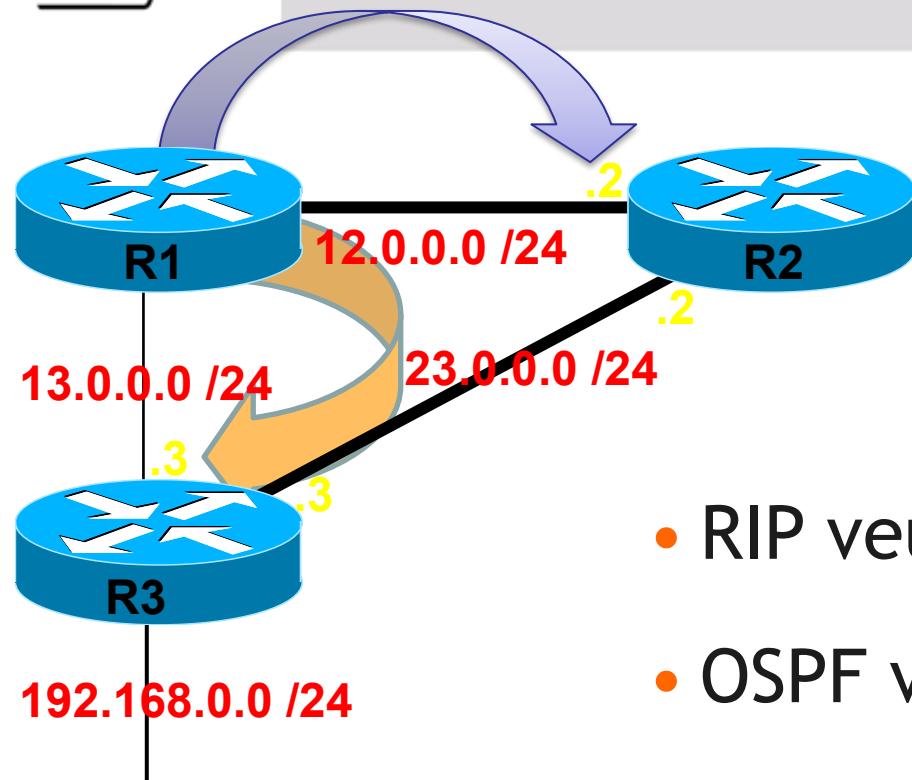
- C'est le **hop-count** :
 - = le nombre de routeurs à traverser.
 - via R2 : métrique = 2
 - via R3 : métrique = 1
- RIP indique à R1 de passer par **R3**.
- Se peut-il que RIP lui indique de passer par **R2** ?

La métrique d'OSPF



- C'est le **coût** :
 - = inversement proportionnel à la bande passante de chaque segment traversé
 - via R2, supposons une métrique de 7
 - via R3, supposons une métrique de 10
- OSPF indique à R1 de passer par **R2**.

Que DECIDE R1 ?



- RIP veut passer par 13.0.0.3
- OSPF veut passer par 12.0.0.2
- 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.

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.

Règle de sélection du meilleur chemin.

```
ROUTER# show ip route
```

```
10.0.0.0/24 is subnetted, 3 subnets,  
R      10.1.1.0/24 [120/1] via 10.1.2.2, 00:00:05, Ethernet0  
C      10.1.2.0/24 is directly connected, Ethernet0  
O      10.1.0.0/16 [110/200] via 10.1.2.3, 00:00:05, Ethernet0  
R      192.168.24.0/24 [120/2] via 10.1.2.2, 00:00:16, Ethernet0
```

1^{er} critère :
LONGUEUR du MASQUE

2^{ème} critère :
AD

3^{ème} critère :
METRIQUE

PARTAGE de CHARGE
entre les NEXT HOP

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

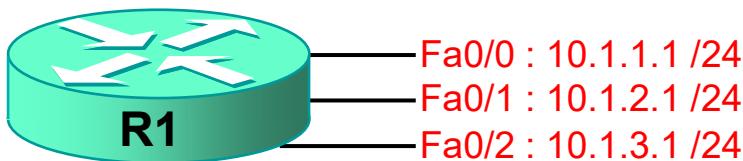
Activer RIP sur une interface

- configure terminal
- router rip
- network 10.0.0.0

signifie :

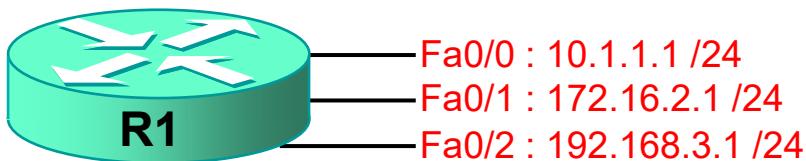
« active RIP dès
qu'une de tes **propres** interfaces
est dans le pool 10.0.0.0 /8 »

Exercice 1



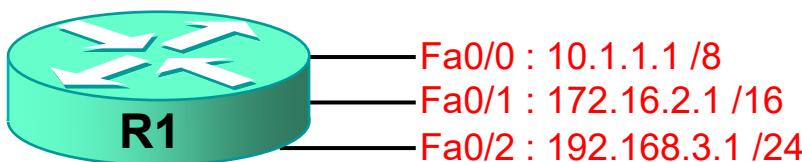
- Activer RIP sur toutes les interfaces
- `router rip`
- `network 10.0.0.0`

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`

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 ?
- 0

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**

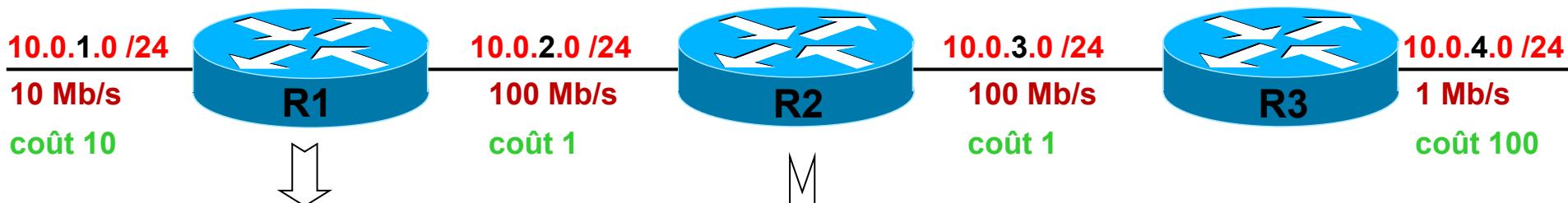
$$\frac{10^8}{\text{BW}}$$

- Exemples :

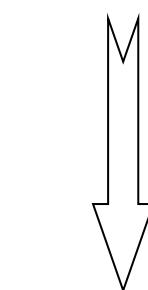
• FastEthernet	100 Mb/s	coût = 1
• Ethernet	10 Mb/s	coût = 10
•	1 Mb/s	coût = 100
• Serial	1,544 Mb/s	coût ≈ 65

La métrique d'OSPF 2/2

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



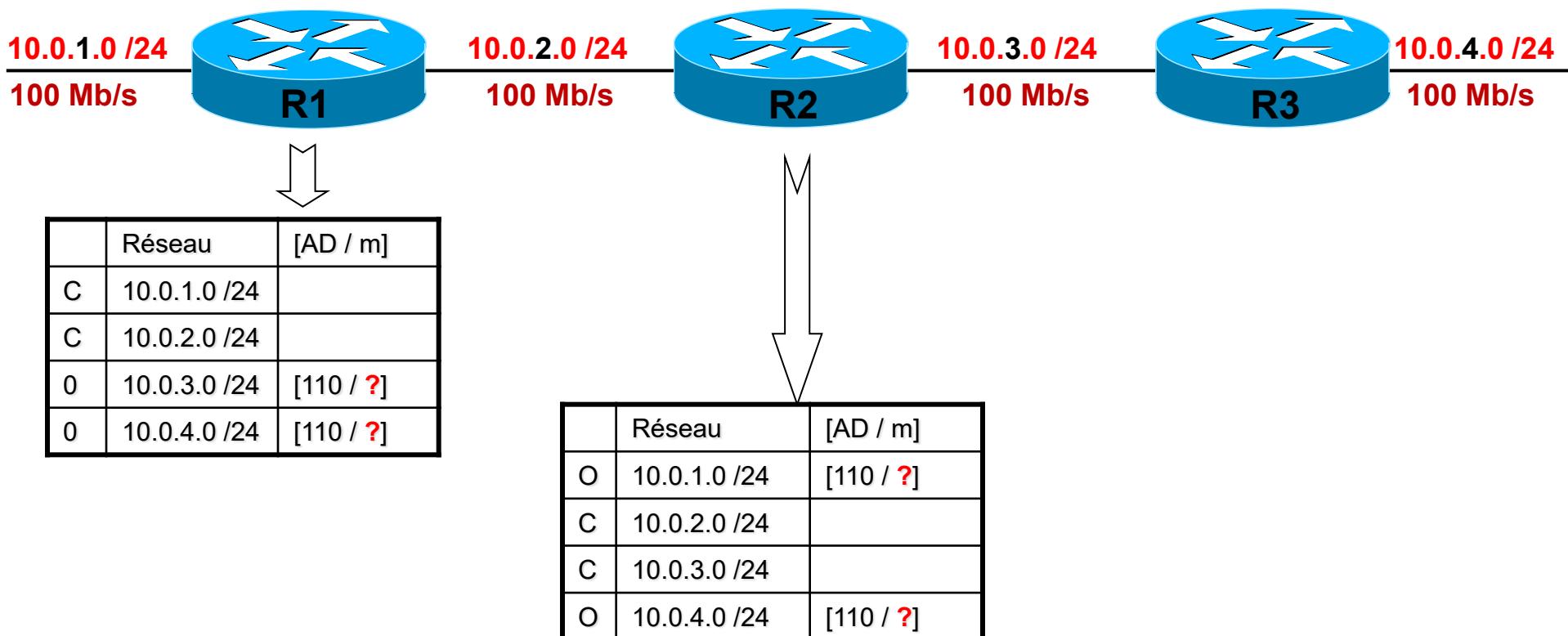
	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
O	10.0.3.0 /24	[110 / 2]	1+1
O	10.0.4.0 /24	[110 / 102]	1+1+100



	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

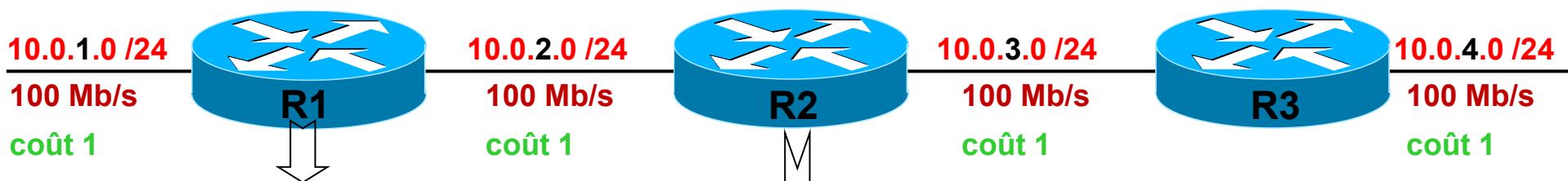
Exercice 1

- La métrique est la **somme** des coûts.



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		
O	10.0.3.0 /24	[110 / 2]	1+1
O	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

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

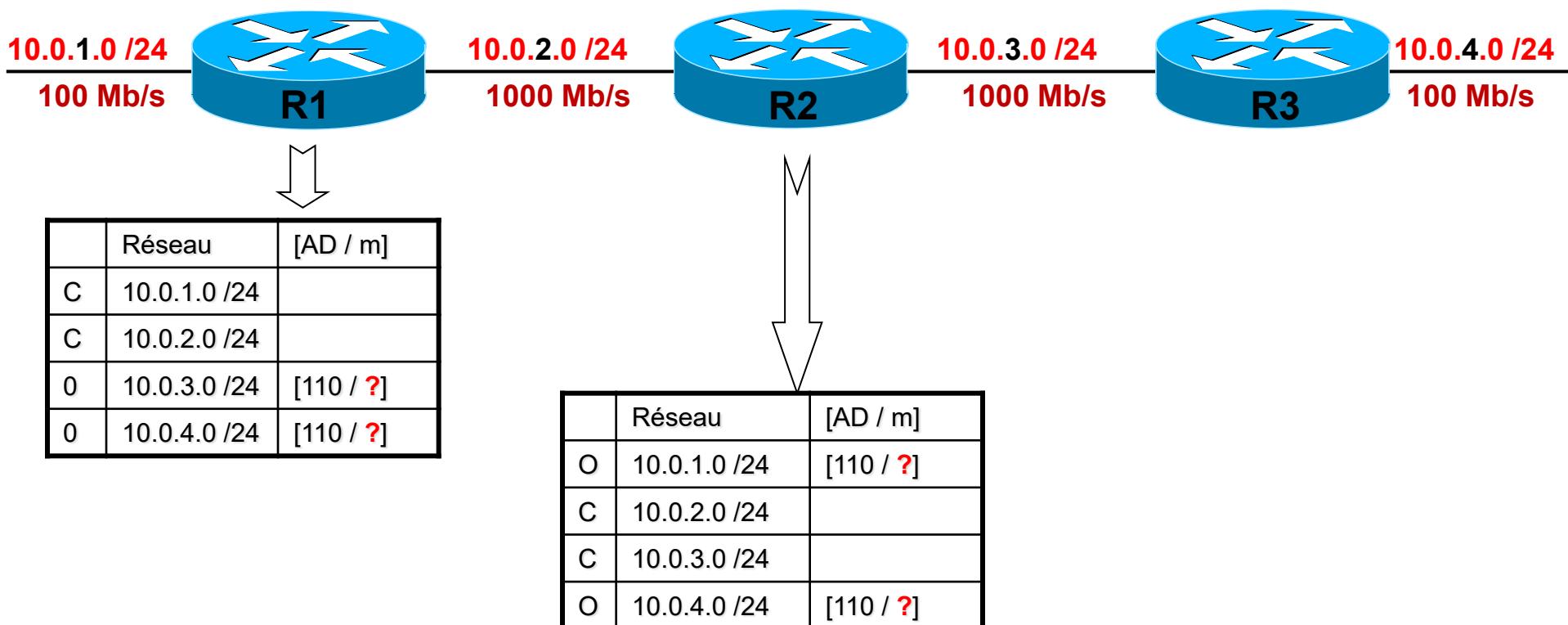
Adapter la formule 2/2

- 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 !

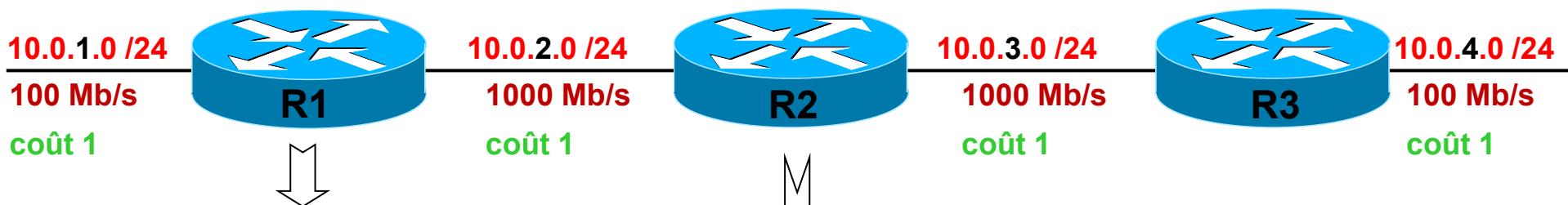
Exercice 2

auto-cost reference-bandwidth **100**

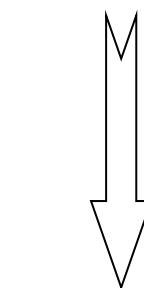


Solution 2

auto-cost reference-bandwidth **100**



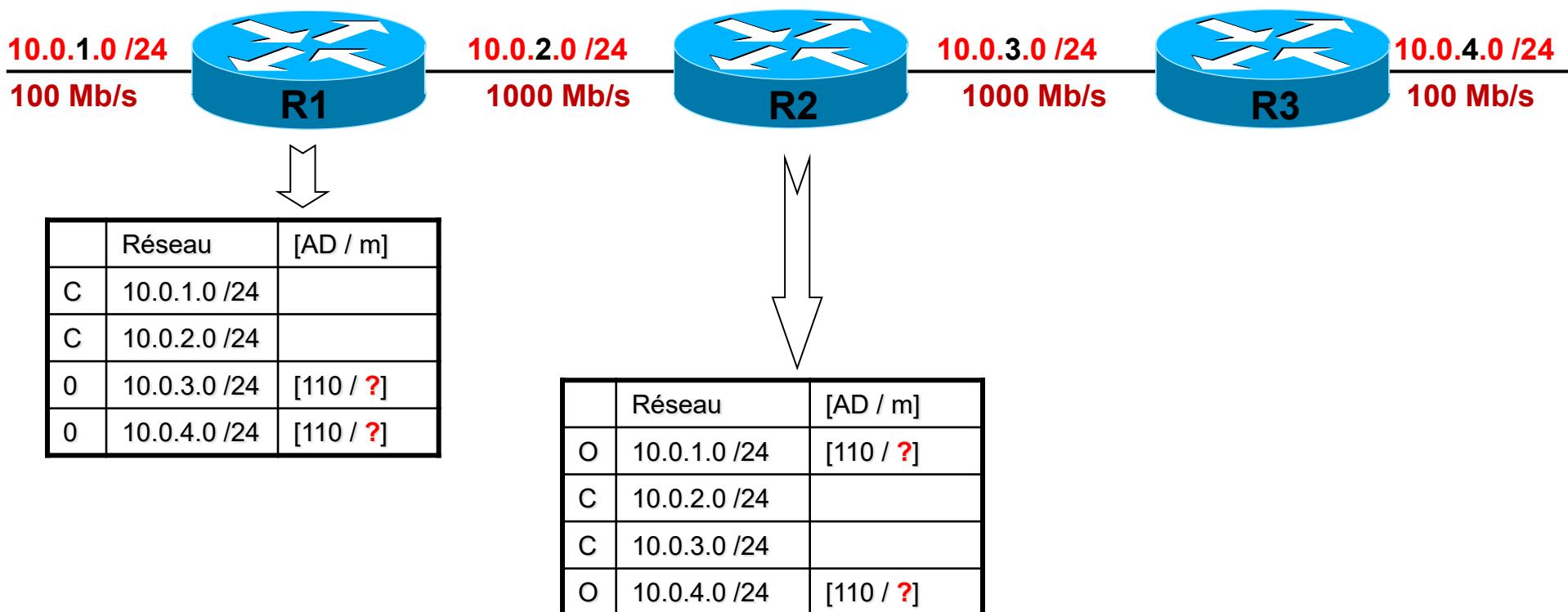
	Réseau	[AD / m]	somme des coûts
C	10.0.1.0 /24		
C	10.0.2.0 /24		
O	10.0.3.0 /24	[110 / 2]	1+1
O	10.0.4.0 /24	[110 / 3]	1+1+1



	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

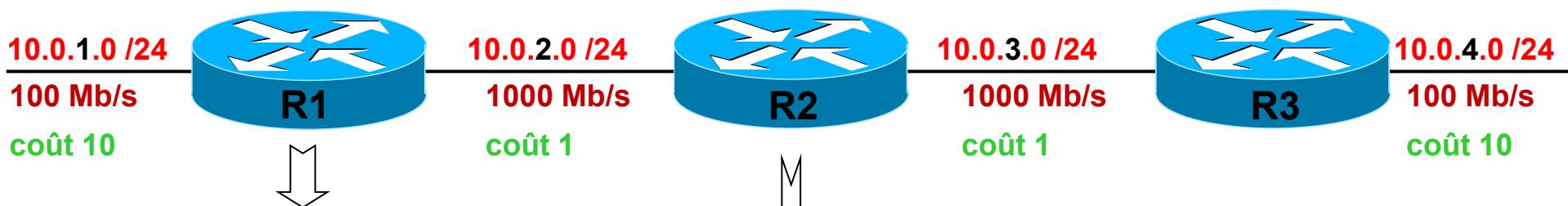
Exercice 3

auto-cost reference-bandwidth **1000**



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 : EIGRP

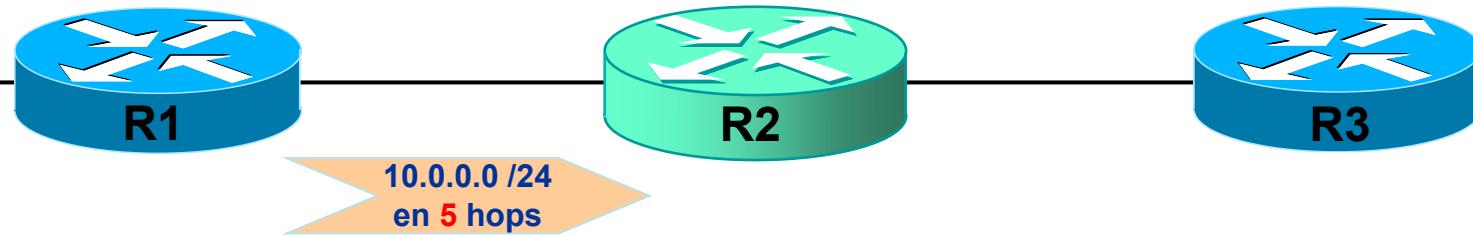
OSPF

Un protocole à ETATS de LIENS : LS

« Link State »

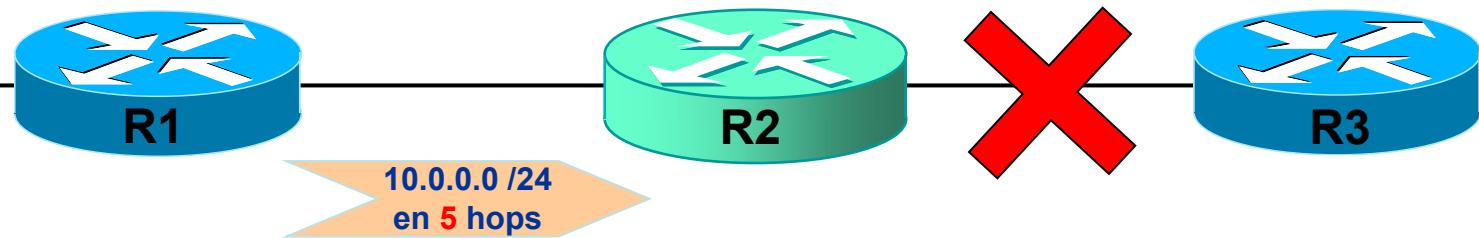
- Les protocoles à Vecteur de distance envoient à leurs voisins une partie de leur table de routage.
 - cette information sera-t-elle transférée par le voisin à un tiers ?
- Les protocoles à Etat de Lien envoient à leurs voisins des données sur les réseaux auxquels ils sont connectés.
 - cette information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

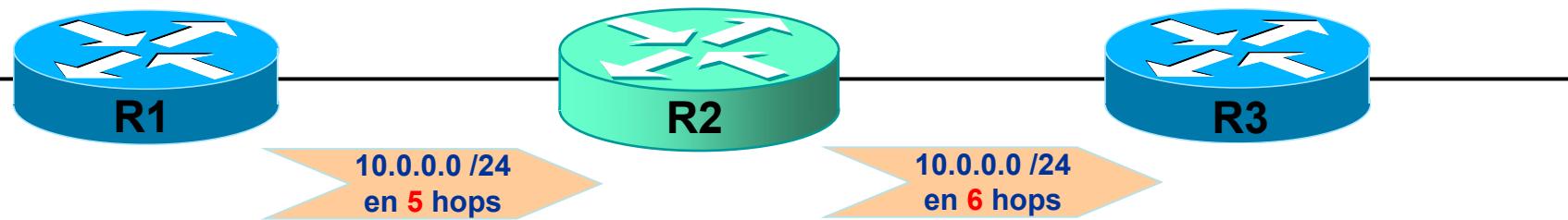


OUI : j'ai une meilleure route vers 10.0.0.0 /24 !

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

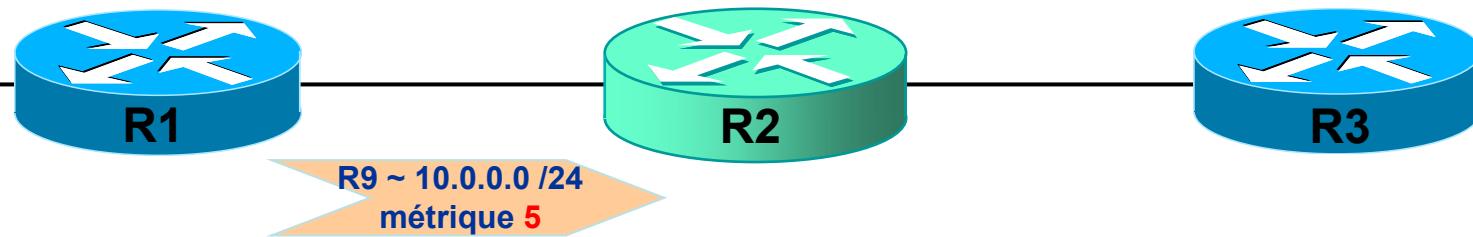


NON : je n'ai pas de meilleure route
vers 10.0.0.0 /24 !

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.

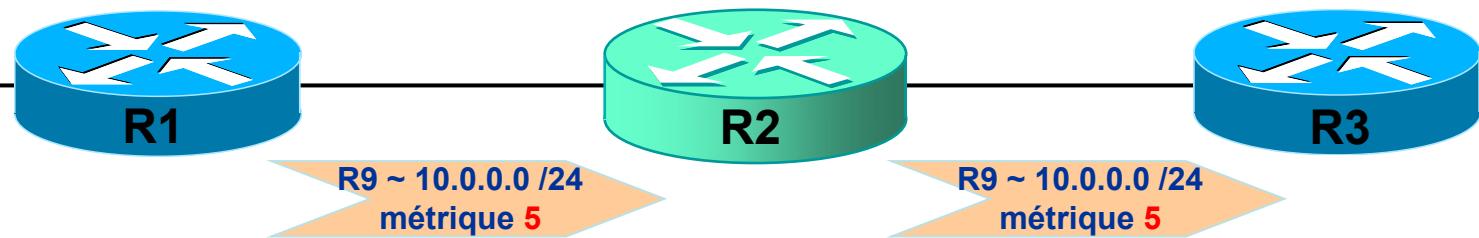
LS : Le transfert d'une annonce



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. »
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

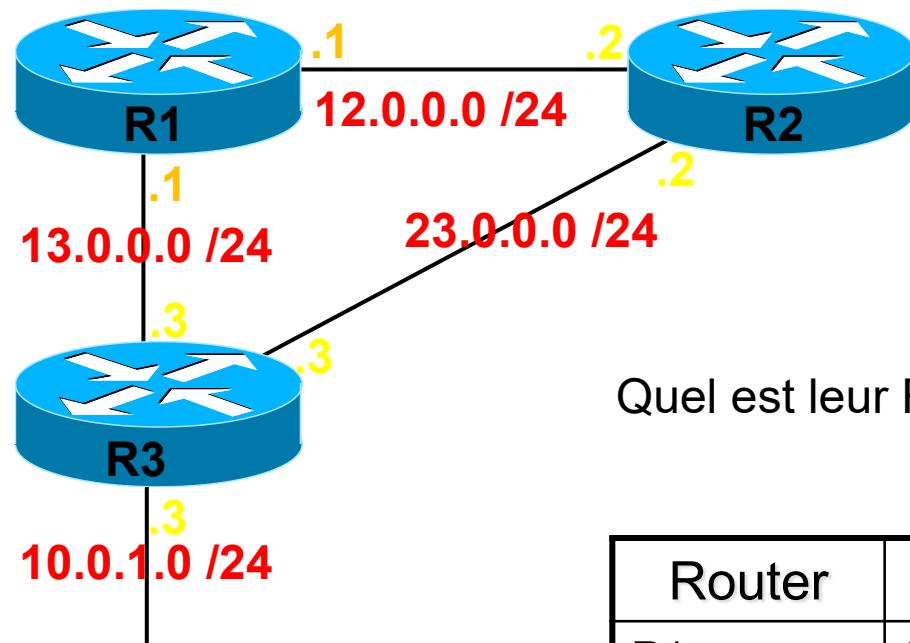
LS : les annonces

- Ces annonces s'appellent des LSA :
 - Link State Advertisement
- Elles contiennent :
 - l'identité du routeur qui a générée l'annonce
 - le ROUTER-ID
 - le sous-réseau annoncé
 - le masque de sous-réseau
 - 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

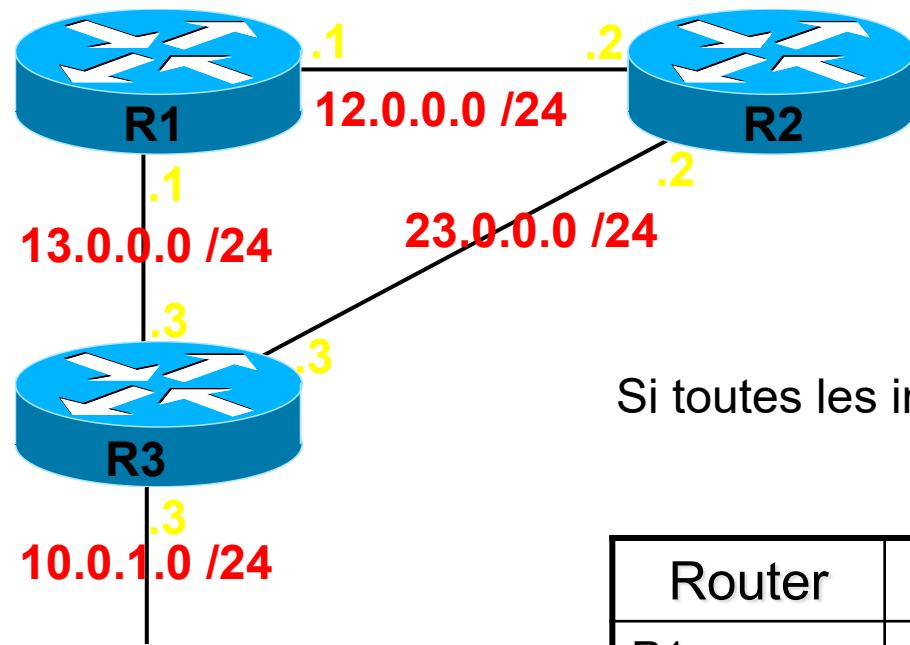
Exercice 1



Quel est leur Router-ID ?

Router	Router-ID
R1	?
R2	?
R3	?

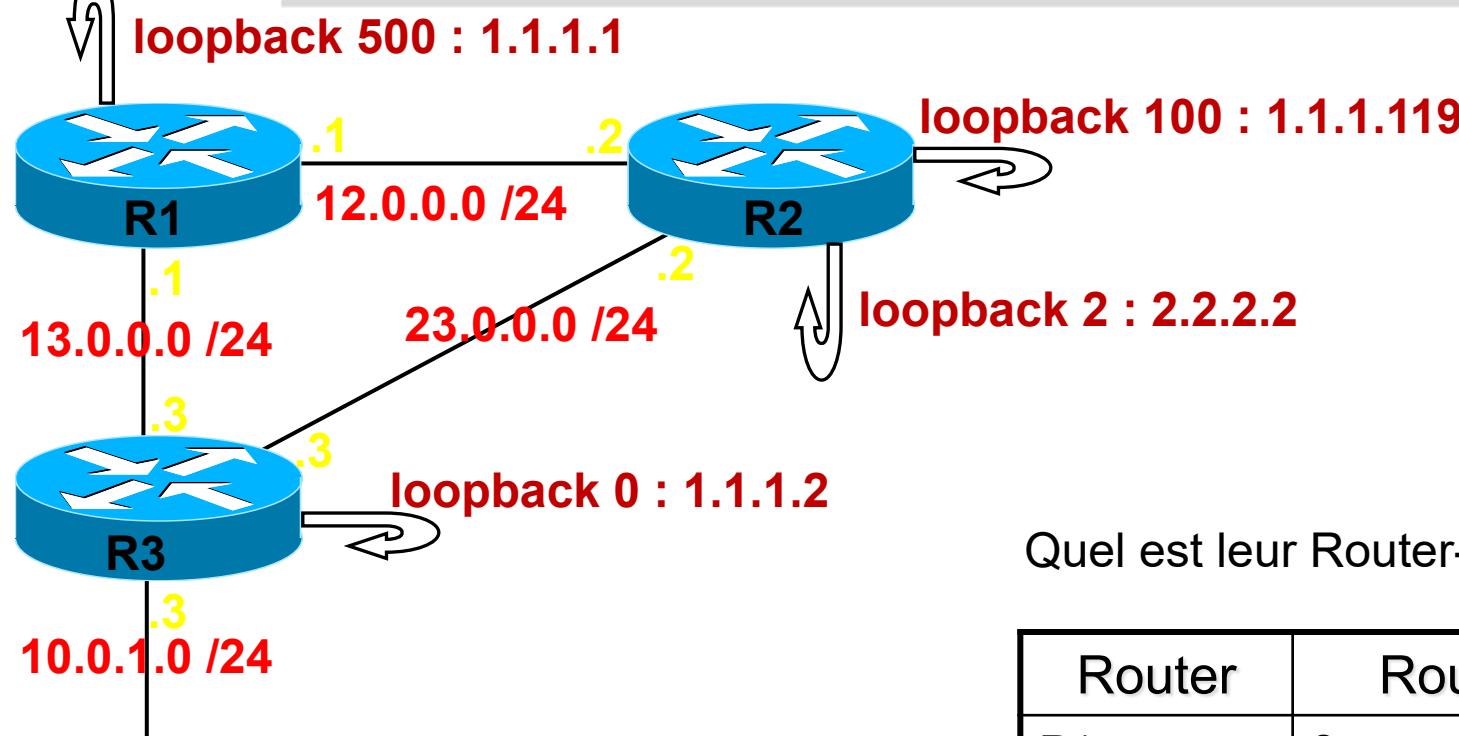
Solution 1



Si toutes les interfaces sont UP :

Router	Router-ID
R1	13.0.0.1
R2	23.0.0.2
R3	23.0.0.3

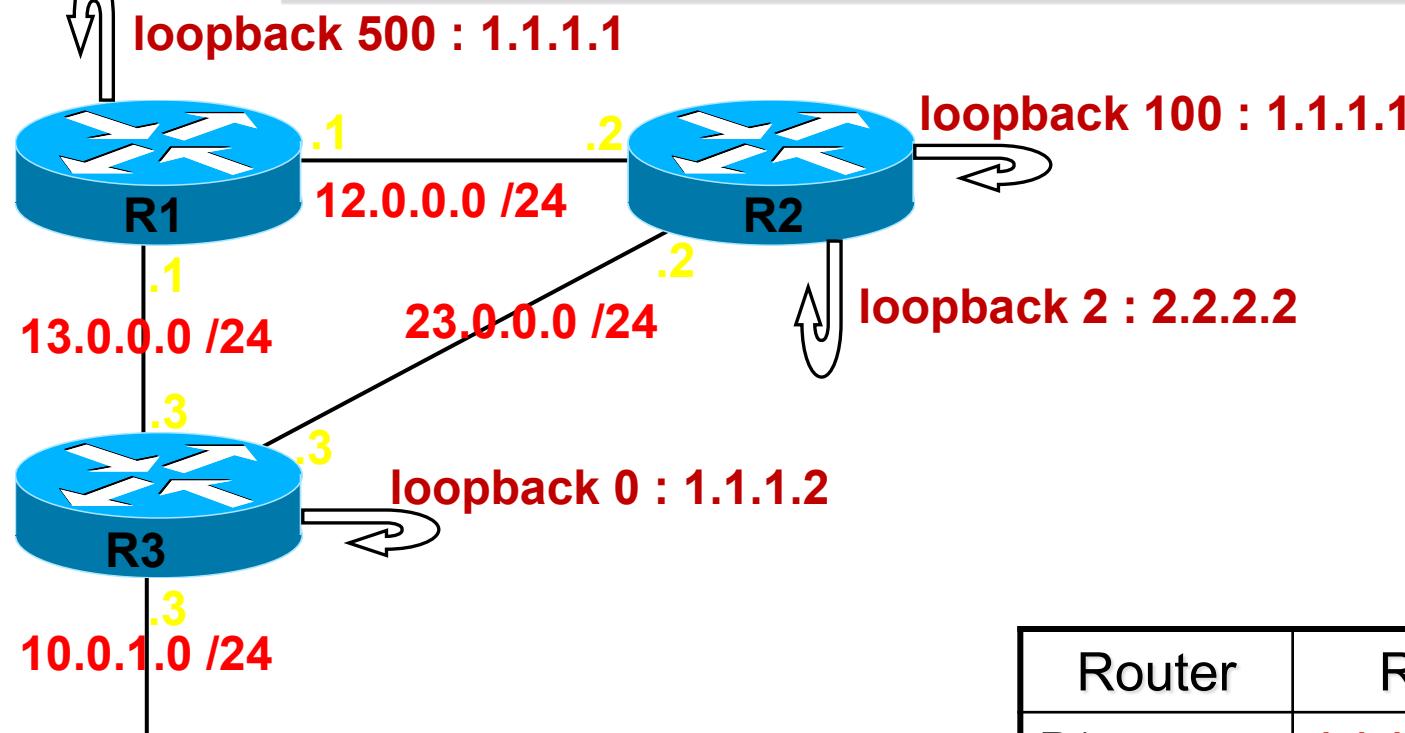
Exercice 2



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 !

- 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**

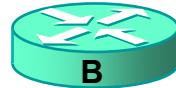
Problèmes pour « grands » réseaux.

Solution :
découper la réseau en plusieurs AIRES

OSPF

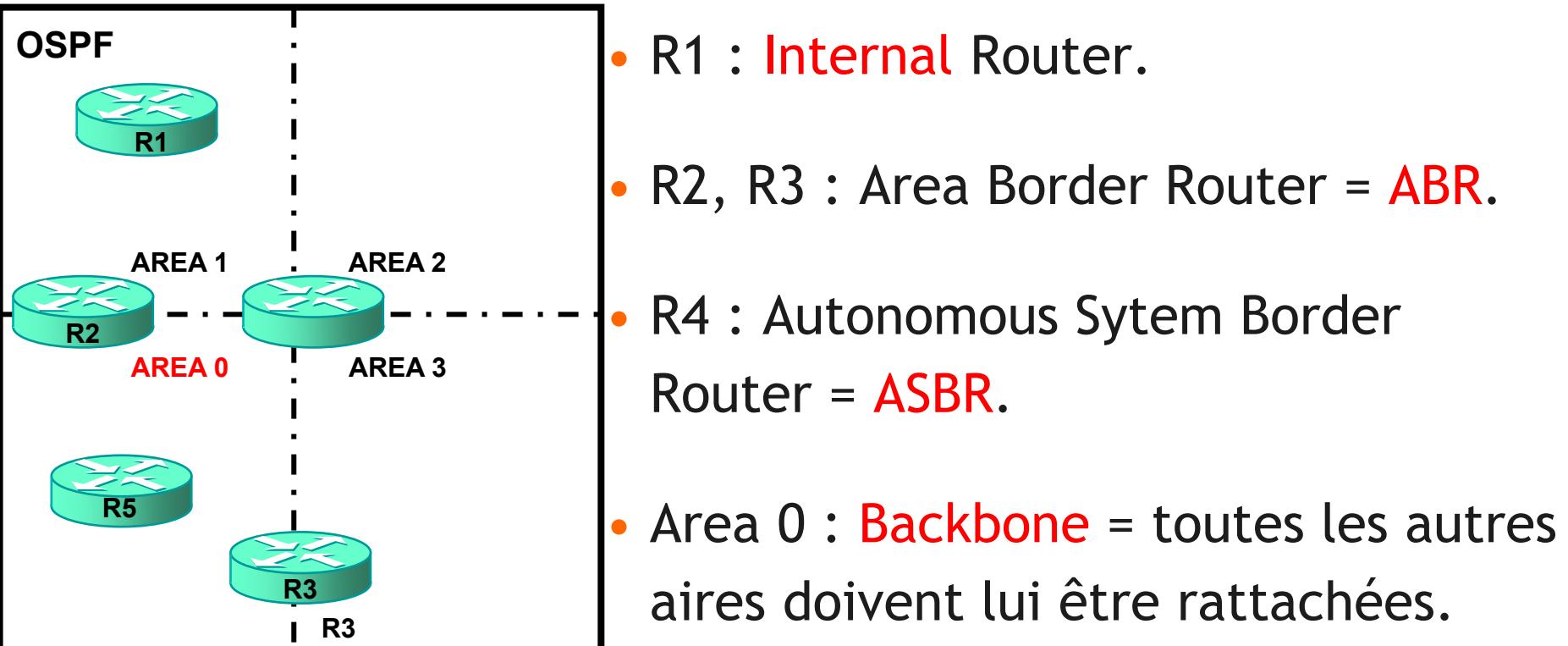
Optimiser les ressources

Sans aires

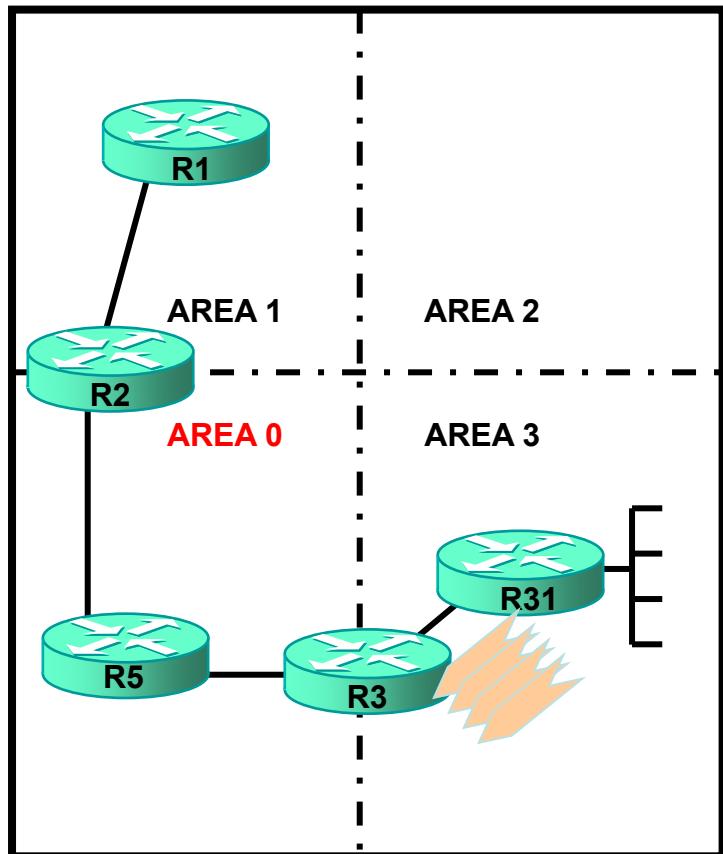


- A et B auront en mémoire la même cartographie, i.e. **TOUT** le réseau.
- A et B devront appliquer l'algorithme à toute la cartographie, i.e. **TOUS** les sous-réseaux.

Rôles

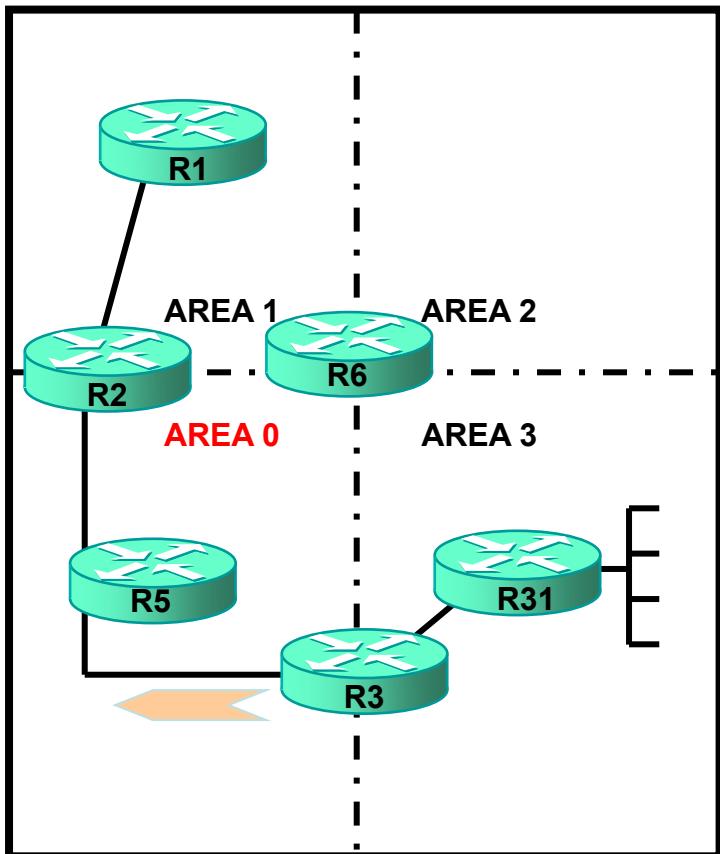


Intérêts des Aires 1/3



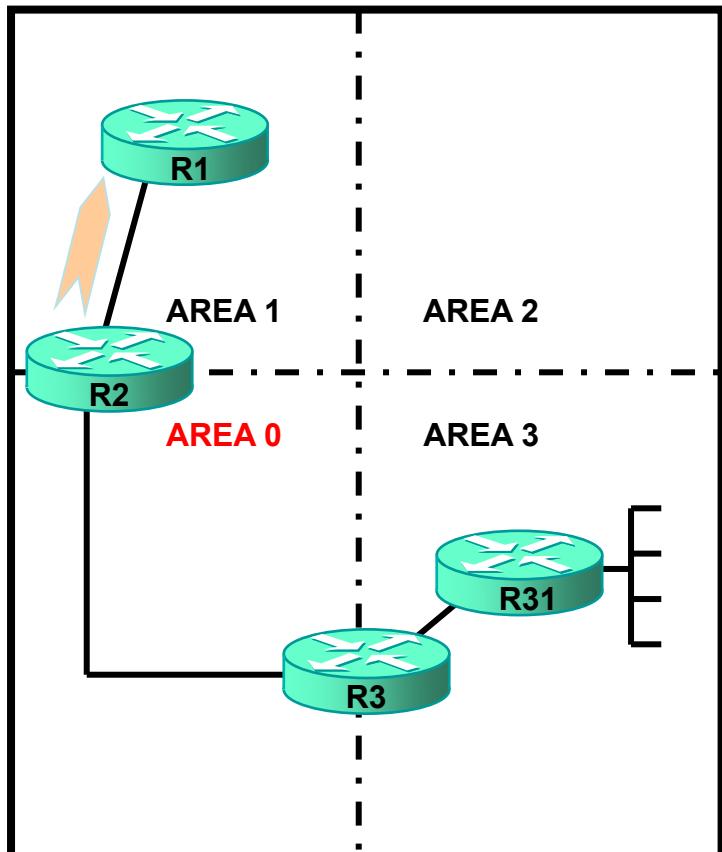
- R31 (**internal**) va générer au moins 4 LSA, une pour chacun de ses 4 sous-réseaux.

Intérêts des Aires 2/3

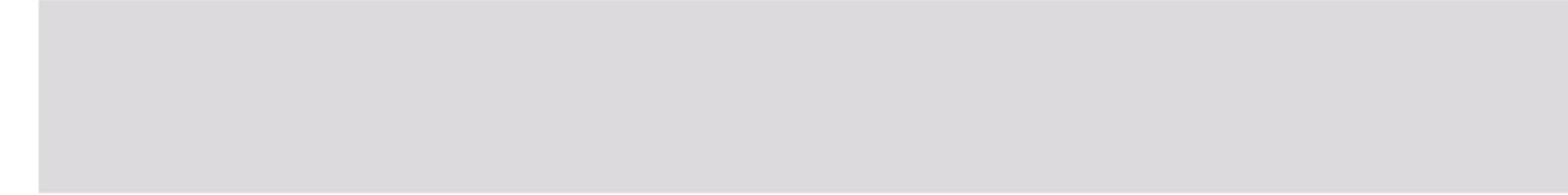


- R3 (**ABR**) va résumer les 4 sous-réseaux en un seul sous-réseau.

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 
masque inversé area 0

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 F/C	PID	Area	IP Address/Mask	Cost	State	Nbrs
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
<p><u>Objectif :</u> Découvrir tous mes voisins directs.</p>	<p><u>Objectif :</u> Construire la cartographie du réseau.</p>	<p><u>Objectif :</u> Décider du chemin le plus court pour atteindre chaque sous-réseau annoncé.</p>

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 reconnaiss 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

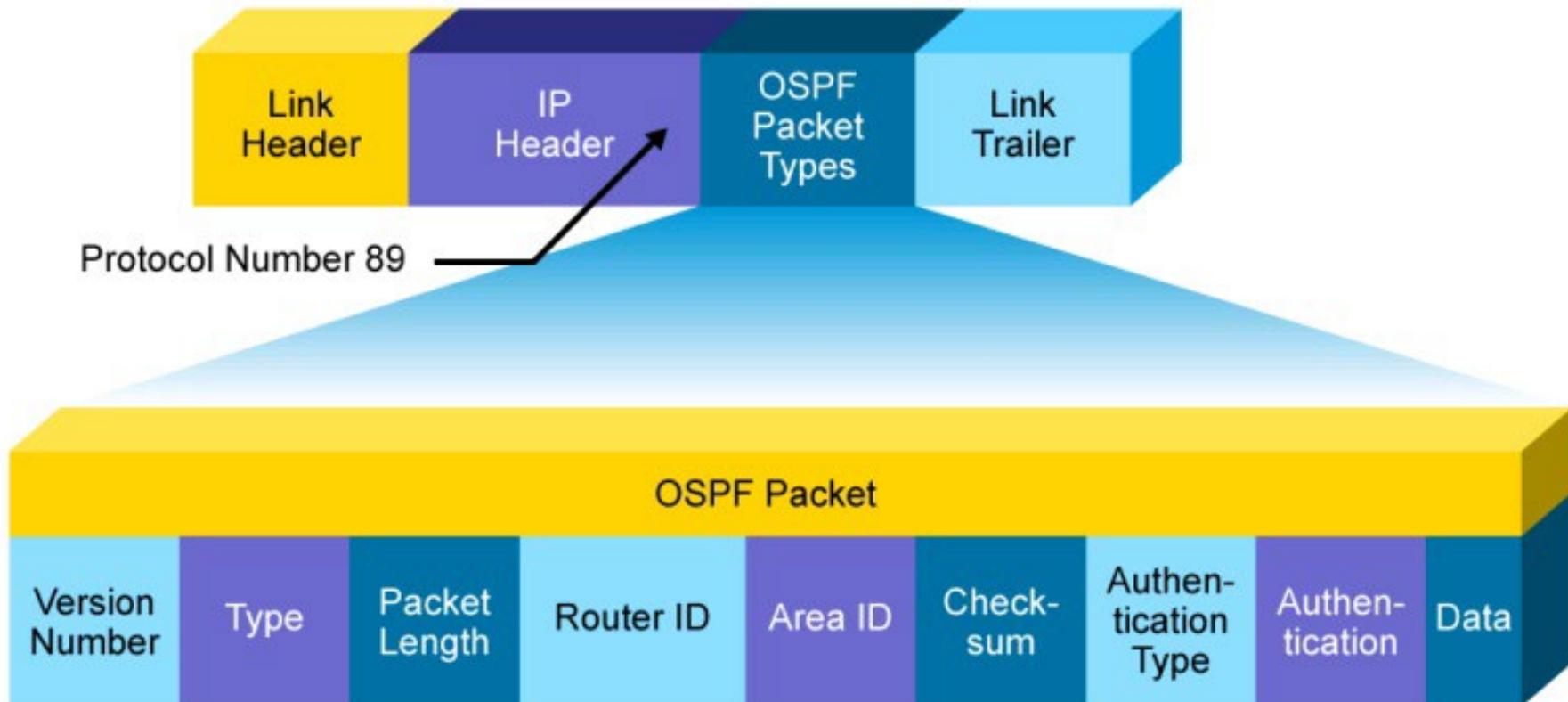
Cinq types de paquets OSPF

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
<p><u>Objectif :</u> Découvrir tous mes voisins directs.</p>	<p><u>Objectif :</u> Construire la cartographie du réseau.</p>	<p><u>Objectif :</u> Décider du chemin le plus court pour atteindre chaque sous-réseau annoncé.</p>

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

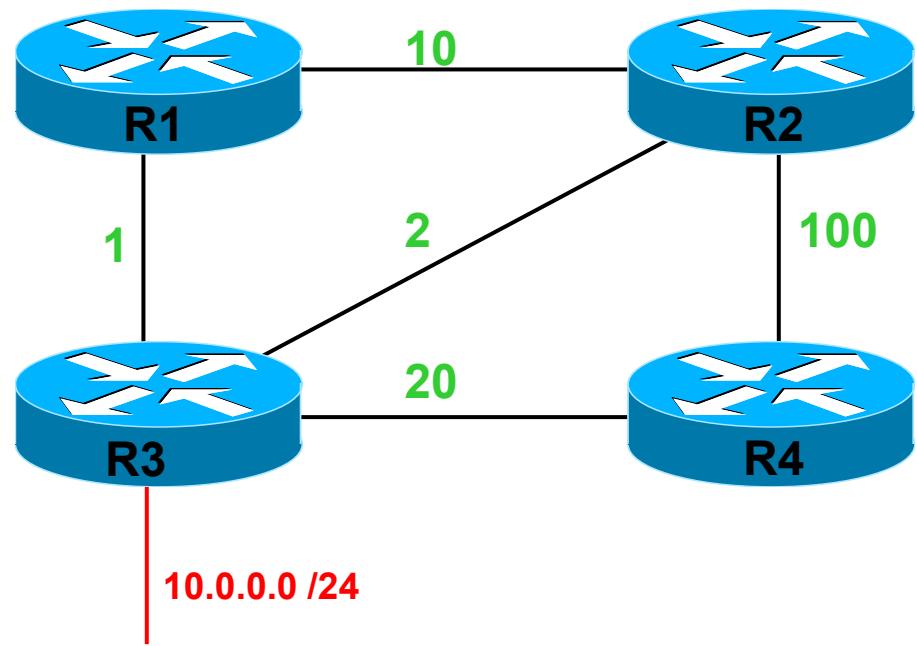
TROIS étapes

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

Dijkstra

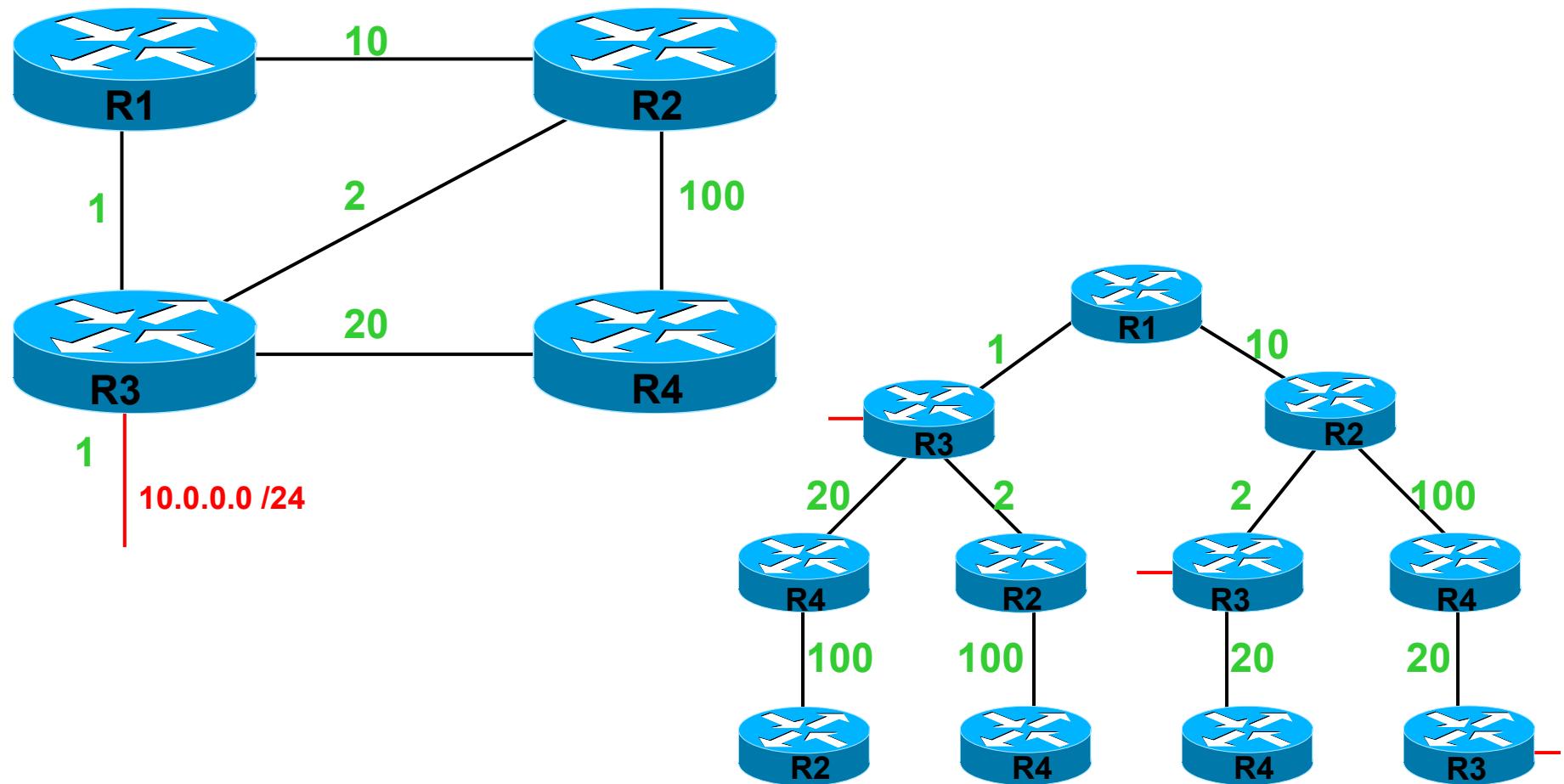
- également appelé algorithme **SPF** : Shortest Path First
- **Déterminer** le chemin le plus court pour atteindre chaque réseau annoncé.
- **Injecter** ce chemin dans la table de routage, si pas de meilleur chemin déjà présent.

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



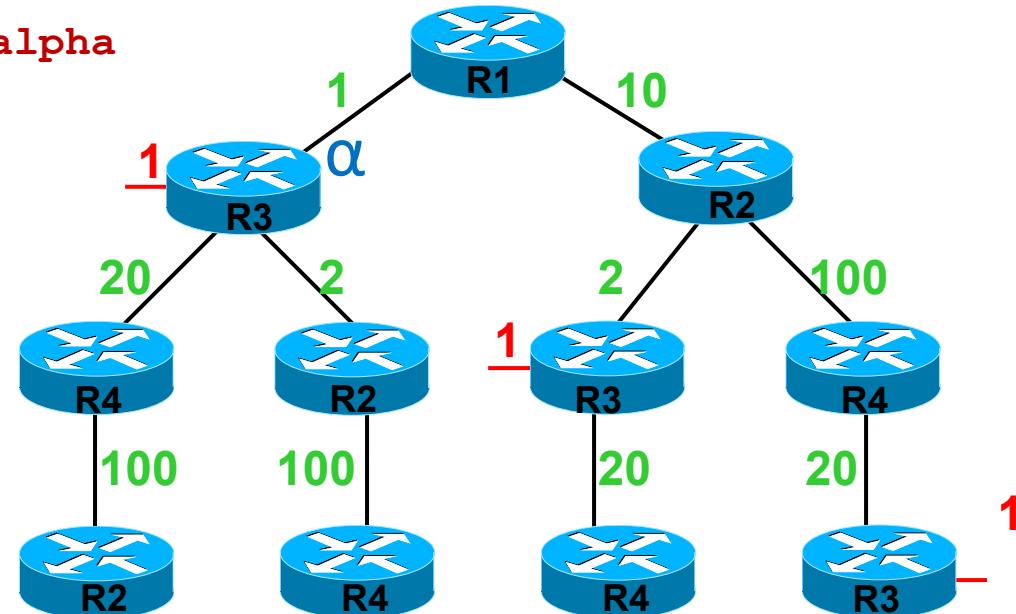
Métrique = somme des coûts

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

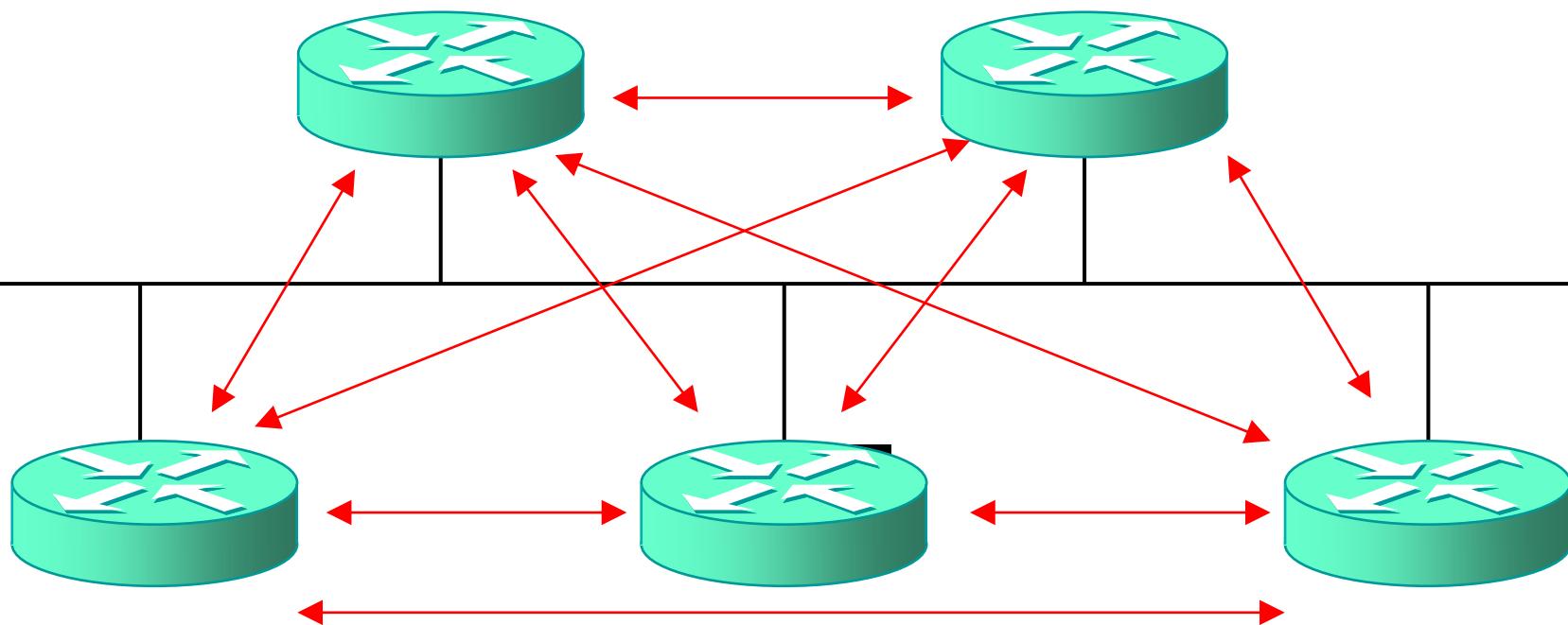
ETAPE 1	ETAPE 2	ETAPE 3
show ip ospf neighbor	show ip ospf database	show ip route ospf

OSPF

Optimisation

DR et BDR

10 relations 'FULL'

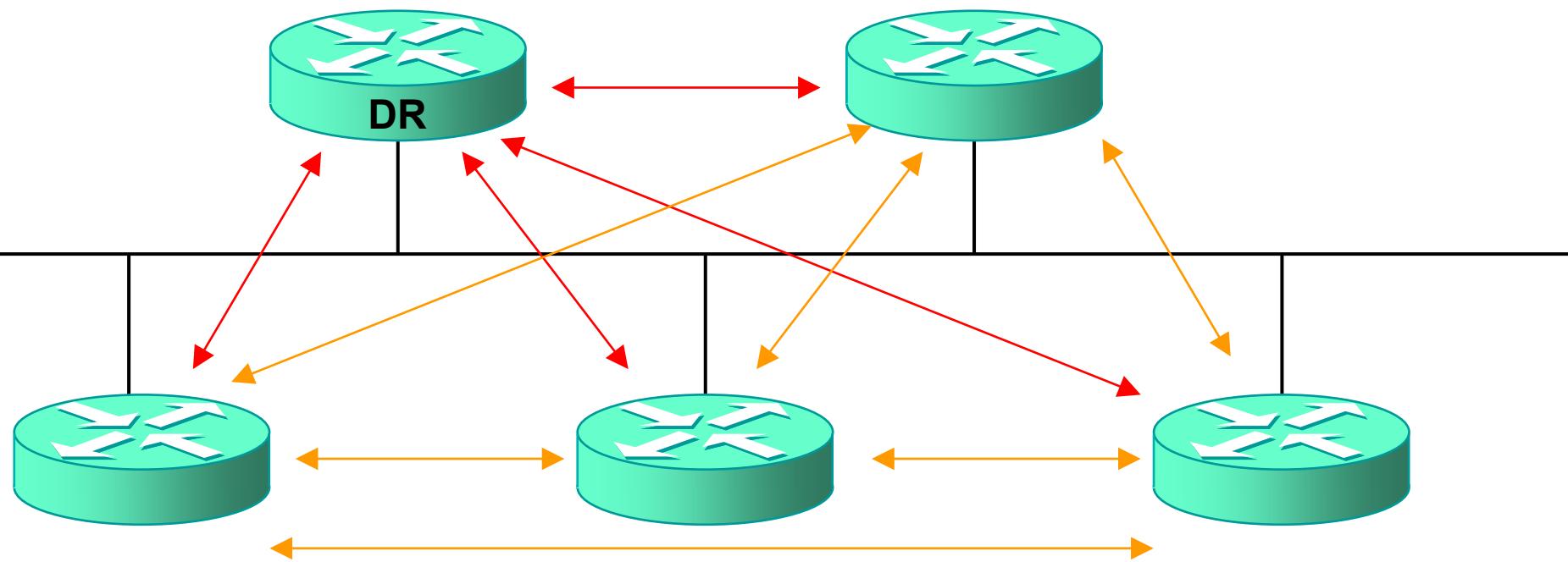


Avec 5 routeurs sur un même segment :

- Chaque routeur a 4 voisins.
- Il est '**FULL**' avec chacun des 4 voisins.

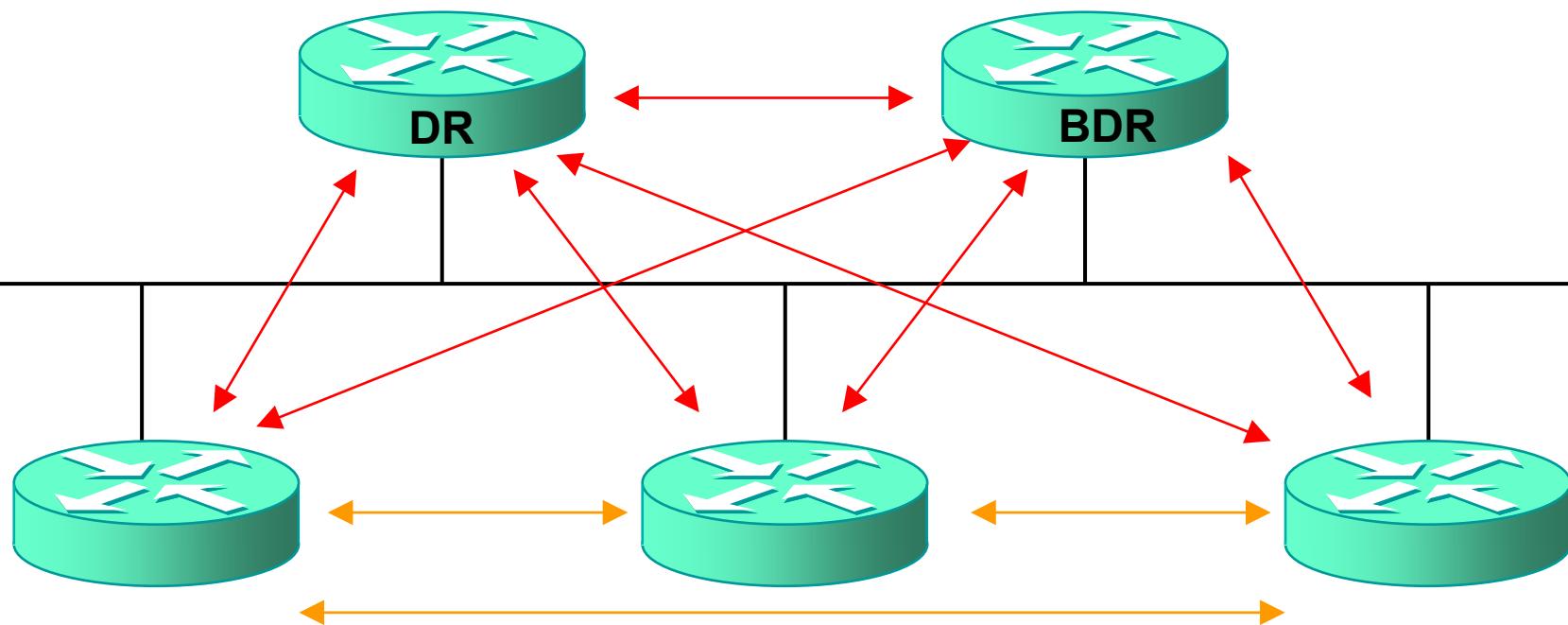
Avec N routeurs :

4 relations 'FULL'



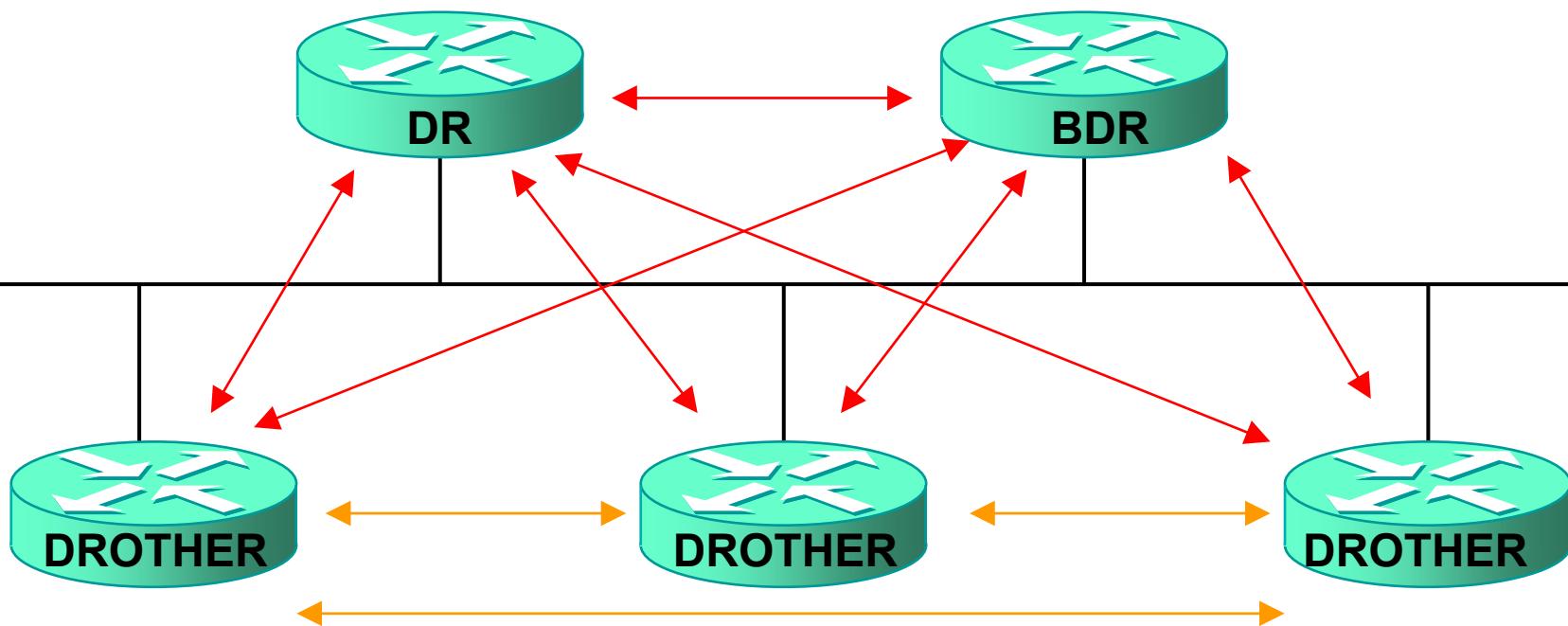
- Un routeur joue le rôle de compilateur :
 - DR = Designated Router.
- Tous les routeurs sont '**FULL**' avec les DR.
- Les autres relations de voisinage sont '**TWO-WAY**'.

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 annonçant 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.

- R1:** Ethernet0 is up, line protocol is up
Internet address 192.168.1.2/24, Area 0
Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
No backup designated router on this network
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
-
- R2:** Ethernet0 is up, line protocol is up
Internet address 192.168.1.1/24, Area 0
Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

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 = $256 * ((10^7 / \text{BW}) + \sum \text{DLY})$
 - 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 = [$K1 * 256 * 10^7 / BW + K2 * (BW / 256 - charge) + K3 * 256 \sum DLY$] * $(K5 / (K4 + fiabilité))$

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 !

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 = $256 * ((10^7 / \text{BW}) + \sum \text{DLY})$
 - 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 = [$K1 * 256 * 10^7 / BW + K2 * (BW / 256 - charge) + K3 * 256 \sum DLY$] * $(K5 / (K4 + fiabilité))$

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

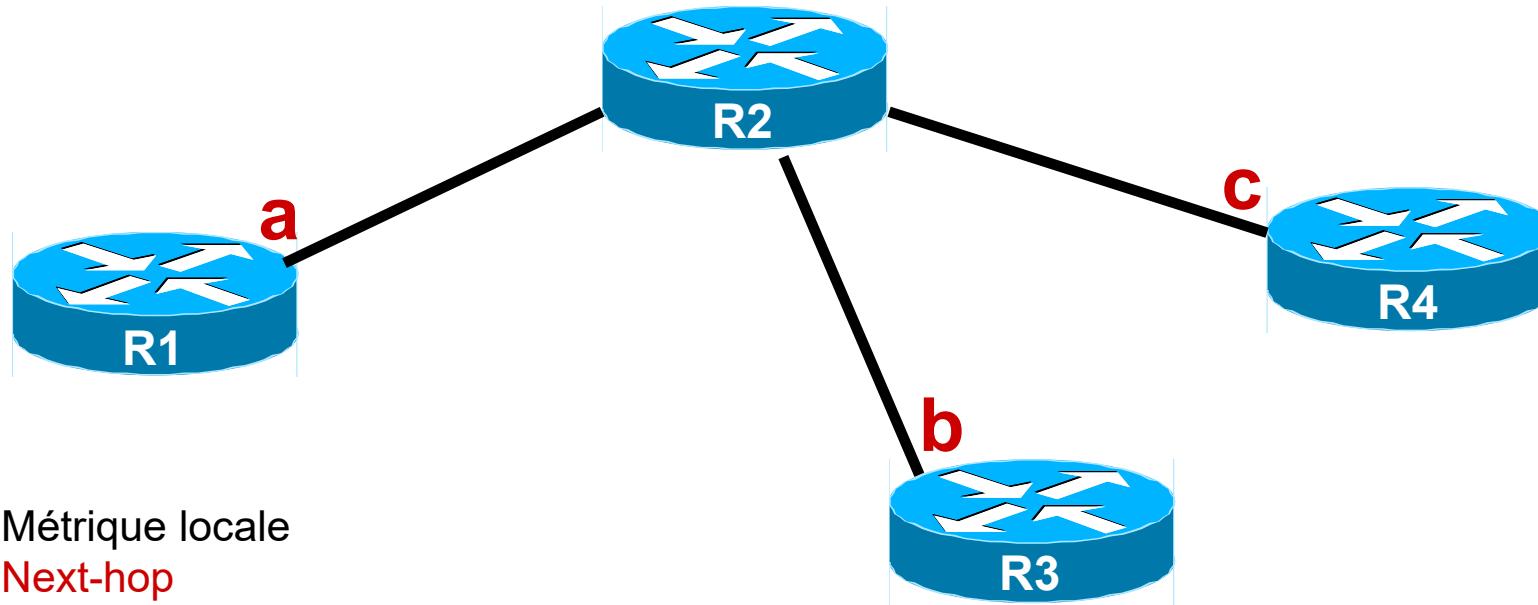
Masque annoncé

- 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

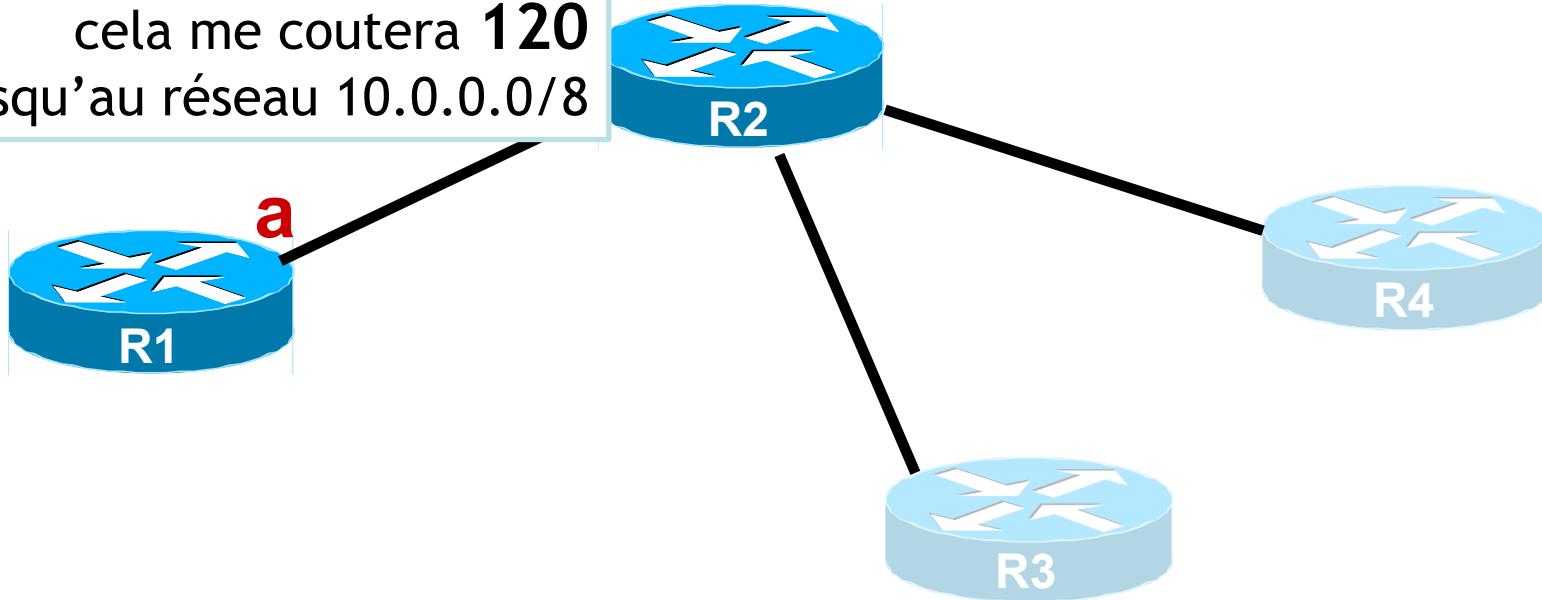
La terminologie DUAL



Quel est le meilleur chemin depuis R2 vers le sous-réseau 10.0.0.0/24 ?
R2 calcule les métriques **TOTALES** pour aller de R2 jusqu'au réseau 10.0.0.0/24

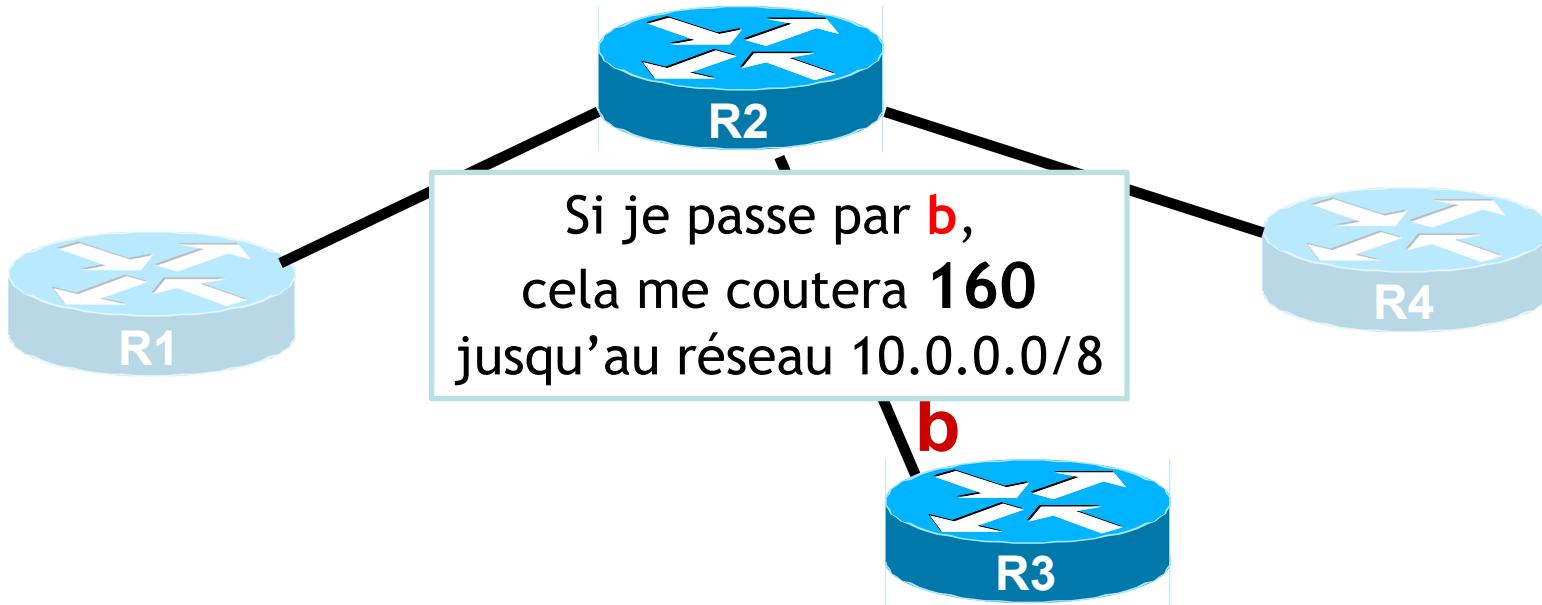
La terminologie DUAL

Si je passe par **a**,
cela me coutera **120**
jusqu'au réseau 10.0.0.0/8



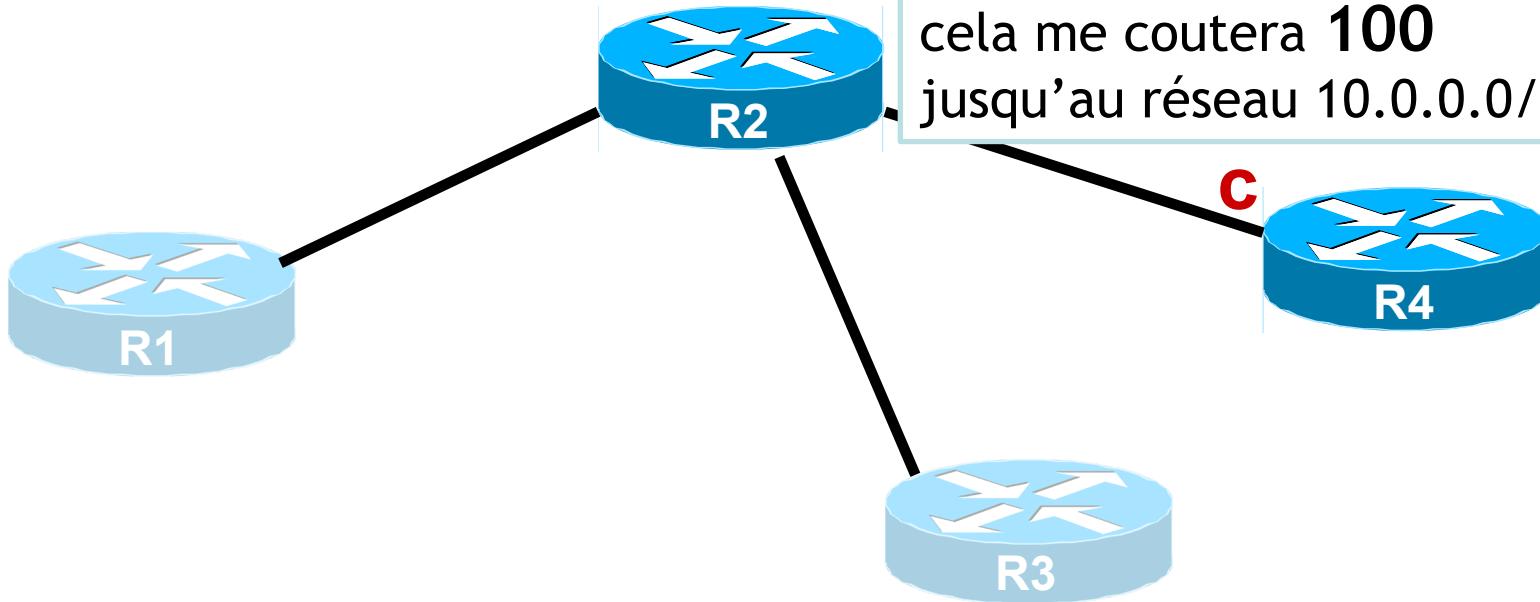
Métrique totale
Next-hop

La terminologie DUAL



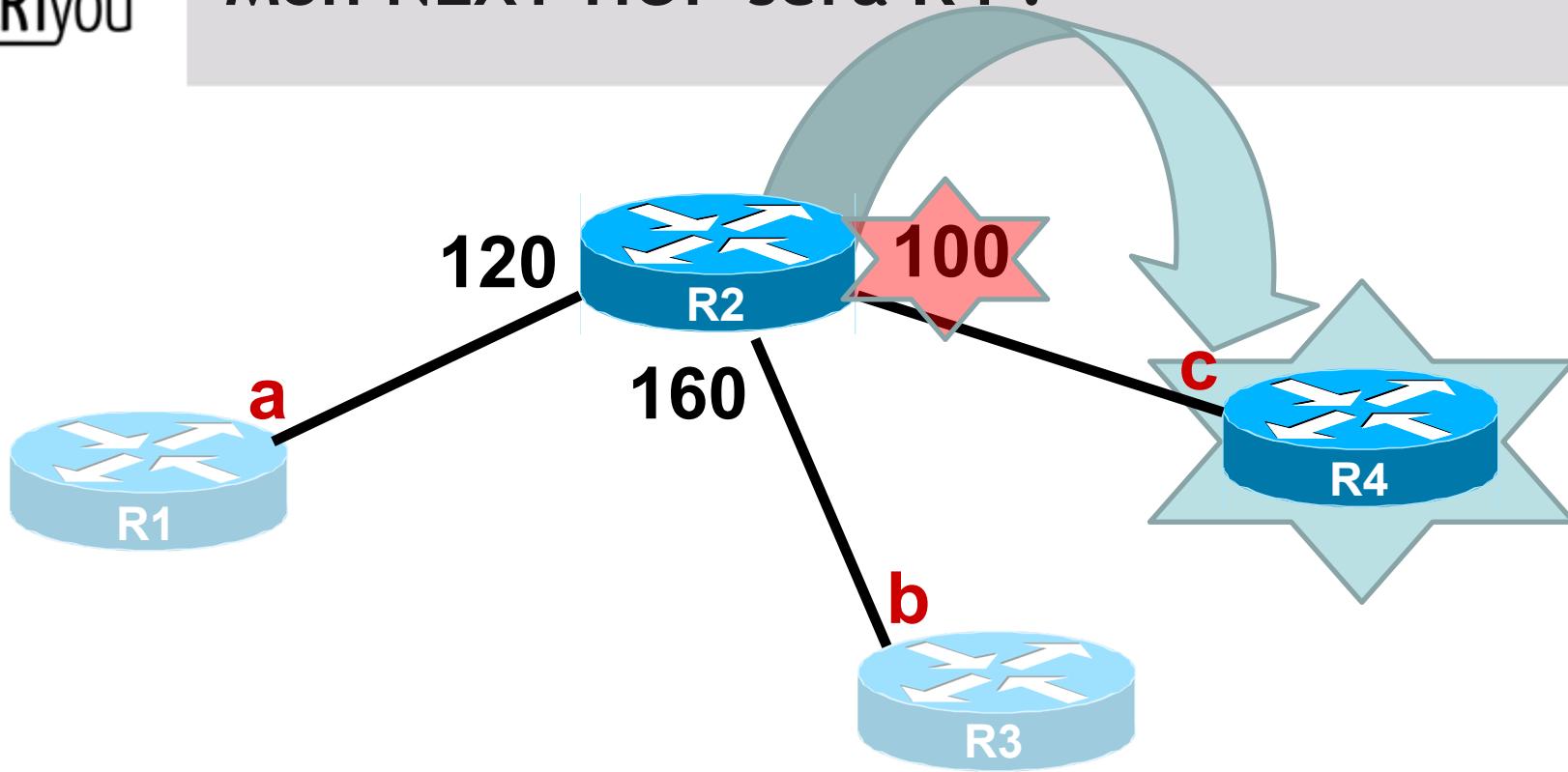
Métrique totale
Next-hop

La terminologie DUAL



Métrique totale
Next-hop

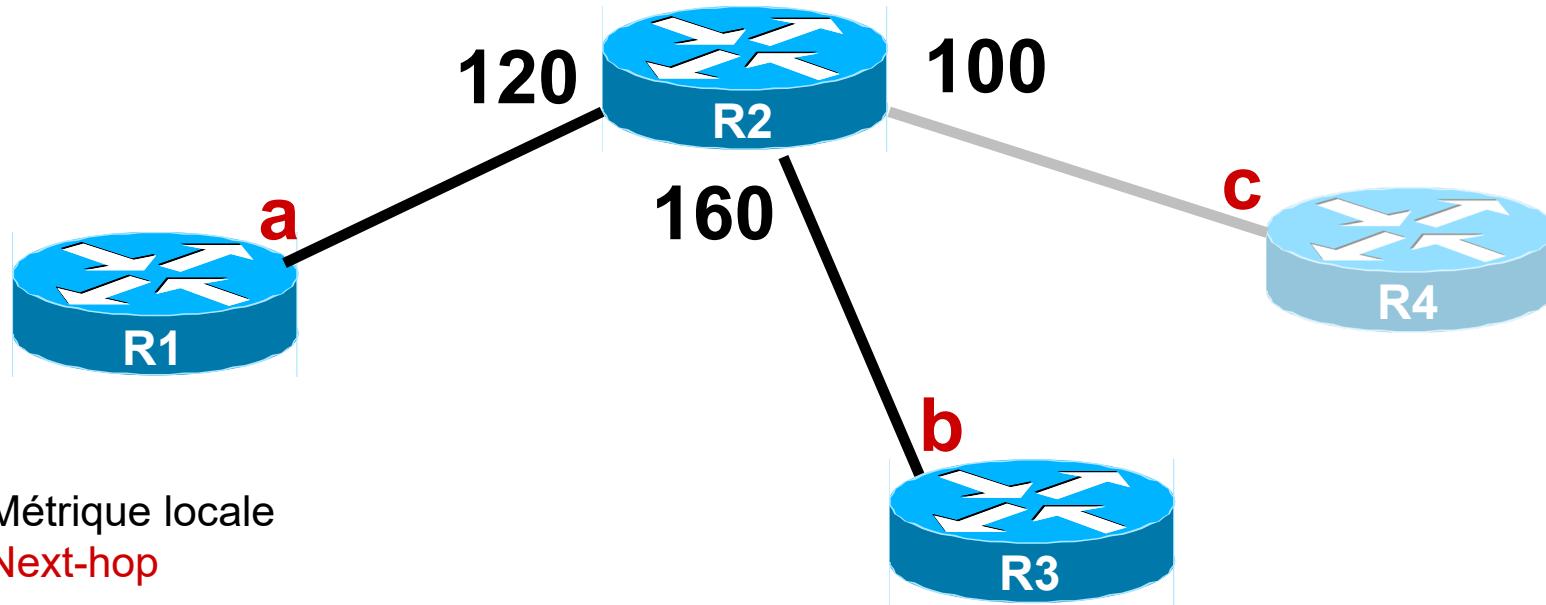
Mon NEXT HOP sera R4 !



Ma MEILLEURE métrique est 100
(feasible Distance = 100)

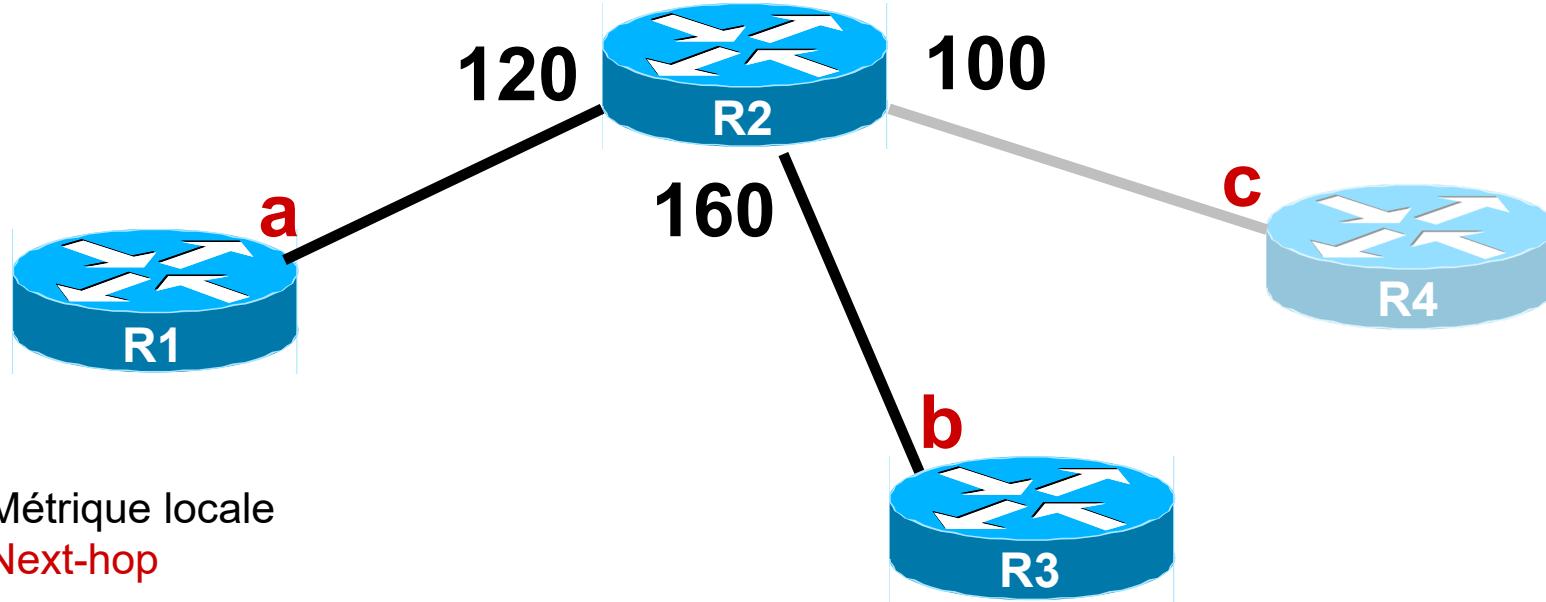
Mon NEXT HOP sera C (Successor = c)

Et si R4 devenait INJOIGNABLE ?!



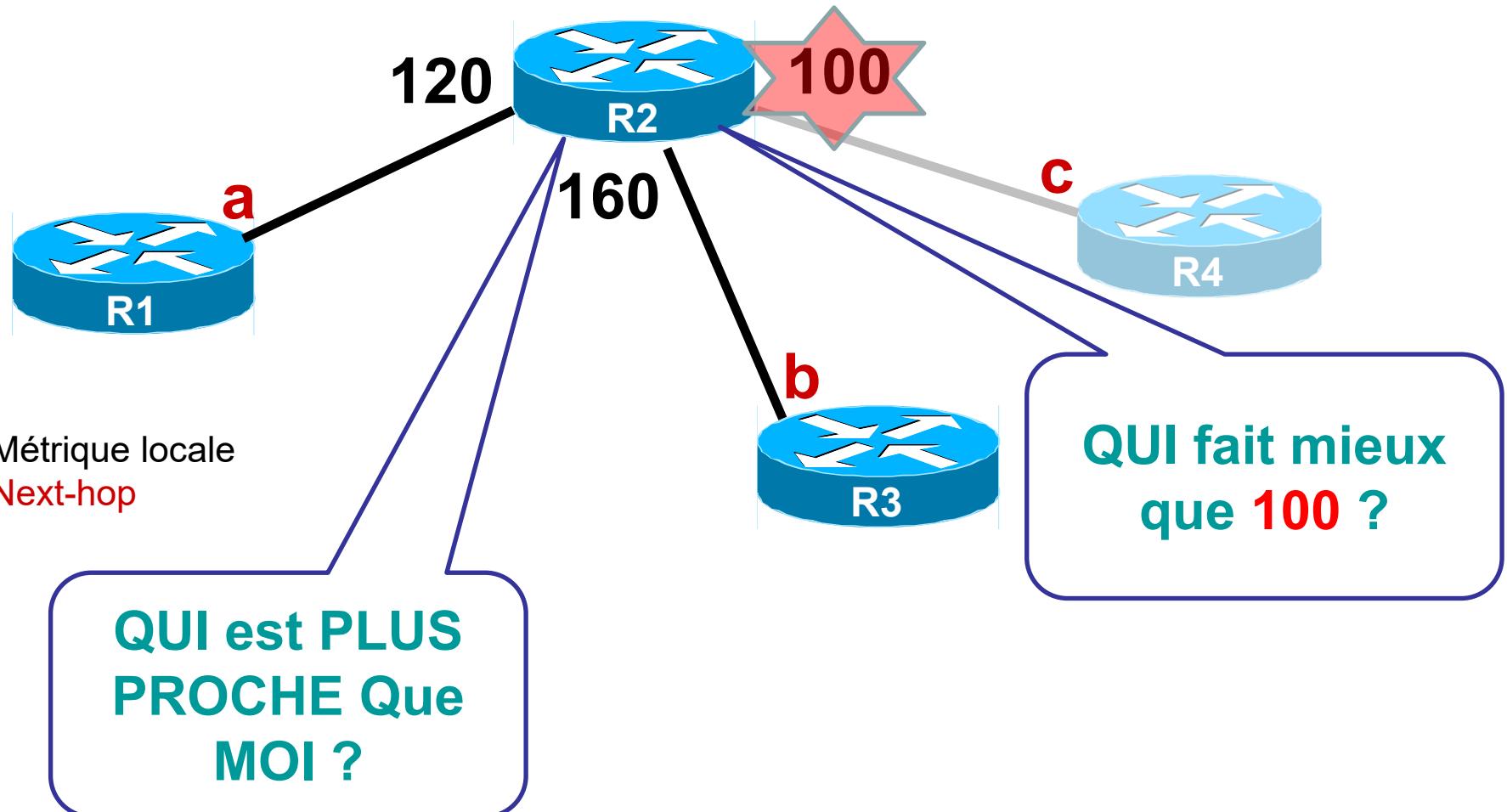
R2 essaie de définir une route de BACK-UP
Mais Attention aux boucles !!

Et si R4 devenait INJOIGNABLE ?!

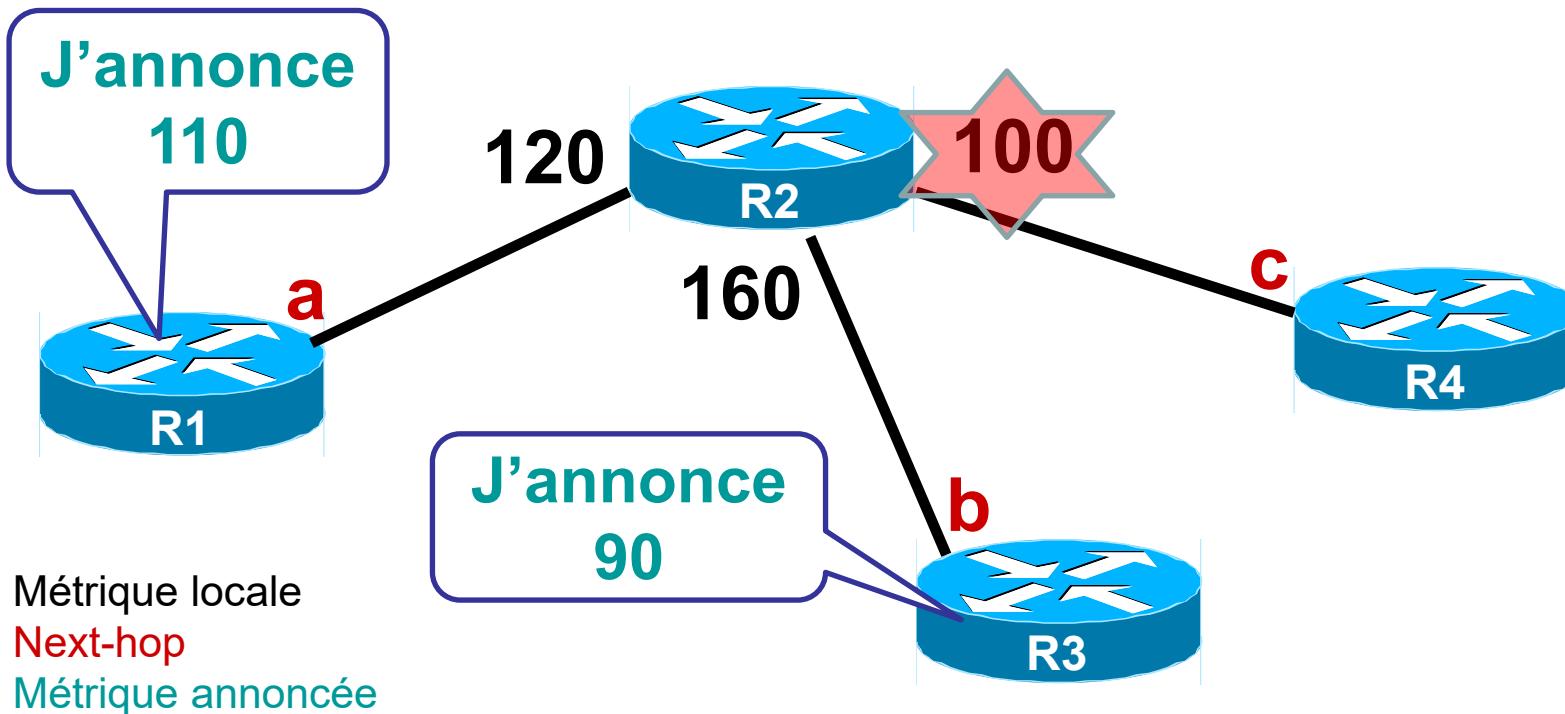


Pour éviter de créer une boucle, je choisis un BACK-UP qui est plus proche que MOI

Et si R4 devenait INJOIGNABLE ?!

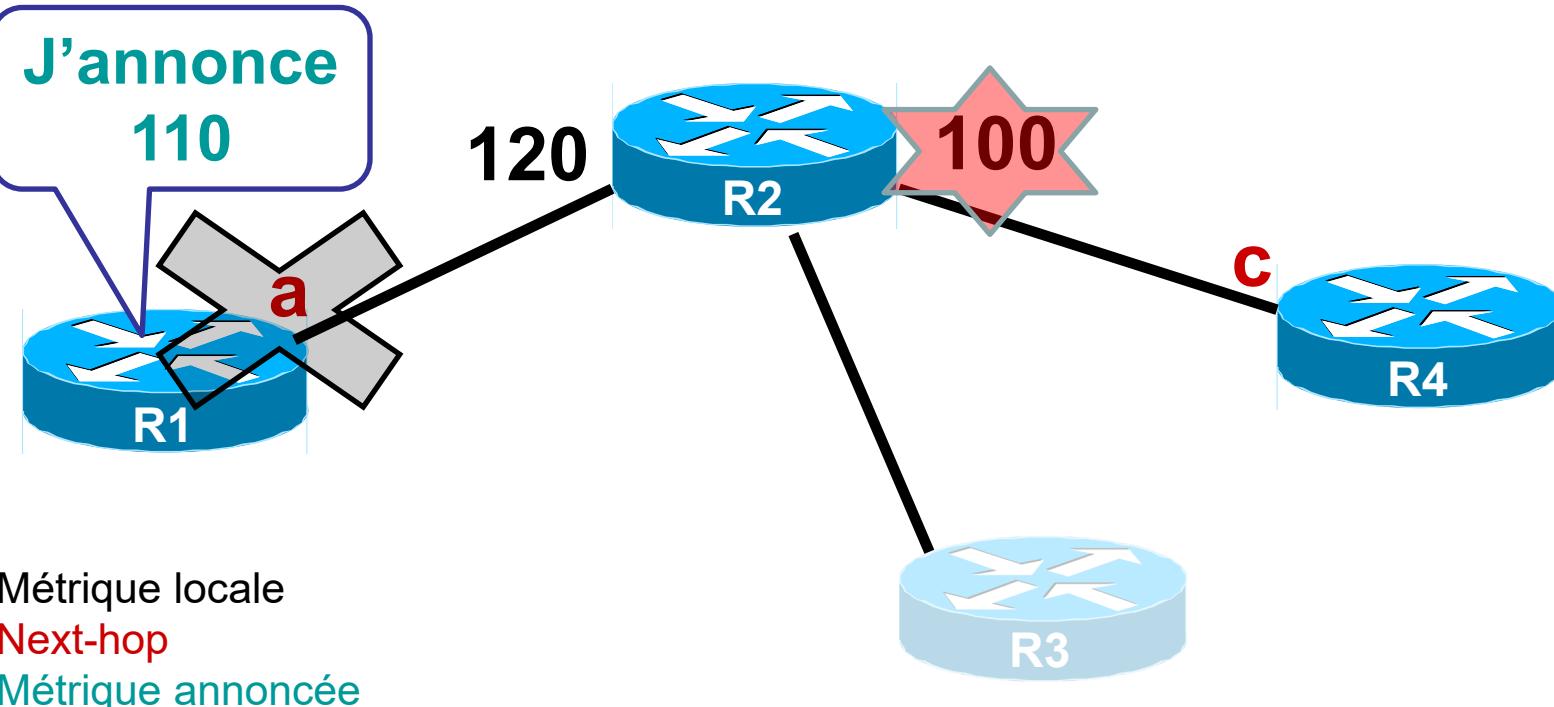


R2 analyse les annonces reçues



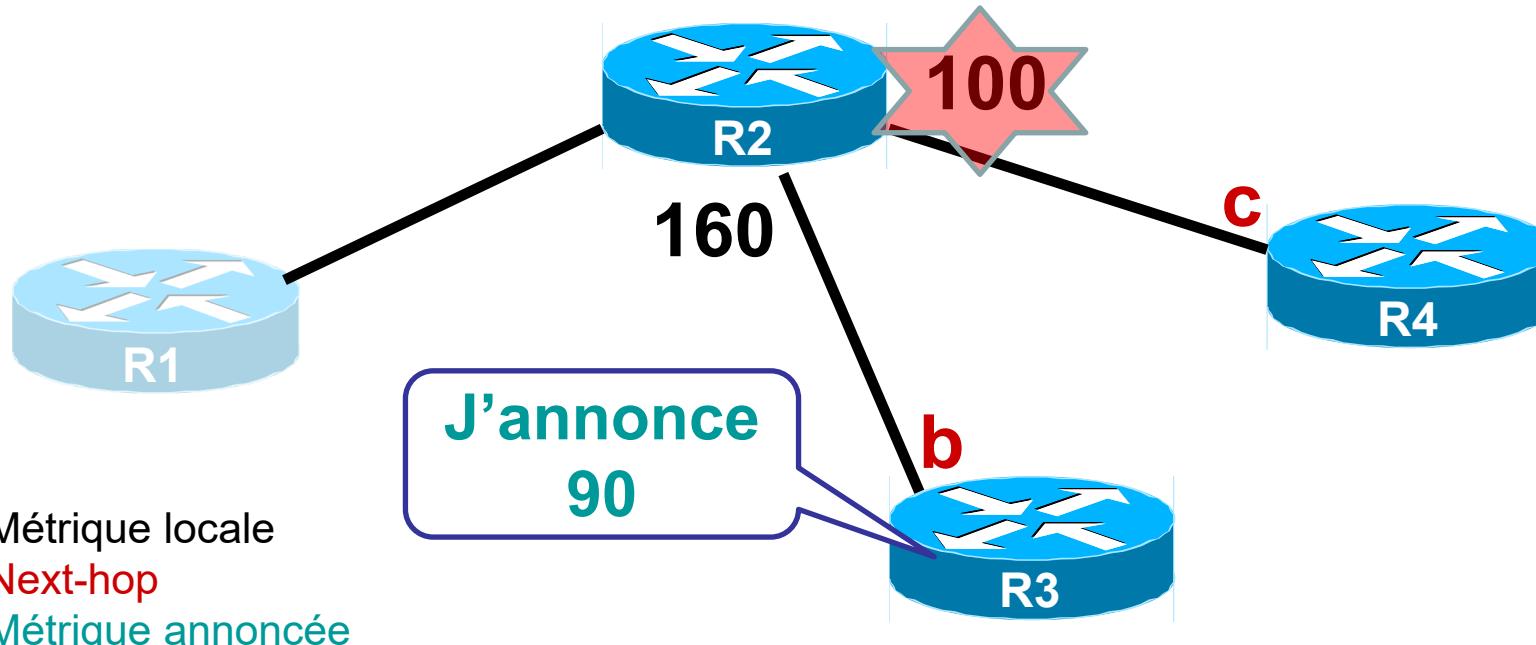
R1 **annonce** à R2 une métrique de **110**.
R3 **annonce** à R2 une métrique de **90**

R1 est-il éligible ?



$110 > \star 100$
DONC RISQUE de BOUCLE !

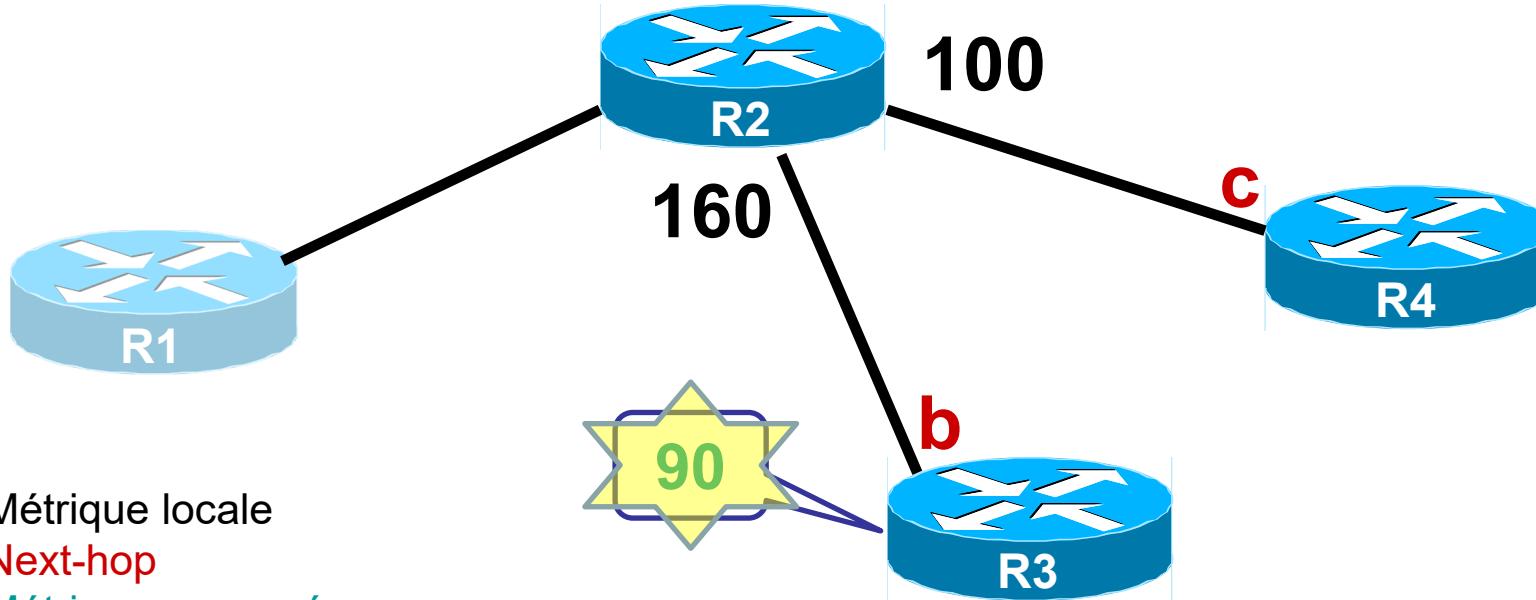
R2 analyse les annonces reçues



90 < 100

DONC R3 est plus PROCHE que MOI !

Terminologie DUAL : RD & FS



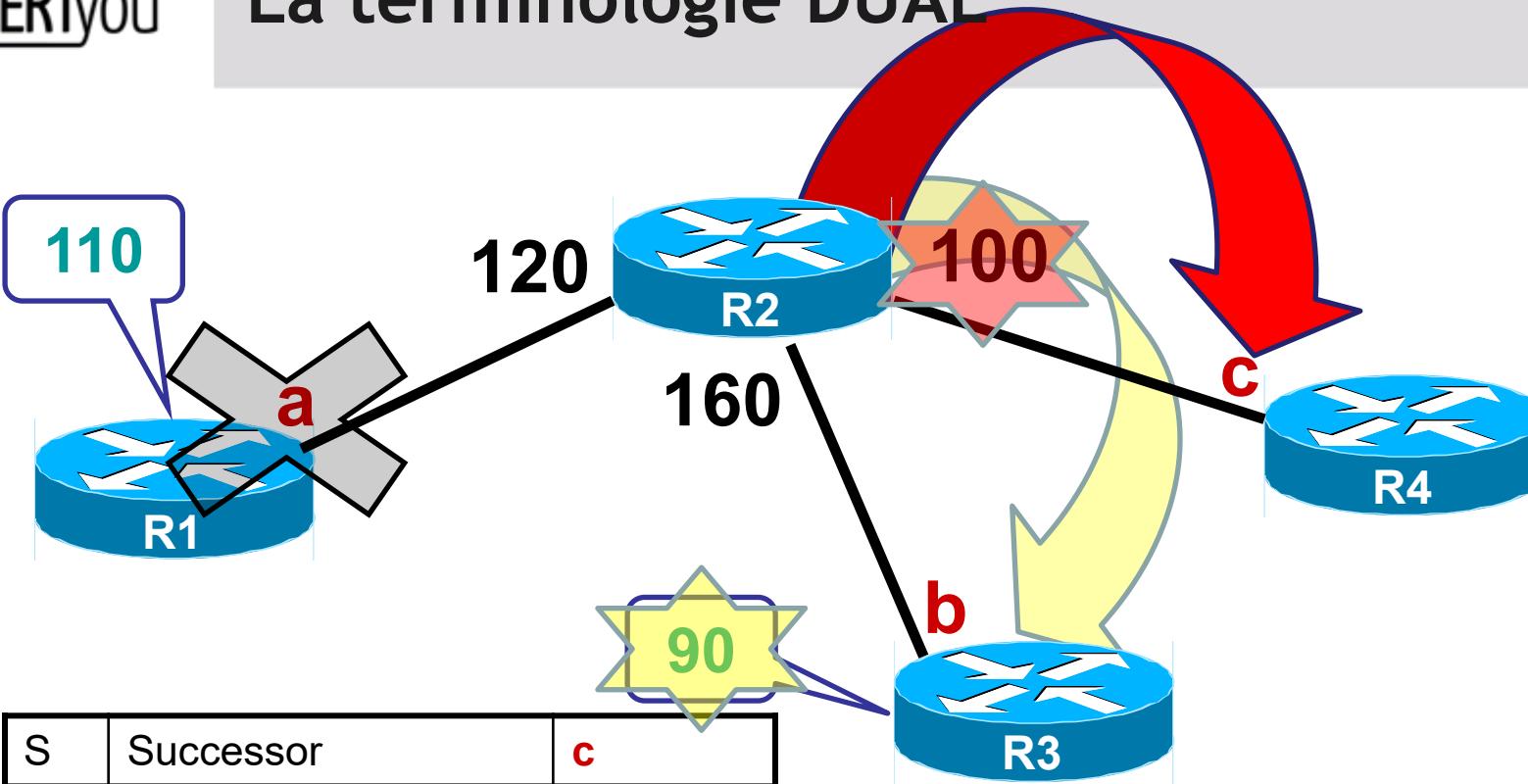
R3 sera mon BACK UP

(Feasible Successor = b)

car il est plus proche que moi

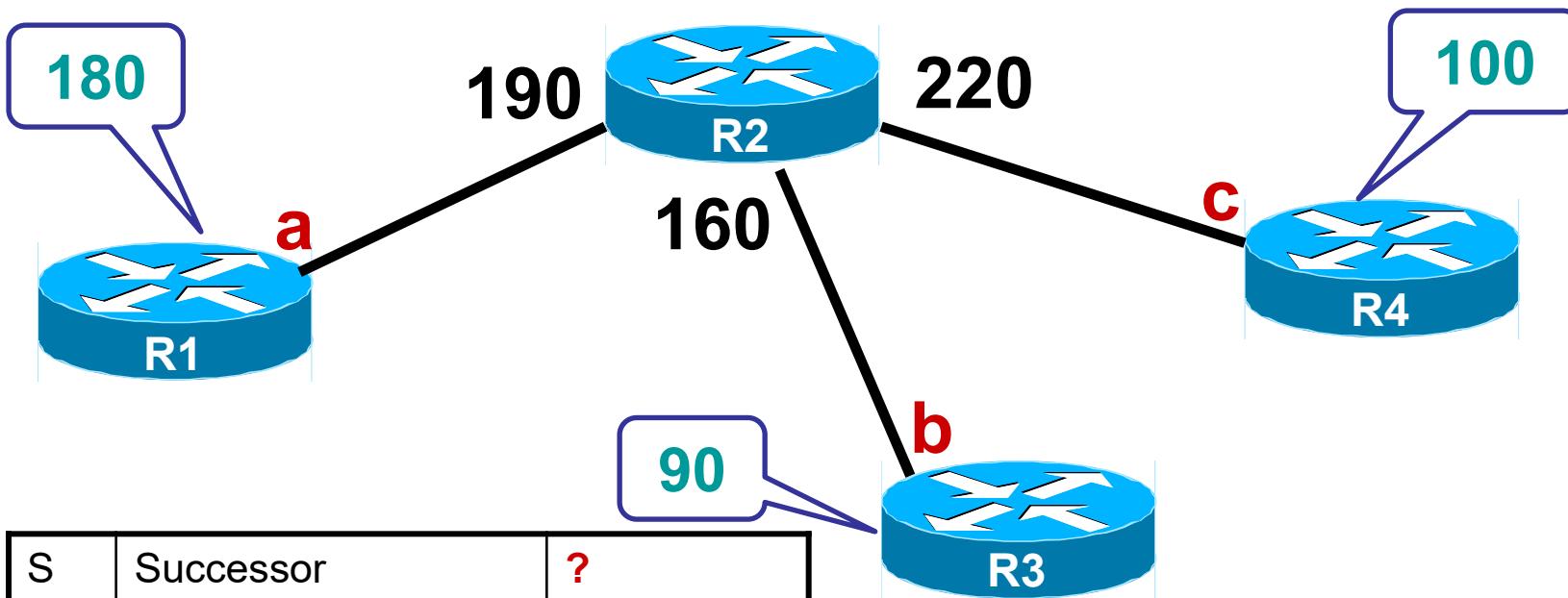
(Reported Distance = 90 < 100)

La terminologie DUAL



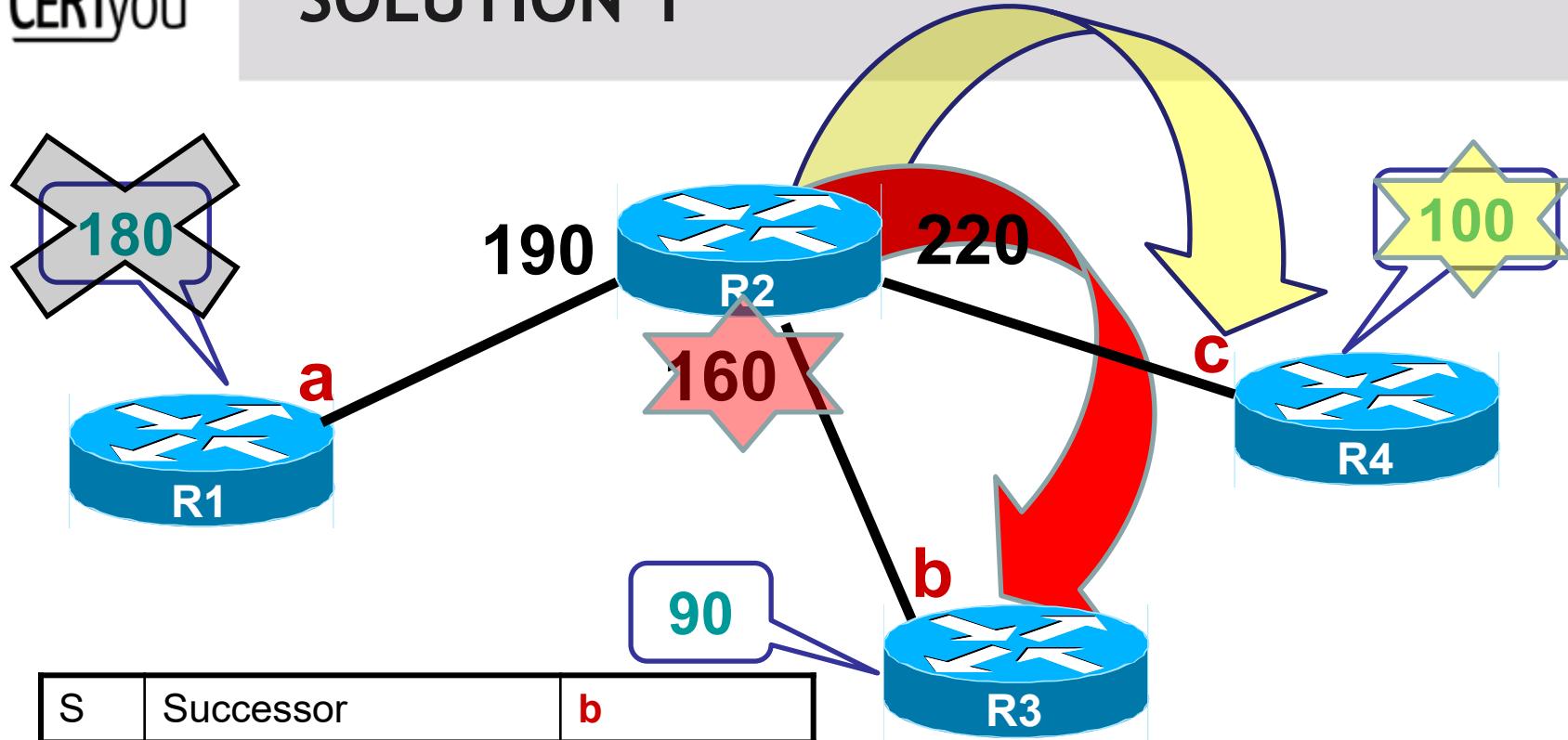
S	Successor	c
FS	feasible successor	b
FD	feasible distance	100
RD	Reported distance	90
FC	Feasible condition	$90 < 100$

Exercice 1



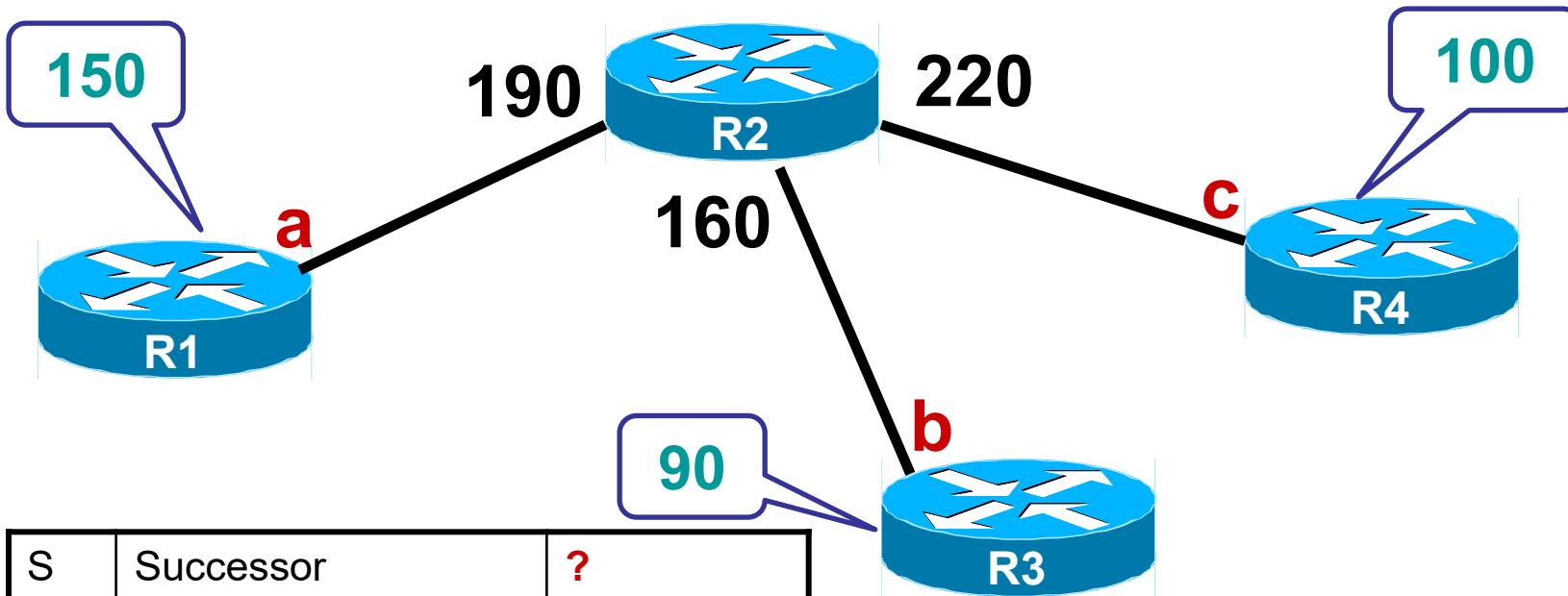
S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

SOLUTION 1



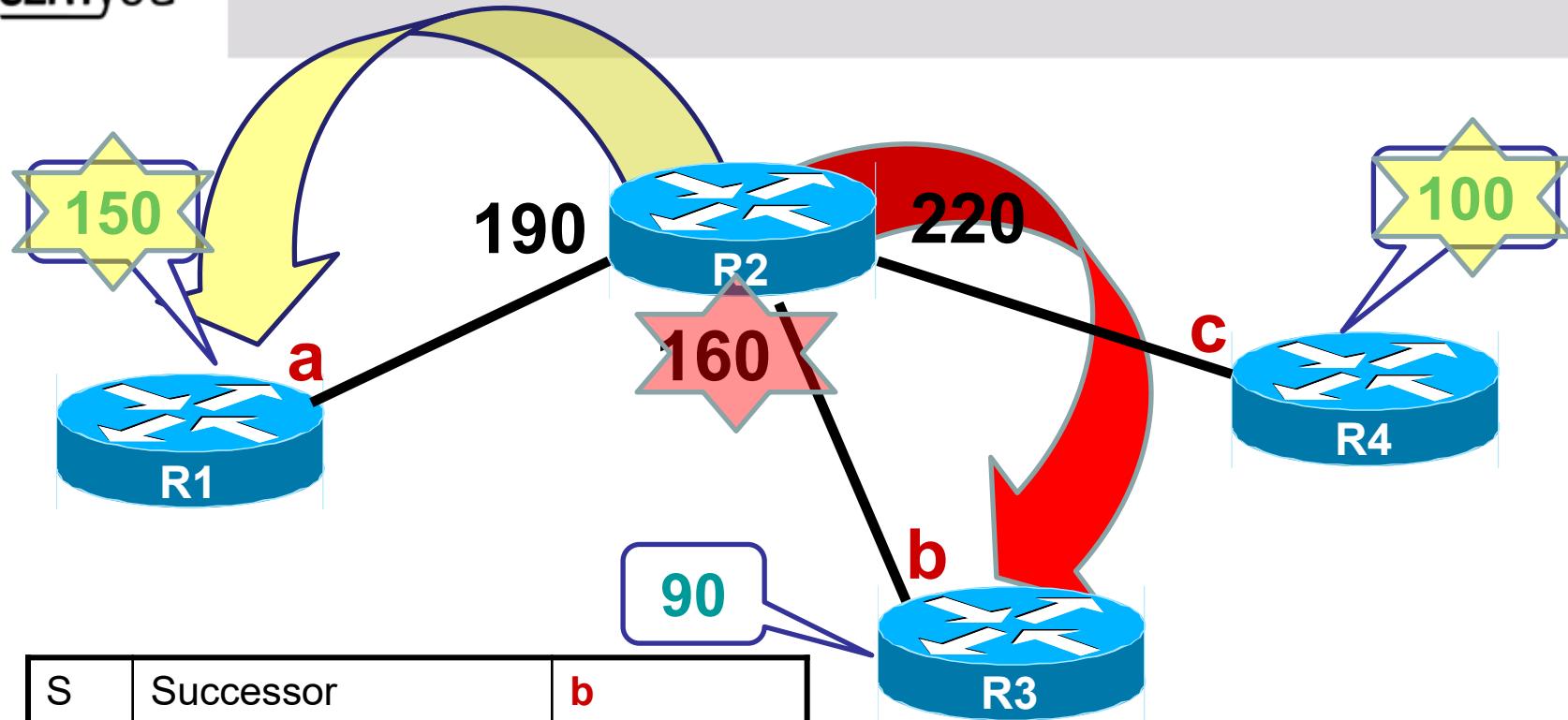
S	Successor	b
FS	Feasible successor	c
FD	Feasible distance	160
RD	Reported distance	100
FC	Feasible condition	$100 < 160$

Exercice 2



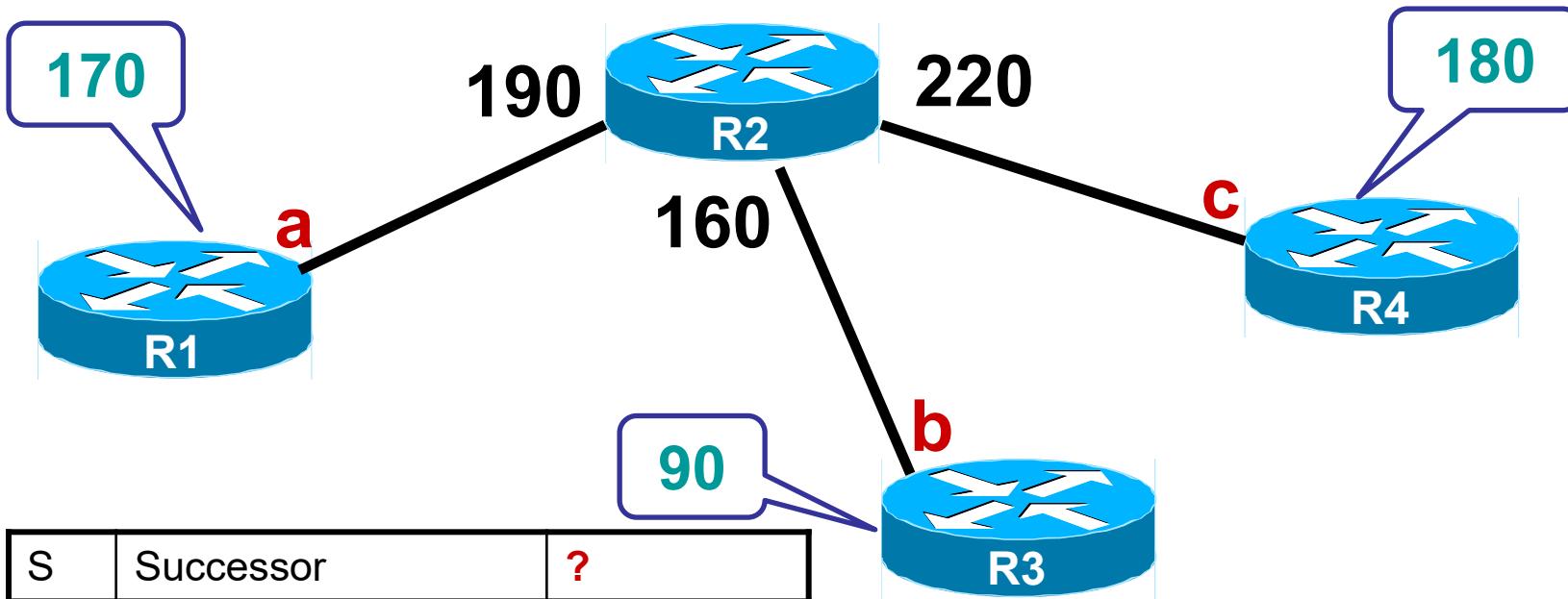
S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

SOLUTION 2



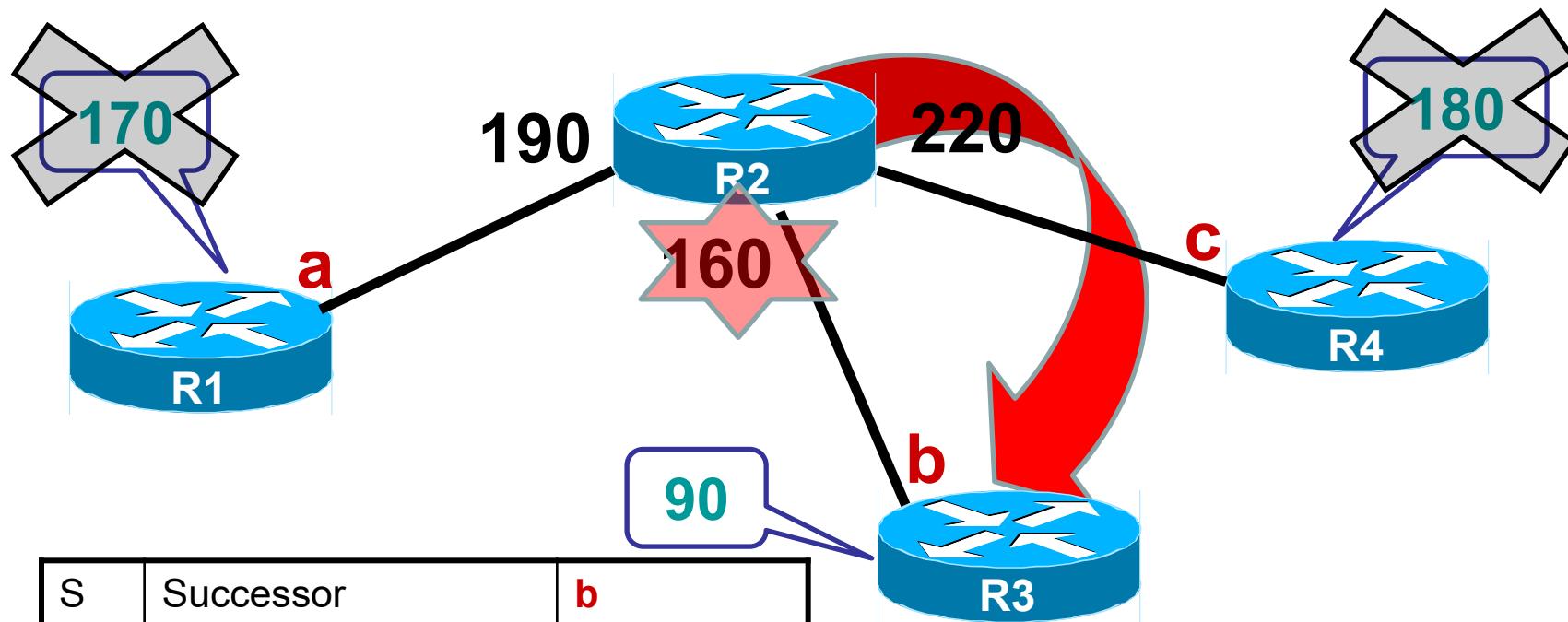
S	Successor	b
FS	Feasible successor	a
FD	Feasible distance	160
RD	Reported distance	150
FC	Feasible condition	$150 < 160$

Exercice 3



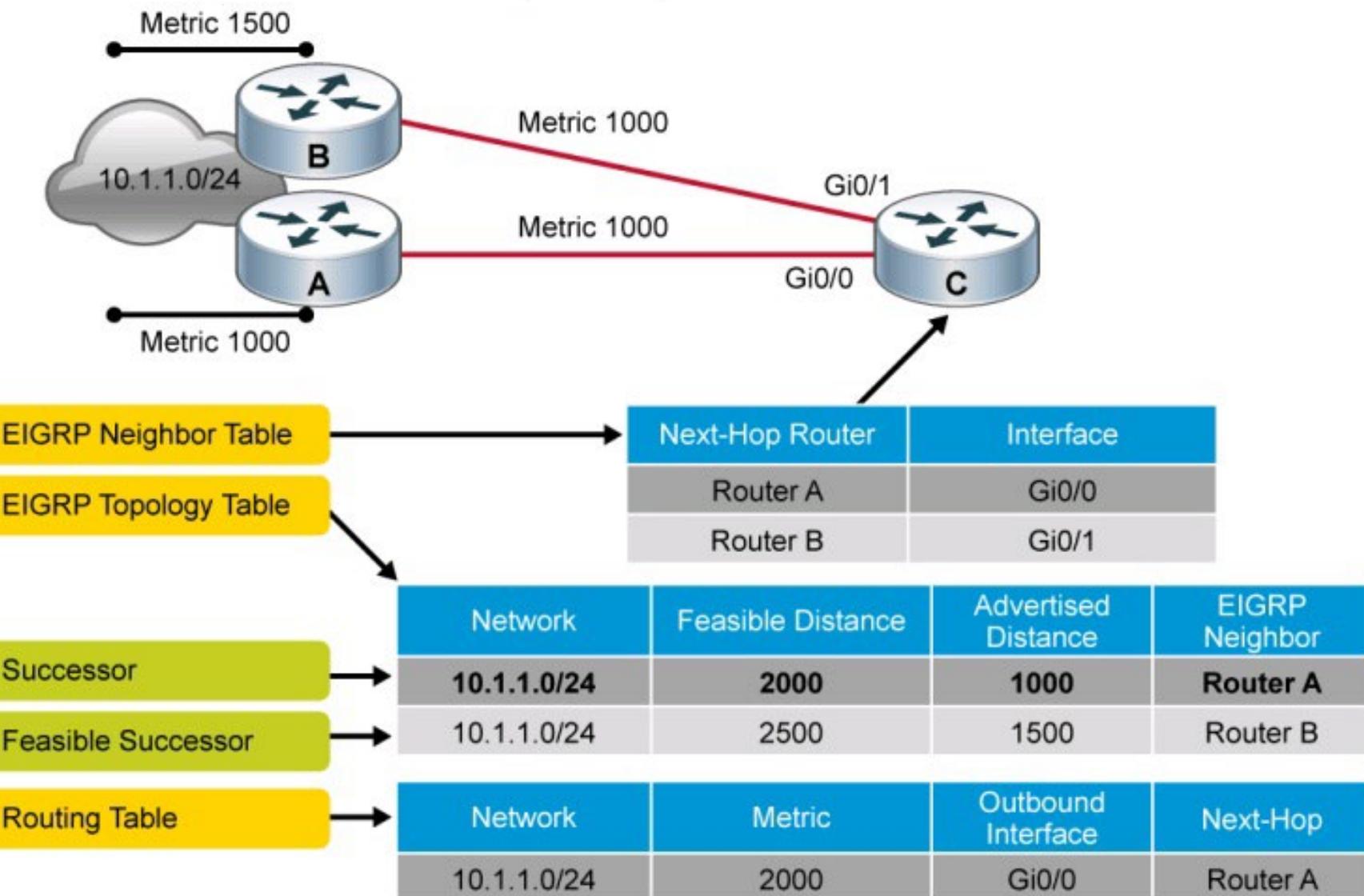
S	Successor	?
FS	Feasible successor	?
FD	Feasible distance	?
RD	Reported distance	?
FC	Feasible condition	?

SOLUTION 3



S	Successor	b
FS	Feasible successor	AUCUN
FD	Feasible distance	160
RD	Reported distance	-
FC	Feasible condition	-

EIGRP Path Selection (Cont.)



Successseurs 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

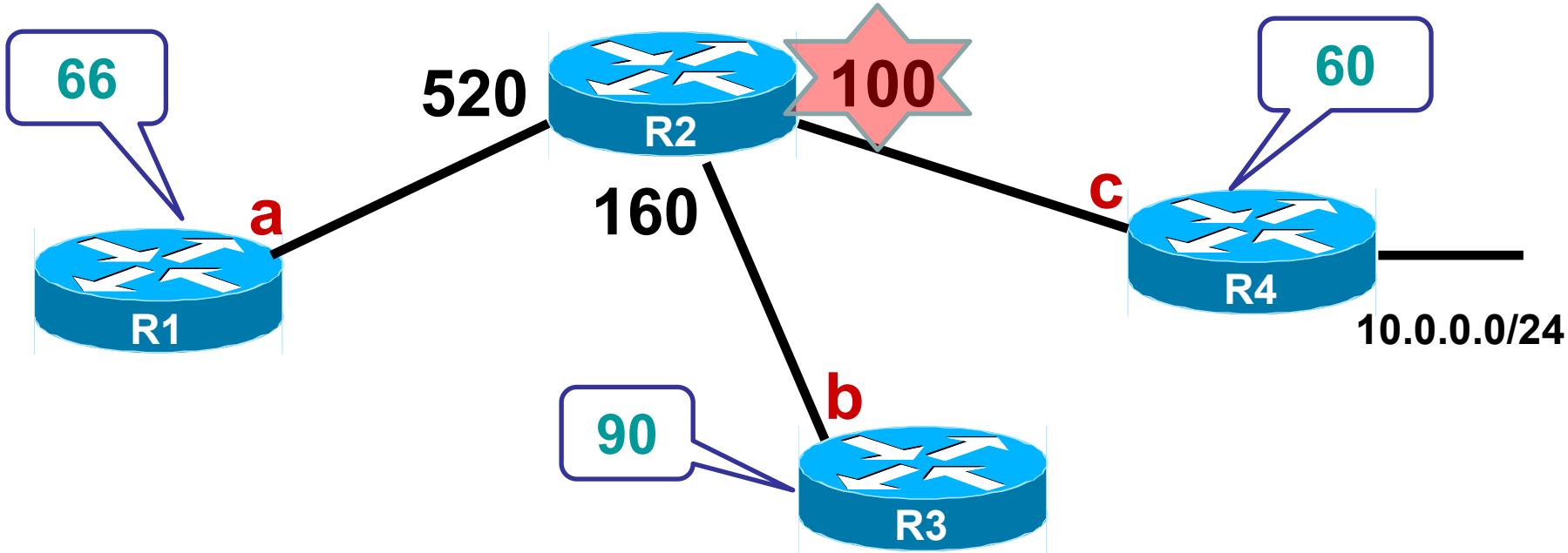
Variance

Par défaut EIGRP ne fait pas de partage de charge à métriques inégales : **variance = 1**.

Pour faire du partage de charge à métriques inégales :

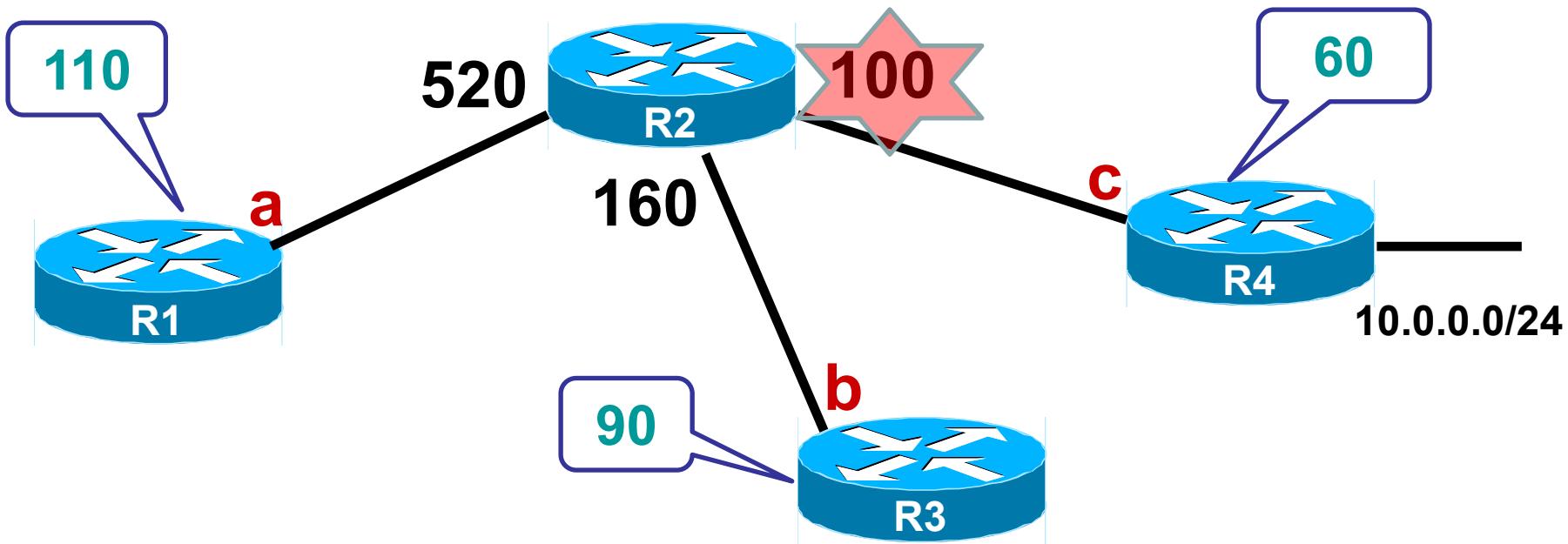
- configurer la variance à **V > 1**
- permet d'utiliser tout chemin qui est V fois moins bon que mon meilleur chemin
- la commande `maximum-path` contrôle le nombre maximum de chemins injectés dans la table de routage

Variance



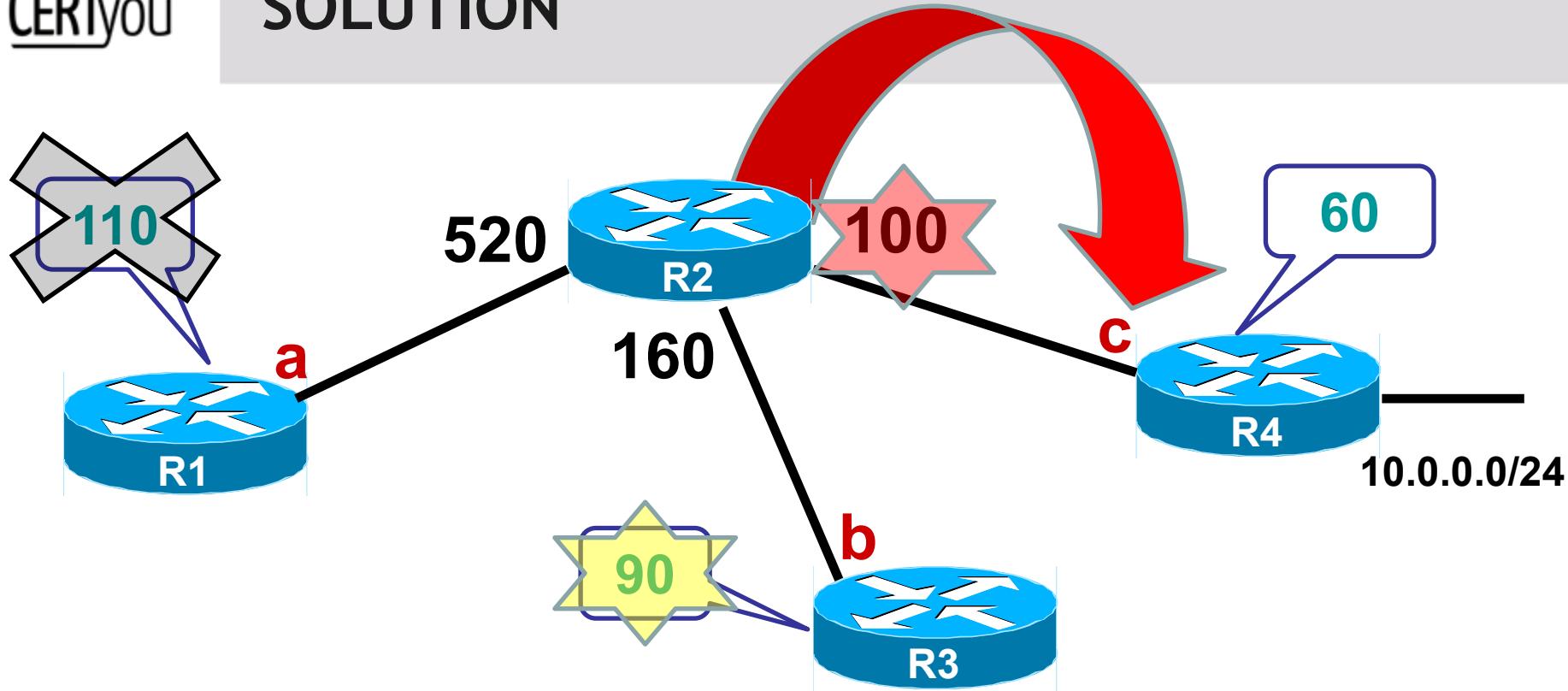
- Variance = 1 → NEXT-HOP **c**
- Variance = 2 → NEXT-HOP **c, b**
- Variance = ? → NEXT-HOP **c, b, a**

Exercice



- Variance = 1 → NEXT-HOP ?
- Variance = 2 → NEXT-HOP ?
- Variance = 6 → NEXT-HOP ?

SOLUTION



- Variance = 1 → NEXT-HOP c
- Variance = 2 → NEXT-HOP b, c
- Variance = 6 → NEXT-HOP b, c

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 »

Vérifier le partage de charge

```
Show ip route 10.0.0.88
```

Routing entry for 10.0.0.0/24

Known via "eigrp 1", distance 90, metric 409856, type internal

Redistributing via eigrp 1

Last update from 13.1.1.3 on FastEthernet0/0, 00:10:58 ago

Routing Descriptor Blocks:

13.1.1.3, from 13.1.1.3, 00:10:58 ago, via FastEthernet0/0

Route metric is **460800**, **traffic share count is 71**

Total delay is 8000 microseconds, minimum bandwidth is 10000 Kbit

Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 2

* **12.1.1.2**, from 12.1.1.2, 00:10:58 ago, via FastEthernet0/1

Route metric is **409856**, **traffic share count is 80**

Total delay is 6010 microseconds, minimum bandwidth is 10000 Kbit

Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 2

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

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:	2021 :	0000:	0000:	00aa:	0000:	3330:	2000
OK	0011:	2021 :		:	00aa:	0000:	3330:	2000
OK	0011:	2021:	0000:	0000:	00aa :	:	3330:	2000
KO	0011:	2021 :		:	00aa :	:	3330:	2000
OK	11:	2021:	0000:	0000:	aa:	0000:	3330:	2000
KO	0011:	202 :	0000:	0000:	00aa:	0000:	333 :	2
Adresse finale	11:	2021:		:	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 :

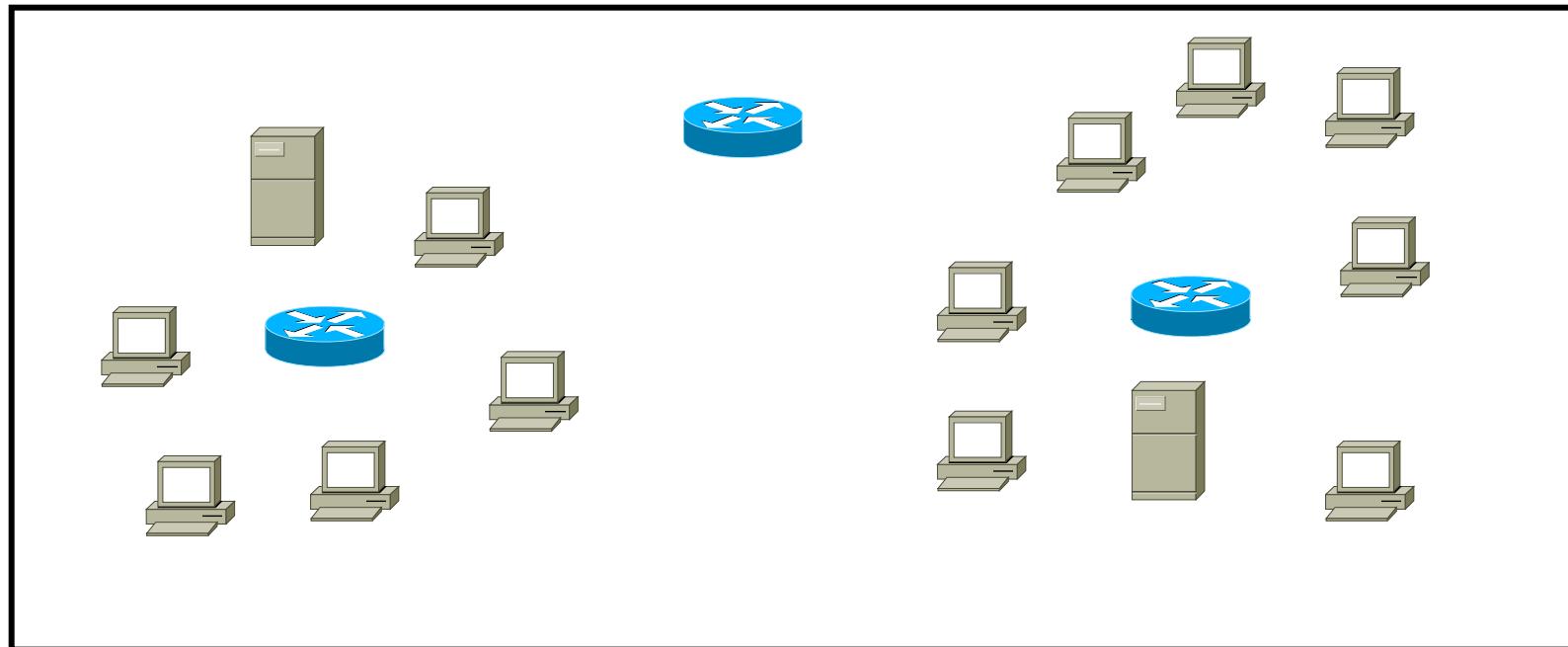
- Unicast
- Multicast
 - FF00::/8
- Anycast
 - « One-to-nearest »

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 :

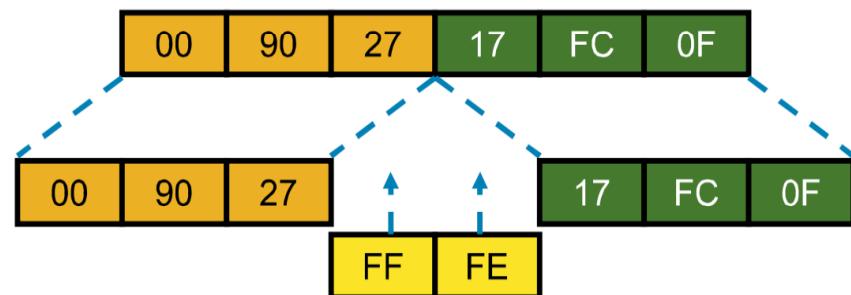
- Privées :
 - Link local = FE80::/10
 - Unique Local Address = FC::0/7
- Publiques = uniques globalement :
 - 2000::/3 =001x xxxx xxxx xxxx ::
- ::1 = adresse de loopback
- :: = adresse non spécifiée (par exemple source de paquet DHCPv6)

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, 0:0:0:0:0:0:1, 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, 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

Ethernet MAC Address
(48 Bits)



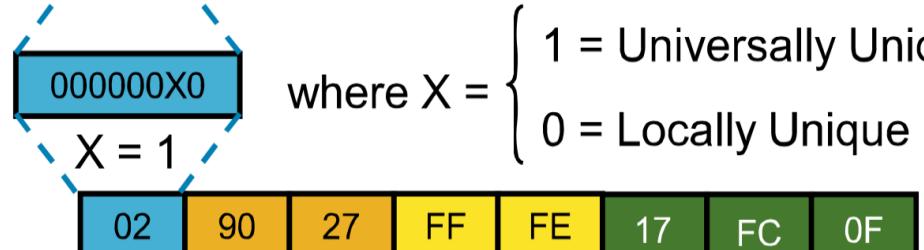
64-Bit Version



U/L Bit

where $X = \begin{cases} 1 & \text{Universally Unique} \\ 0 & \text{Locally Unique} \end{cases}$

Modified EUI-64 Address



Exemple EUI-64

Avec une Mac address **1111.2222.3333** :

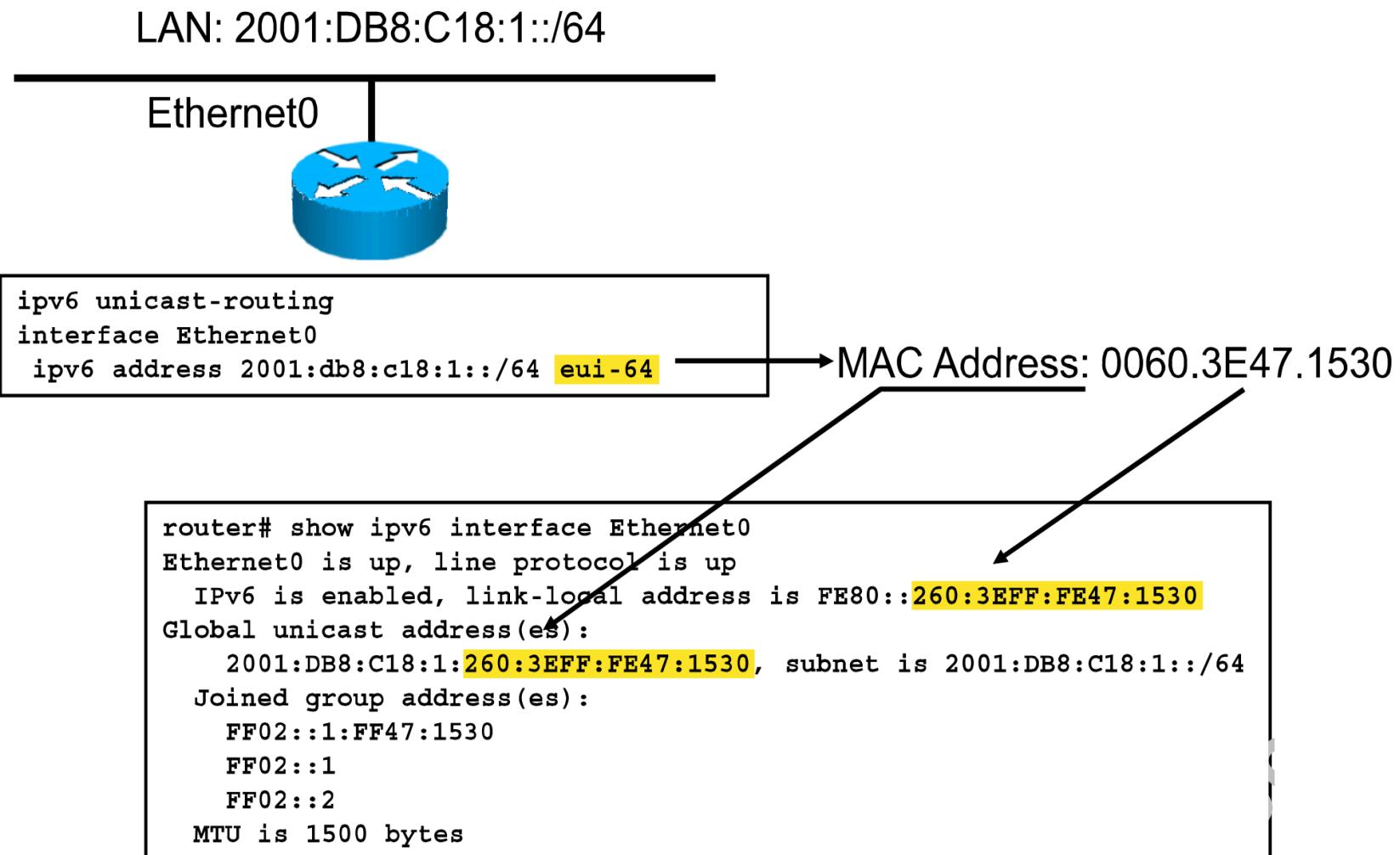
1111.22 est l' OUI = Organizational Unique Identifier

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**

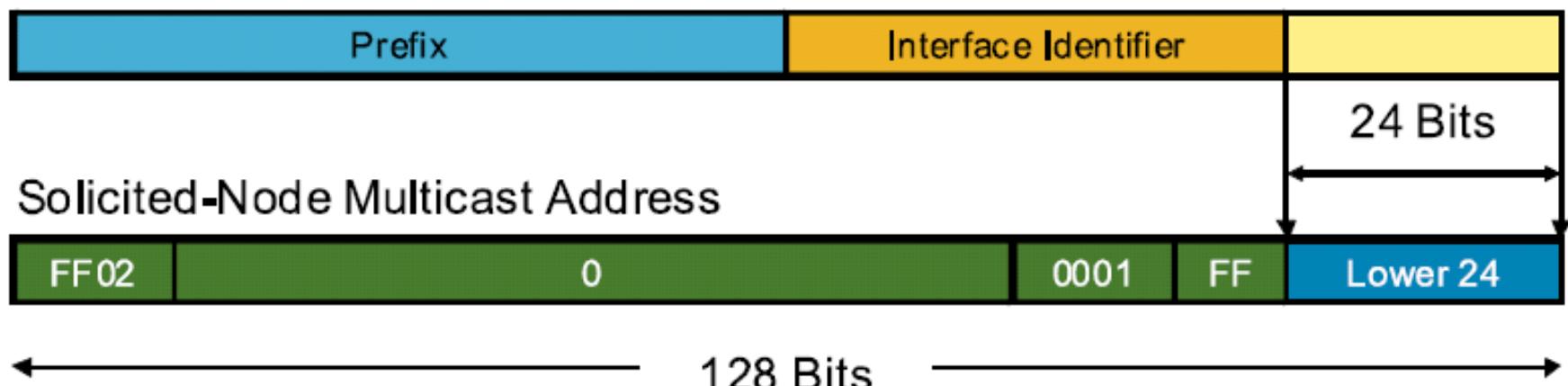
Exemple de configuration



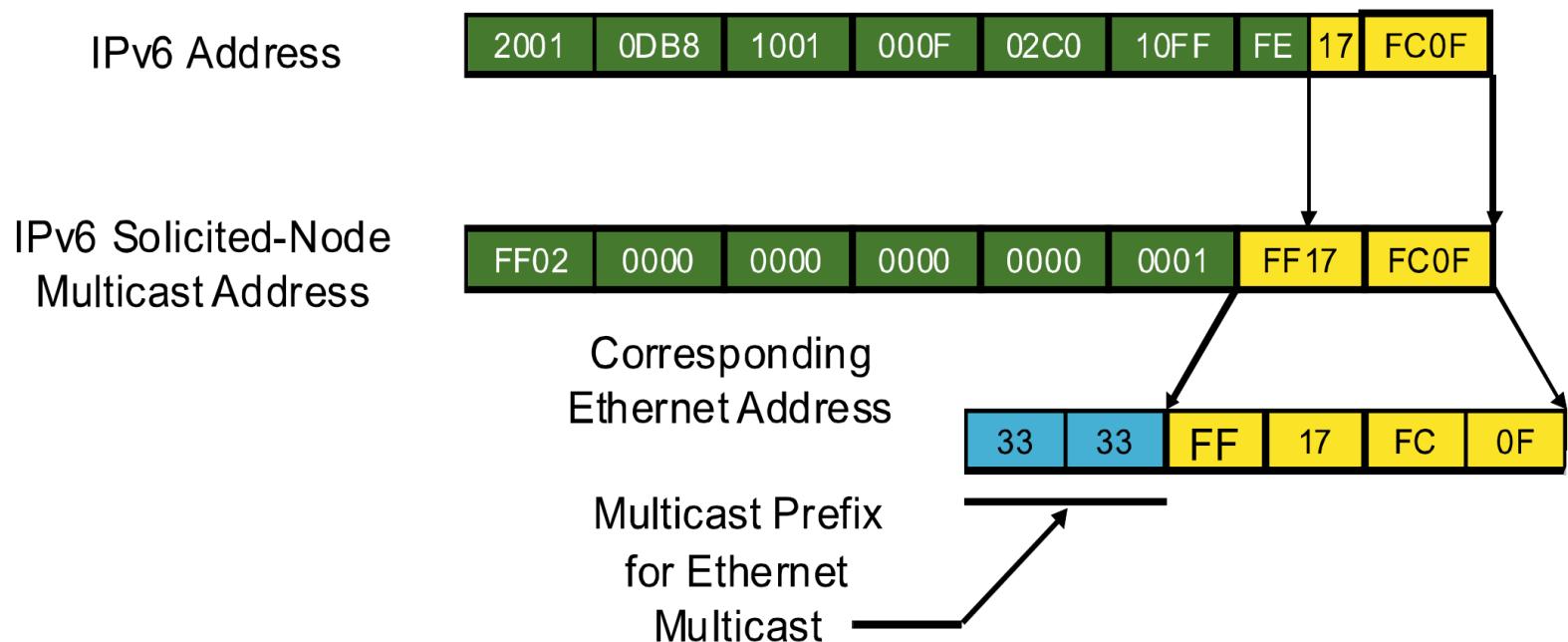
Solicited Node Multicast Address

- 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 »

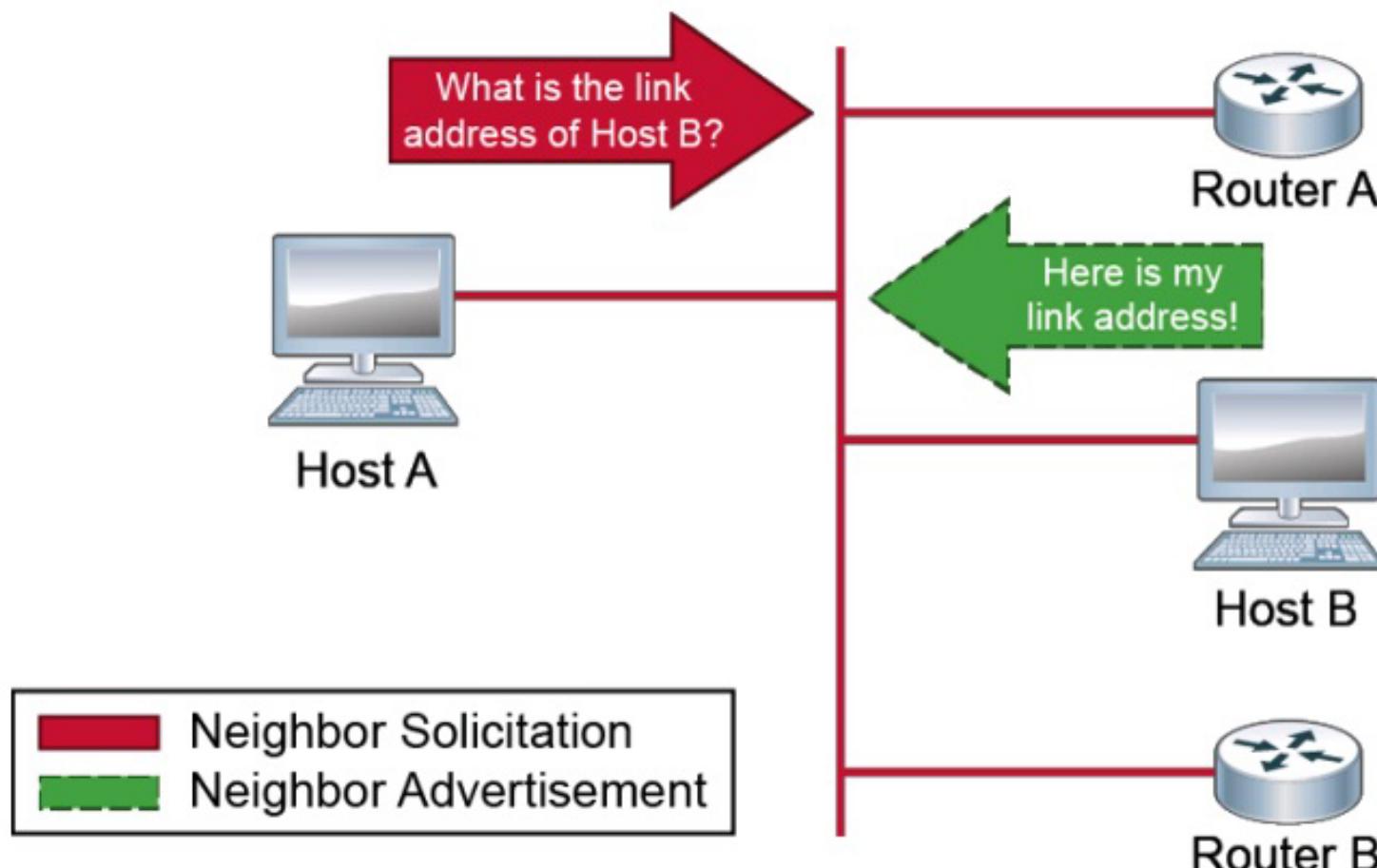
IPv6 Address



Exemple SNMA



Neighbor Discovery

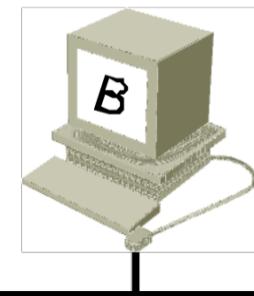
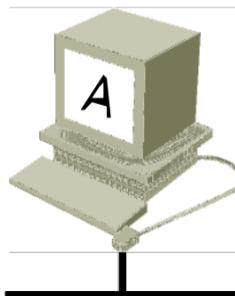


Neighbor discovery performs the same functions in IPv6 as ARP does in IPv4.

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



ICMP Type 135

Source = ::

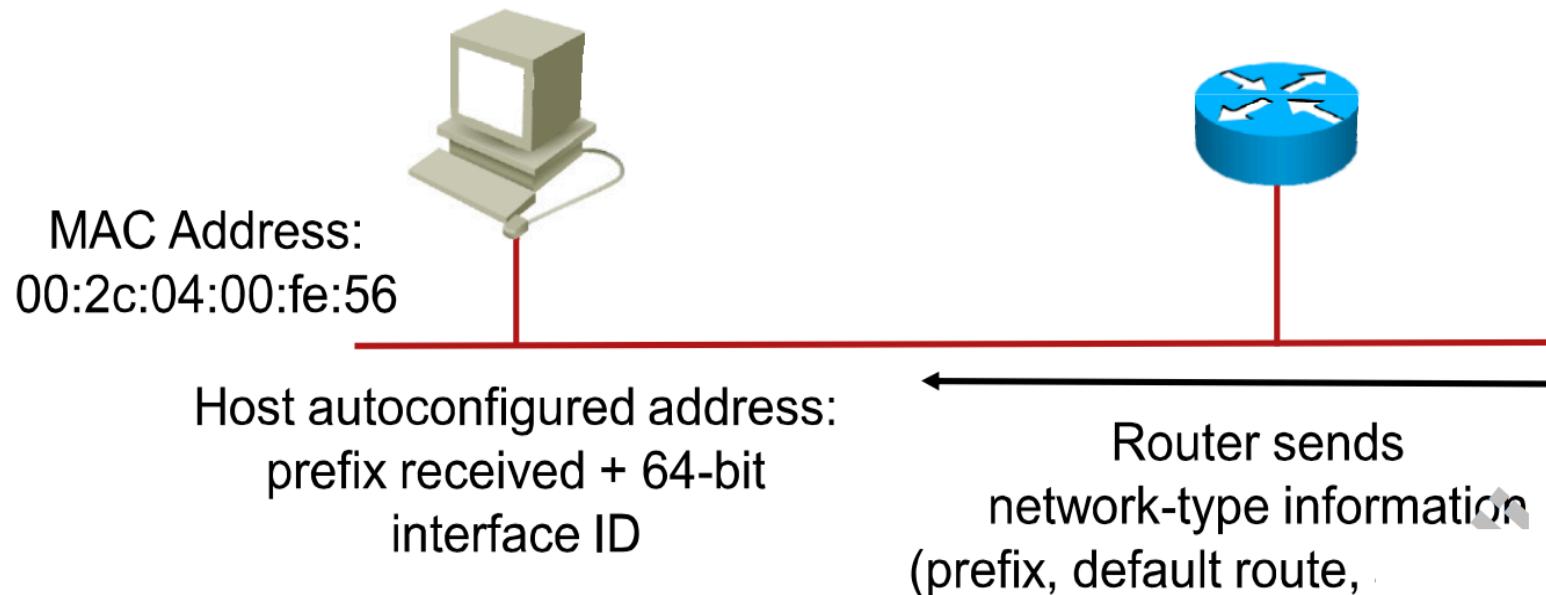
Destination = Solicited-Node Multicast Address of A

Data = Link Layer Address of A

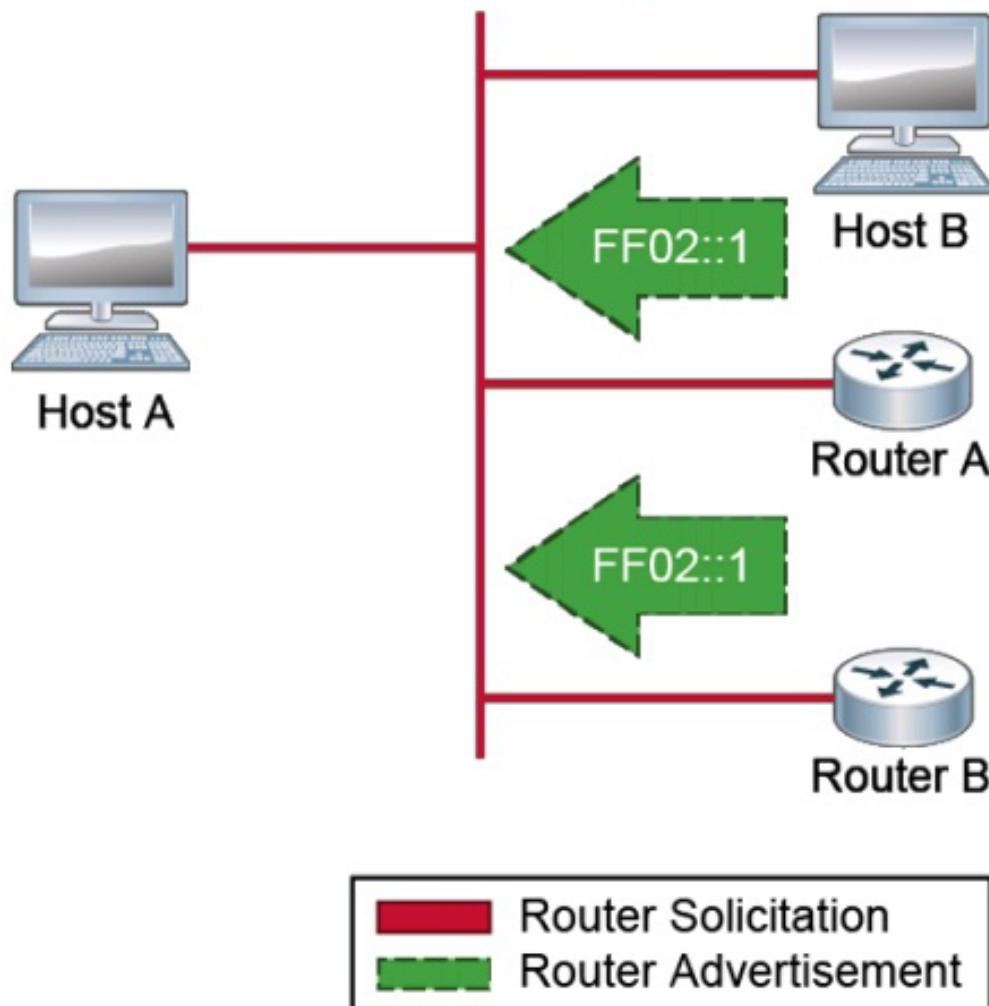
Query = What Is Your Link Address?



Stateless auto-configuration



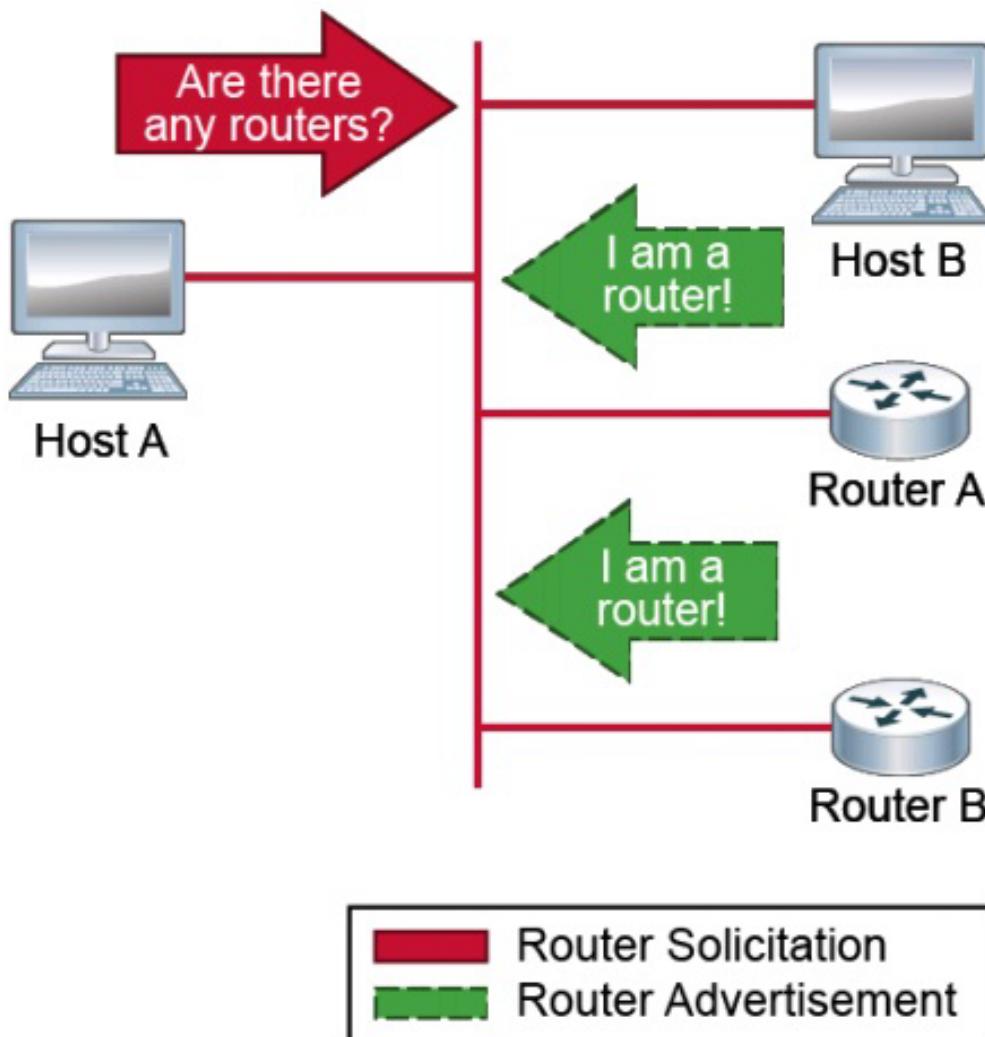
Stateless Autoconfiguration



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.)



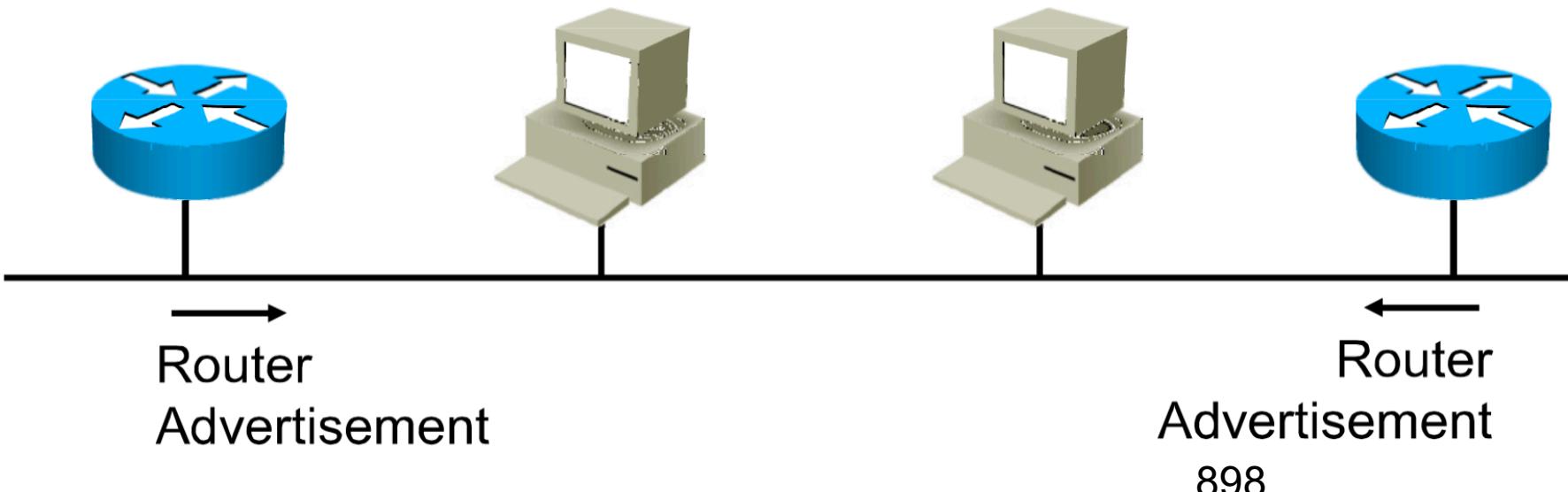
The router solicitation packet:

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

- NDP, 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**

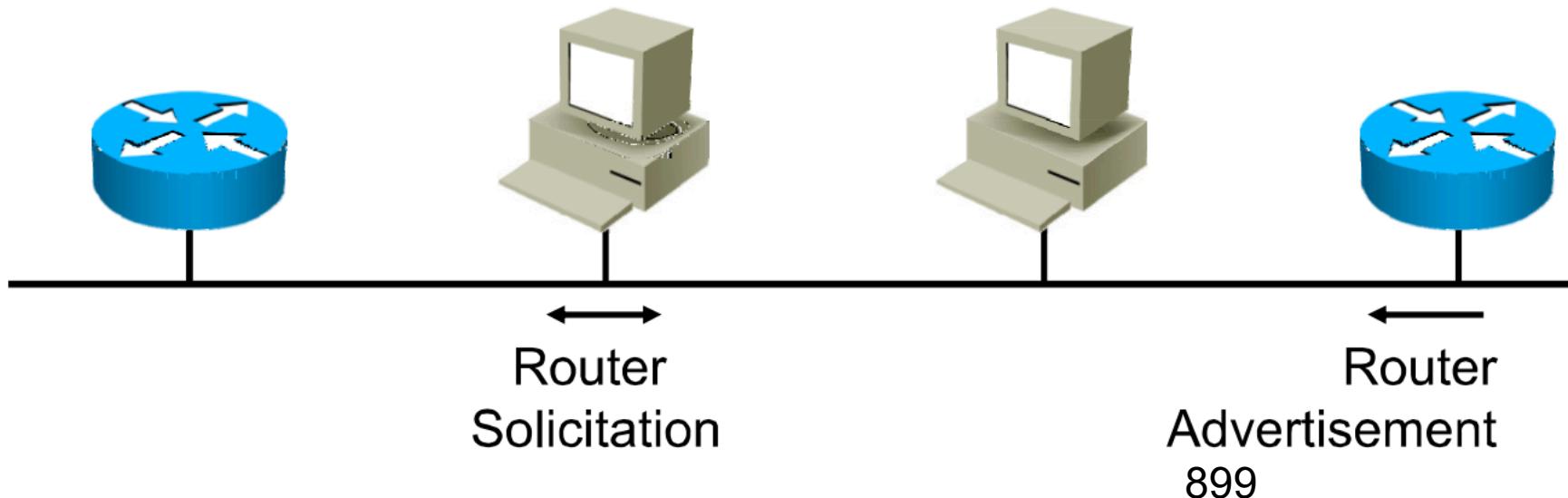
Exemple RA

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



Exemple RS

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



Bilan des méthodes de config

link-local	statique		ipv6 address FE80::1 link-local
	eui 64		<i>[automatique]</i>
routeable	statique		ipv6 address 2001:abcd::1/64
	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 traiter
 - 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

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 :

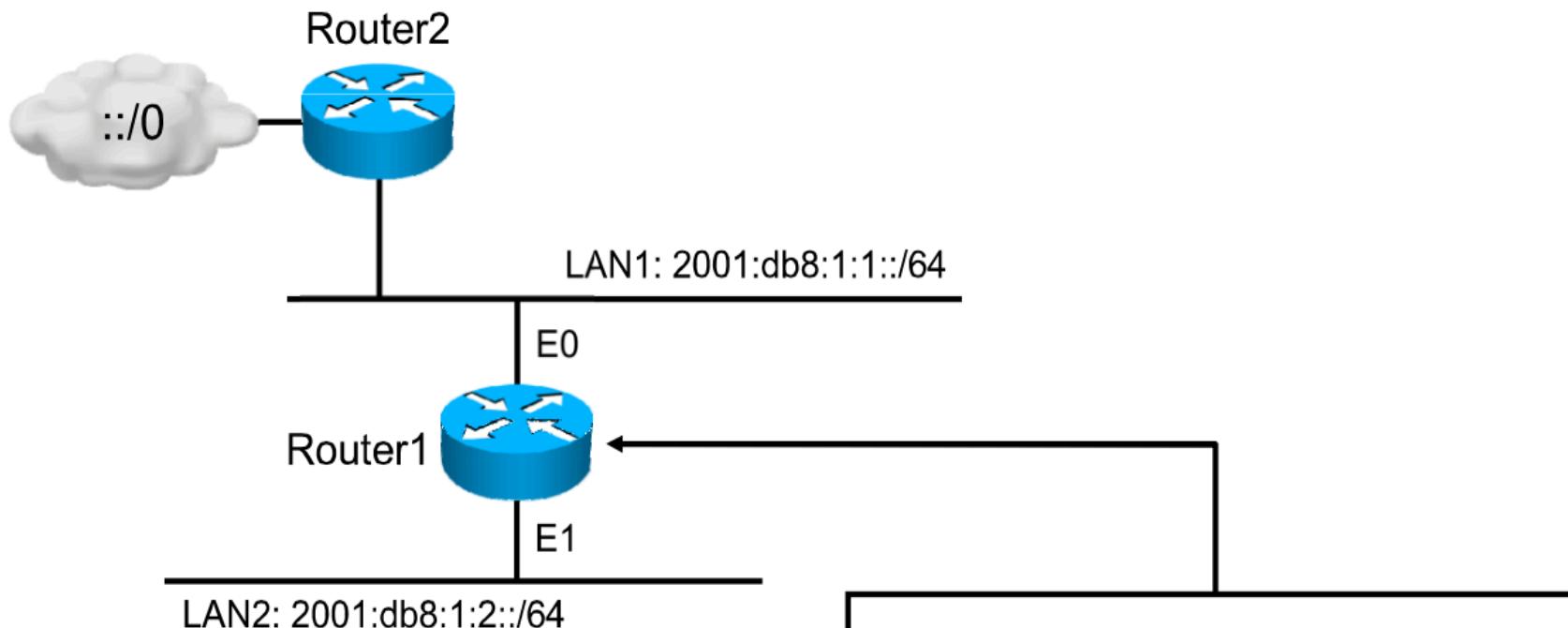
- RIPng
- OSPFv3
- EIGRP for IPv6

- 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



```
interface Ethernet0
    ipv6 address 2001:db8:1:1::/64 eui-64
    ipv6 rip RT0 enable

Interface Ethernet1
    ipv6 address 2001:db8:1:2::/64 eui-64
    ipv6 rip RT0 enable
```

- **Similaire** à OSPFv2:

- état de lien
- découverte des voisins
- AD 110
- métrique = somme des couts
- multicast FF02::5 & 6

- **Déférence** 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 = $256 * ((10^7/BW) + \text{somme (délais)})$
- 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

3 chapitres

- Comment interconnecter les équipements entre eux ?

1. Architecture du LAN
2. Architecture du WAN
3. Architecture Cloud

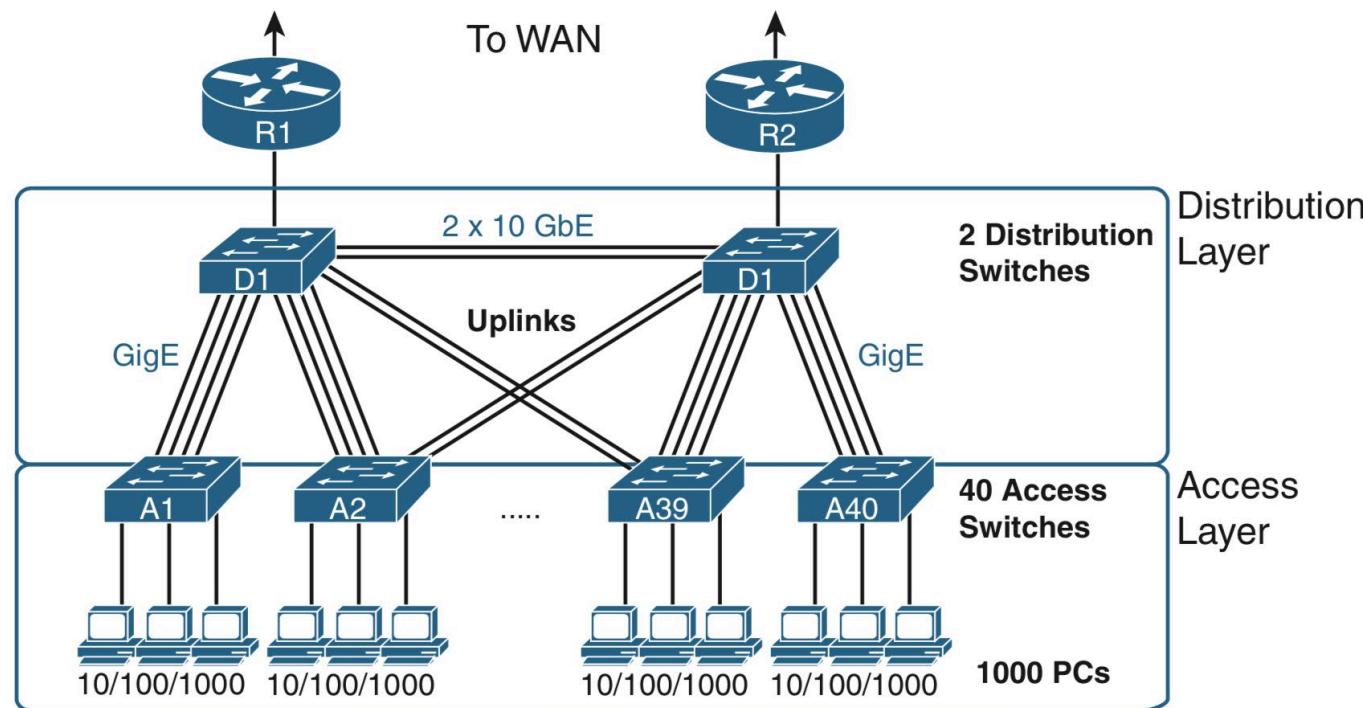
Architecture du LAN

Architecture du LAN

1. Topologie des réseaux câblés LAN:
 - Deux niveaux, « Two Tier »
 - Trois niveaux, « Three Tier »
 - selon le nombre de couches entre les hôtes et le routeur de sortie du campus
2. SOHO, « Small Office Home Office »
3. PoE, « Power Over Ethernet »

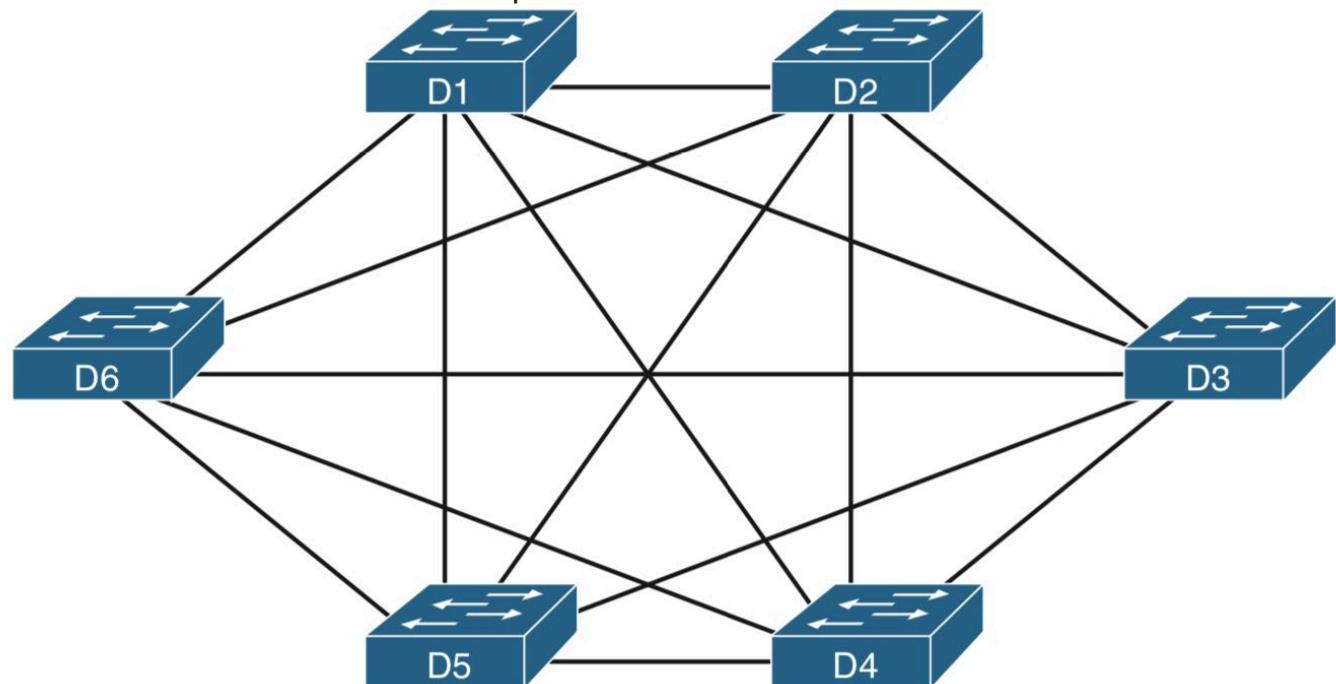
Two-Tier Design

- « **Collapsed core** »
 - Premier niveau : switch d'accès
 - Second niveau : switch de distribution



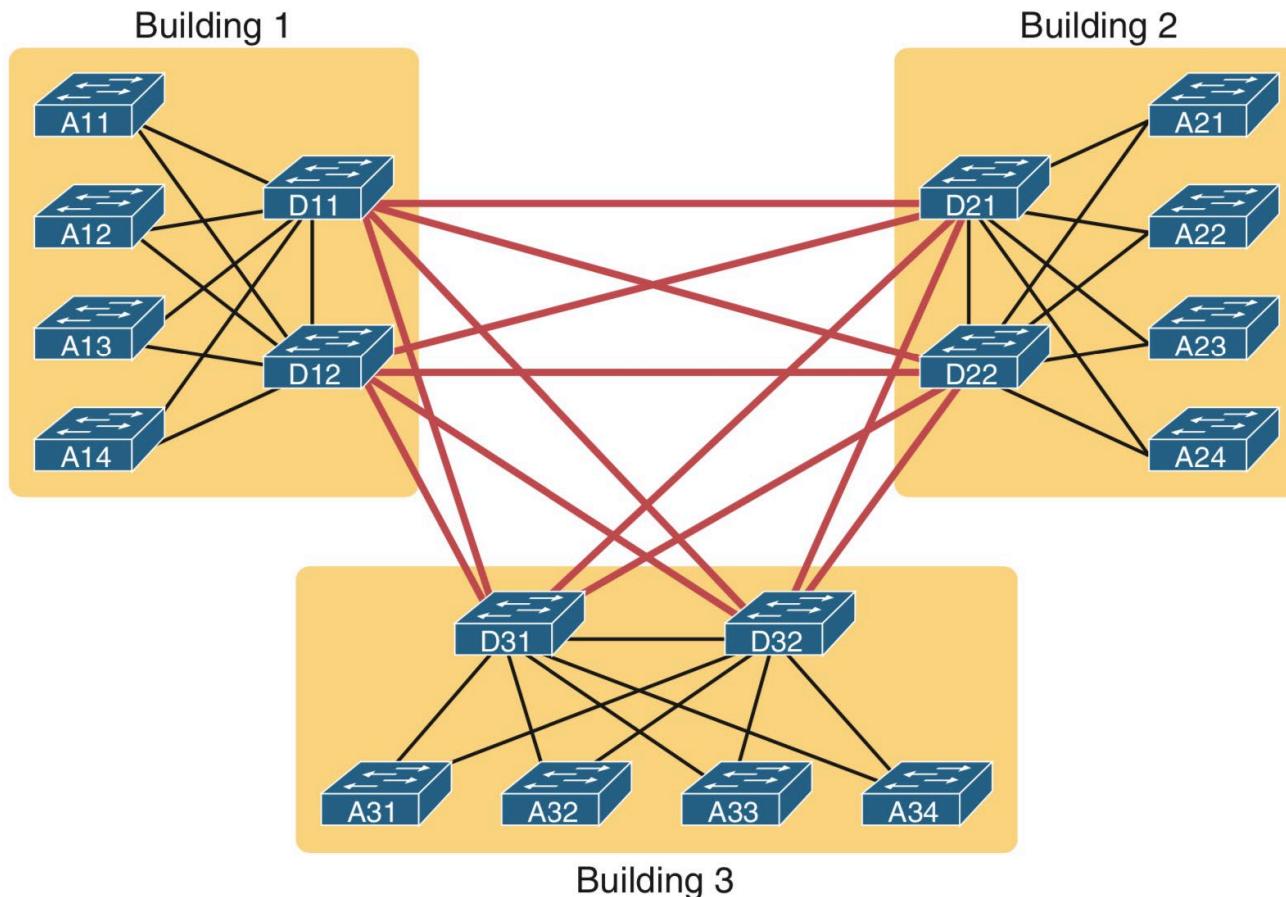
Two-Tier **vs** Full-mesh

- Avantage principal :
 - interconnecter tous les switch en **réduisant** le nombre de liens
 - comparatif pour 1000 PC et 40 switch
 - « 2-tier » : 40×2 uplink = 80 liaisons ou 160 ports
 - « full-mesh » : $40 \times 39 / 2$ = 780 liaisons ou 1560 ports
- « Full-mesh » :



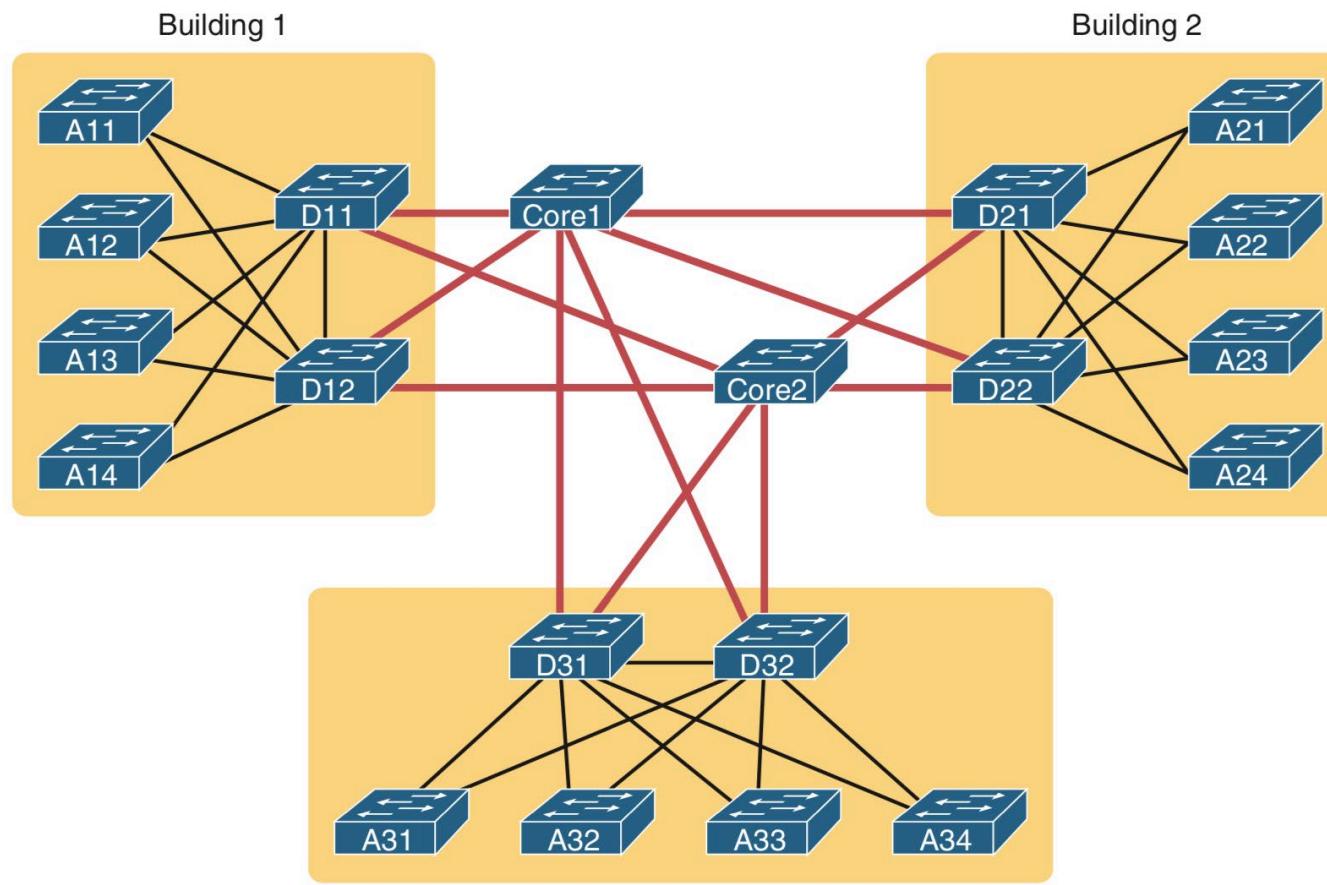
Two-Tier Design

- Entre 3 bâtiments :



Three-Tier Design

- Entre 3 bâtiments :



Three-Tier Design

- Avantages :
 - réduire le nombre de liaisons entre distribution
 - liaisons à haut débit
 - installation coûteuse

Architecture Cloud

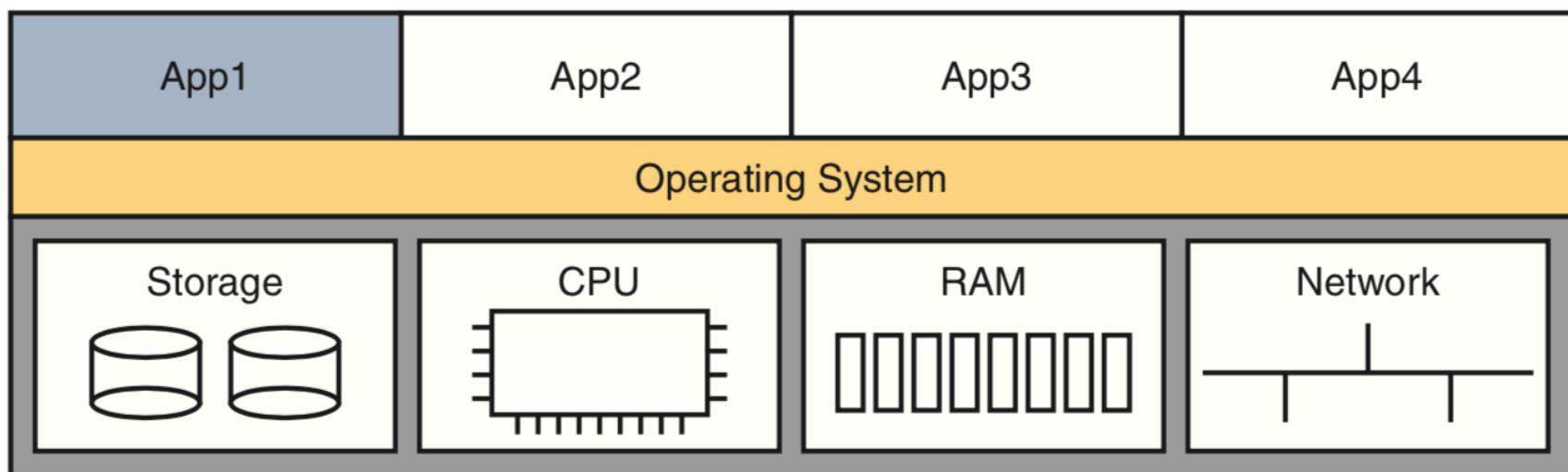
Serveur

- Définition :
 - équipement sur lequel tourne une application, à laquelle accèdent des utilisateurs
- Caractéristiques :
 - **No KVM**
 - « No Keyboard, Video display, Mouse »
 - **Rack**
 - pour réduire l'espace occupé
- Exemple :
 - **Cisco UCS**, « Unified Computing System »
 - Exemple : 4 unités de rack - 8 blades



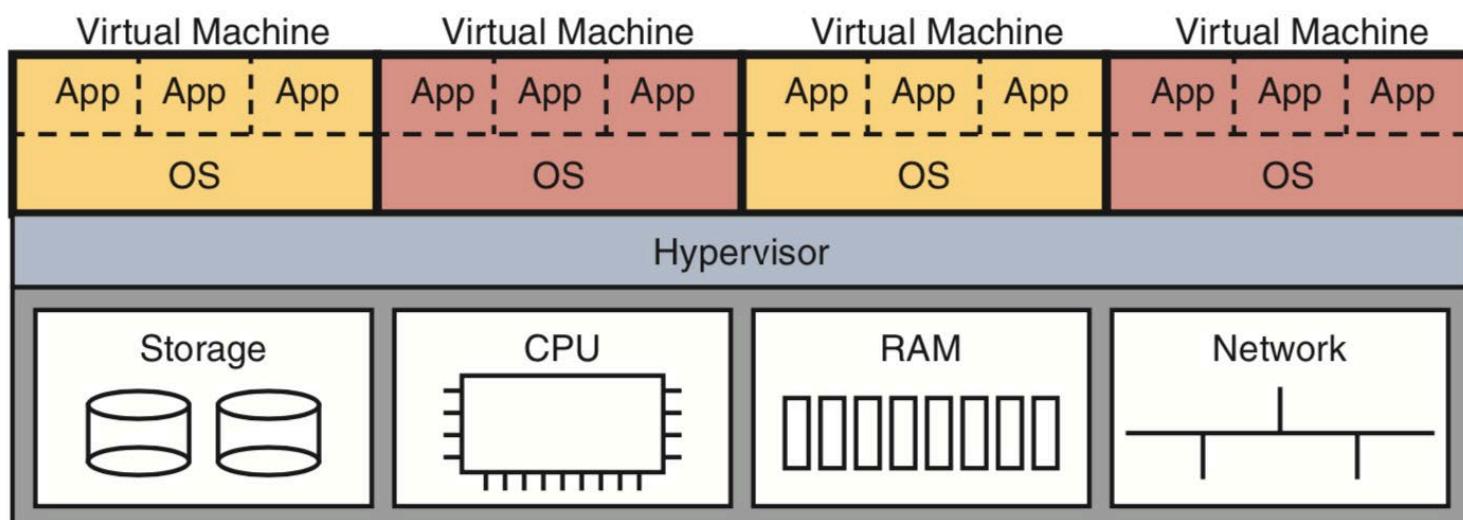
Schéma d'un serveur

- Un seul OS :
 - qui accède à l'ensemble des **ressources hardware**
 - sur lequel tournent les applications



Virtualisation d'un serveur

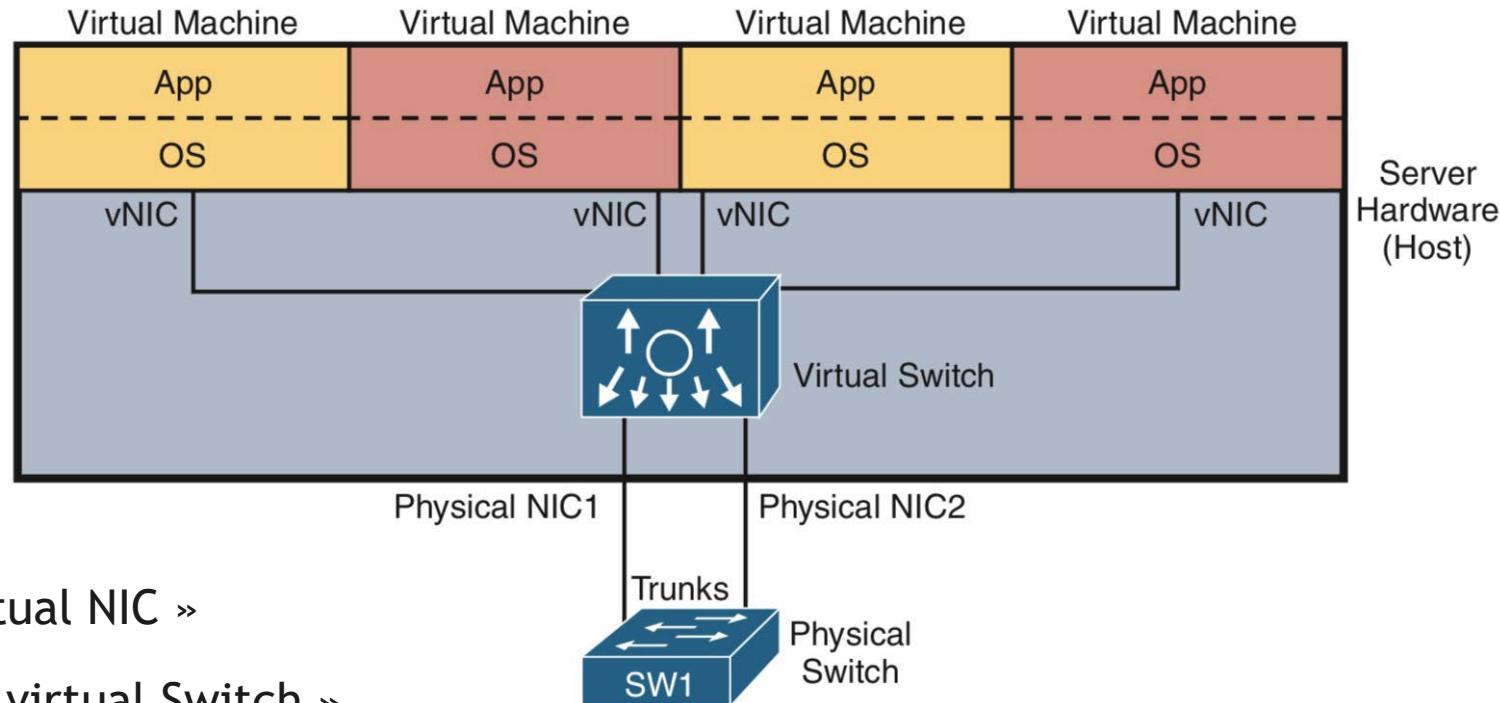
- Virtualiser :
 - Plusieurs OS exploitent les mêmes ressources hardware
- **VM**, « Virtual Machine » : une instance d'OS
- « **Host** » : la machine physique
- « **Hyperviseur** » : manage les VM
 - alloue les ressources à chaque VM



Exemples

- VMware vCenter
- Microsoft HyperV
- Citrix XenServer
- Red Hat KVM
- Hyperviseur permet de :
 - créer une VM
 - modifier une VM
 - déplacer une VM
 - supprimer une VM

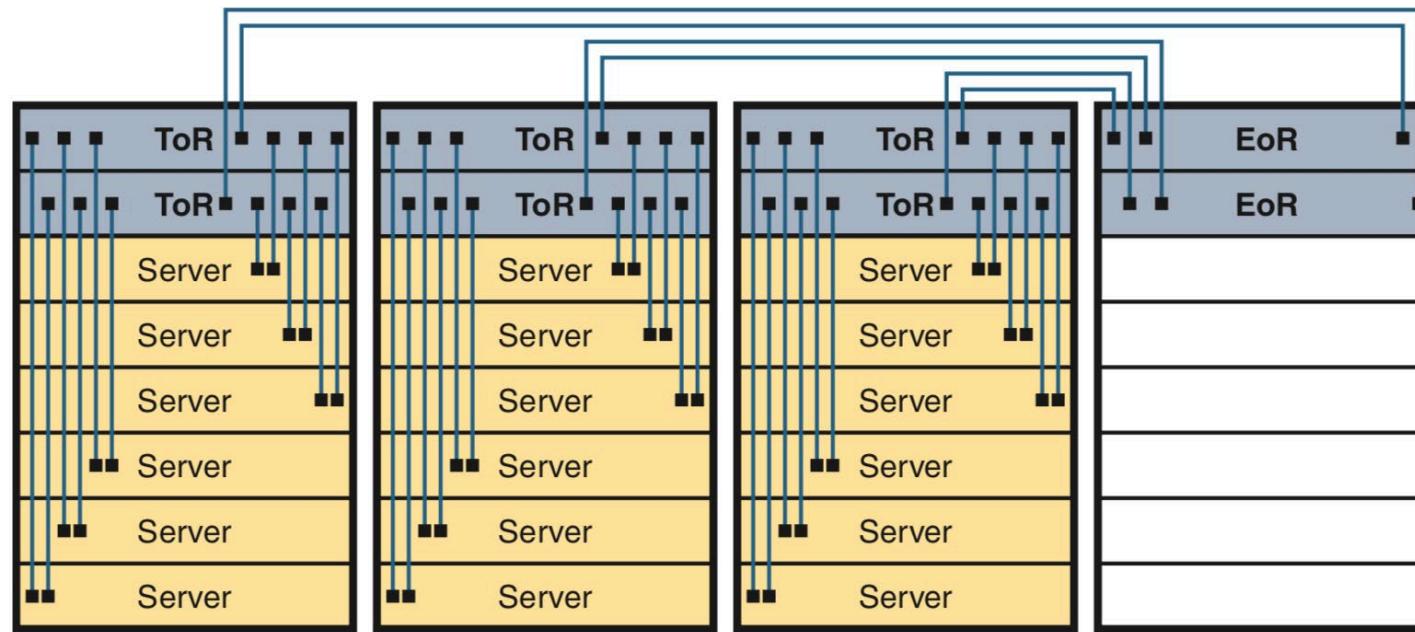
Communication réseau



- **vNIC**, « virtual NIC »
- **vSwitch**, « virtual Switch »
 - ports connectés au vNIC
 - access ou trunk
 - ports connectés à la carte réseau physique
 - trunk

Data Center

- Chaque « host » est connecté à 2 switch **ToR**
 - « Top of Rack » : switch d'accès
- Chaque ToR switch est connecté à 2 switch **EoR**
 - « End of Row » : switch de distribution



« Cloud »

- C'est une **manière de fournir un service** à un client :
 1. Le service doit pouvoir être activé et mis en place **sur demande** par le client
 2. Le service doit pouvoir **s'adapter** à une hausse de capacité (élasticité)
 3. Le service doit être fourni pas un **pool** de ressources partagées, et dynamiquement allouées
 4. Le service doit pouvoir être accessible via plusieurs options d'accès au **réseau**
 5. Le service doit pouvoir être **mesuré** (pour facturation par exemple)

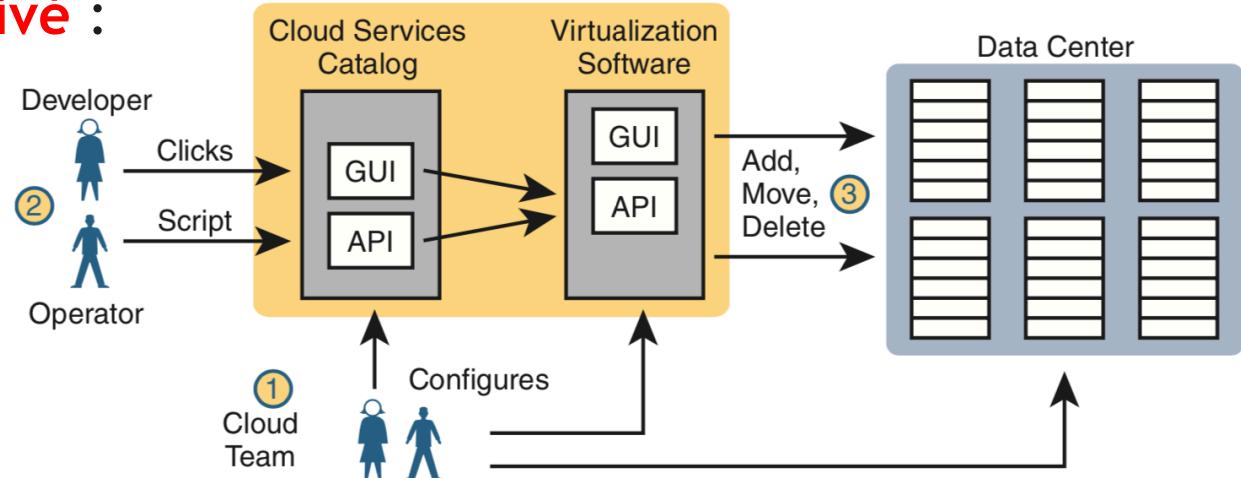
Deux options

1. Cloud **privé** :
 - Sur site, « **on-premise** »
 - Le fournisseur du Cloud et les consommateurs du Cloud sont dans la même entreprise

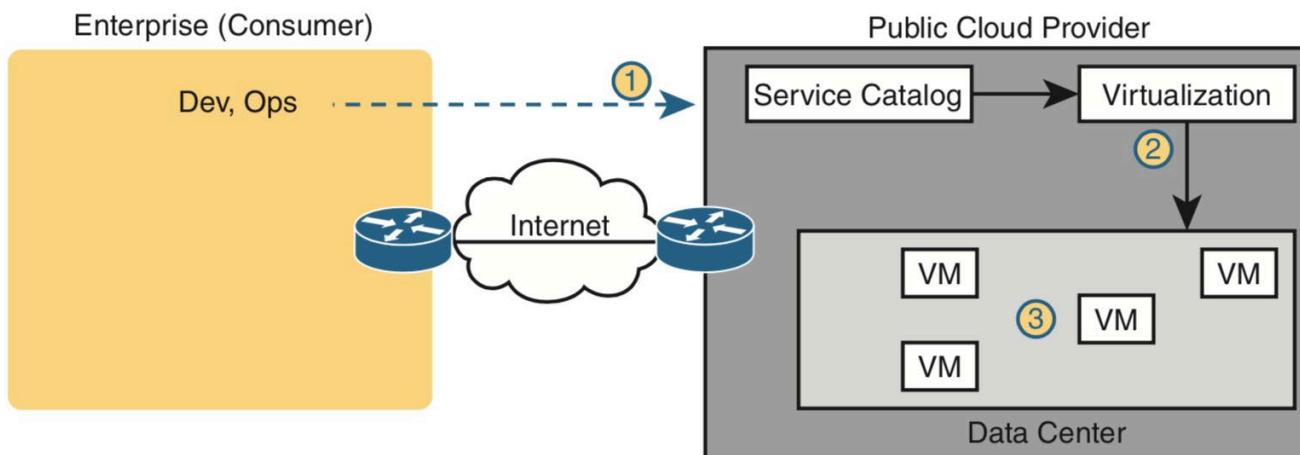
2. Cloud **public** :
 - Les services du Cloud sont fournies depuis un Data Center qui n'appartient pas à l'entreprise du consommateur
 - Exemples :
 - Amazon Web Services
 - Google Compute Cloud
 - Microsoft Azure
 - Rackspace

Deux options

1. Cloud privé :



2. Cloud public :

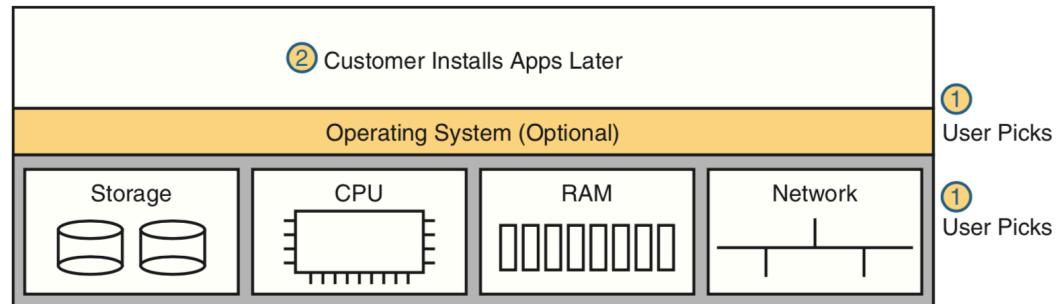


Trois types de services Cloud

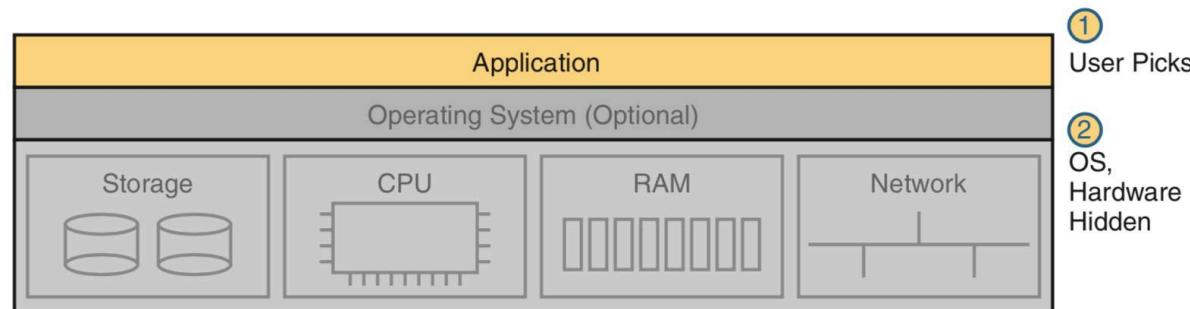
- **IaaS**, « **Infrastructure** as a Service » :
 - le client demande l'accès à une **VM**
 - il spécifie les performances & capacités attendues
 - il sélectionne un OS
 - exemple : AWS, « Amazon Web Services »
- **SaaS**, « **Software** as a Service » :
 - le client demande l'accès à une **application**
 - le fournisseur gère l'installation, les licences
 - le fournisseur surveille les performances
 - exemple : Apple iCloud, Dropbox, Google Drive, Exchange (MS Azure)
- **PaaS**, « **Platform** as a Service » :
 - le client demande l'accès à une environnement de développement, **IDE** « **Integrated Development Environment** »
 - exemple : Google's App Engine, Eclipse, Jenkins

Trois types de services Cloud

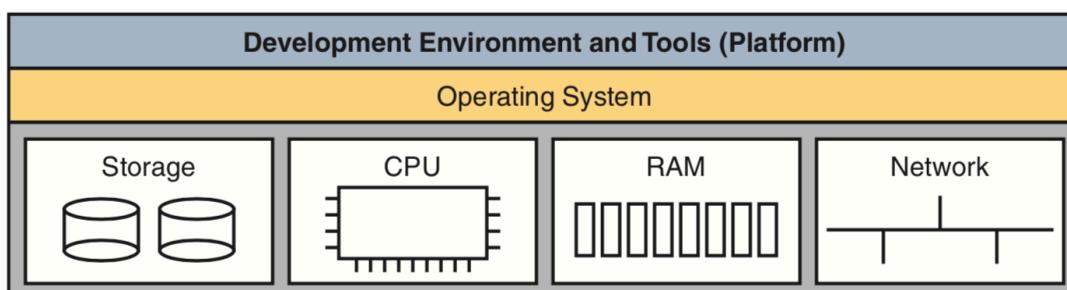
- **IaaS :**



- **SaaS :**



- **PaaS :**



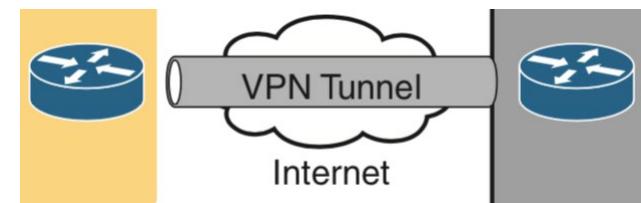
Trois manières d'accéder au Cloud

1. Via l'accès Internet :

- Avantages :
 - Agilité : rapide et simple à mettre en œuvre
 - Migration : facilité de changer de Cloud
 - Adapté au modèle de clients distribués
- Désavantages :
 - Sécurité
 - Capacité (ex : services authentification en interne)
 - QoS
 - Absence de SLA

2. Via un tunnel VPN par Internet :

- a. Service VPN offert par le fournisseur de Cloud
- b. Router virtuel configuré par le client
 - exemple : Cisco CSR, « Cloud Service Router », routeur Cisco dans une VM



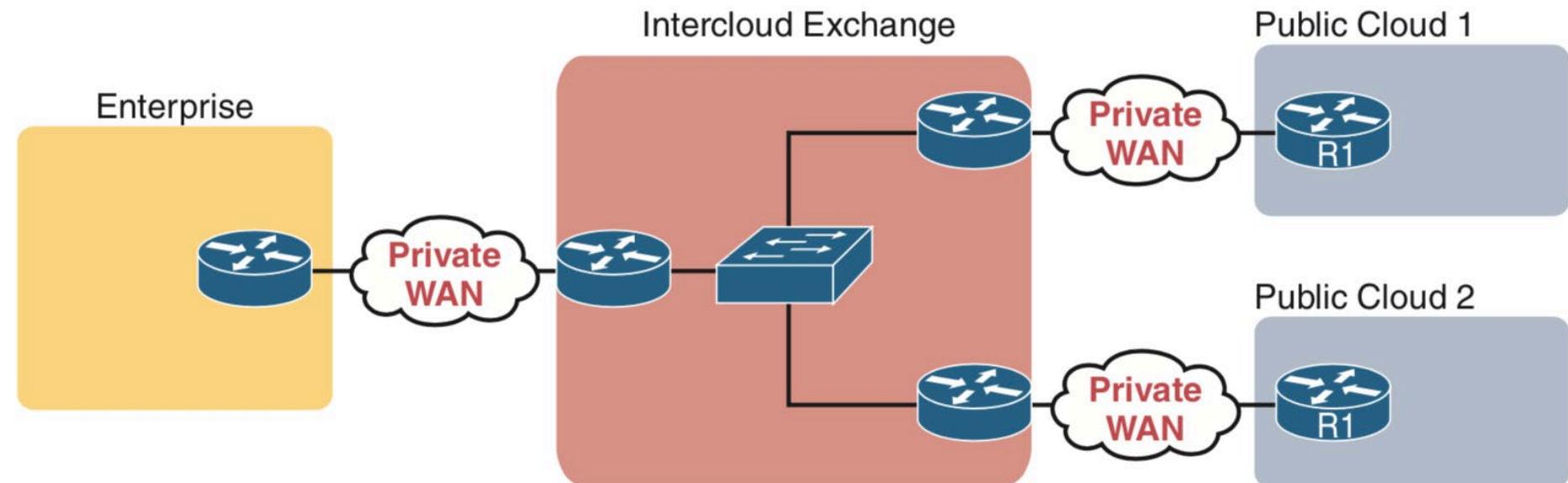
3. Via un accès WAN privé :

- a. Réseau MPLS
- b. Réseau Ethernet WAN
- le client doit donc travailler avec 2 fournisseurs :
 - le fournisseur de Cloud
 - le fournisseur d'accès au WAN privé



Intercloud Exchange

- Objectif :
 - faciliter la migration entre fournisseurs de Cloud sans changer de fournisseur d'accès
 - « Private Network as a Service »



Bilan des options d'accès au Cloud

	Internet	Internet VPN	MPLS VPN	Ethernet WAN	Intercloud Exchange
Makes data private	No	Yes	Yes	Yes	Yes
Supports QoS	No	No	Yes	Yes	Yes
Requires capacity planning	Yes	Yes	Yes	Yes	Yes
Eases migration to a new provider	Yes	Yes	No	No	Yes
Speeds initial installation	Yes	Yes	No	No	No



Quiz

Quiz

Three **virtual machines** run on one physical server.

Which of the following server **resources** are commonly **virtualized** so each VM can use the required amount of that resource? (Choose three answers.)

- 
- a. NIC
 - b. RAM
 - c. Power
 - d. Hypervisor
 - e. CPU

Quiz

Eight virtual machines run on one physical server; the server has two physical Ethernet NICs.

Which answer describes a method that allows all eight VMs to communicate?

- a. The VMs must share two IP addresses and coordinate to avoid using duplicate TCP or UDP ports.
- b. The hypervisor acts as an IP router using the NICs as routed IP interfaces.
- c. Each VM uses a virtual NIC that is mapped to a physical NIC.
- d. Each VM uses a virtual NIC that logically connects to a virtual switch.



Quiz

Which of the following cloud services is most likely to be used for software development?

- a. IaaS
- b. PaaS
- c. SaaS
- d. SLBaaS



Quiz

Which of the following cloud services is most likely to be purchased and then used to later **install your own software applications?**



- a. IaaS
- b. PaaS
- c. SaaS
- d. SLBaaS

Quiz

An enterprise plans to start using a **public cloud service** and is considering different WAN options.

The answers list four options under consideration.

Which one option has the most issues if the company chooses one cloud provider but then later wants to **change** to use a different cloud provider instead?



- a. Using private WAN connections directly to the cloud provider
- b. Using an Internet connection without VPN
- c. Using an intercloud exchange
- d. Using an Internet connection with VPN

Quiz

An enterprise plans to start using a **public cloud service** and is considering different WAN options.

The answers list four options under consideration.

Which options provide **good security** by keeping the data private while also providing **good QoS services**? (Choose two answers.)

-  a. Using private WAN connections directly to the cloud provider
-  b. Using an Internet connection without VPN
- c. Using an intercloud exchange
- d. Using an Internet connection with VPN

Les RESEAUX INTELLIGENTS

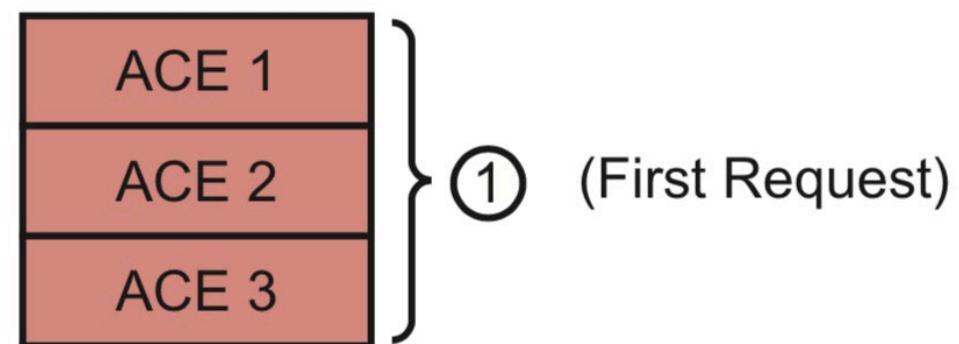
Pourquoi ce changement ?

Les objectifs d'un réseau intelligent

- Réduire les temps de déploiement
- Faciliter le dépannage
- Réduire les coûts
- Réduire les erreurs

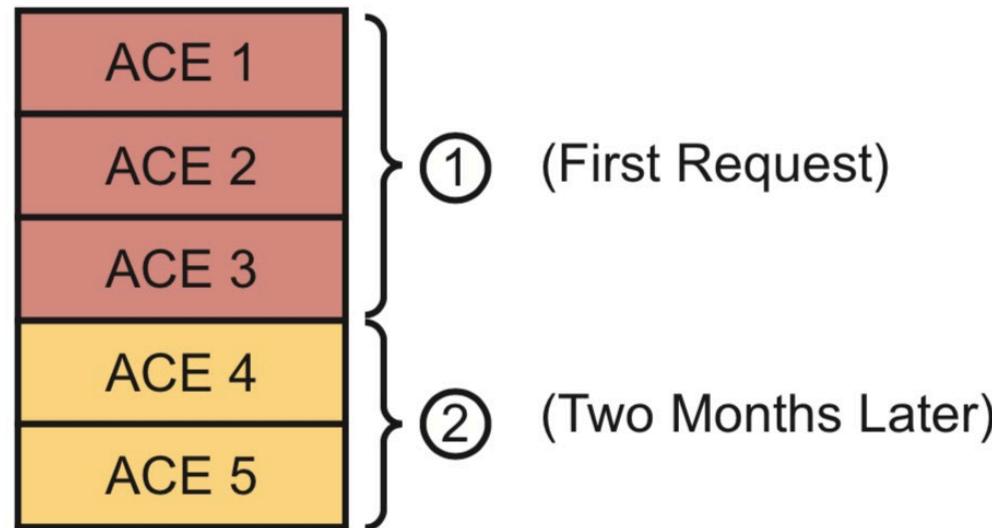
Exemple : gestion des ACL

- Dans un réseau traditionnel :
 - l'ingénieur réseau configure des ACL sur chaque équipement
 - selon les **besoins** de l'entreprise, il doit adapter ces ACL
 - 1ère version de l'ACL :
 - adaptée à la 1ère demande :
 - contient 3 lignes



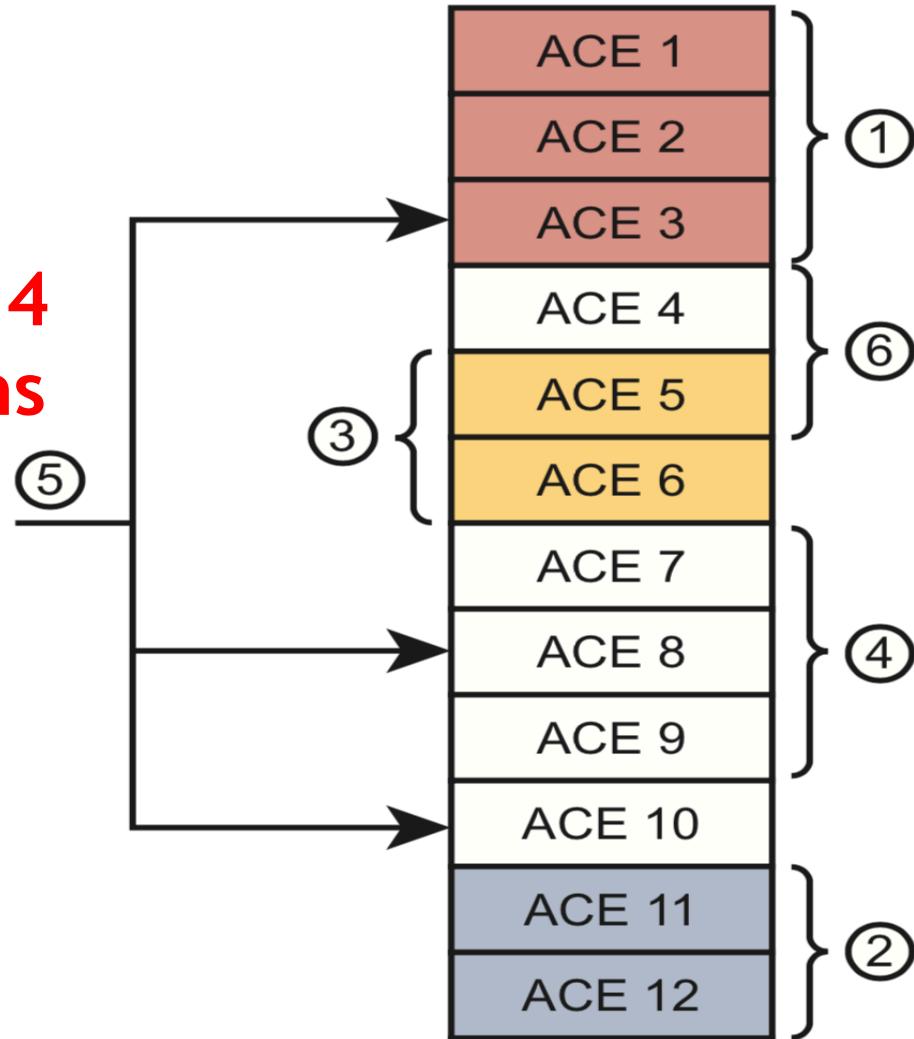
Gestion des ACL

- Deux mois plus tard :
 - identification d'un **nouveau besoin**
 - modification de l'ACL
 - ajout de 2 lignes supplémentaires



Gestion des ACL

- Quelques mois plus tard :
 - identification de **4 nouveaux besoins**
- Comment simplifier l'ACL ?



Le réseau intelligent : IBN

- L'ingénieur réseau indique à un **organe central** quelles sont ses « **intentions** » :
 - « ***Intent Based Networking*** »
- Exemple : la gestion des flux ne nécessite plus la configuration d'ACL sur chaque équipement par l'ingénieur réseau :
 - il indique quels échanges sont autorisés entre chaque « **groupe d'utilisateurs** »
 - un organe central configure les ACL sur chaque équipement

Flux autorisés entre groupes

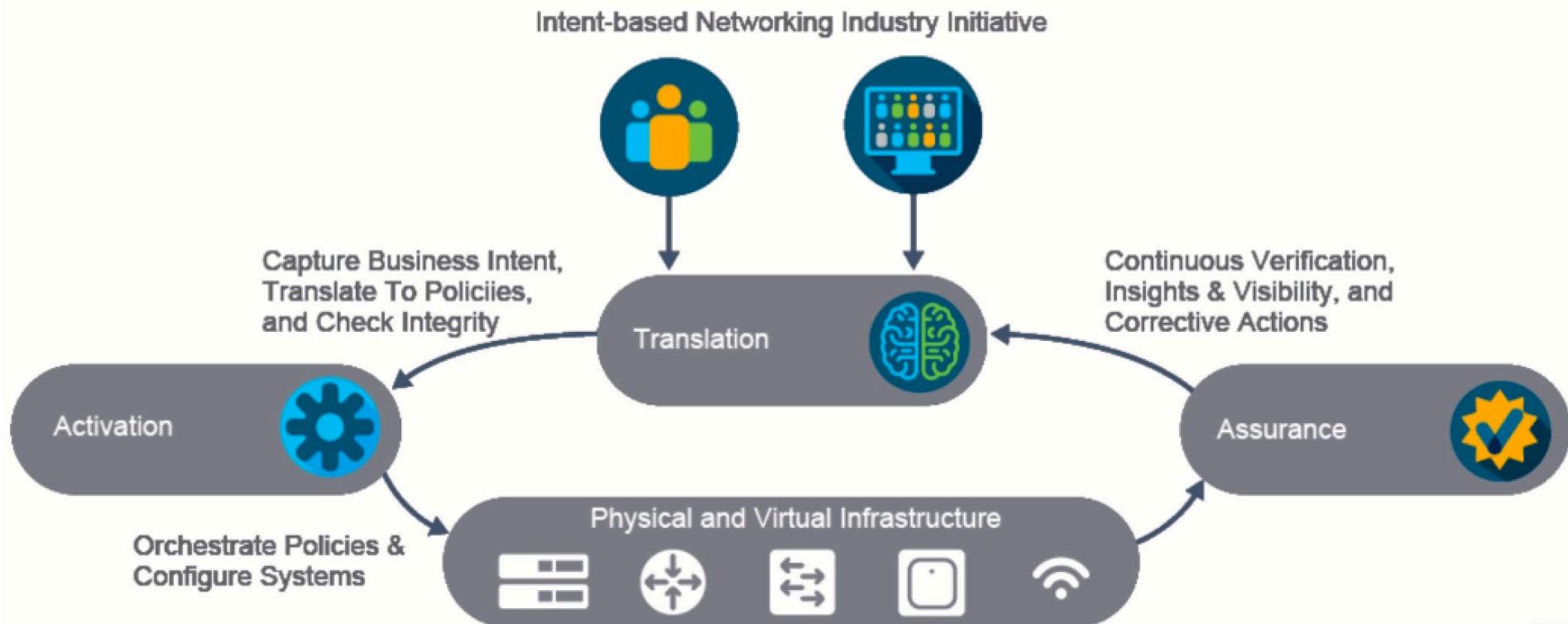
- Les utilisateurs sont **regroupés** dans des SG
 - « *Scalable Groups* »
- L'ingénieur réseau indique les droits de chaque SG

Source \ Dest.	Employee	Internet	Partner	Guest
Employee	N/A	Permit	Permit	Deny
Internet	Permit	N/A	Permit	Permit
Partner	Permit	Permit	N/A	Deny
Guest	Deny	Permit	Deny	N/A

Avantage du système IBN

- Les **changements** de configuration des équipements réseaux sont effectués :
 - plus rapidement
 - moins de risque d'erreur
 - de manière cohérente

Le Modèle IBN



Quatre termes équivalents

- SDN
 - **Software-Defined Networks**
- SDA
 - Software-Defined Architecture
- CBN
 - **Controller-Based Networks**
- PN
 - **Programmable Networks**

Le Contrôleur

- Application
- Centralise l'intelligence du réseau
 - Connaît tous les équipements du réseau
 - Est capable de les configurer en se basant sur les « intentions » définies par l'ingénieur réseau
- Que fait le contrôleur ?
- Il contrôle ...
... **le plan de contrôle** de chaque équipement!

Les « plans »

Trois plans

- Toutes les actions d'un équipement réseau sont effectuées par l'un des 3 plans :
 - plan de **données**
 - plan de **contrôle**
 - plan de **management**

Plan de données

- « Data plane » ou « Forwarding plane » :
 - reçoit un message + le traite + l'envoie
- Toutes les **actions effectuées sur un message** sont faites par le plan de contrôle
 - Routeur :
 - dés-encapsuler, re-encapsuler une trame
 - chercher une adresse IP dans la table de routage
 - supprimer un paquet (ACL)
 - ajouter une seconde entête IP (VPN, GRE)
 - modifier un champ de l'entête IP (NAT)
 - Switch :
 - chercher une adresse MAC dans la table des adresses MAC
 - rajouter / supprimer le tag 802.1Q

Plan de contrôle

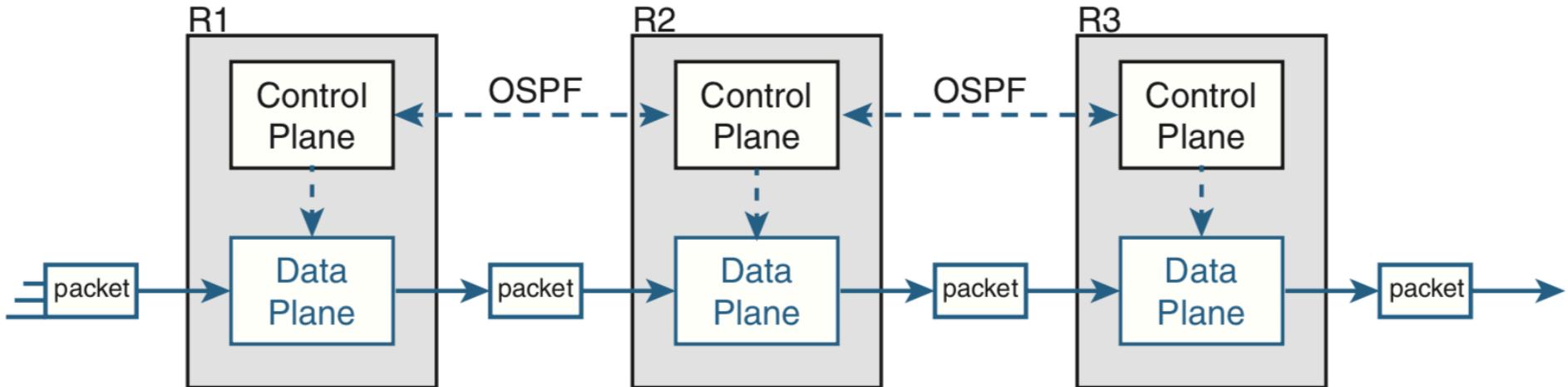
- « **Control plane** »
- Toute action qui contrôle le plan de données :
 - mettre à jour la table de routage
 - mettre à jour la table d'adresse MAC
 - mettre à jour la table ARP
 - identifier les ports que STP doit bloquer
- Protocoles concernés :
 - OSPF, STP, ARP, BGP, CDP ...

Plan de management

- « **Management plane** »
- Permet aux ingénieurs réseau de manager les équipements
- Protocoles concernés :
 - Telnet, SSH, SNMP, Syslog

Réseau traditionnel

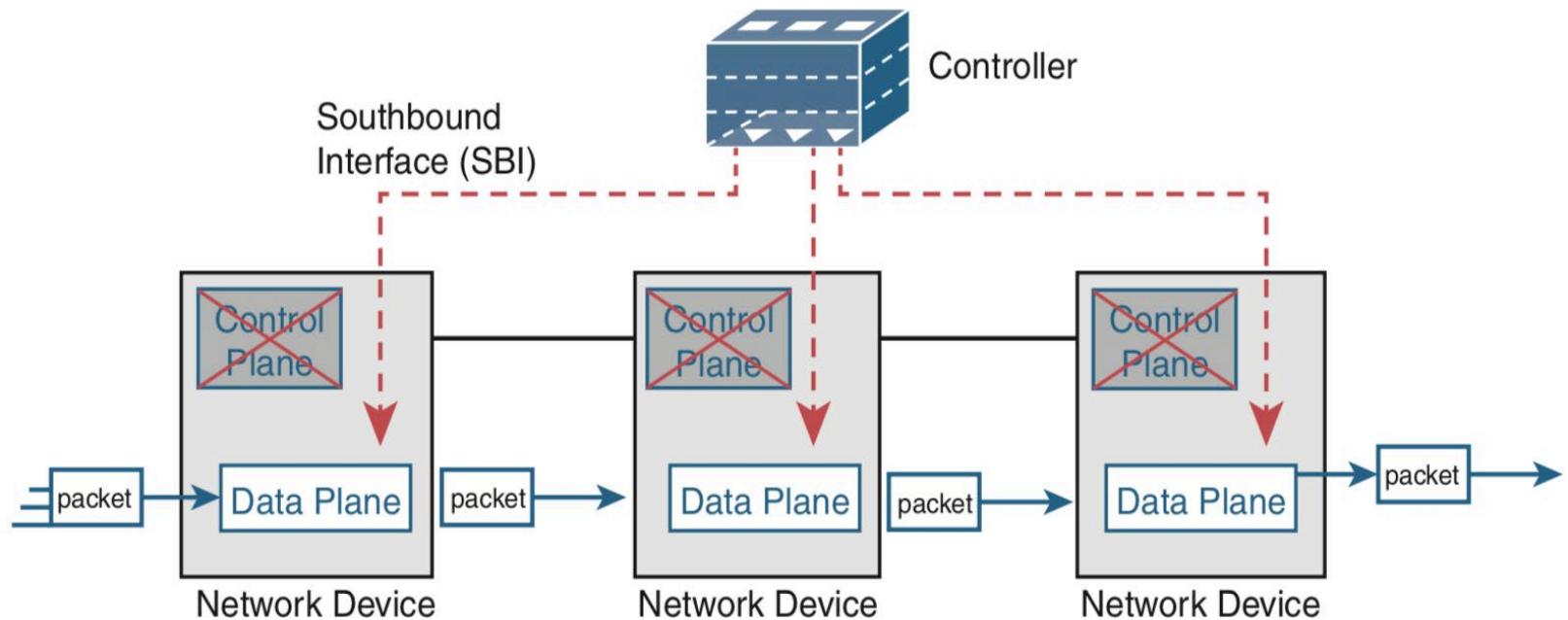
- Modèle **distribué**
 - « **Distributed control plane** »
- Chaque équipement possède :
 - son plan de contrôle
 - son plan de données



Réseau intelligent

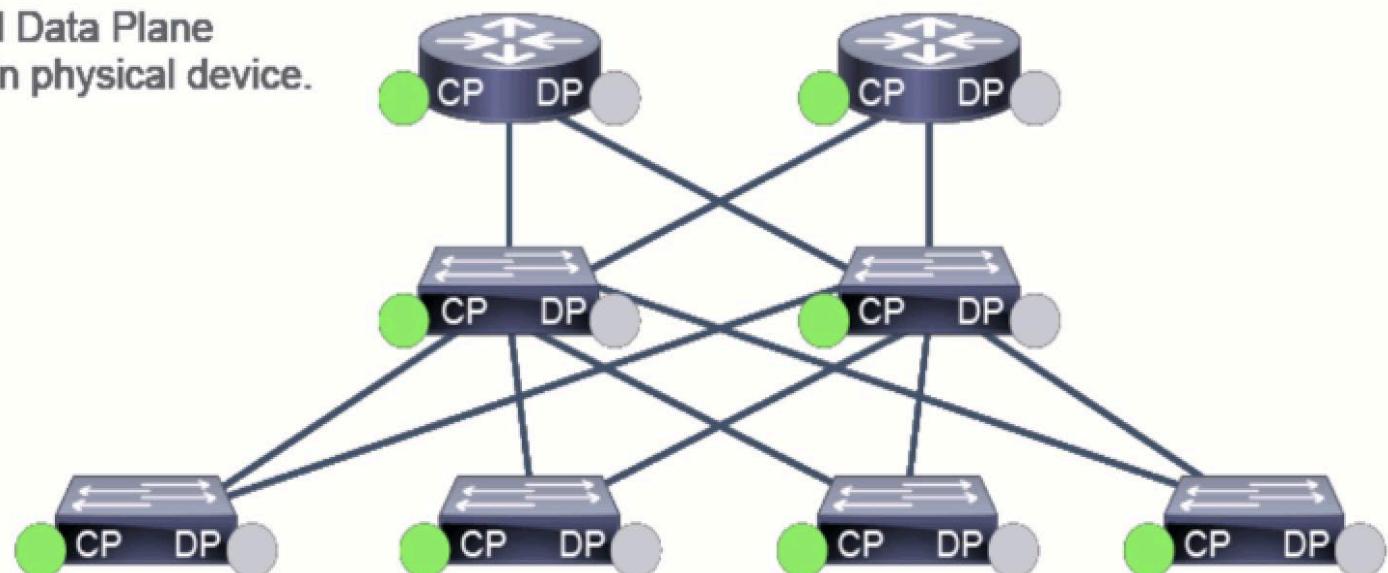
- Modèle **centralisé**
 - Chaque équipement possède son plan de données
 - Un partie du plan de **contrôle** est centralisé
 - sur une application,
 - appelée le contrôleur, ou « SDN controller »
 - récupère les informations sur les équipements
 - centralise la prise de décision
 - met à jour le plan de données de chaque équipement

« SDN controller »

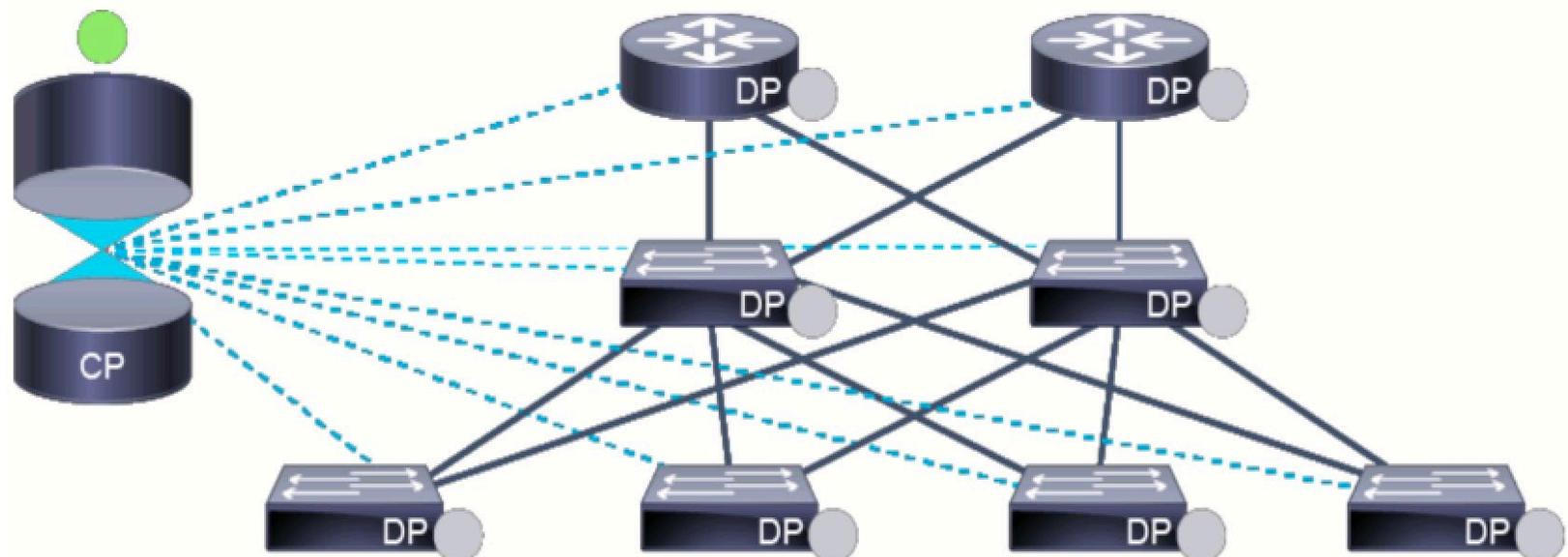


Réseau traditionnel

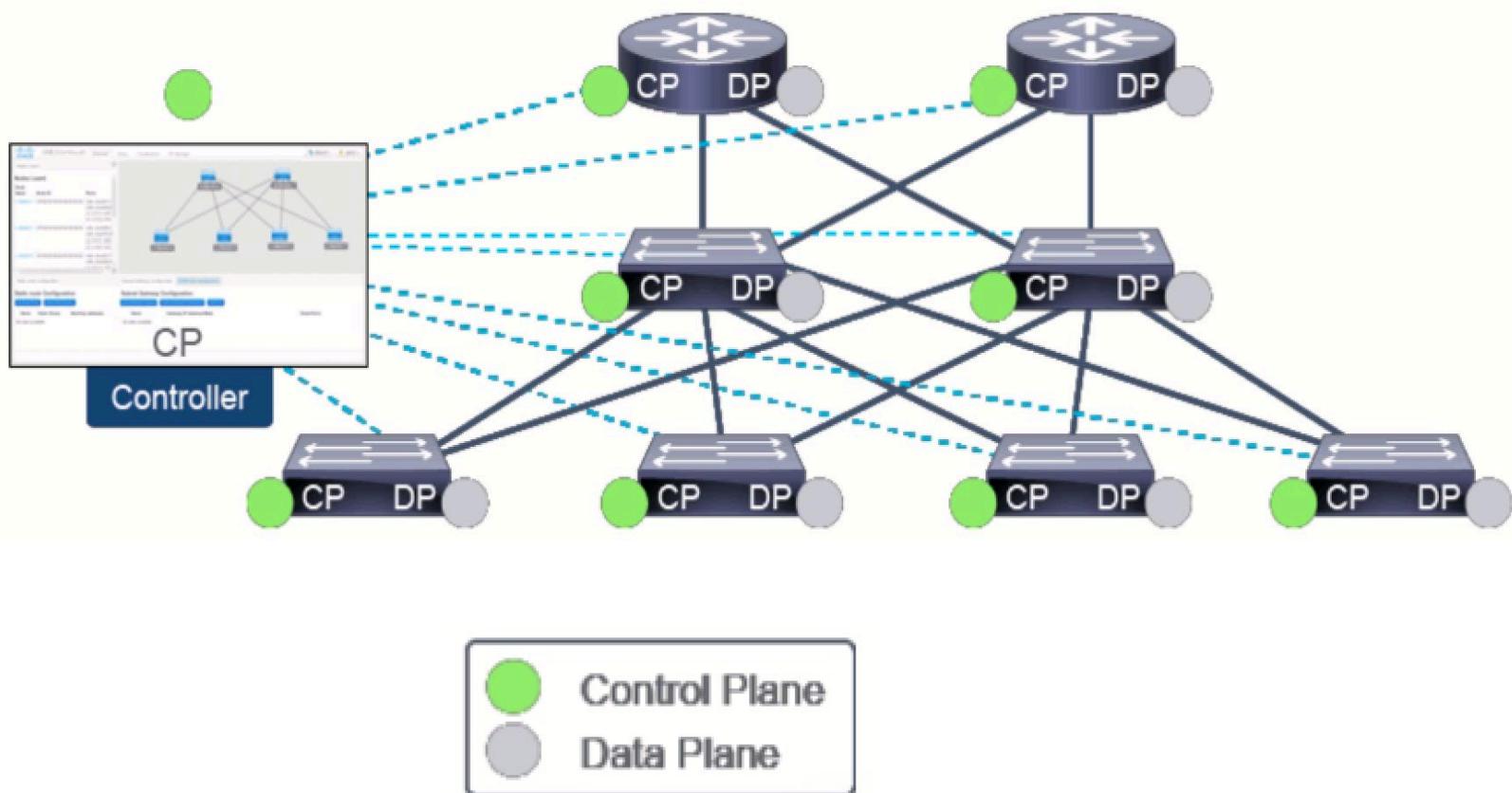
Control and Data Plane
reside within physical device.



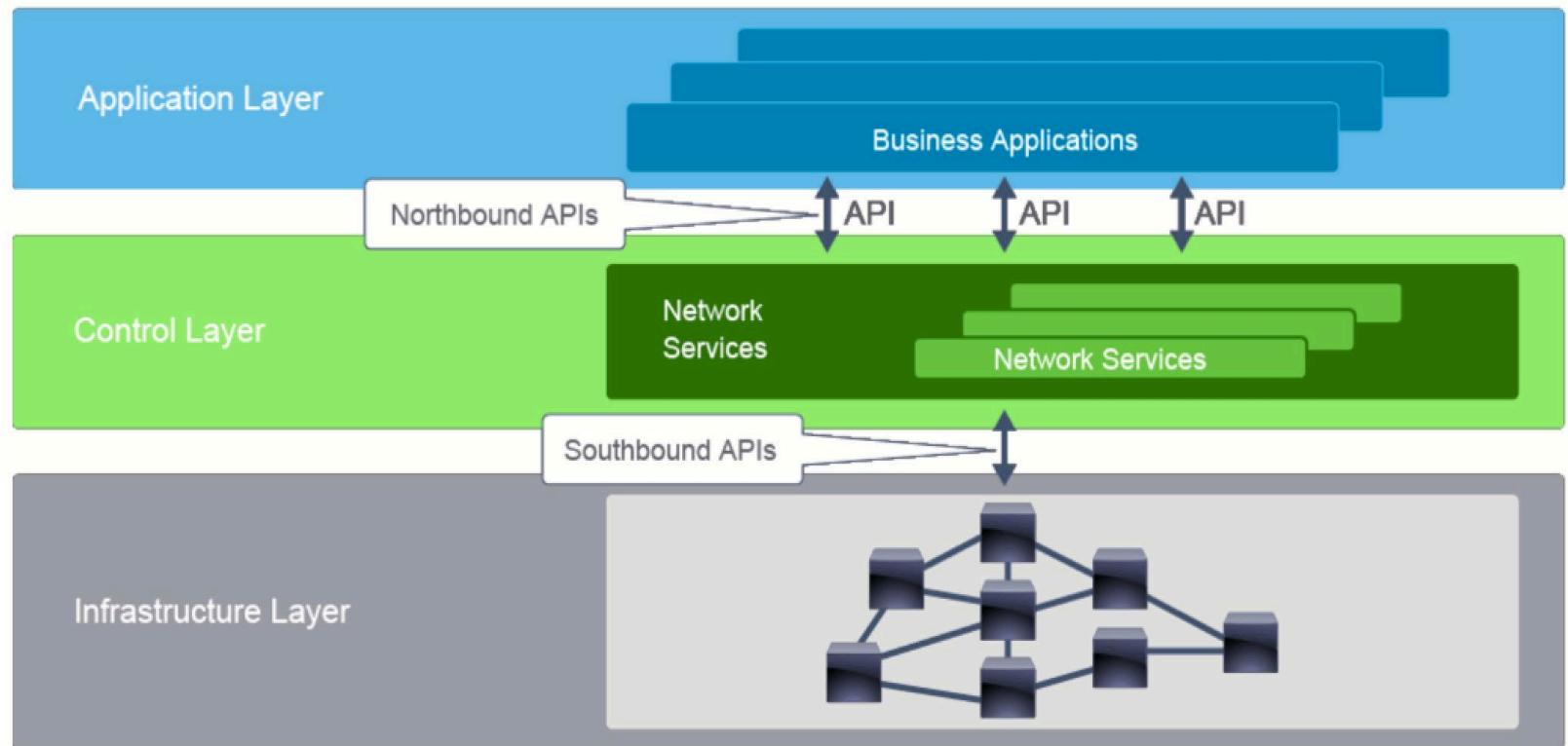
Réseau SDN « puriste »



Réseau SDN hybride



Les couches d'un réseau SDN



- « **South Bound Interface** »
 - permet au contrôleur de communiquer avec chaque équipement réseau
- Objectif :
 - mettre à jour le plan de données de l'équipement
- **C'est donc une communication entre 2 applications :**
 - **API : « Application Programming Interface »**

4 types de **Southbound Interface**

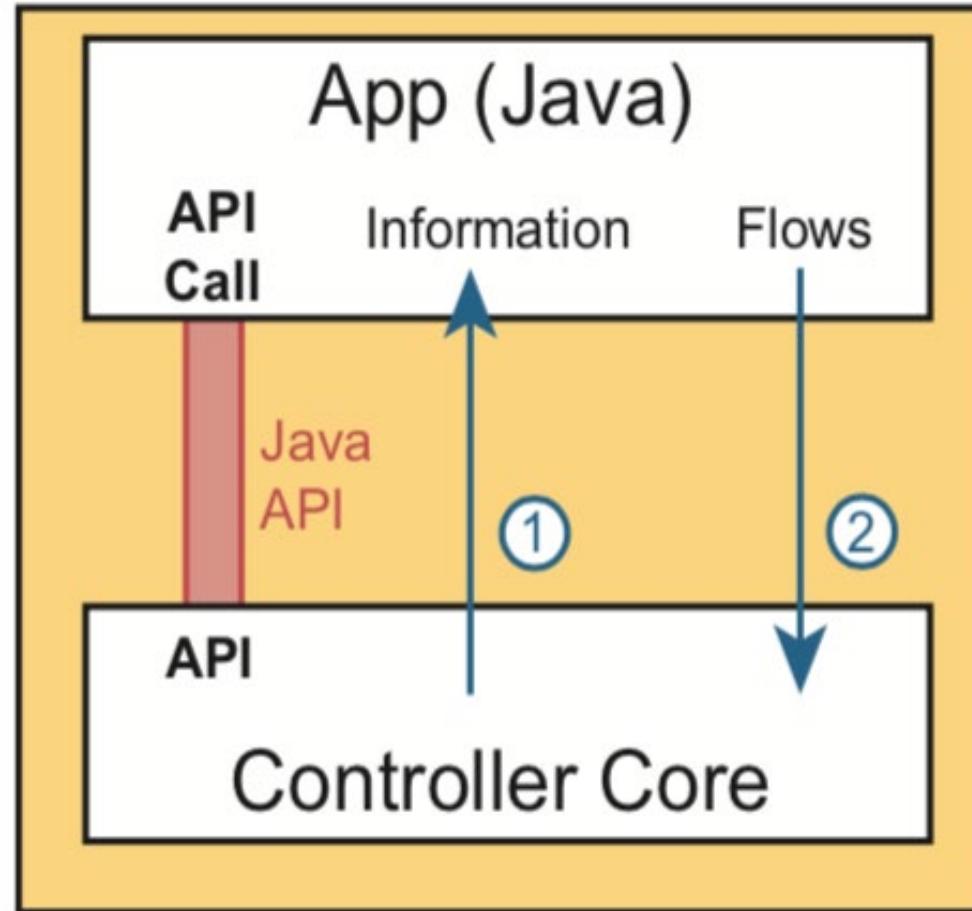
1. OpenFlow
 - standard Open Networking Foundation
2. OpFlex
 - utilisé par le contrôleur Cisco APIC
3. CLI, SNMP
 - utilisé par le contrôleur Cisco APIC-EM
4. CLI, SNMP, NETCONF, RESTCONF
 - utilisé par le contrôleur Cisco DNA

Base de données centralisée

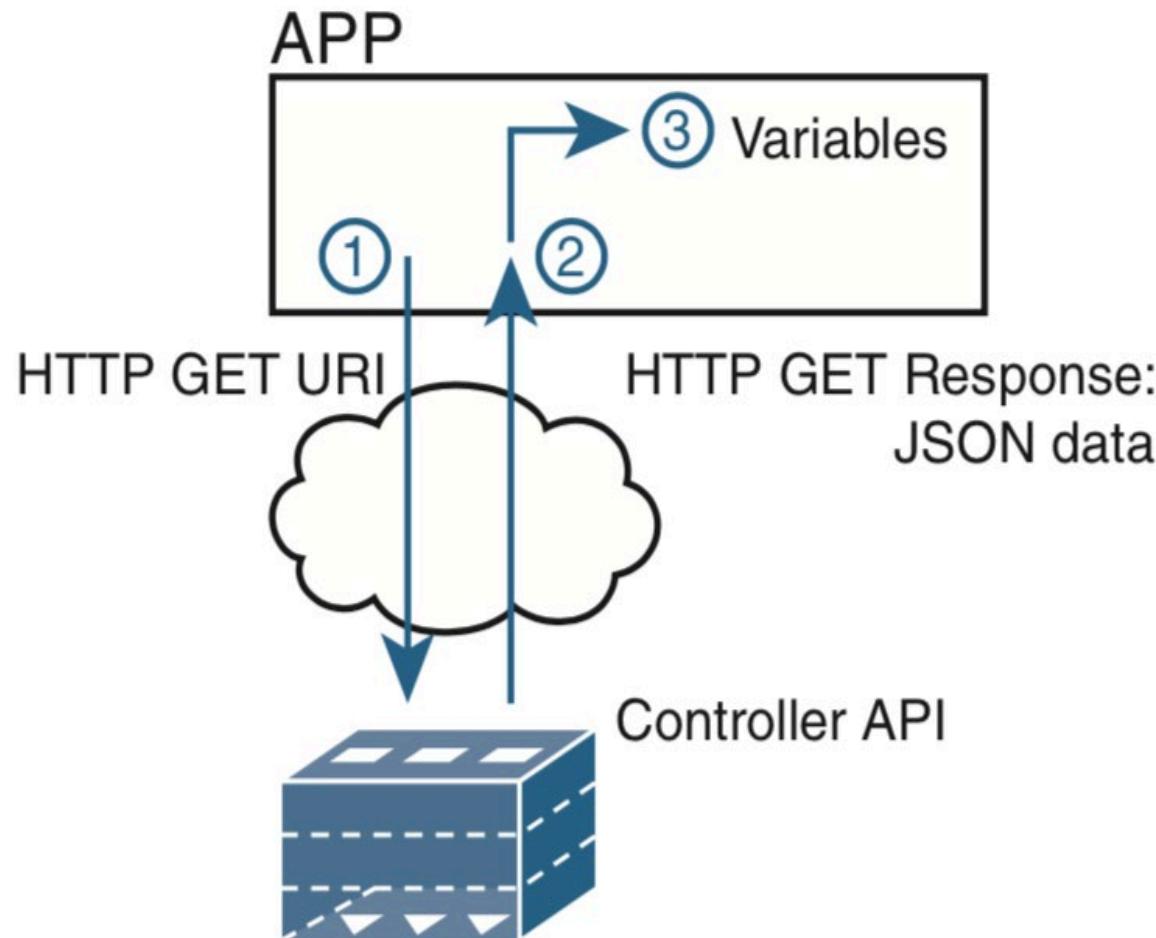
- Grâce au SBI, le contrôleur **compile des informations sur le réseau** :
 - inventaire des équipements
 - capacités de chacun
 - interfaces disponibles
 - statuts des interfaces
 - topologie d'interconnexion
 - configuration des équipements
 - ...

- « **North Bound Interface** »
 - permet à l'ingénieur réseau
 - d'accéder à la base de données centralisée
 - de demander au contrôleur de changer la configuration des équipements : « **Network programmability** »
 - L'ingénieur réseau utilise une application qui va communiquer avec le contrôleur.
 - **C'est donc une communication entre 2 applications :**
 - **API : « Application Programming Interface »**

Contrôleur et APP sur le même serveur



Controller et APP sur 2 serveurs



Network programmability

- Divers **degrés de centralisation** des fonctionnalités du plan de contrôle :
 - centralisation partielle
 - centralisation quasi totale
- **Architectures** IBN de Cisco :
 - Application Centric Infrastructure (ACI)
 - Software Defined Access (SDA)
 - Software Defined WAN (SD-WAN)
- **Contrôleurs** de Cisco :
 - APIC Enterprise Module (APIC-EM)
 - Application Policy Infrastructure Controller (APIC)
 - Digital Network Architecture (DNA)

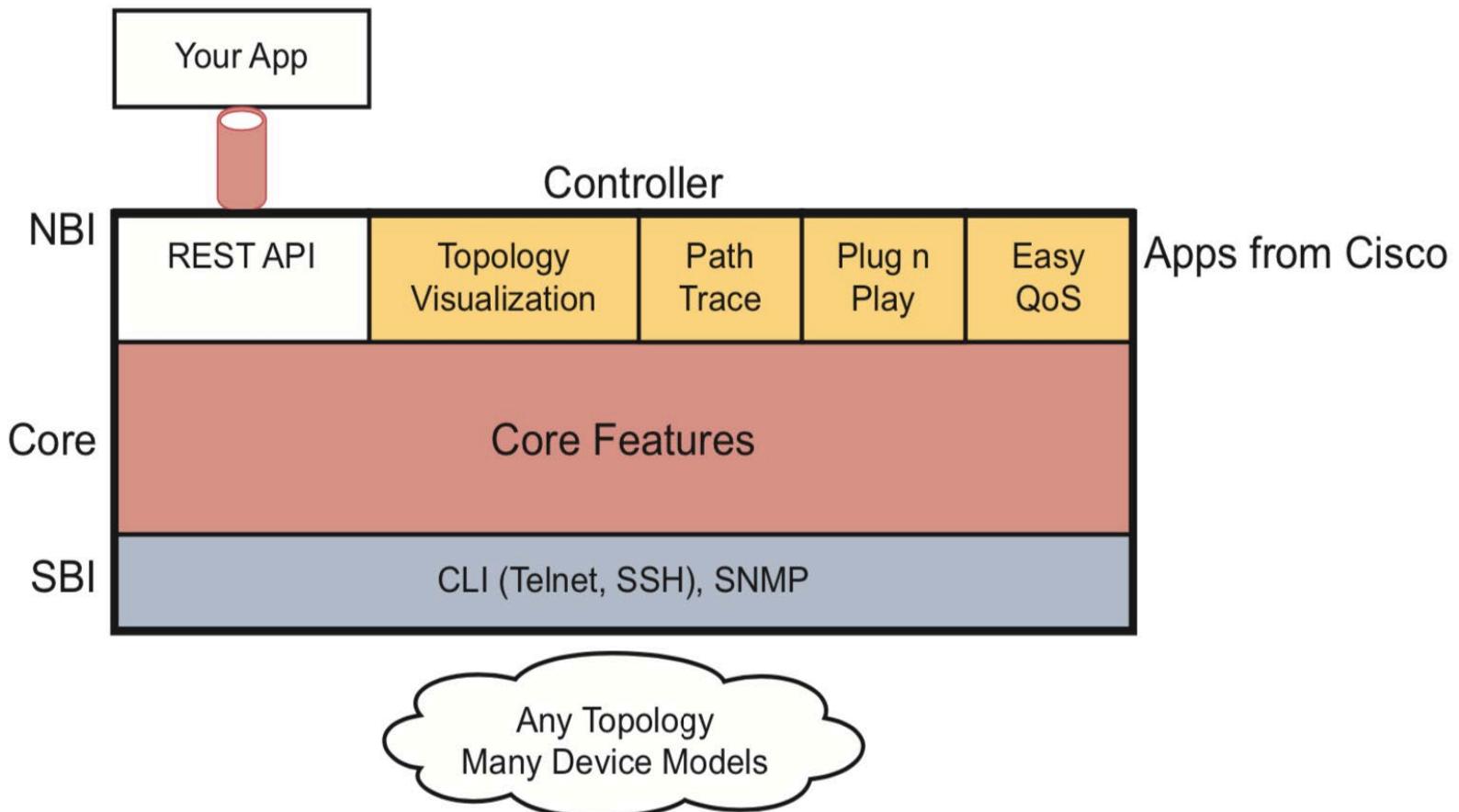
APIC Enterprise Module

APIC-EM

Historique

- Comment déployer le SDN sans changer tous les équipements réseau ?
 - La flotte actuelle ne sait pas interagir avec les nouveaux API !
- Comment déployer un contrôleur centralisé dans une architecture distribuée ?
 - Solution : APIC-EM
 - n'interagit pas avec le plan de contrôle ou le plan de données des équipements
 - interagit avec **leur plan de management**
 - end of sale : Feb 2019
 - end of support : Feb 2024

Fonctionnalités de APIC-EM

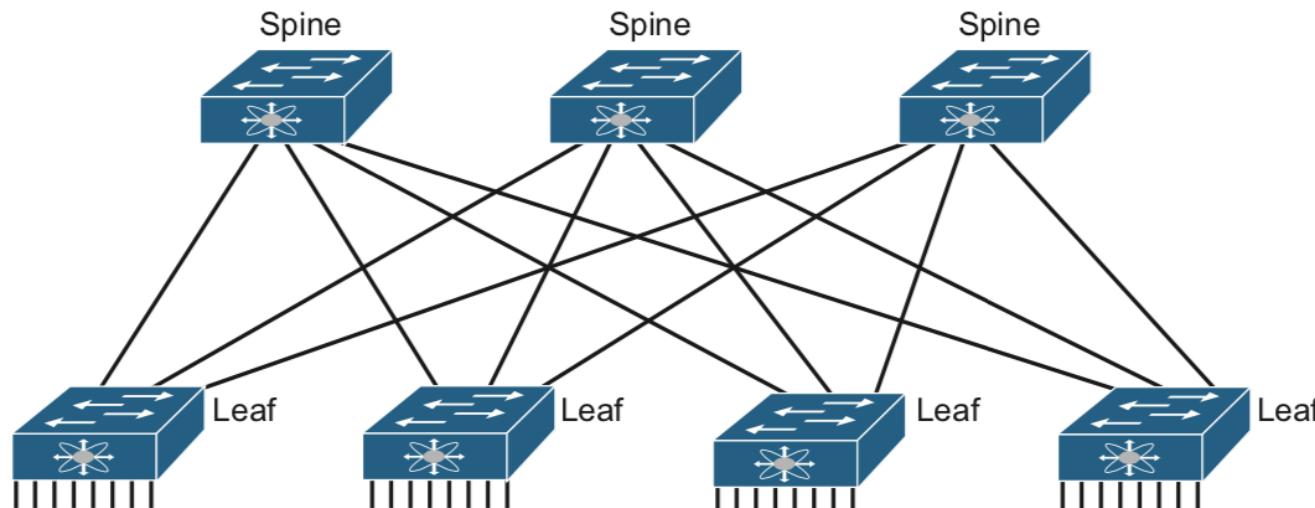


Application Centric Infrastructure

ACI

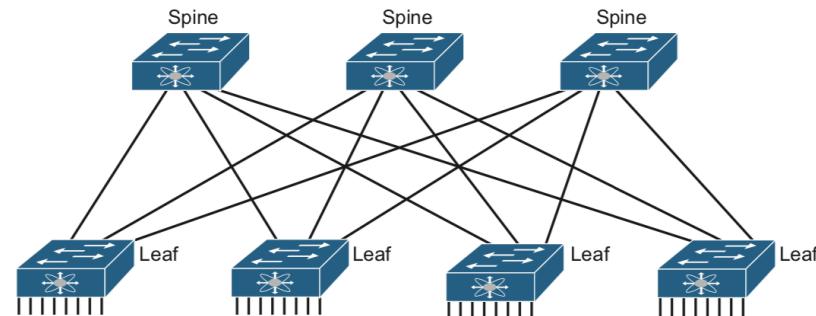
Application Centric Infrastructure

- Conçu pour les applications des **data center** :
 - permet de gérer un réseau dans lequel des Machines Virtuelles sont régulièrement ajoutées, modifiées, supprimées
 - utilise une topologie « **Spine & leaf** » :



« Spine and leaf »

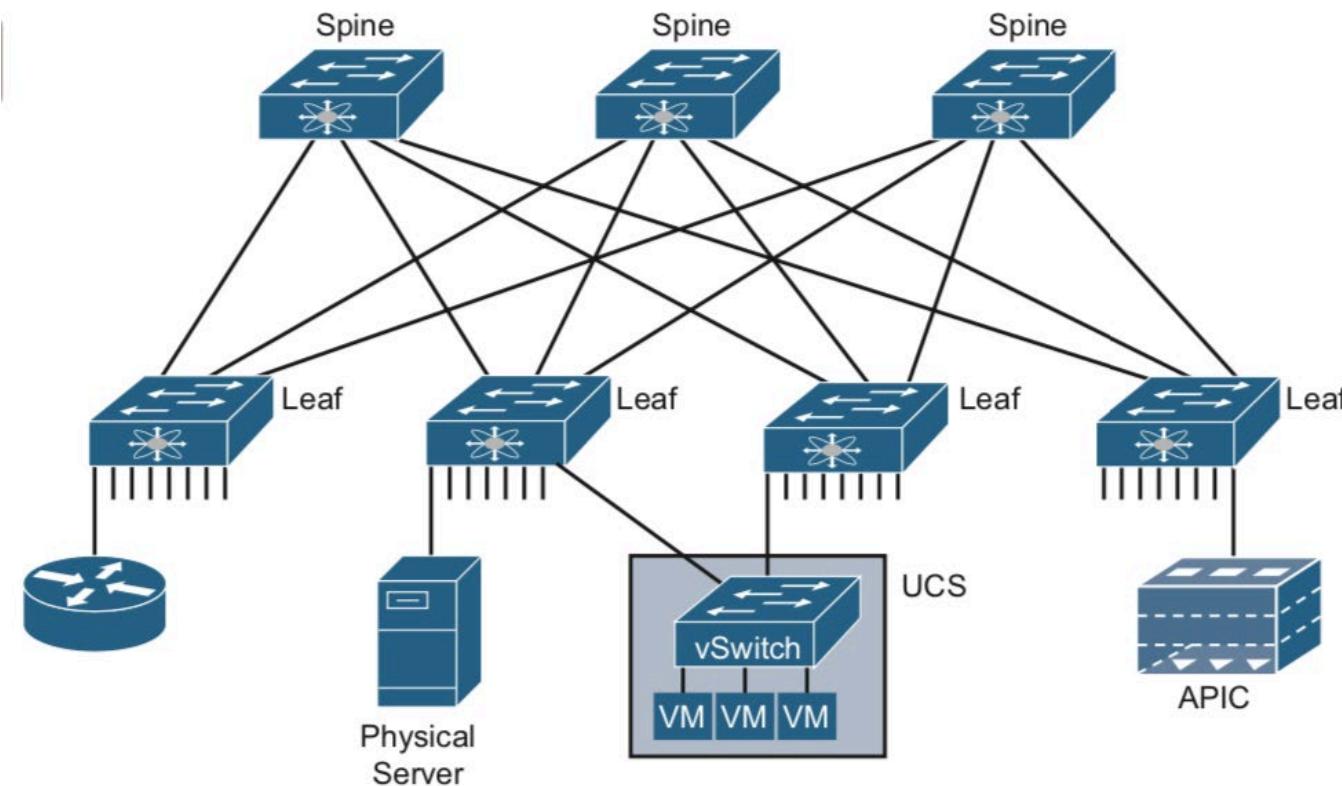
- Les hôtes (VM, servers) sont connectés uniquement aux « leafs »



- Les « **leafs** » ne sont pas inter-connectés
- Chaque « leaf » doit être connecté à tous les « spines »
- Les « **spines** » ne sont pas inter-connectés
- Chaque « spine » doit être connecté à tous les « leafs »

Le contrôleur de l'ACI

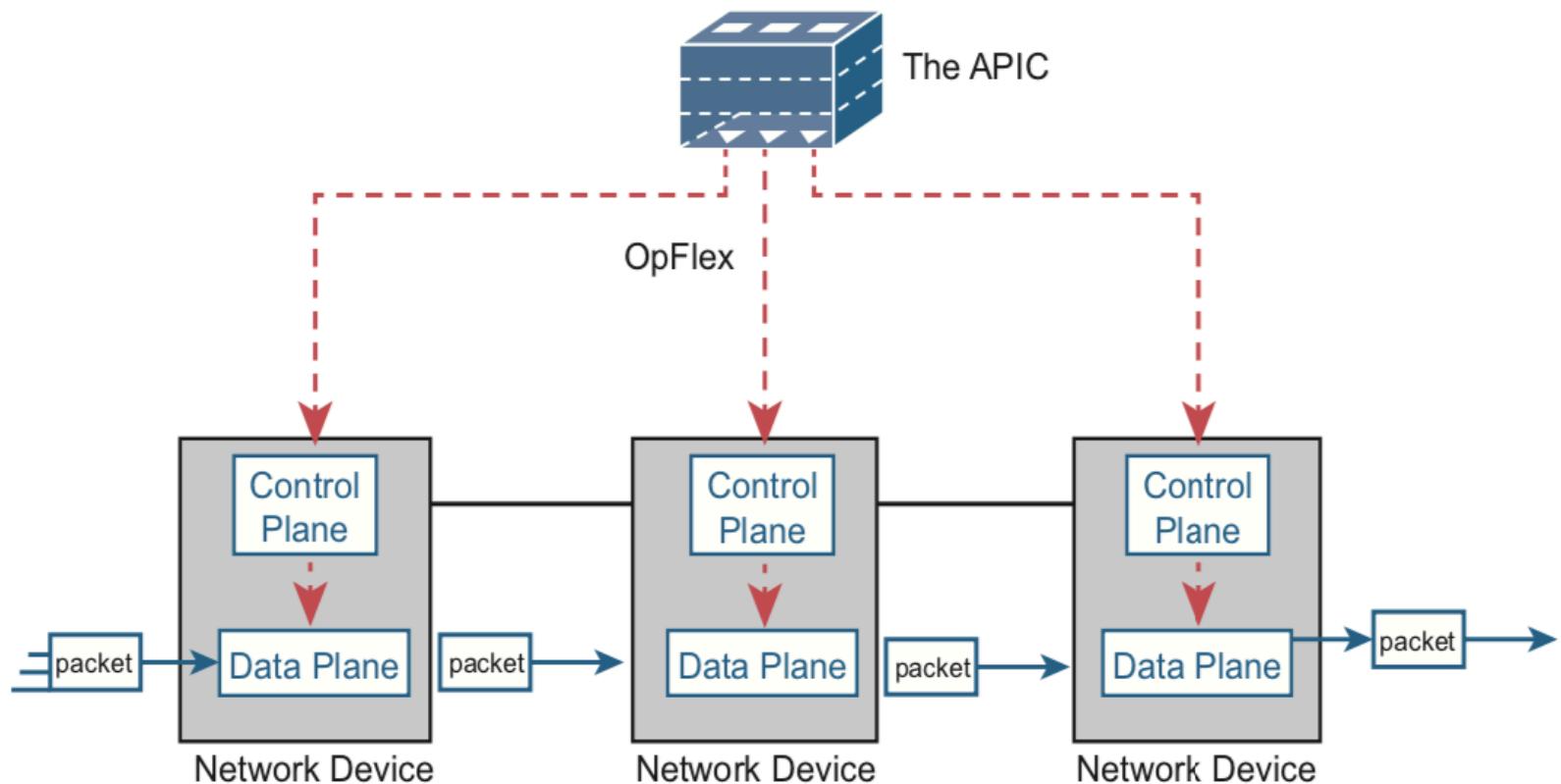
- Le réseau est contrôlé par l'application **APIC** :
 - « Application Policy Infrastructure Controller »



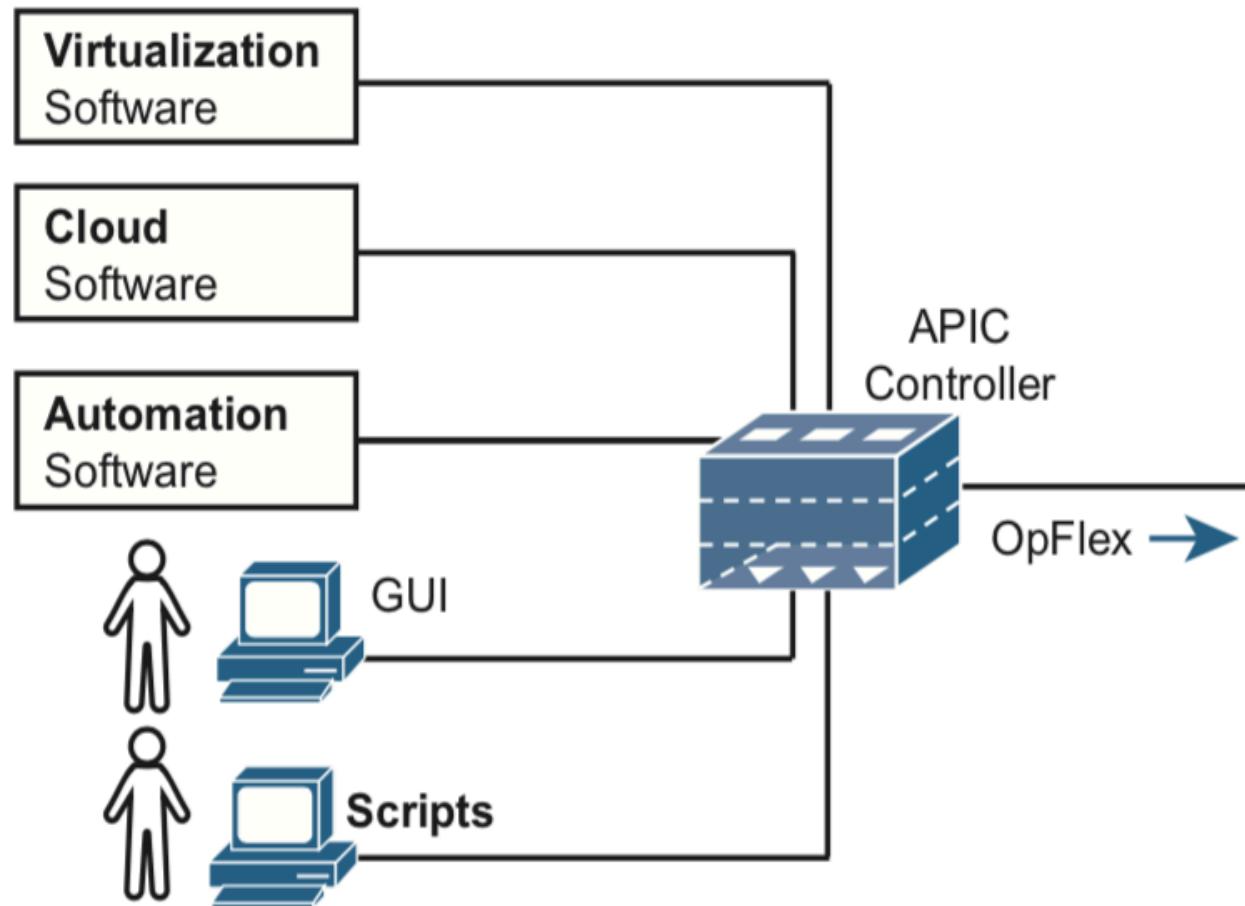
Exemple de configuration

- L'ingénieur configure des **polices** pour indiquer les communications autorisées
 - les VM sont regroupés dans des « Endpoint group », EPG
 - les polices sont définies entre paires d'EPG
- Le contrôleur APIC traduit cette « **intention** » en configuration du réseau, selon la localisation des hosts.
 - → Principe du « Intent Based Networking »

Southbound Interface de l'APIC



Northbound Interfaces de l'APIC



Comparatif APIC vs APIC-EM

Criteria	ACI	APIC Enterprise
Changes how the device control plane works versus traditional networking	Yes	No
Creates a centralized point from which humans and automation control the network	Yes	Yes
Degree to which the architecture centralizes the control plane	Partially	None
SBIs used	OpFlex	CLI, SNMP
Controllers mentioned in this chapter	APIC	APIC-EM
Organization that is the primary definer/owner	Cisco	Cisco

Management des réseaux SDN

Quel impact sur le management ?

- Management =

1. configuration :

- l'ingénieur ne configure pas directement les équipements
 - il configure des polices sur le contrôleur
 - le contrôleur interprète ces polices et modifie en conséquence les configurations des équipements

2. monitoring :

- exemple : le contrôleur vérifie les images IOS

Le Modèle de Données

- Avant le déploiement des contrôleurs :
 - les scripts d'automatisations devaient **scanner** le résultat textuel d'un show pour obtenir des informations sur l'équipement

```
SW1# show interfaces gigabit 0/1 switchport
```

Name: Gi0/1

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: On

Le Modèle de Données

- En présence d'un contrôleur :
 - le contrôleur **définit** un modèle de données
 - il récupère les informations auprès des équipements
 - il les **formalise** dans le modèle de données sous forme de **variables** :

```
>>> interface1
```

```
{'trunk-config': 'dynamic auto', 'trunk-status': 'static access'}
```

```
>>>
```

- le modèle de données facilite l'**automatisation** de nouvelles fonctionnalités, plus complexes !
 - exemple : Path Trace

Avantages des contrôleurs

- L'ingénieur réseau n'a pas besoin de configurer chaque commande sur chaque équipement
- C'est le contrôleur qui configure les équipements selon un **modèle cohérent et rationalisé**
- Exemple :
 - Sans contrôleur :
 - configurer les ports dans un VLAN, configurer les trunk, mettre en œuvre OSPF, configurer des ACL
 - Avec APIC :
 - rassembler les VM dans des EPG « Endpoint group »
 - configurer des polices entre les EPG

Avantages du contrôleur

- Il offre un nouveau modèle opérationnel :
 - on ne configure pas chaque équipement
 - on configure le réseau
- Ses API Northbound permettent l'automatisation
 - via des méthodes robustes
 - basées sur des données rationalisées
- Ses API Southbound configurent les équipements
 - avec cohérence
 - avec moins de risques d'erreur
 - plus rapidement

Avantages des réseaux SDN

- Les API Northbound et les modèles de données facilitent **l'automatisation** des fonctions complexes de management
- L'automatisation **simplifie** les opérations de management
- La simplification garantie la **cohérence** des configurations et réduit les risques **d'erreur**
- Le modèle de données centralisé permet la mise en œuvre d'outils modernes **d'analyse de données**, qui fournissent une meilleure visibilité du réseau, et donc une meilleure réactivité
- Les projets sont terminés plus **rapidement**
- Les modèles opérationnels savent tenir compte de **paramètres externes** : l'heure, le jour, la charge du réseau



Quiz

Quiz

A Layer 2 switch examines a frame's destination MAC address and chooses to **forward that frame** out port G0/1 only.

That action occurs as part of which plane of the switch?

- 
- a. Data plane
 - b. Management plane
 - c. Control plane
 - d. Table plane

Quiz

A router uses OSPF to learn routes and **adds those routes to the IPv4 routing table**.

That action occurs as part of which plane of the switch?

- a. Data plane
- b. Management plane
- c. Control plane
- d. Table plane



Quiz

A network uses an SDN architecture with switches and a centralized controller.

Which of the following terms describes a function or functions expected to be found **on the switches but not on the controller?**

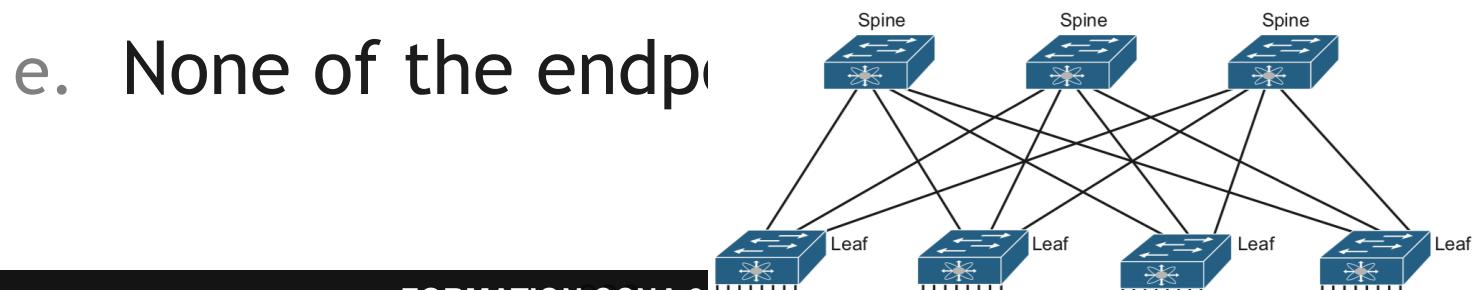
- a. A northbound interface
- b. A southbound interface
- c. Data plane functions
- d. Control plane functions



Quiz

To which types of nodes should an ACI leaf switch connect in a typical single-site design? (Choose two answers.)

- a. All of the other leaf switches
- b. A subset of the spine switches
- c. All of the spine switches
- d. Some of the endpoints
- e. None of the endpoints



Quiz

Which answers list an advantage of controller-based networks **versus** traditional networks? (Choose two answers.)

- a. The ability to configure the features for the network rather than per device
- b. The ability to have forwarding tables at each device
- c. Programmatic APIs available per device
- d. More consistent device configuration

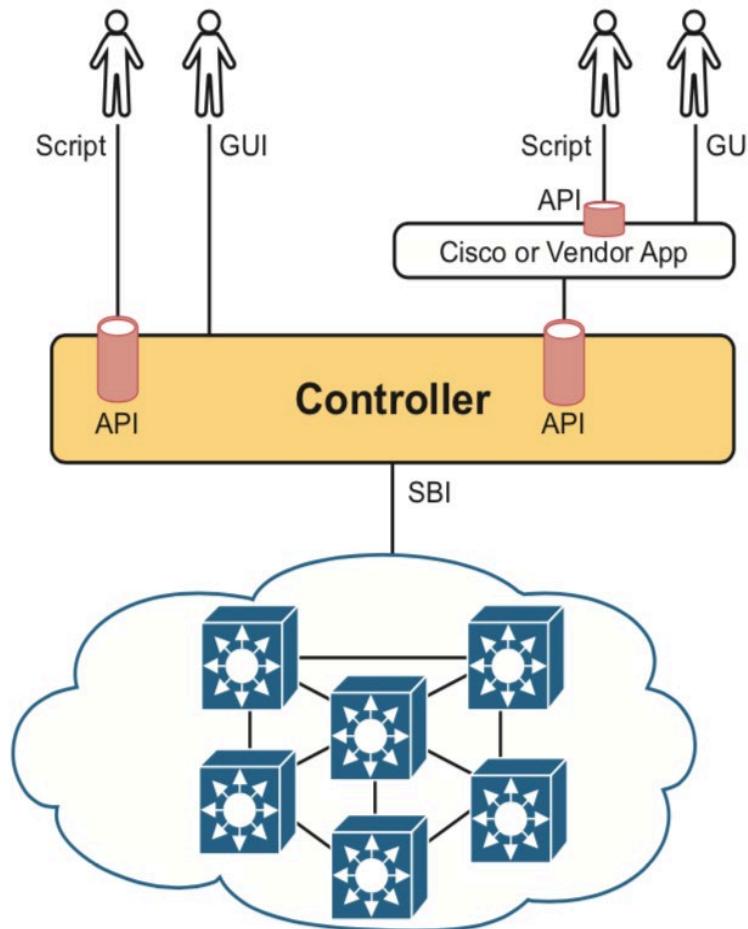
Software-Designed Access

SDA

Le SDA

- Objectif :
 - Concevoir une architecture SDN pour le **LAN**
- Le contrôleur :
 - **Cisco DNA Center**
 - DNA : Digital Network Architecture

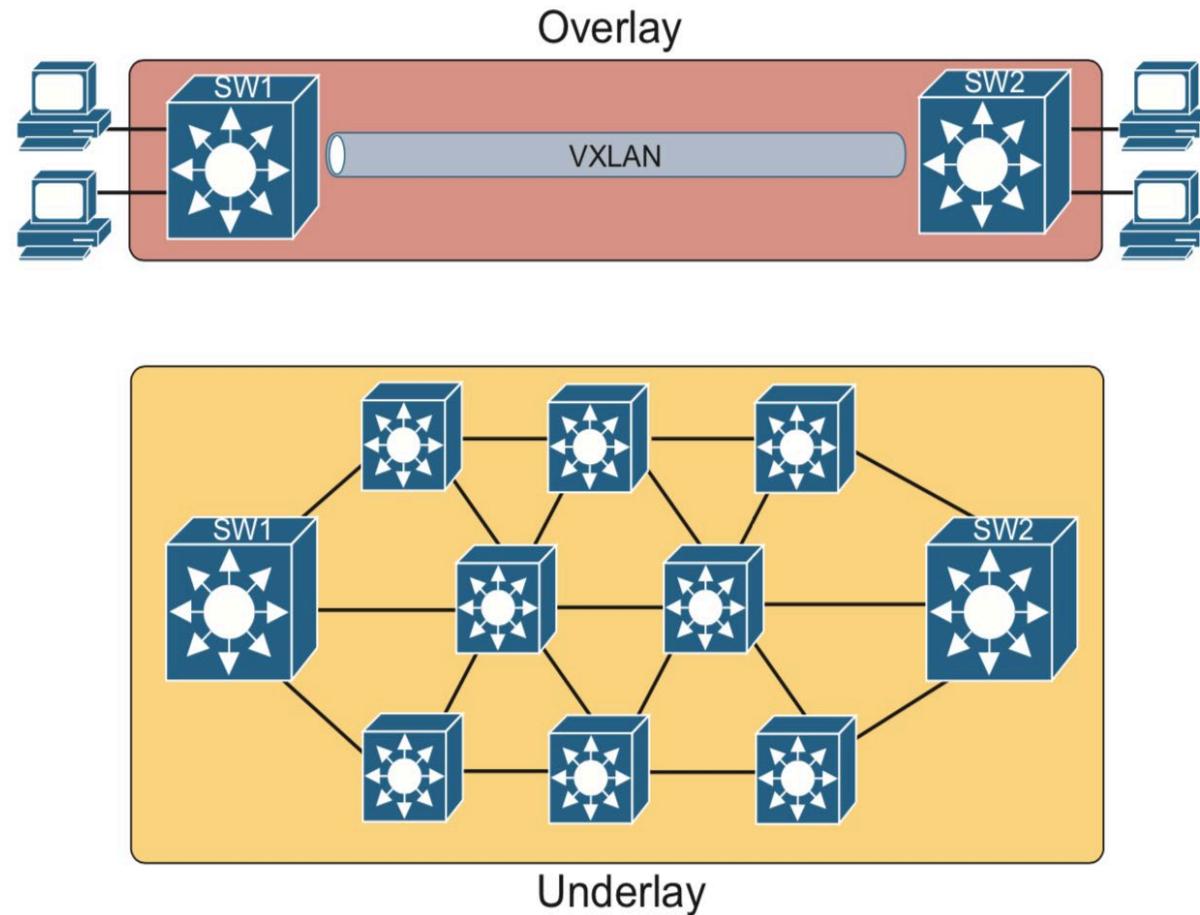
Architecture SDA



Southbound

- « **Fabric** » :
- « **Underlay** »
 - les équipements physique du réseau
 - routeurs, switch, cables, liens WiFi
 - un protocole de routage traditionnel
- « **Overlay** »
 - mécanisme permettant de créer des tunnels appelés VXLAN, « Virtual eXtensible LAN »
 - à chaque extrémité, le tunnel est connecté à 2 switchs appelés **FED** « **Fabric Edge Nodes** »
 - il transporte des données entre ces 2 **FED**

Fabric



Déployer un **underlay** : 2 options

- Conserver les équipements actuels :
 - Vérifier la compatibilité !
 - compatibilité hardware
 - Catalyst 3850, 3650, 9300, 9400, 9500 = oui
 - Catalyst 2960X, 2960 XR = non
 - compatibilité IOS
 - www.cisco.com/go/sda
 - Configuration **manuelle** !
 - risque d'interruption de la production...
 - Acquérir de nouveaux équipements :
 - Configuration **automatique** par le contrôleur DNA
 - « Plug & Play » (PnP)

Changement de topologie

- Topologie **traditionnelle** :
 - chaque switch d'accès connecté à 2 switchs de distribution

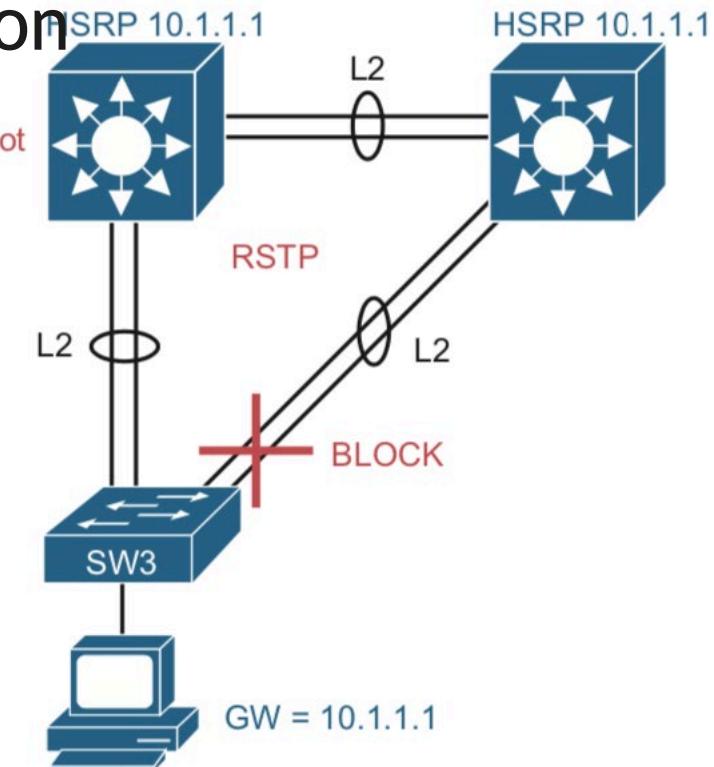
Distribution Layer
(Layer 3 Switches)

Root

• implémentation de :

- HSRP
- Etherchannel
- STP

Access Layer
(Layer 2 Switches)



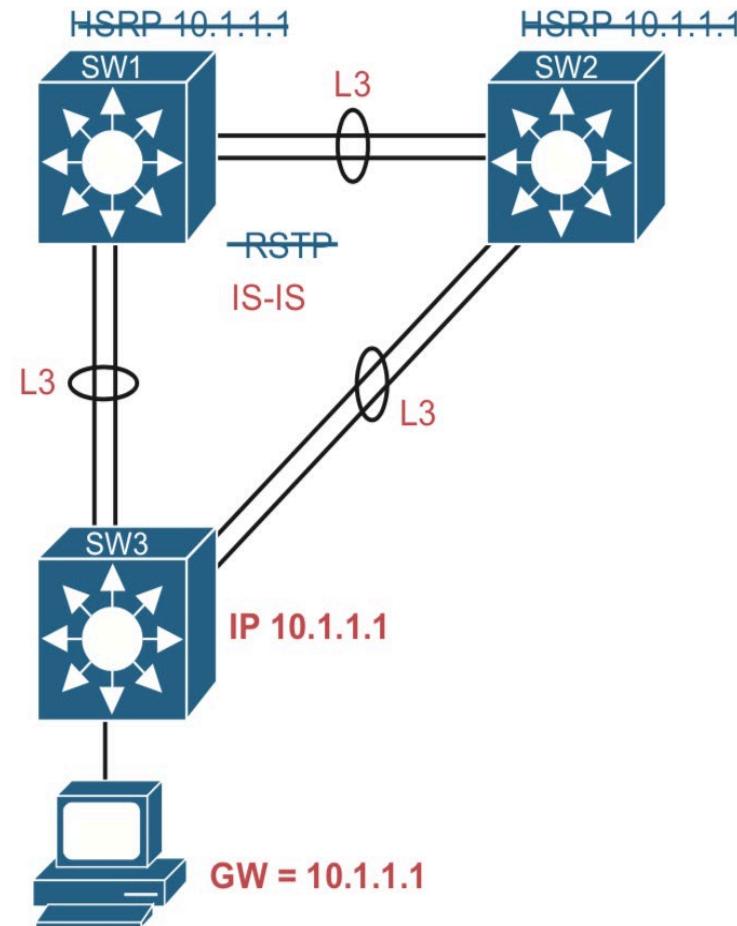
Changement de topologie

- Nouvelle topologie pour SDA :
 - « **Routed access layer** »
 - tous les switchs sont de **niveau 3**
 - toutes les inter-connections entre switchs sont de **niveau 3**
 - plus besoin de STP
 - les **GW** sont sur les switchs d'accès
 - **FED « Fabric Edge nodes »**
 - plus besoin de FHRP (HSRP, VRRP, GLBP)
 - Configuration optimale automatiquement effectuée par le contrôleur DNA

Topologie « Routed access »

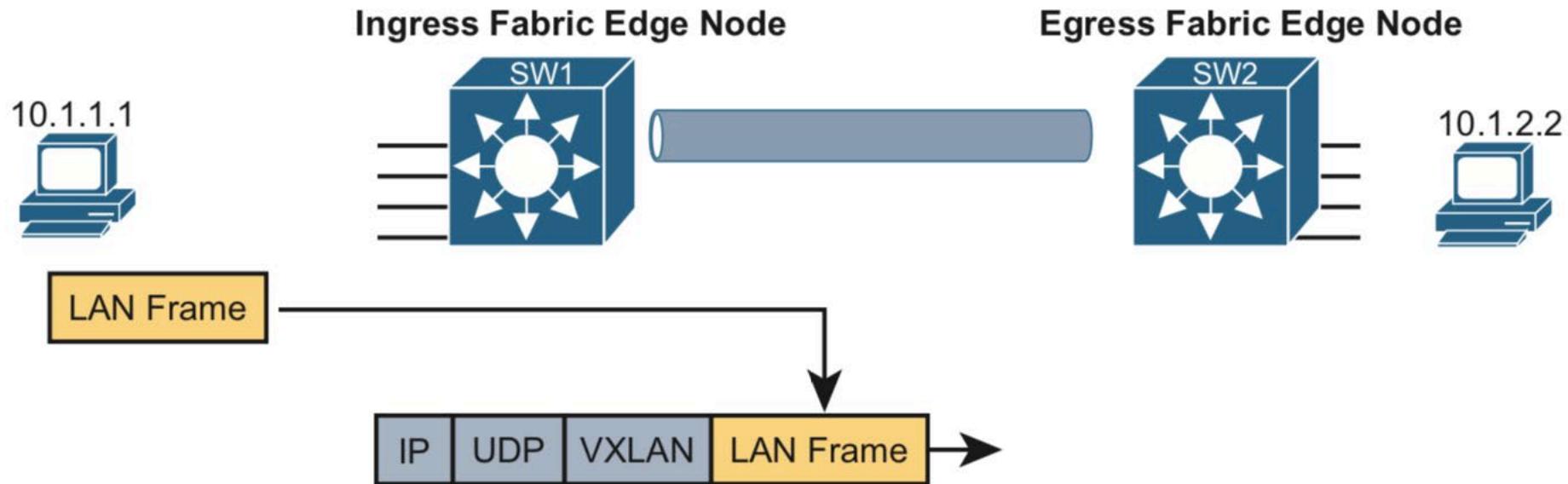
**Distribution
Layer
(Layer 3 Switches)**

**Access
Layer
(Layer 3 Switches)**



Overlay

- Processus de transmission des trames :
 - Le **FED « Fabric Edge Node » d'entrée encapsule la trame**
 - La trame parcourt la « Fabric »
 - Le **FED « Fabric Edge Node » de sortie dés-encapsule la trame**
- Pas d'impact sur les performances :
 - Processus effectués en **ASIC**

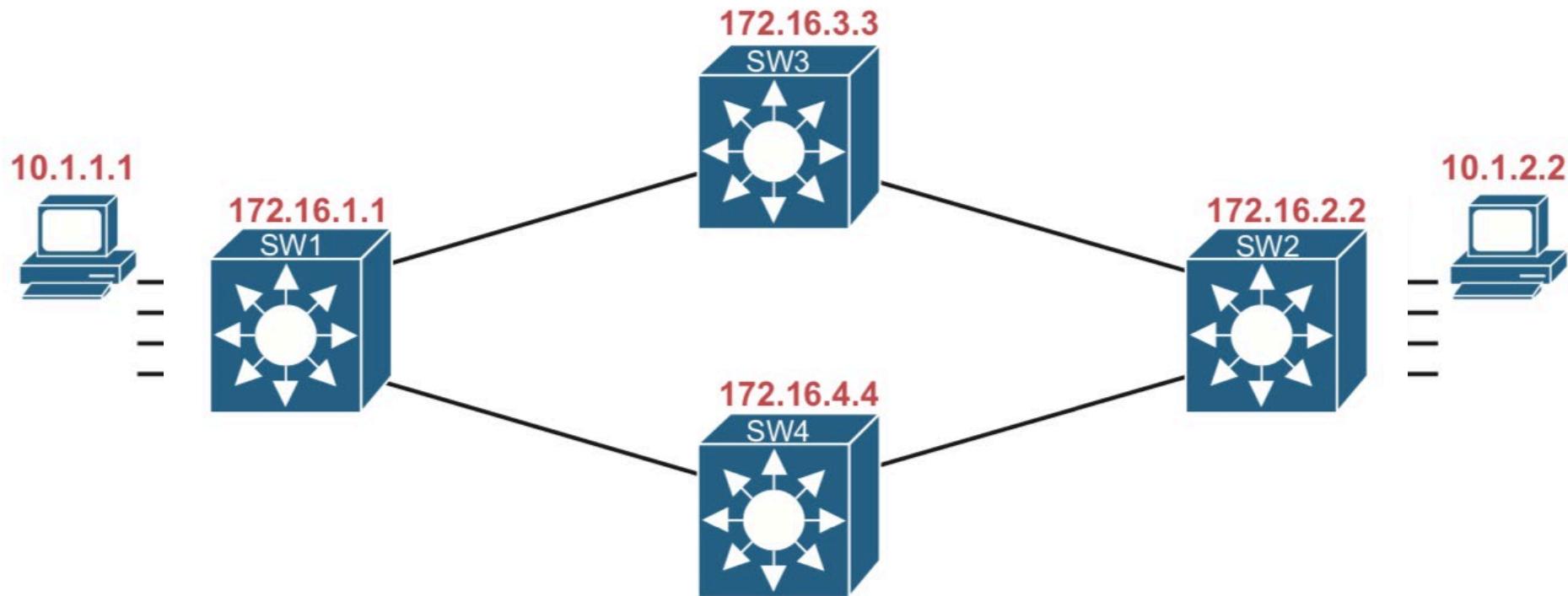


Adressage

- Overlay :
 - utilise le **même** plan d'adressage que l'entreprise
- Underlay :
 - utiliser un plan d'adressage **distinct**
- Le tunnel overlay crée un chemin entre les 2 switch **FED**
« **Fabric Edge Nodes** »

Exemple

- OVERLAY :



UNDERLAY

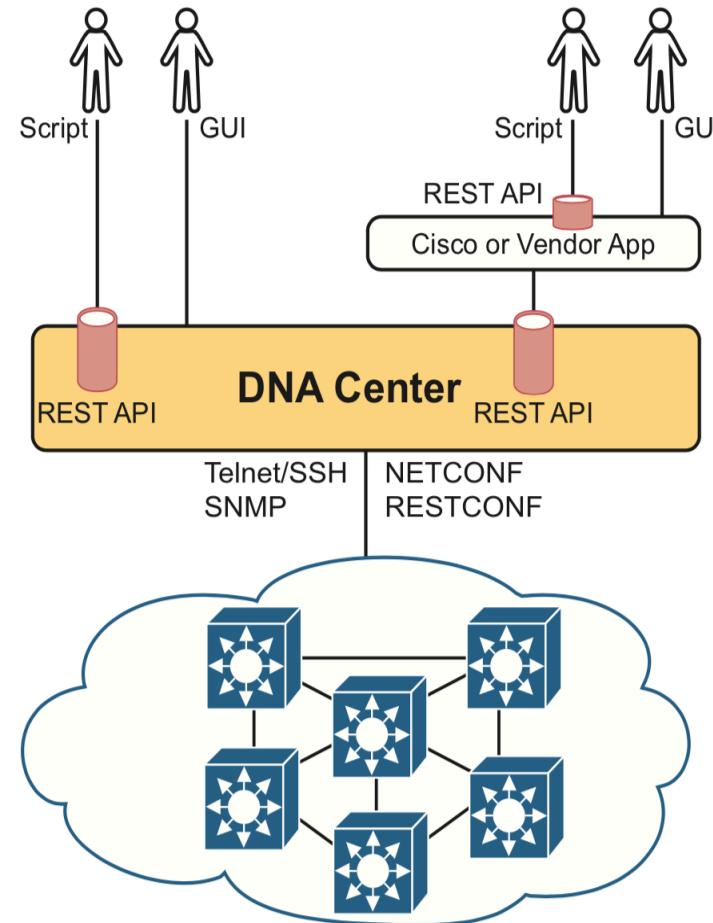
Cisco Digital Network Architecture Center

Le contrôleur Cisco DNA Center

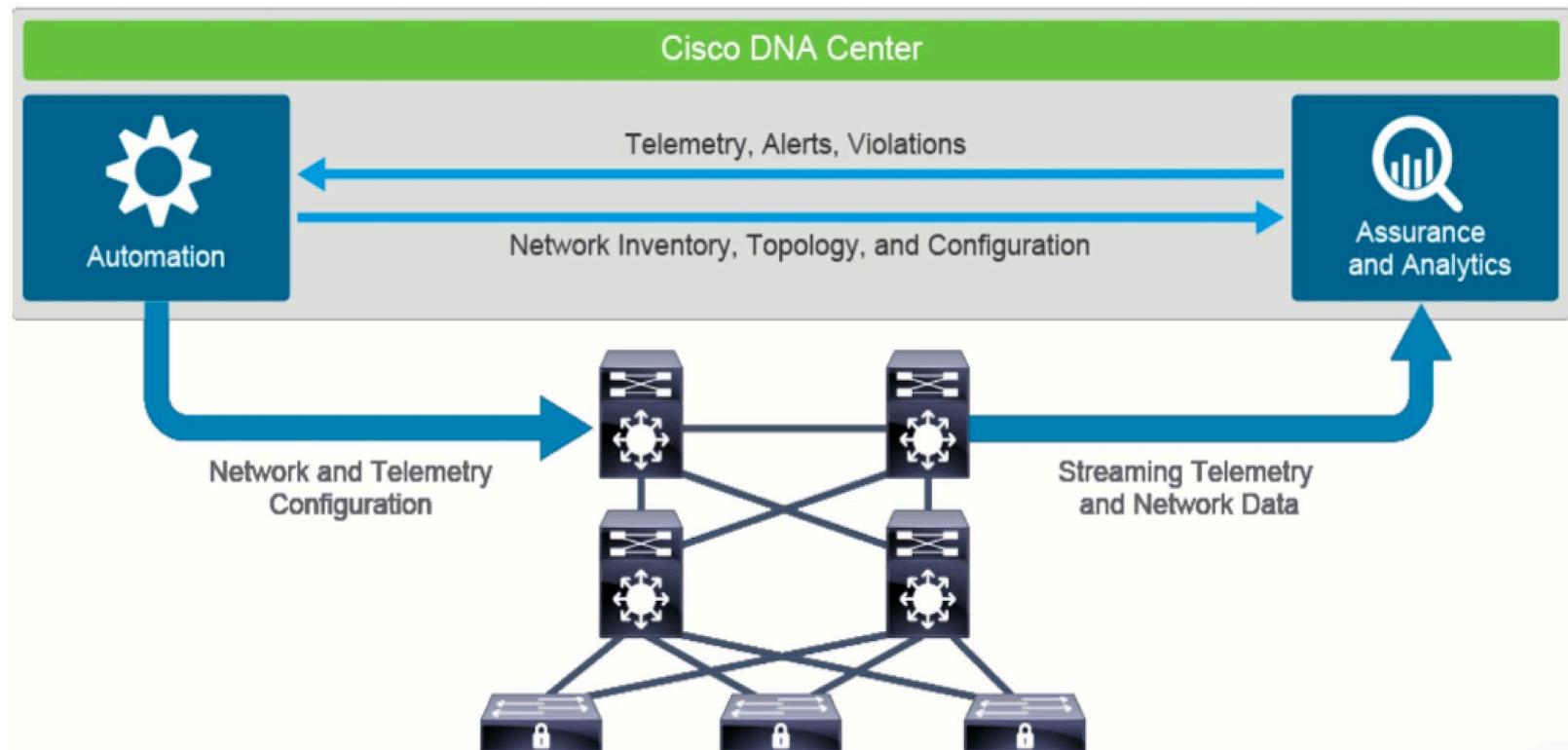
Présentation de DNA

- Soft livré sur une appliance
- Deux rôles :
 - **contrôleur** d'une architecture SDA
 - plateforme de **management** de toute architecture (SDA ou non)
 - similaire à PI : Prime Infrastructure

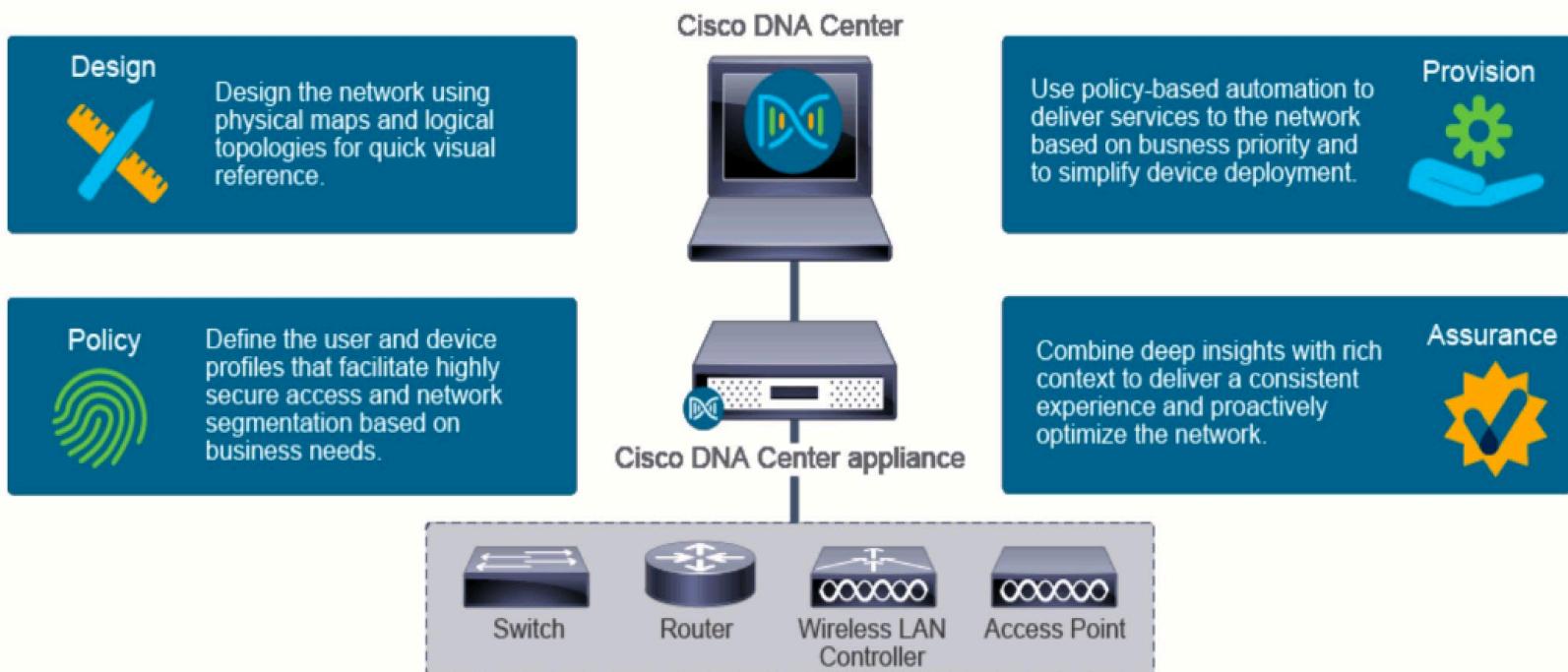
DNA en tant que contrôleur



Fonctionnement du DNA Center



Rôles du DNA Center



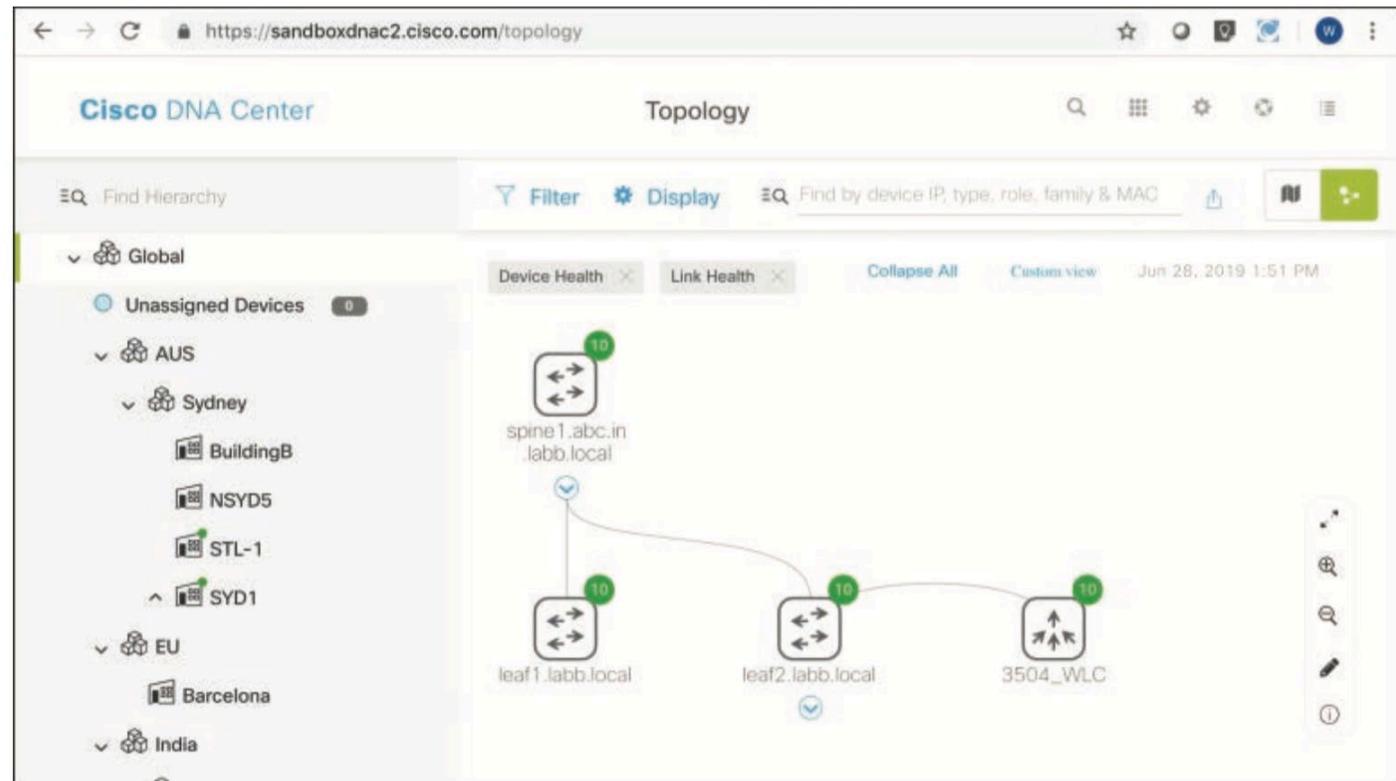
A complete system for intent-based networking

Modules du DNA Center

 Discovery Automate addition of devices to controller inventory	 Inventory Add, update or delete devices that are managed by the controller	 Topology Visualize how devices are interconnected and how they communicate	 Image Repository Download and manage physical and virtual software images automatically
 Command Runner Allows you to run diagnostic CLIs against one or more devices	 License Manager Visualize and manage license usage	 Template Editor An interactive editor to author CLI templates	 Network Plug and Play A simple and secure approach to provision networks with a near zero touch experience
 Telemetry Telemetry Design and Provision	 Data and Reports Access Data Sets, Schedule Data Extracts for Download in multiple formats like PDF Reports, CSV, Tableau etc.		BETA

Module « Topology »

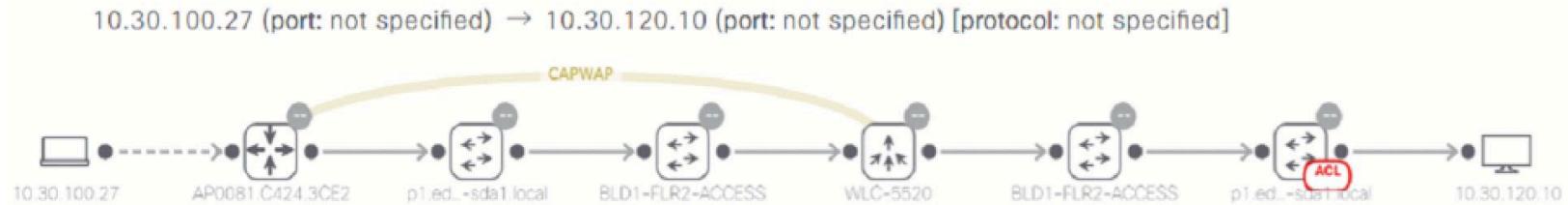
- Découverte des équipements réseau & affichage d'une carte topologique indiquant leur état de santé :



Outil « Path Trace »

✓ Path Trace

To find the location of an issue, perform a path trace between two nodes in your network.





Quizz

Quiz

In Cisco Software-Defined Access (SDA), which term refers to the **devices and cabling**, along with configuration that allows the network device nodes enough IP connectivity to send IP packets to each other?

- 
- a. Fabric
 - b. Overlay
 - c. Underlay
 - d. VXLAN

Quiz

In Cisco Software-Defined Access (SDA), which term refers to the **functions that deliver endpoint packets across the network using tunnels** between the ingress and egress fabric nodes?

- 
- a. Fabric
 - b. Overlay
 - c. Underlay
 - d. VXLAN

Quiz

In Software-Defined Access (SDA), which of the answers are part of the **overlay data plane**?

- a. LISP
- b. GRE
- c. OSPF
- d. VXLAN



Quiz

Which of the following protocols or tools could be used as part of the Cisco DNA Center **southbound** interface? (Choose three answers.)

- a. Ansible
- b. SSH
- c. NETCONF
- d. SNMP
- e. Puppet



Application Programming Interface

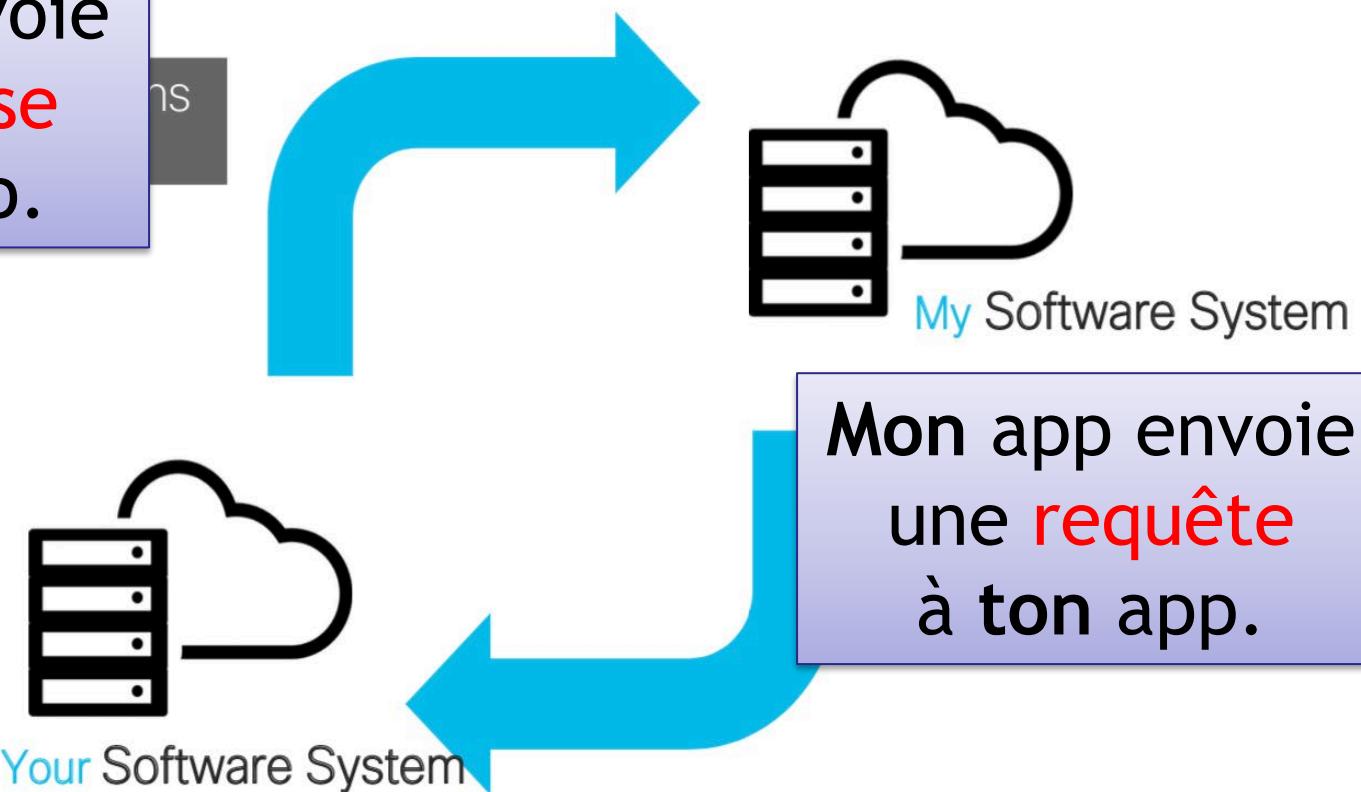
API

Objectif des API

- Permettre à **2 applications** de communiquer ensemble
- Exemples :
 - **le contrôleur** souhaite obtenir des informations sur les interfaces d'un **switch**
 - **le contrôleur** souhaite modifier la configuration d'un **routeur**
 - **l'ingénieur réseau** souhaite, via une **application**, modifier les polices du **contrôleur**, qui définissent les droits entre 2 groupes d'utilisateurs

Communication entre 2 app

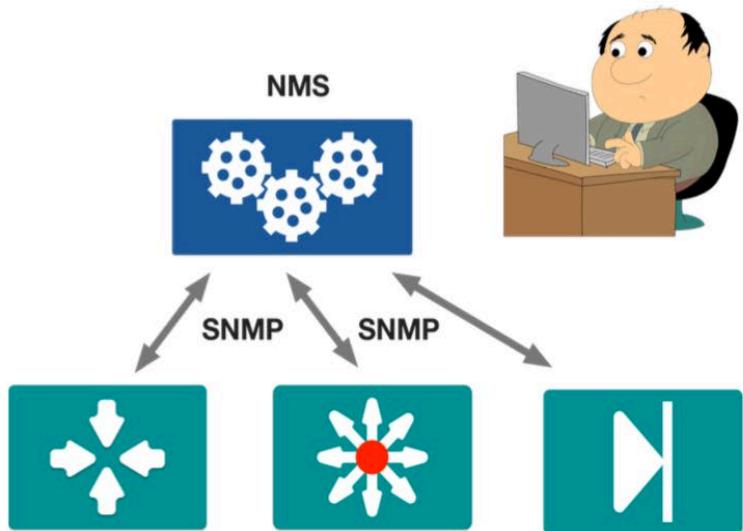
Ton app envoie
une réponse
à mon app.



Mon app envoie
une requête
à ton app.

Exemple 1 : SNMP !

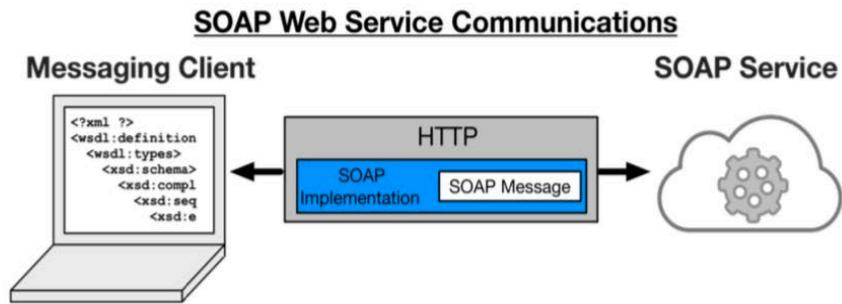
- “designed as a programmatic interface between management applications and devices”*
- Widely used for monitoring
- Limited use for configuration
- Network Management Systems primary consumer



* <https://tools.ietf.org/html/rfc3535>

Exemple 2 : SOAP

- Mature standard designed by Microsoft
- Used to build “Web Services” (software available over the internet)
- Typically uses HTTP, and dependent on XML
- Sometimes considered complex and rigid



Exemple 3 : REST

- API framework intended to build simpler web services than SOAP
- Another use for the HTTP protocol
- Popular due to performance, scale, simplicity, and reliability
- Technically an API framework

GET
POST
PUT
DELETE

{REST}

Exemple 4 : XML-RPC et JSON-RPC

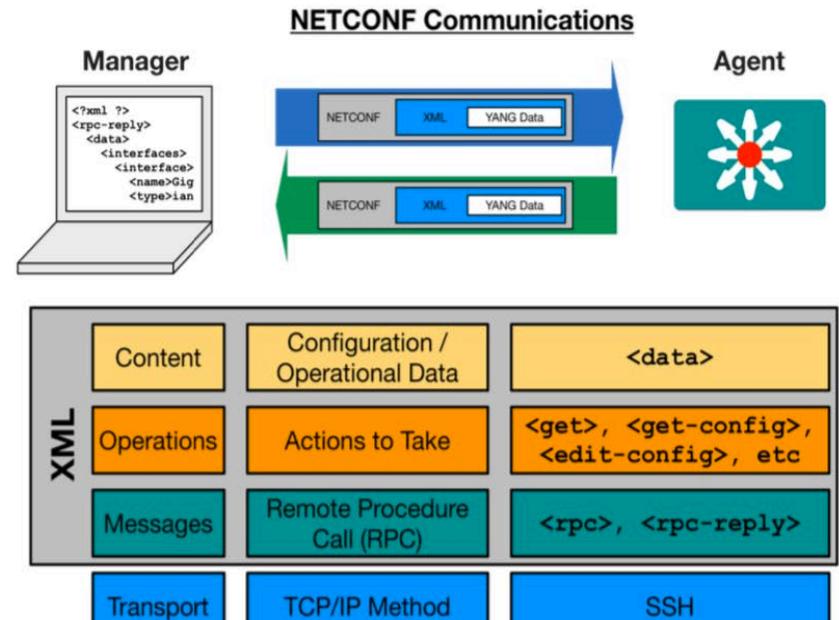
- Simple frameworks for communicating over HTTP
- RPC = Remote Procedure Call
 - When one system requests another system to execute code
- Offer XML and JSON data formats respectively

HTTP POST
REQUEST BODY:

```
[  
  {  
    "jsonrpc": "2.0",  
    "method": "cli",  
    "params":  
    {  
      "cmd": "show version",  
      "version": 1  
    },  
    "id": 1  
  }  
]
```

Exemple 5 : NETCONF

- Designed as replacement for SNMP
 - Standardized in 2006 / Updated 2011
 - Leverages SSH and XML
 - Defines transport and communication
 - Titled coupled to YANG for data



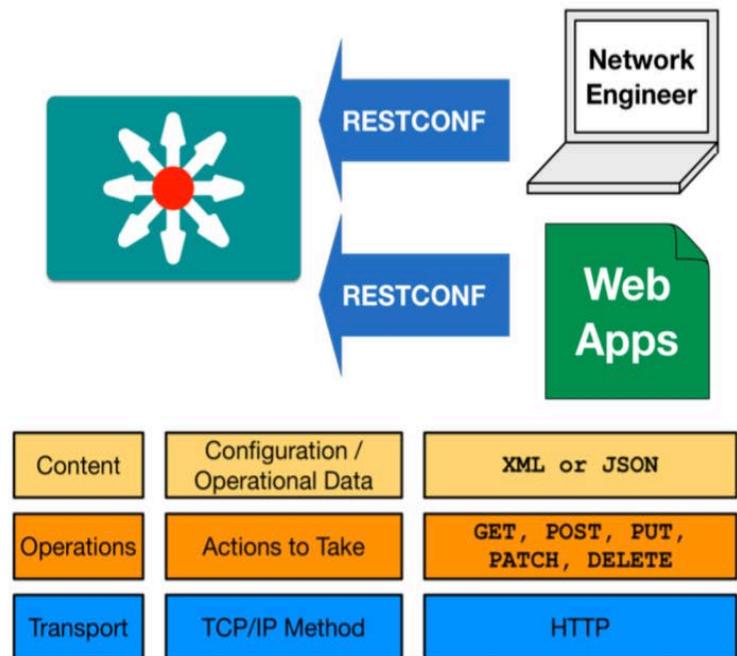
NETCONF

- Puissant :
 - peut lire les données opérationnelles
 - exemple : statistiques, utilisation mémoire, erreurs ...
 - peut lire et modifier les données de configuration
 - exemple : adresses IP des interfaces, protocoles de routage
- Les données sont encodées avec **XML**
- Complexe :
 - Statefull
 - met en place des **transactions** :
 - toutes les modifications sont regroupées
 - si l'une d'elle échoue, toutes les modif de la même transaction écouhent
 - utilise des **RPC** : « Remote Procedure Call »
 - met en œuvre **3 registres** (« data stores） :
 - running
 - start-up
 - candidate : toutes les modifications en cours (« uncommitted »)



Exemple 6 : RESTCONF

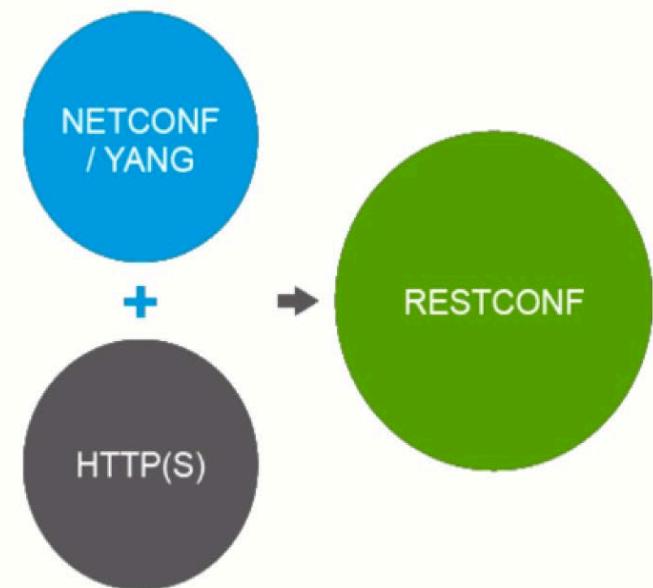
- Provide REST API like interface to network
- Standardized in 2017
- Supports XML and JSON
- Defines transport and communication
 - Titled coupled to YANG for data



De NETCONF à RESTCONF

RESTCONF characteristics are:

- Functional sub-set of NETCONF
- Exposes YANG models via a REST API (URL)
- Uses HTTP(S) as transport
- Uses XML or JSON for encoding
- Developed to use HTTP tools and programming libraries
- Uses common HTTP verbs in REST APIs



REpresentational State Transfer Application Programming Interface

REST API

- Les API qui respectent certaines règles sont dites « RESTful » ou « REST-based » :

1. **Architecture client / serveur**

- le client envoie une requête (« API Call ») au serveur

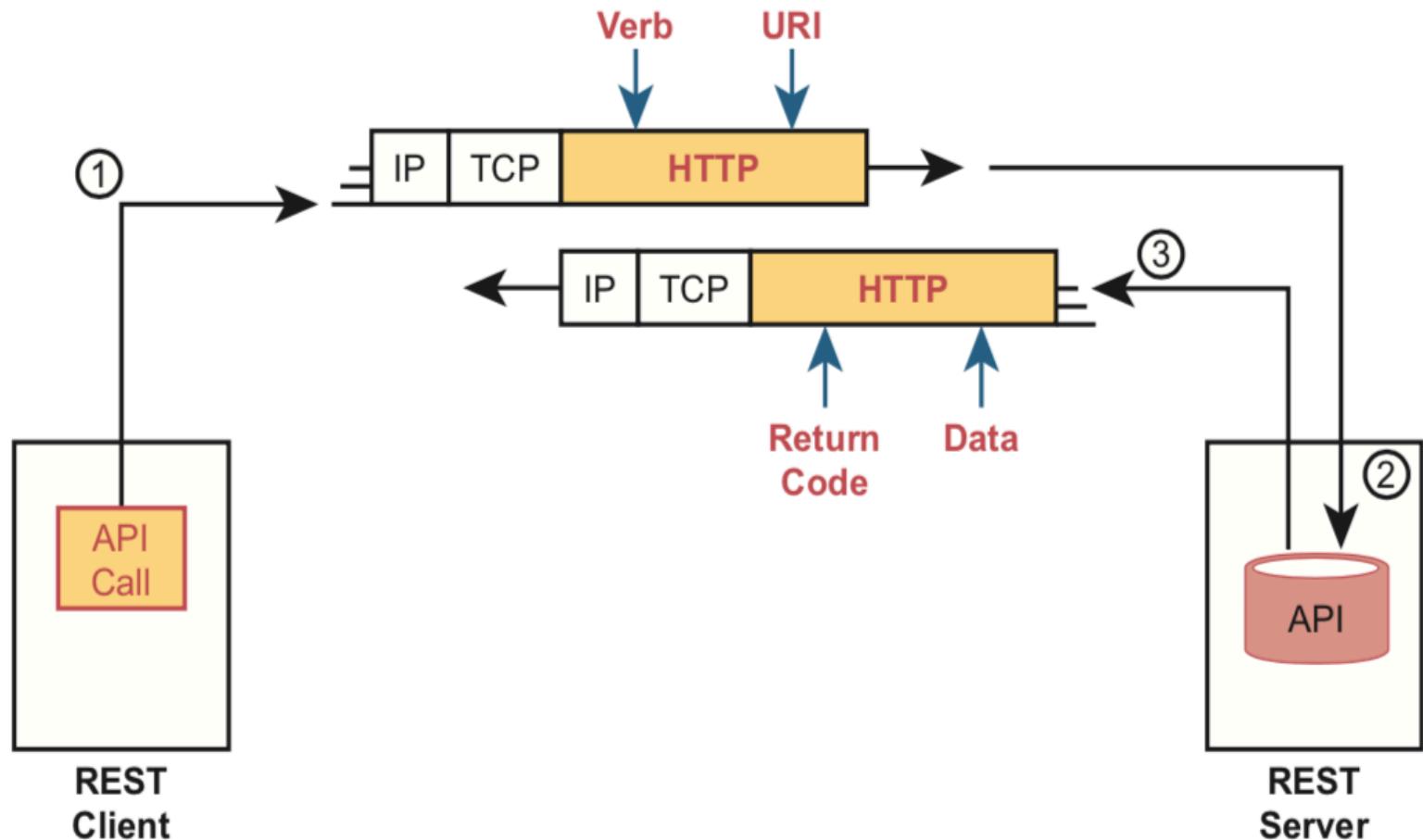
2. Mode opérationnel **stateless**

- chaque requête est indépendante des requêtes précédentes ou ultérieures

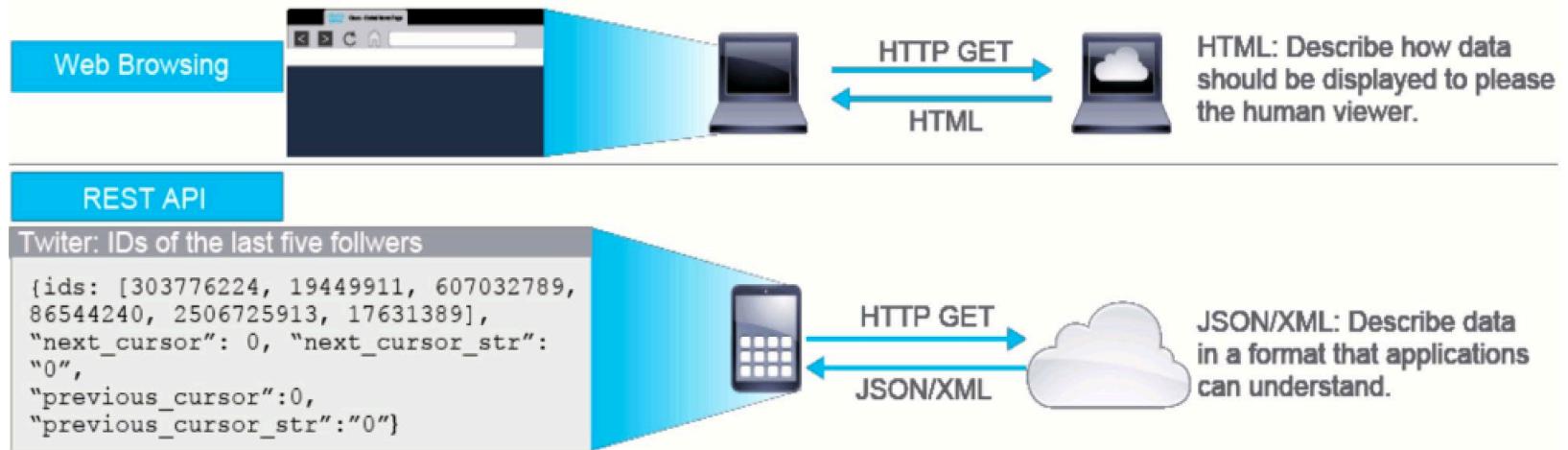
3. Indication de la possibilité de **mémoriser** la valeur de certaines variables

- évite de redemander la valeur d'une variable pendant un certain temps
- améliore les performances

Architecture client / serveur



Similitude REST & HTTP



REST & HTTP

- Pour communiquer entre 2 équipements, la plupart des REST API utilisent HTTP

- logique similaire
- utilisation de **verbes**

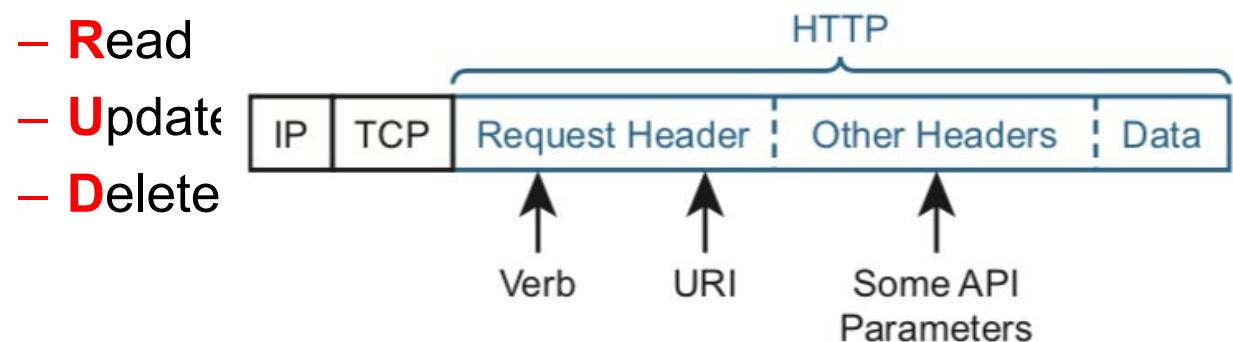
- pour indiquer l'action requise
- **CRUD**

- **C**reate

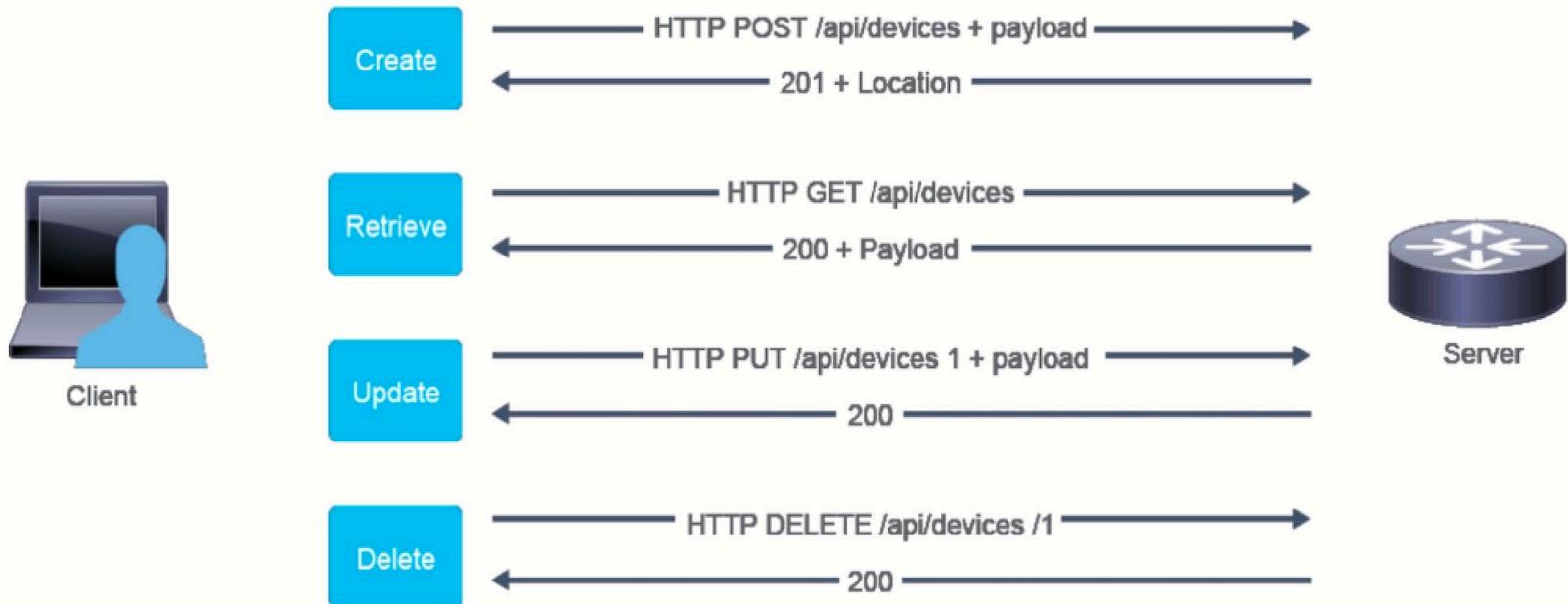
- **R**ead

- **U**pdate

- **D**elete



Verbes REST



Actions CRUD vs Verbes REST

HTTP Verb	Typical Purpose (CRUD)	Description
POST	Create	Used to create a new object, or resource. <i>Example: Add new book to library</i>
GET	Read	Retrieve resource details from the system. <i>Example: Get list of books from the library</i>
PUT	Update	Typically used to replace or update a resource. Can be used to modify or create. <i>Example: Update the borrower details for a book</i>
PATCH	Update	Used to modify some details about a resource. <i>Example: Change the author of a book</i>
DELETE	Delete	Remove a resource from the system. <i>Example: Delete a book from the library.</i>

PUT vs PATCH

- **PATCH** avec 1 route statique :
 - **rajoute** la route statique à la conf actuelle

- **PUT** avec 1 route statique :
 - **remplace** toutes les routes statiques par la route transmise

- Pour communiquer avec le DNA Center :
 - utiliser des **URI « Unique Ressource Identifier »**
 - spécifient à quelle ressource on souhaite accéder :

Hostname/Address
Protocol

HTTPS://dnac.example.com/dna/intent/api/v1/network-device

Path (Resource)

- spécifie les paramètres optionnels .

Hostname/Address
Protocol

HTTPS://dnac.example.com/dna/intent/api/v1/network-device?parm1=10.1.1.1...

Path (Resource)

Query (Parameters)

Autre exemple d'URI



- `http://` or `https://`
 - Define whether secure or open http
- **Server or Host**
 - Resolves to the IP and port to connect to
- **Resource**
 - The location of the data or object of interest on the server
- **Parameters**
 - Details to scope, filter, or clarify a request. Often optional.

Codes de réponse

Status Code	Status Message	Meaning
200	OK	All looks good
201	Created	New resource created
400	Bad Request	Request was invalid
401	Unauthorized	Authentication missing or incorrect
403	Forbidden	Request was understood, but not allowed
404	Not Found	Resource not found
500	Internal Server Error	Something wrong with the server
503	Service Unavailable	Server is unable to complete request

Meta Data

Header	Example Value	Purpose
Content-Type	application/json	Specify the format of the data in the body
Accept	application/json	Specify the requested format for returned data
Authorization	Basic dmFncmFudDp2YWdyYW50	Provide credentials to authorize a request
Date	Tue, 25 Jul 2017 19:26:00 GMT	Date and time of the message

- Used to pass information between client and server
- Included in both REQUEST and RESPONSE
- Some APIs will use custom headers for authentication or other purpose

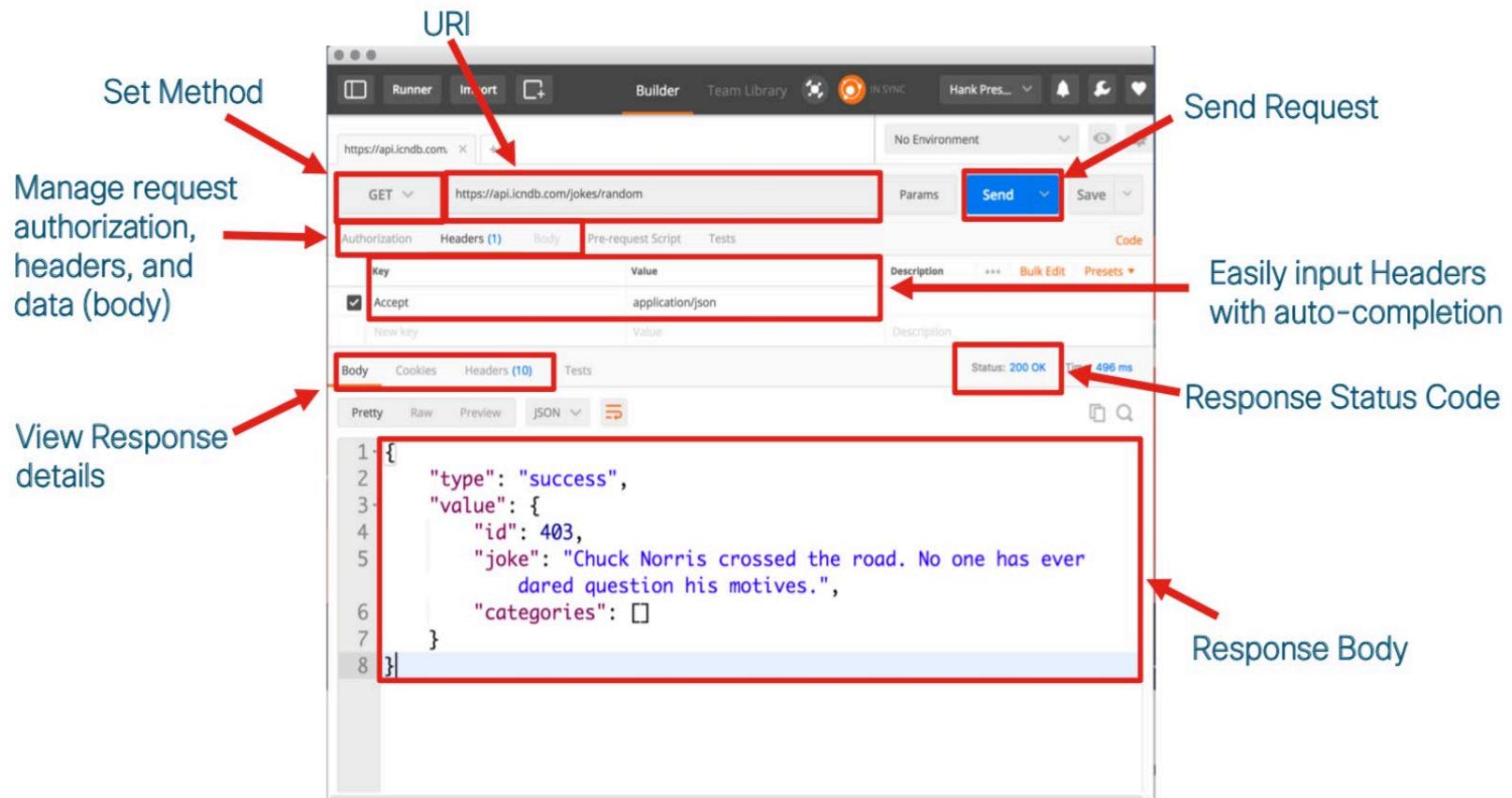
Exemple de client API : Postman

- Quickly test APIs in GUI
- Save APIs into Collections for reuse
- Manage multiple environments
- Auto generate code from API calls
- Standalone Application or Chrome Plugin

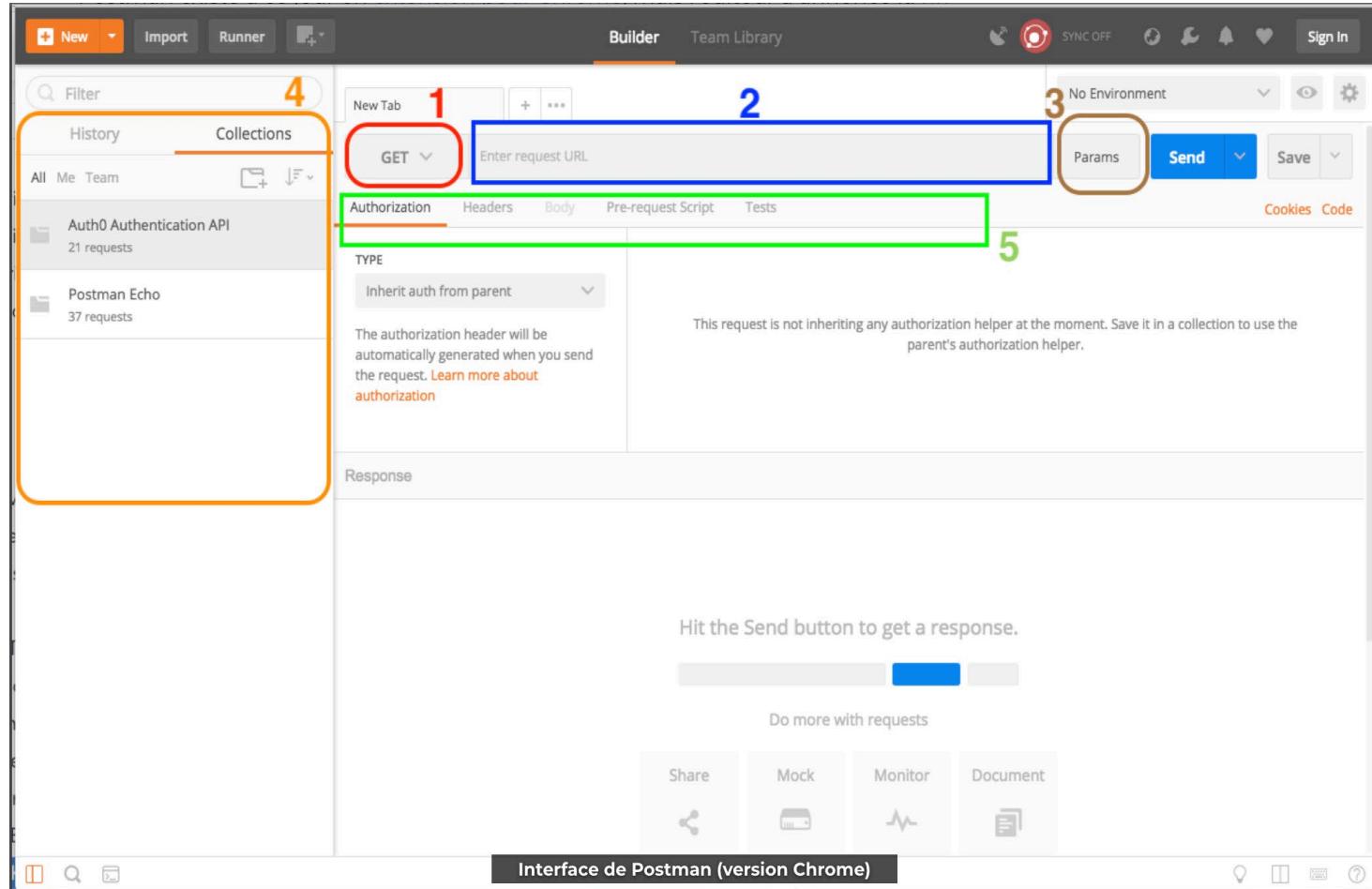


<https://www.getpostman.com>

Interface Postman



Demo avec Postman



Fonctionnalités des API

- **Obtenir** la valeur d'une variable :
 - Exemple : le statut d'une interface
- **Modifier** la valeur d'une variable :
 - Exemple : l'adresse IP d'une interface
- **Créer** une nouvelle variable
 - Exemple : rajouter une route statique
- **Supprimer** une variable
 - Exemple : supprimer un VLAN

Les variables

- Variables Simples :
 - alphanumérique
 - Exemple : **NOM = « DUPONT »**
 - numérique entière
 - Exemple : **AGE = 44**
- Variables complexes :
 - de type **liste** de données (ou tableau) :
 - Exemple : **NOMS = « DUPONT, DURAN, MARTIN »**
 - de type **dictionnaire** de données :
 - Exemple : **INDIVIDU = « Nom:Dupont, Age:44 »**

Exercice 1

- Quel est le type de cette variable ?

g0/0

g0/1

g0/2

Exercice 2

- Quel est le type de cette variable ?

config_speed → auto

config_duplex → auto

config_ip → 10.1.1.1

Format d'encodage

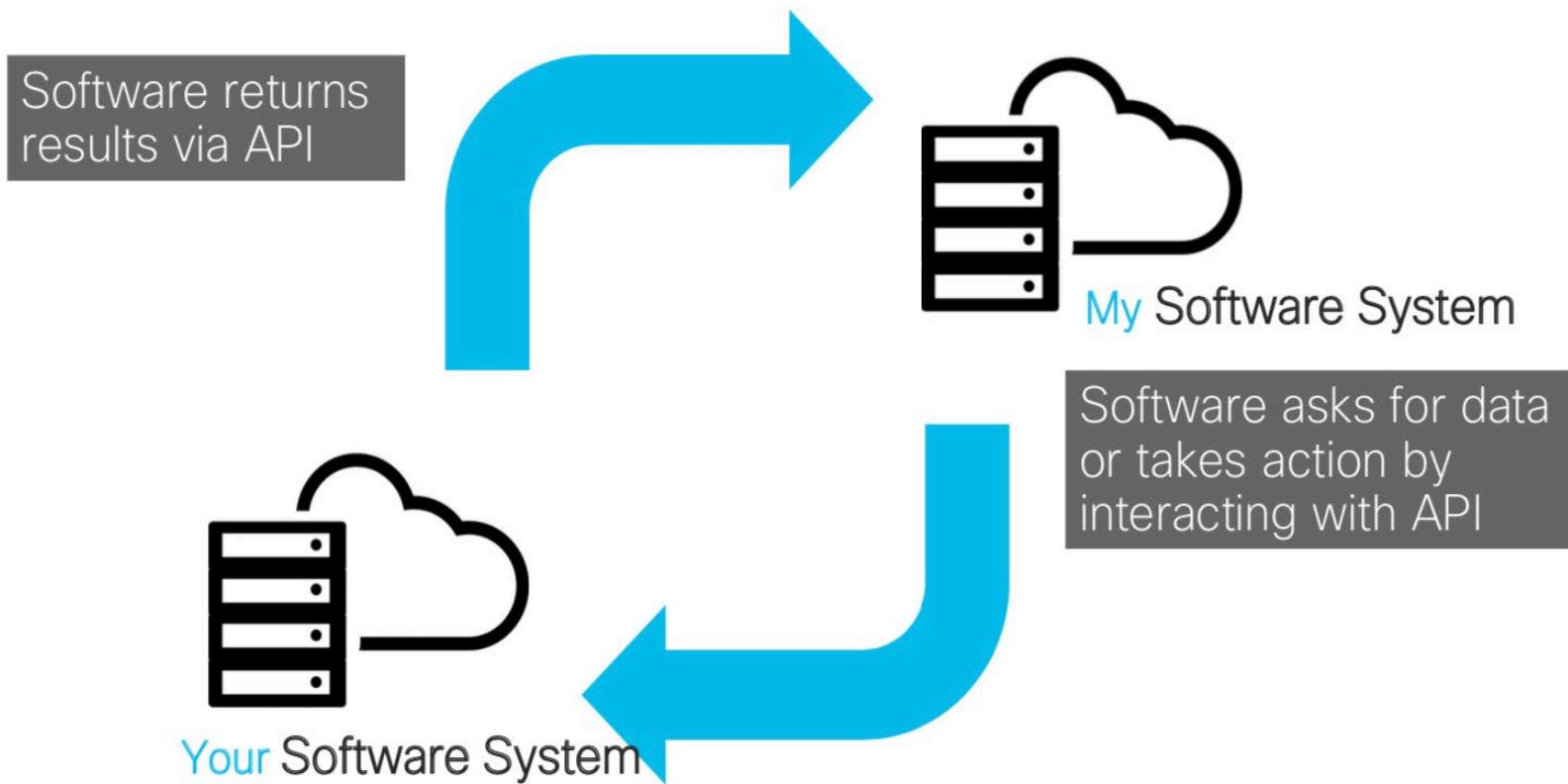


Formatage de données pour interface homme-machine

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.1.1    YES manual up       up
GigabitEthernet0/1  192.168.2.1    YES manual up       up
GigabitEthernet0/2  unassigned     YES unset  administratively down down
|
```



Formatage des données pour interface machine-machine



Formatage des données pour interface machine-machine

- Comment les données sont-elles échangées entre les applications ?
- Langages les plus courants :
 - JSON
 - XML
 - YAML

A **human readable** data structure that **applications use** to store, transfer, and read data.

Exemple pour NOM="DUPONT"

- JSON :

```
{ "nom" : "DUPONT" }
```

- XML

```
<nom> "DUPONT" </nom>
```

- YAML

```
nom: "DUPONT"
```

Encodage des données

- Les **mêmes** données peuvent être présentées (encodées) avec **différents langages** :

```
{  
    "ietf-interfaces:interface": {  
        "name": "GigabitEthernet5",  
        "description": "WAN",  
        "enabled": true,  
        "ietf-ip:ipv4": {  
            "address": [  
                {  
                    "ip": "172.16.0.5",  
                    "netmask": "255.255.255.0"  
                }  
            ]  
        }  
    }  
}
```

JSON

```
---  
ietf-interfaces:interface:  
  name: GigabitEthernet5  
  description: WAN  
  enabled: true  
  ietf-ip:ipv4:  
    address:  
      - ip: 172.16.0.5  
        netmask: 255.255.255.0
```

YAML

```
<?xml version="1.0" encoding="UTF-8" ?>  
<interface xmlns="ietf-interface">  
  <name>GigabitEthernet5</name>  
  <description>WAN</description>  
  <enabled>true</enabled>  
  <ipv4>  
    <address>  
      <ip>172.16.0.5</ip>  
      <netmask>255.255.255.0</netmask>  
    </address>  
  </ipv4>  
</interface>
```

XML

Les variables

"Key" : "Value"

"key": value

key: value

<key>value</key>

Exemple 1 JSON

{

```
"response": {  
    "type": "Cisco Catalyst 9300 Switch",  
    "family": "Switches and Hubs",  
    "role": "ACCESS",  
    "macAddress": "f8:7b:20:67:62:80",  
    "hostname": "cat_9k_1",  
    "serialNumber": "FCW2136L0AK",  
    "softwareVersion": "16.6.1",  
    "upTime": "17 days, 22:51:04.26",  
    "interfaceCount": "41",  
    "lineCardCount": "2",  
    "managementIpAddress": "10.10.22.66",  
    "series": "Cisco Catalyst 9300 Series Switches",  
    "softwareType": "IOS-XE"
```

}

}

Exemple 1 XML

```
<?xml version="1.0" encoding="UTF-8"?>  
<root>  
  <response>  
    <family>Switches and Hubs</family>  
    <hostname>cat_9k_1</hostname>  
    <interfaceCount>41</interfaceCount>  
    <lineCardCount>2</lineCardCount>  
    <macAddress>f8:7b:20:67:62:80</macAddress>  
    <managementIpAddress>10.10.22.66</managementIpAddress>  
    <role>ACCESS</role>  
    <serialNumber>FCW2136L0AK</serialNumber>  
    <series>Cisco Catalyst 9300 Series Switches</series>  
    <softwareType>IOS-XE</softwareType>  
    <softwareVersion>16.6.1</softwareVersion>  
    <type>Cisco Catalyst 9300 Switch</type>  
    <upTime>17 days, 22:51:04.26</upTime>  
  </response>  
</root>
```

Exemple 2 JSON

```
{  
  "ietf-interfaces:interface": {  
  
    "name": "GigabitEthernet2",  
  
    "description": "Wide Area Network",  
  
    "enabled": true,  
    "ietf-ip:ipv4": {  
  
      "address": [  
        {  
          "ip": "172.16.0.2",  
          "netmask": "255.255.255.0"  
        }  
      ]  
    }  
  }  
}
```

Exemple 2 XML

```
<?xml version="1.0" encoding="UTF-8" ?>

<interface xmlns="ietf-interfaces">

    <name>GigabitEthernet2</name>

    <description> Wide Area Network </description>

    <enabled>true</enabled>

    <ipv4>

        <address>
            <ip>172.16.0.2</ip>
            <netmask>255.255.255.0</netmask>
        </address>
    </ipv4>
```

Exemple YAML

```
ietf-interfaces:interface:  
    name: GigabitEthernet2  
    description: Wide Area Network  
    enabled: true  
    ietf-ip:ipv4:  
        address:  
        - ip: 172.16.0.2  
          netmask: 255.255.255.0
```

Comparatif

Acronym	Name	Origin/Definition	Central Purpose	Common Use
JSON	JavaScript Object Notation	JavaScript (JS) language; RFC 8259	General data modeling and serialization	REST APIs
XML	eXtensible Markup Language	World Wide Web Consortium (W3C.org)	Data-focused text markup that allows data modeling	REST APIs, Web pages
YAML	YAML Ain't Markup Language	YAML.org	General data modeling	Ansible

JAVASCRIPT OBJECT NOTATION

JSON

Règles de syntaxe

- Key
entre guillemets =>
- Value :
 - **texte**
=> **entre guillemets**
 - Exemple : "nom" : "Dupont"
 - **numérique
guillemets** => **sans**
 - Exemple : "age" : 44
 - **tableau** = une série de valeurs => **entre crochets,**
valeurs séparées par des virgules
 - Exemple : "prenoms" : ["jean", "pierre", "marie"]
 - **objet** = une série de paires => **entre accolades,**
paires séparées par des virgules
 - Exemple : { "nom": "Dupont", "prenom": "jean" }

4 types simples

- String
 - Example:

```
{  
    "name" : "GigabitEthernet5"  
}
```
- Number
 - Example:

```
{  
    "CRC Errors" : 105  
}
```
- Boolean
 - Example:

```
{  
    "enabled" : true  
}
```
- Null
 - Example:

```
{  
    "msec" : null  
}
```

1^{er} type complexe : l'objet

- Object
 - Example:

```
{  
    "name": "eth0",  
    "type": "ethernetCsmacd",  
    "location": "0",  
    "enabled": true,  
    "if-index": 2  
}
```

2ème type complexe : le tableau

- Array

- Example:

```
{  
    "ned:route": {  
        "ip-route-interface-forwarding-list": [  
            {  
                "prefix": "10.0.0.0",  
                "mask": "255.0.0.0",  
                "fwd-list": [  
                    {  
                        "fwd": "192.168.1.1"  
                    }  
                ]  
            }  
        ]  
    }  
}
```

Exemple :

```
{  
    "ned:route": {  
        "ip-route-interface-forwarding-list": [  
            {  
                "prefix": "10.0.0.0",  
                "mask": "255.0.0.0",  
                "fwd-list": [  
                    {  
                        "fwd": "192.168.1.1"  
                    }  
                ]  
            },  
            {  
                "prefix": "20.20.20.0",  
                "mask": "255.255.255.0",  
                "fwd-list": [  
                    {  
                        "fwd": "192.168.1.1"  
                    }  
                ]  
            }  
        ]  
    }  
}
```

Exercice 1

```
{
```

```
    "1stbest": "Messi",
```

```
    "2ndbest": "Ronaldo",
```

```
    "3rdbest": "Pele"
```

```
}
```

C'est un objet avec 3 variables.

Exercice 2

[

"Messi",

"Ronaldo",

"Dybala"

]

C'est une liste contenant 3 valeurs.

Exercice 3

```
{  
    "favorite_players": [  
        "Messi",  
        "Ronaldo",  
        "Dybala"  
    ],  
    "favorite_teams": [  
        "Barcelona",  
        "Juventus",  
        "Dortmund"  
    ]  
}
```

C'est un objet qui contient 2 variables.
La valeur de chaque variable est une liste.

Exercice 4

```
{  
    "ietf-interfaces:interface": {  
        "name": "GigabitEthernet2",  
        "description": "Wide Area Network",  
        "enabled": true,  
        "ietf-ip:ipv4": {  
            "address": [  
                {  
                    "ip": "172.16.0.2",  
                    "netmask": "255.255.255.0"  
                }  
            ]  
        }  
    }  
}
```

- C'est un objet qui contient 1 variable.
Cette variable est un objet de 4 variables.
La dernière variable est une liste.

Exercice 5

{

```
"addresses": [  
    {  
        "ip": "172.16.0.2",  
        "netmask": "255.255.255.0"  
    },  
    {  
        "ip": "172.16.0.3",  
        "netmask": "255.255.255.0"  
    },  
    {  
        "ip": "172.16.0.4",  
        "netmask": "255.255.255.0"  
    }  
]
```

- C'est un objet qui contient 1 variable.
Cette variable est une liste de 3 objets.

JSON vs Python

JSON	PYTHON
objet	dictionnaire
tableau "array"	liste

eXtensible Markup Language

XML

- Similaire à HTML :
 - utilise des **<tags>**
- Utilise des « **namespaces** » :
 - deux applications pourraient utiliser le même **<tag>** pour des données différentes
 - le « **namespace** » résout ce conflit :
 - identifiant unique permet de distinguer les 2 **<tag>**
 - il fait référence à un modèle de données YANG

Exemple XML

```
<interfaces xmlns:=" [...] yang:ietf-  
interfaces">  
<interface>  
  
    <name>eth0</name>  
    <type>ethernetCsmacd</type>  
  
    <location>0</location>  
    <enabled>true</enabled>  
    <if-index>2</if-index>  
  
    </interface>  
</interfaces>
```

Liste en XML

```
<?xml version="1.0" encoding="UTF-8" ?>

<addresses>
    <ip>172.16.0.2</ip>
    <netmask>255.255.255.0</netmask>
</addresses>
<addresses>
    <ip>172.16.0.3</ip>
    <netmask>255.255.255.0</netmask>
</addresses>
<addresses>
    <ip>172.16.0.4</ip>
    <netmask>255.255.255.0</netmask>
</addresses>
```

Yaml Ain't Markup Language

YAML

- Le plus adapté à la lecture **humaine**
 - de plus en plus populaire chez les développeurs
- Pas compatible avec les API des équipements CISCO
 - utilisé toutefois pour configurer les équipements Cisco avec **Ansible**

Liste en YAML

addresses:

- ip: 172.16.0.2
netmask: 255.255.255.0
- ip: 172.16.0.3
netmask: 255.255.255.0
- ip: 172.16.0.4
netmask: 255.255.255.0

Data Modeling Language

YANG

- Yet Another Next Generation
- Langage formel pour **représenter des données** sous forme arborescente et modulaire
- Langage de haut niveau :
 - définit des types de données et leurs contraintes
- Tout équipement réseau est décrit par des modules Yang
 - Yang modélise ce qu'on peut lire ou modifier
 - JSON ou XML vont permettre d'encoder ces données
 - NETCONF ou RESTCONF vont permettre de modifier ces données

- YANG est un **modèle de données** :
 - un modèle ne contient **aucune donnée** de configuration ou d'état
 - il représente juste **comment** ces dernières sont organisées
- Exemple :

```
module: ietf-interfaces

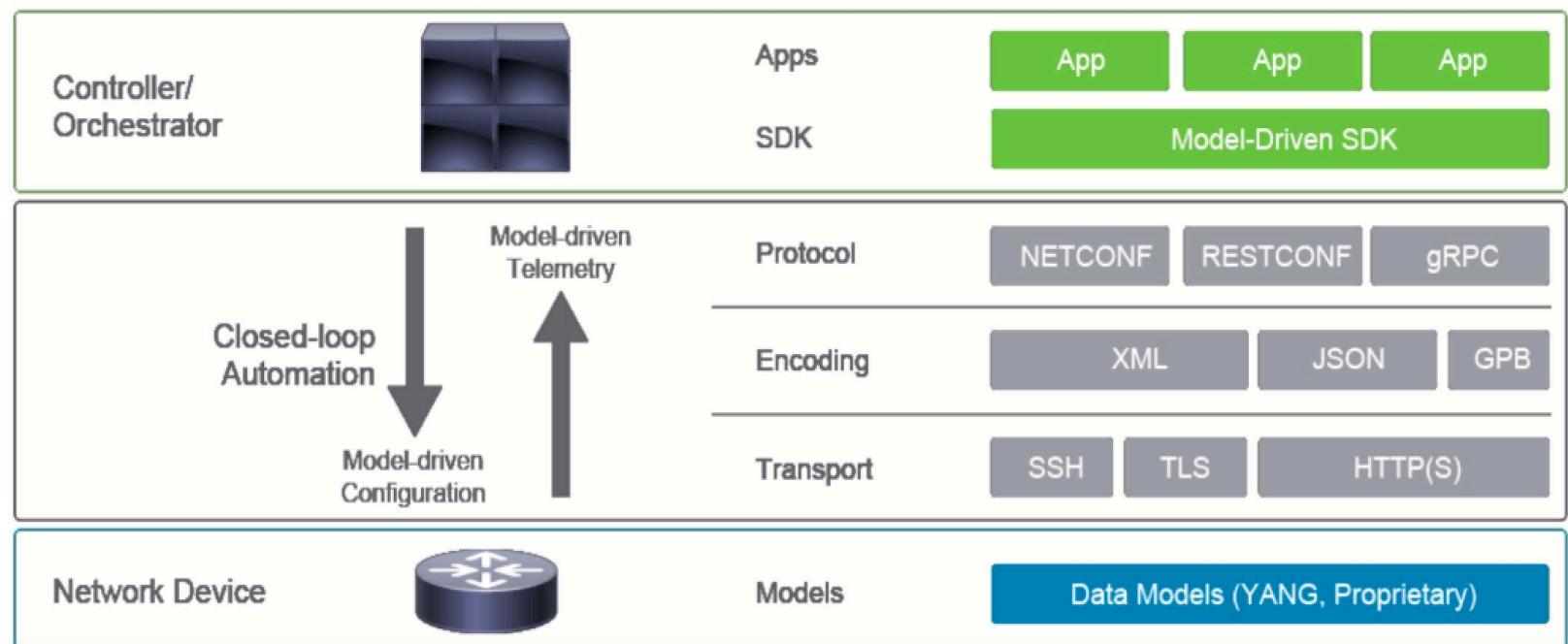
  +-rw interfaces
    |  +-rw interface* [name]
    |    +-rw name                      string
    |    +-rw description?              string
    |    +-rw type                      identityref
    |    +-rw enabled?                 boolean
    |    +- [...]
```

Réponse XML

```
<rpc-reply message-id="1" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
      <interface>
        <name>eth0</name>
        <type xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-iftype">ianaift:ethernetCsmacd</type>
        <enabled>true</enabled>
        [...]
      </interface>
    </interfaces>
  </data>
</rpc-reply>
```

Vue d'ensemble des réseaux SDN

Southbound API



SDK = Software Development KIT : set of tools and software libraries that allows end users to create their own custom applications



Quiz

Quiz

Which of the following are required attributes of a REST-based API? (Choose two answers.)

- a. Uses HTTP
- b. Objects noted as to whether they can be cached
- c. Classful operation
- d. Client/server architecture



Quiz

Which answers list a matching software development **CRUD** action to an **HTTP verb** that performs that action? (Choose two answers.)

- a. CRUD create and HTTP PATCH
- b. CRUD update and HTTP PATCH
- c. CRUD delete and HTTP PUT
- d. CRUD read and HTTP GET



Quiz

Examine the following URI that works with a Cisco DNA Controller:

<https://dnac.example.com/dna/intent/api/v1/network-device?managementIpAddress=10.10.22.74>

Which part of the URI is considered to **identify the resource** but not any parameters?

- 
- a. https://
 - b. dnac.example.com
 - c. dna/intent/api/v1/network-device

Quiz

Which of the following **data modeling languages** would be most likely to be used in a response from a **REST-based server API** used for networking applications? (Choose two answers.)

- a. JSON
- b. YAML
- c. JavaScript
- d. XML



Quiz

Which answers correctly describe the format of the **JSON** text below?
(Choose two answers.)

```
{ "myvariable": [1,2,3] }
```

- 
- 
- a. One JSON object that has one key:value pair
 - b. One JSON object that has three key:value pairs
 - c. A JSON object whose value is a second JSON object
 - d. A JSON object whose value is a JSON array

Quiz

Which answers refer to **JSON values** rather than **JSON keys** as found in the sample JSON data? (Choose two answers.)

```
{  
  "response": {  
    "type": "Cisco Catalyst 9300 Switch",  
    "family": "Switches and Hubs",  
    "role": "ACCESS",  
    "managementIpAddress": "10.10.22.66"  
  }  
}
```

- a. “response”
- b. “type”
- c. “ACCESS”
- d. The entire blue area



Software Defined Network

SDN

Overview of Network Programmability in Enterprise Network

Application Layer

Business Applications

API

API

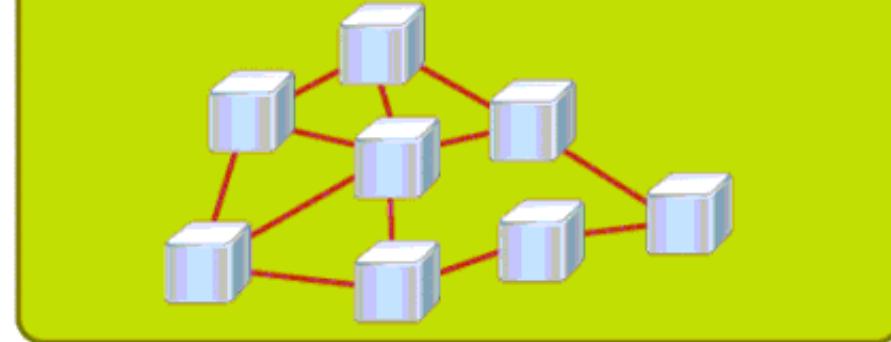
API

Network Services

Network Services

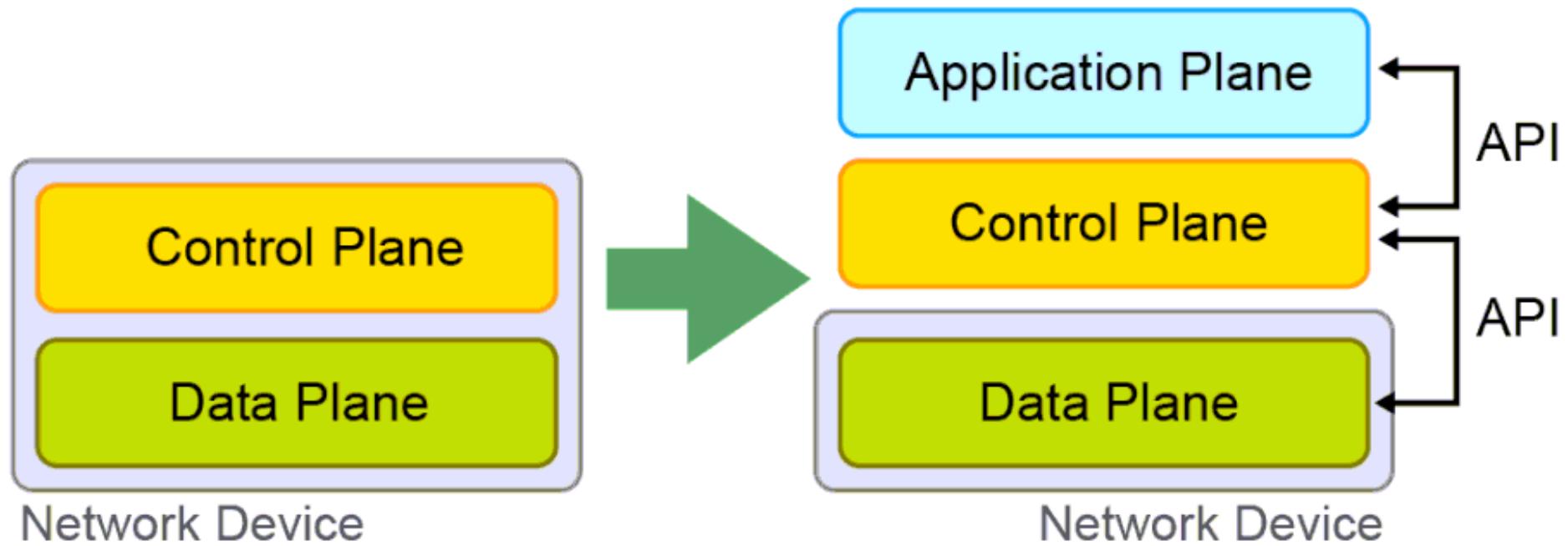
Control Layer

Infrastructure Layer





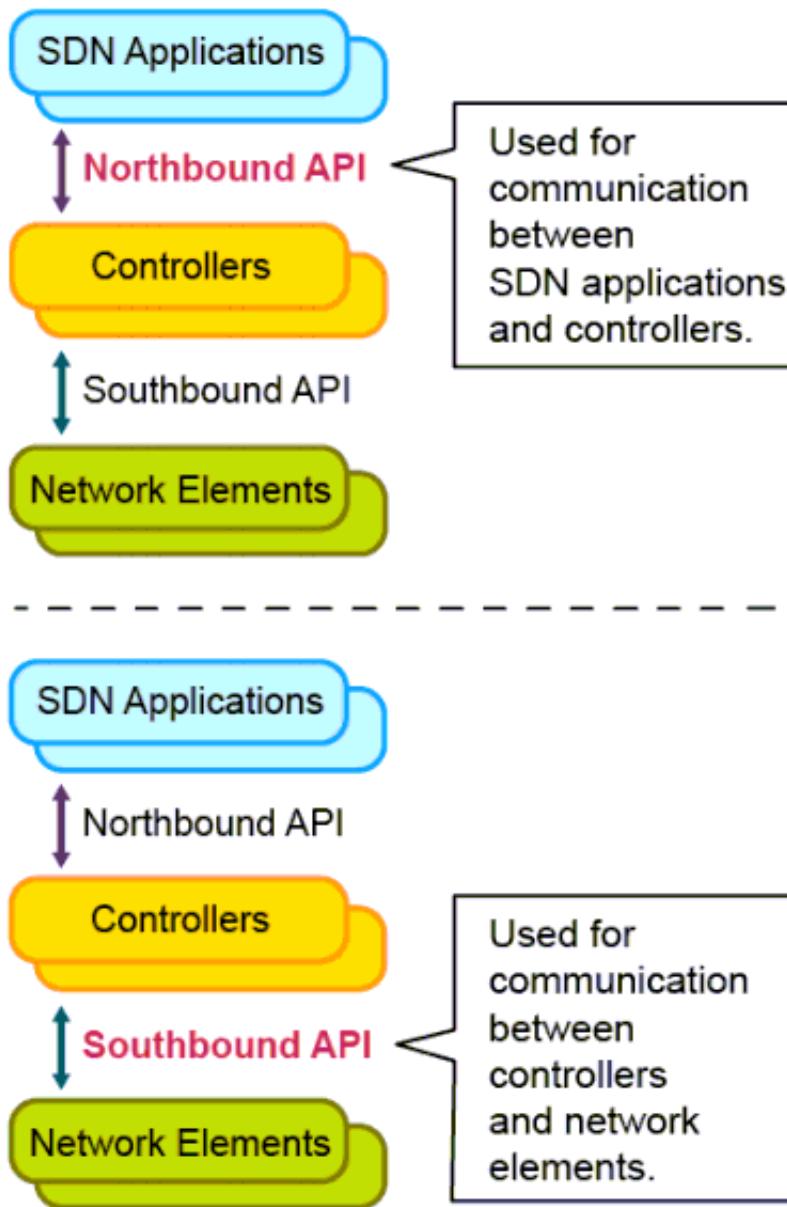
Application Programming Interfaces



Traditional Network
Architecture

SDN Architecture

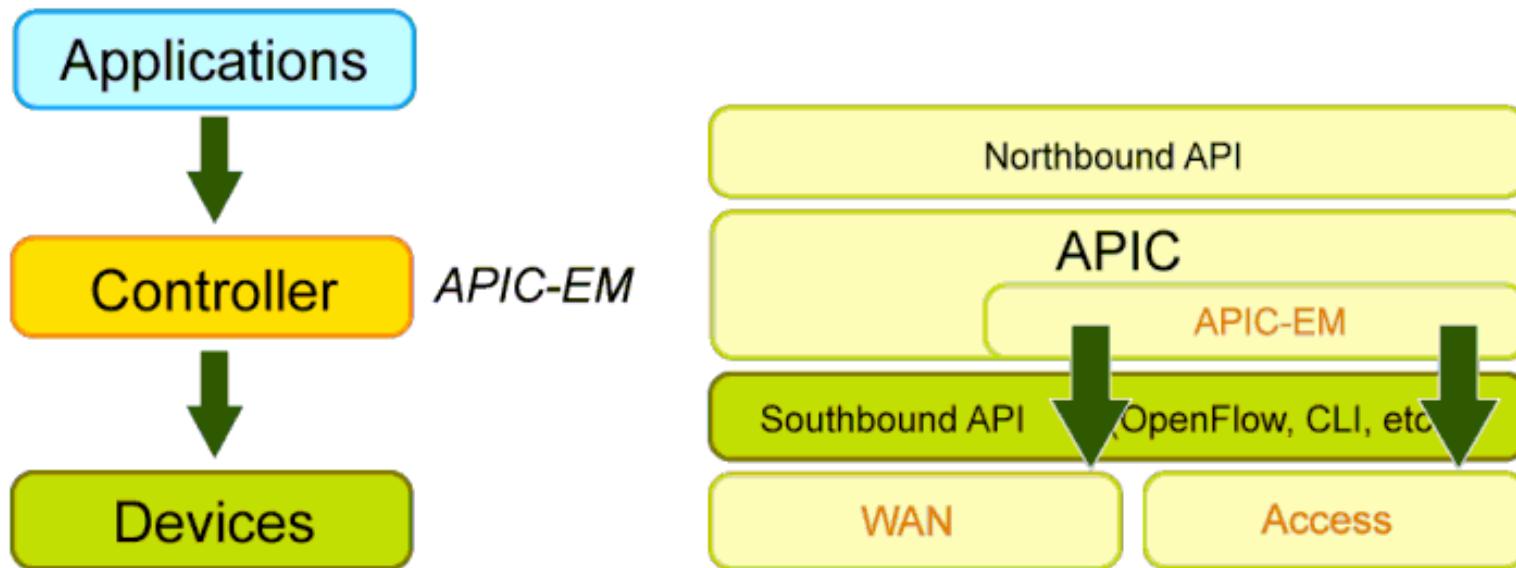
Application Programming Interfaces (Cont.)



- **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:** Configure 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

Screenshot of the APIC-Enterprise Module (APIC-EM) interface showing a network path trace between two hosts (A and B).

The path is traced through the following devices:

- A → SDN-BRANCH-3750-STACK (40.0.5.12)
- SDN-BRANCH-3750-STACK → SDN-BRANCH-ISR3945 (40.0.5.15)
- SDN-BRANCH-ISR3945 → SDN-BRANCH-3850-TB1 (40.0.5.16)
- SDN-BRANCH-3850-TB1 → SDN-BRANCH-ASR1002 (40.0.5.17)
- SDN-BRANCH-ASR1002 → SDN-CAMPUS-CXH-2 (40.0.5.18)
- SDN-CAMPUS-CXH-2 → SDN-BRANCH-C4K (40.0.5.19)
- SDN-BRANCH-C4K → B (40.0.5.14)

Trace Results:

apple quick time
ports 400-800-400

Host A (40.0.5.12) details:

- SDN-BRANCH-3750-STACK
 - GigabitEthernet2/0/2 (ingress)
 - GigabitEthernet2/0/3 (egress)
- SDN-BRANCH-ISR3945
 - GigabitEthernet0/2 (ingress)
 - GigabitEthernet0/0 (egress)
- SDN-BRANCH-3850-TB1
 - GigabitEthernet1/0/4 (ingress)
 - GigabitEthernet1/0/2 (egress)
- SDN-BRANCH-ASR1002
 - GigabitEthernet0/0/0 (ingress)
one_bit_dlc_conflict
 - DENY TCP any any eq 458 Status: Up/Down
 - DENY UDP any any eq 458 Status: Up/Down
 - GigabitEthernet0/0/3 (egress)

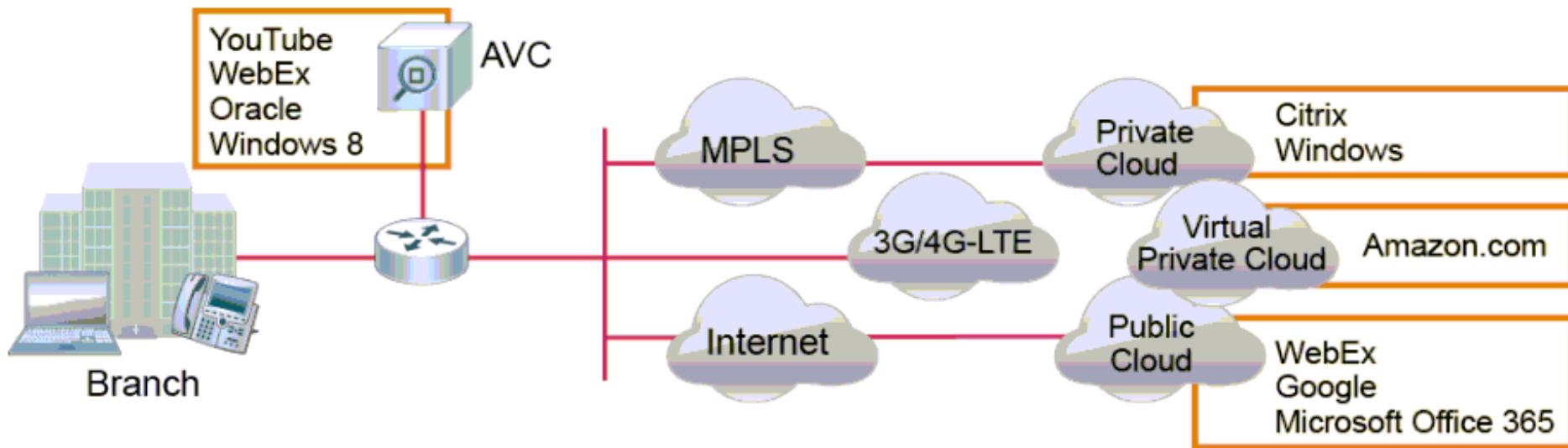
This is where the Apple QuickTime traffic gets blocked.



Introducing Cisco Intelligent WAN

The following are the four components of IWAN:

- Transport Independent Connectivity
- Intelligent Path Control
- Application Optimization
- Highly Secure Connectivity



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

Video



- Bursty
- Greedy
- Drop-sensitive
- Delay-sensitive
- UDP priority

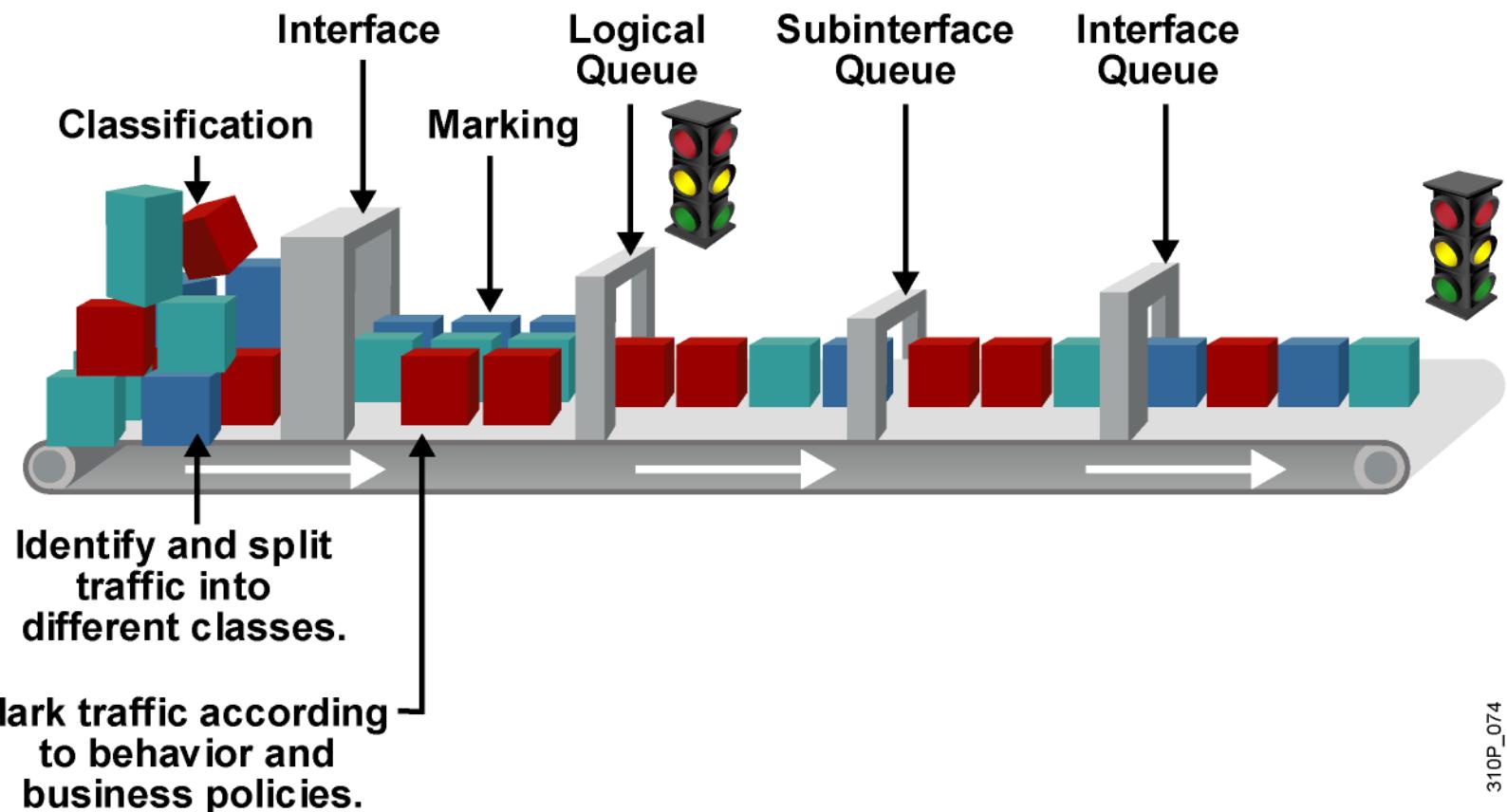
One-Way Requirements

- Latency \leq 150 ms
- Jitter \leq 30 ms
- Loss \leq 1%
- Bandwidth (30–128 Kbps)

One-Way Requirements

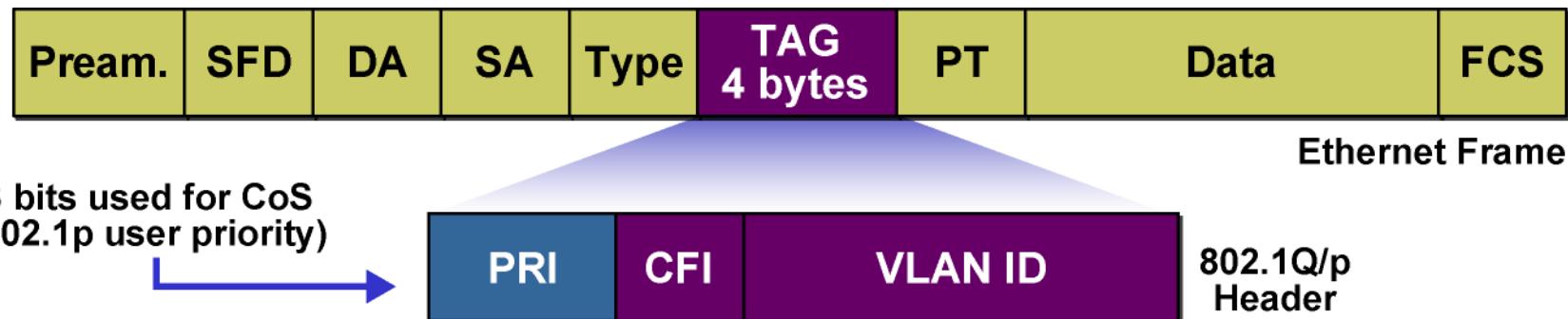
- Latency \leq 150 ms
- Jitter \leq 30 ms
- Loss \leq 0.1–1%
- Bandwidth (384 Kbps–20+ Mbps)

Classification et marquage



310P_074

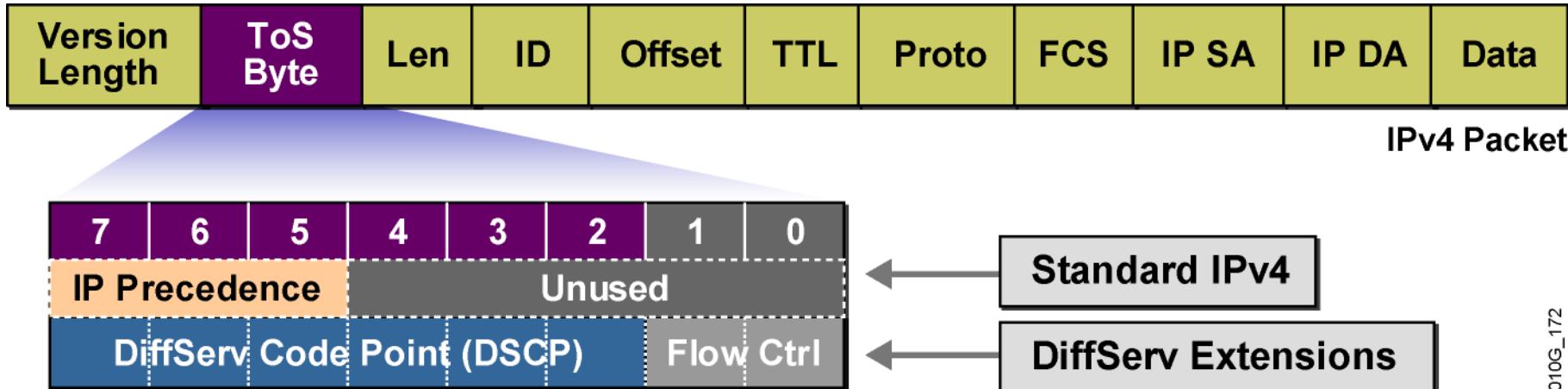
Marquage en couche 2 : 802.1p, CoS



- 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 protocoles de routage et supervision

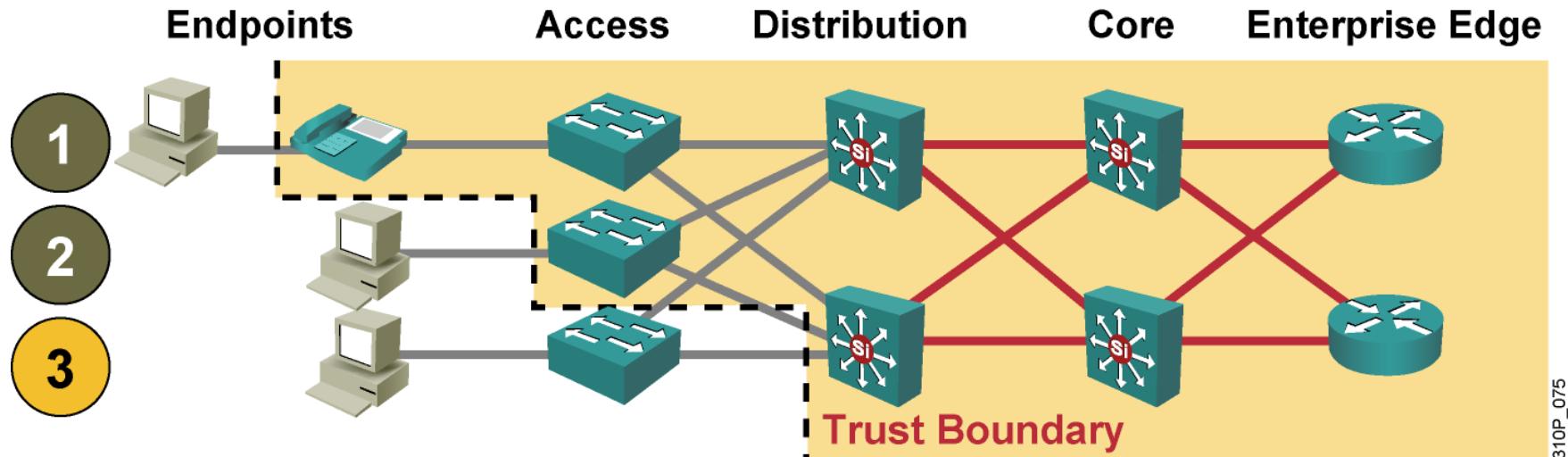
CoS	Typical Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data

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

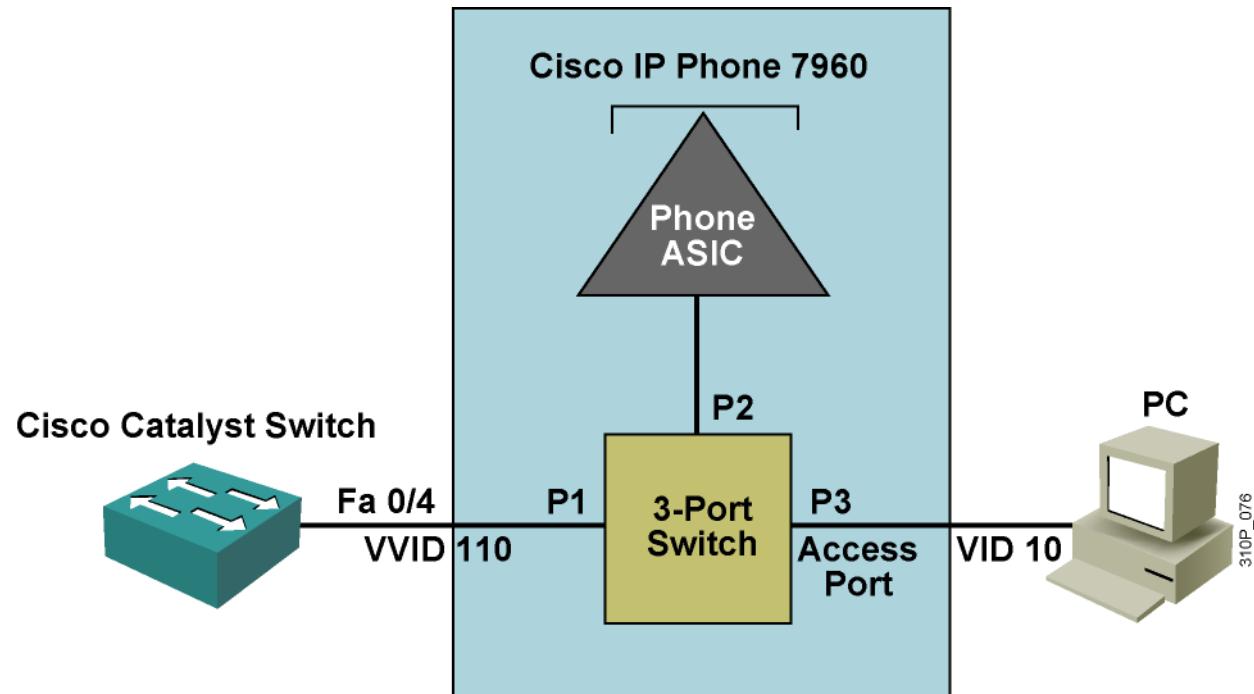
Frontières de la Classification



- 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`

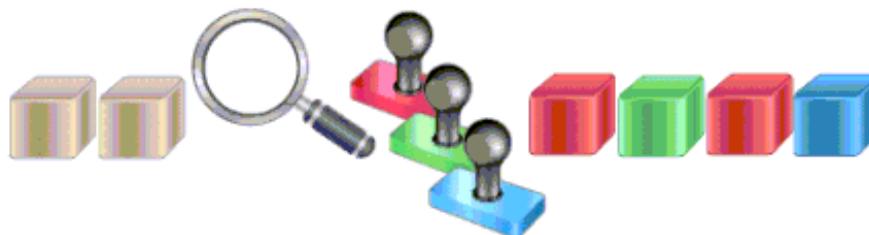
Vérification de la configuration

- `show interfaces fa 0/4 switchport`

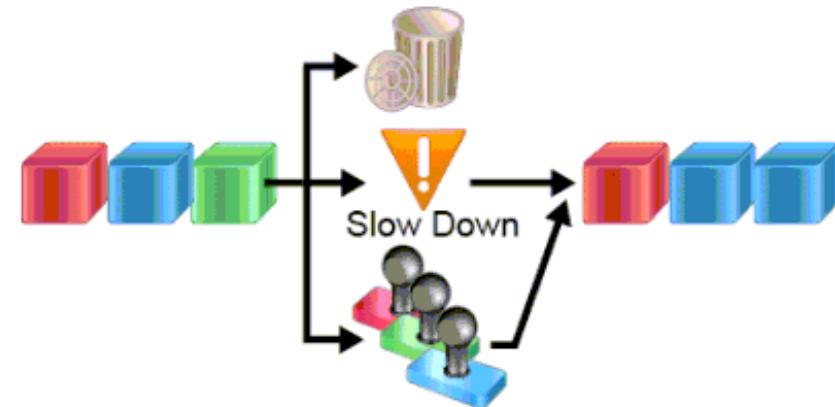


QoS Mechanisms Overview

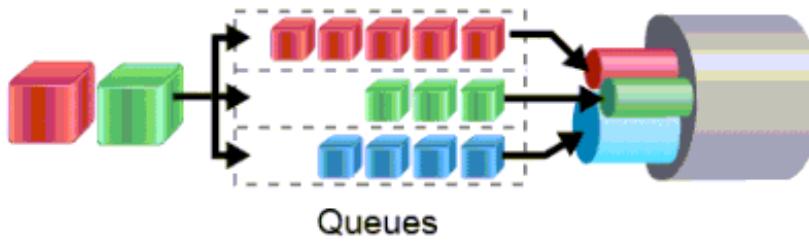
Classification and Marking



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.



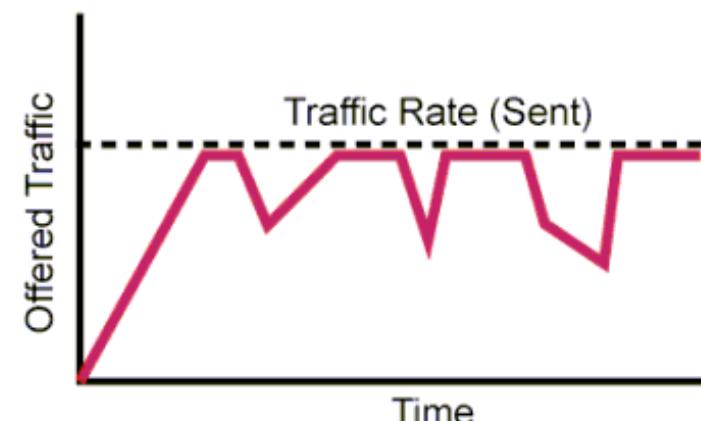
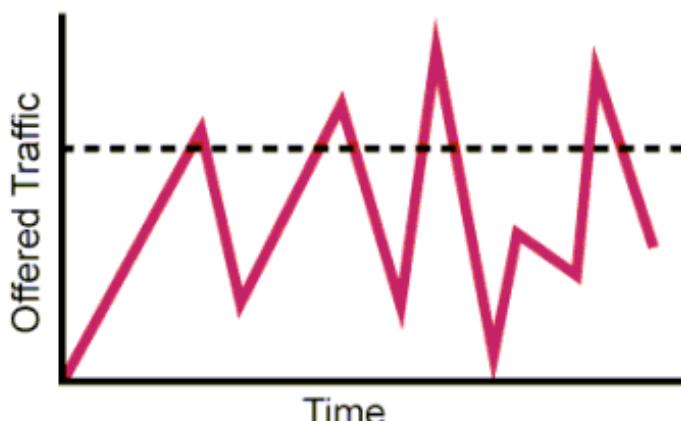
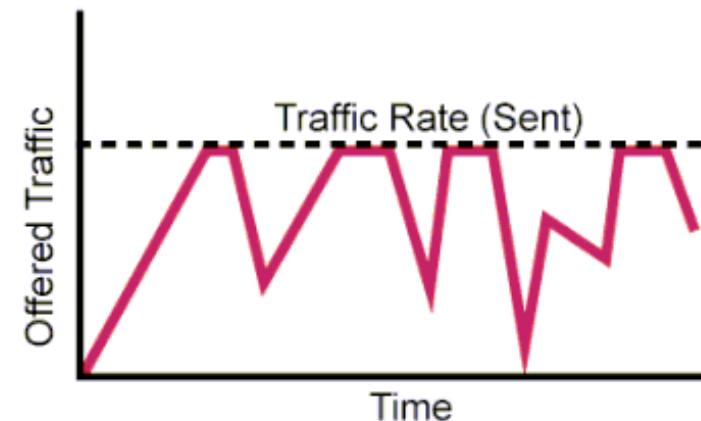
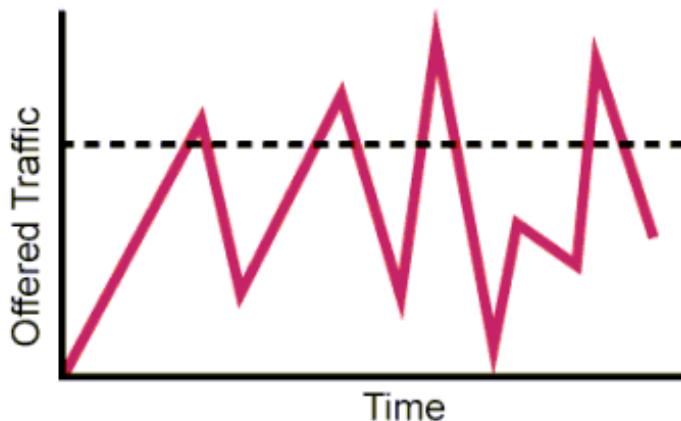
Classification Tools (Cont.)

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.

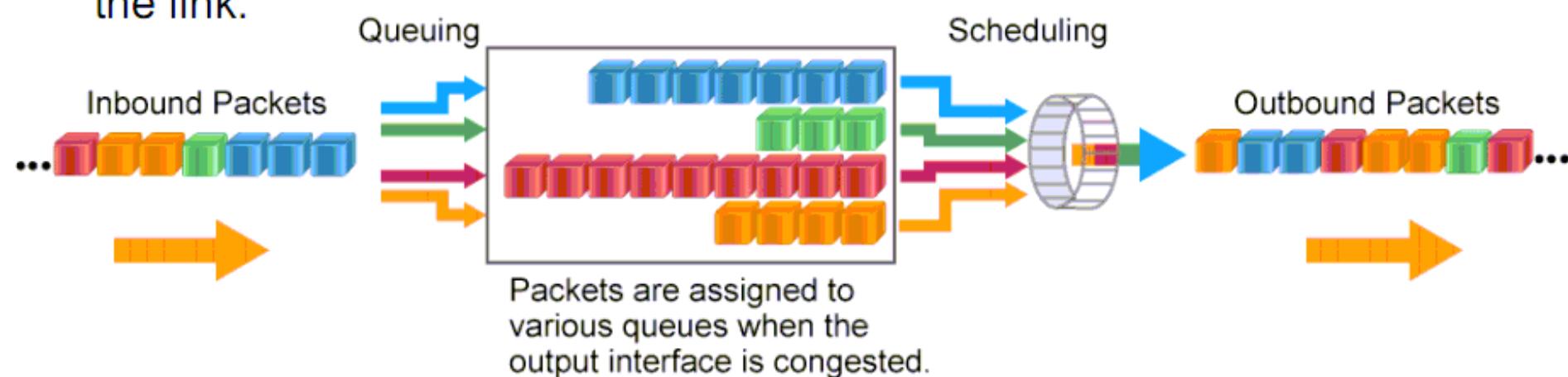




Tools for Managing Congestion

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.)

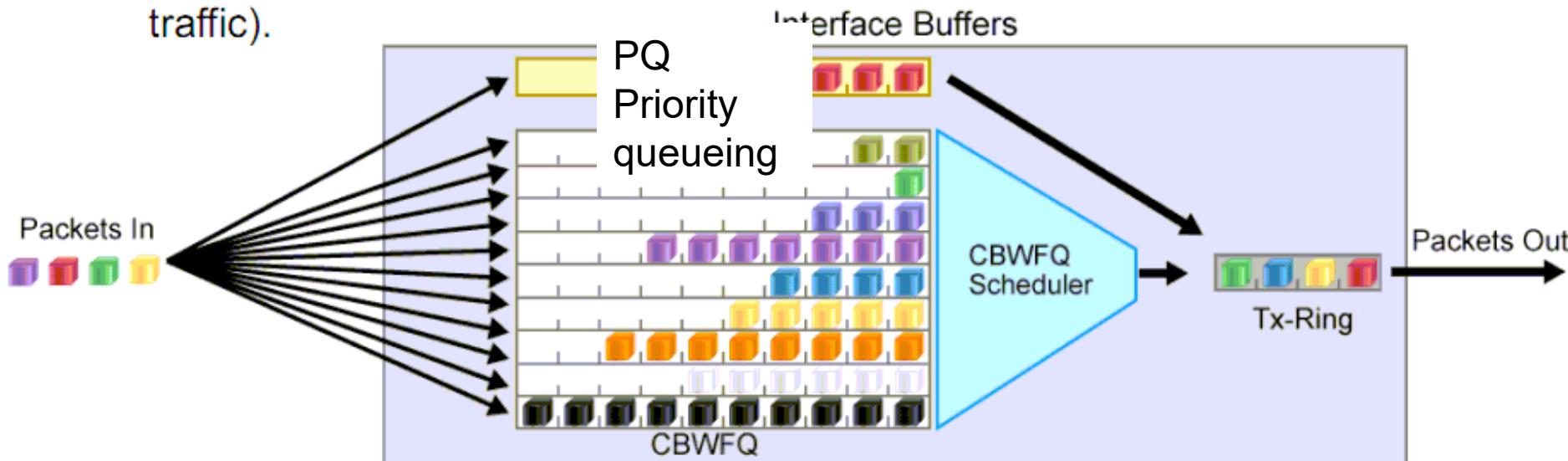
There are many queuing mechanisms. Two modern examples from Cisco are as follows:

- **Class-based weighted fair queuing:**

- Traffic classes get fair bandwidth guarantees.
 - No latency guarantees—only suitable for data networks.

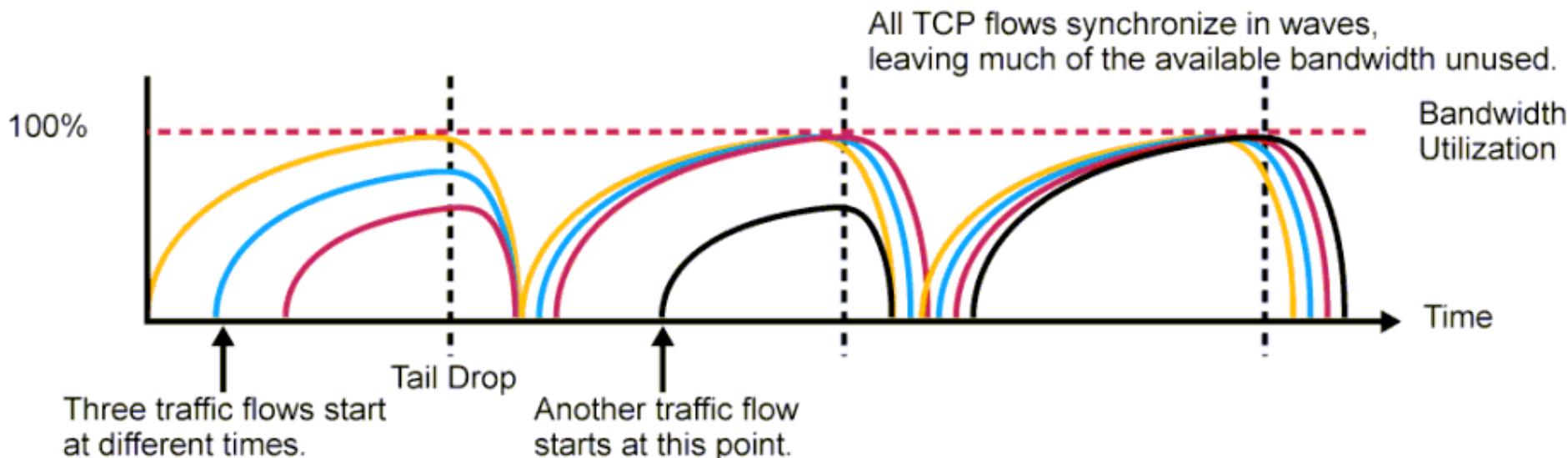
- **Low-latency queuing:**

- Takes the previous model and adds a queue with strict priority (for real-time traffic).



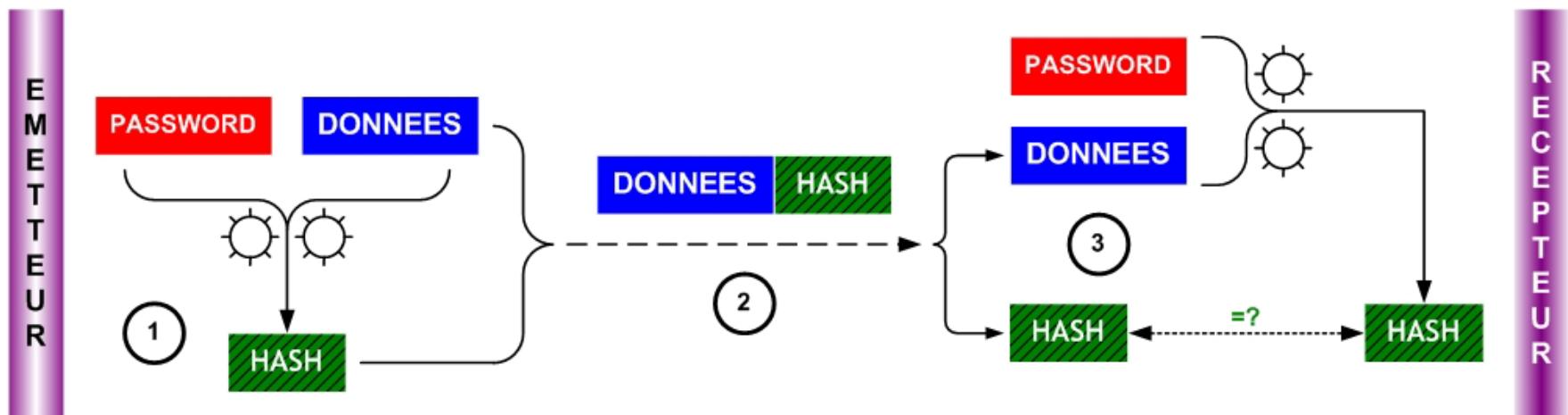
Tools for Congestion Avoidance

- **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).

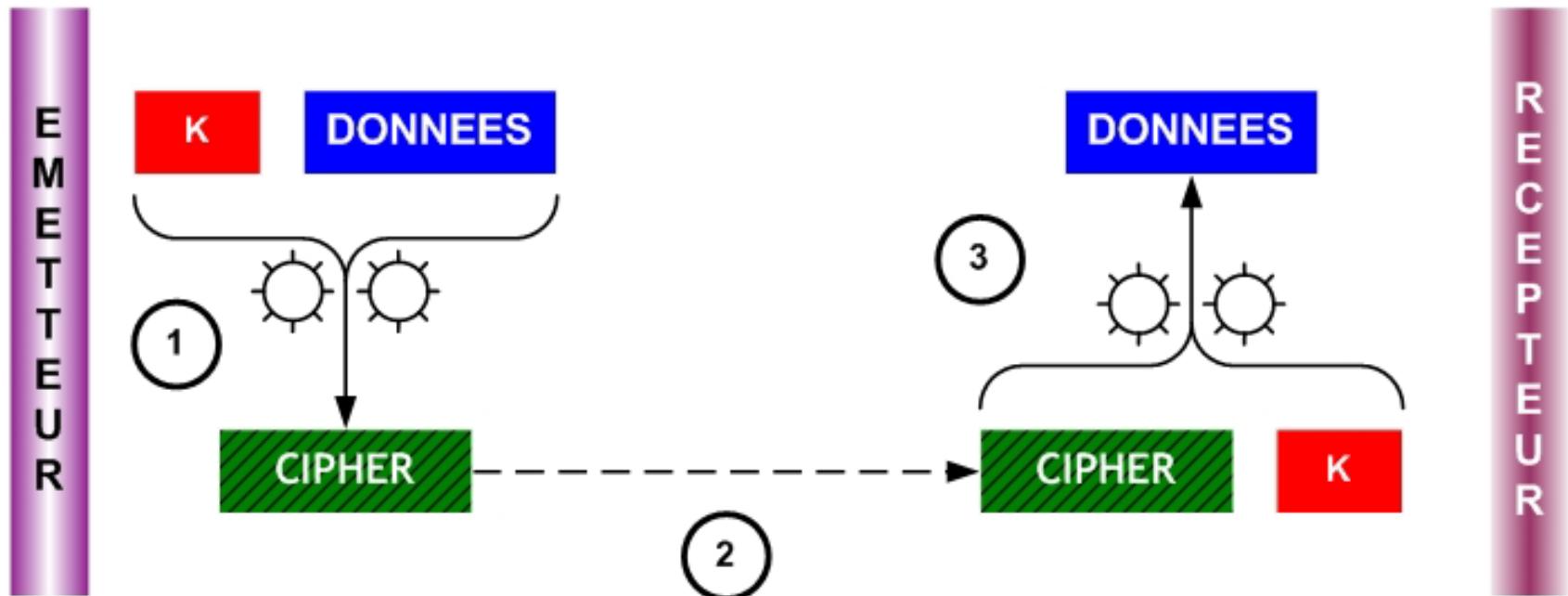


Rappels en sécurité

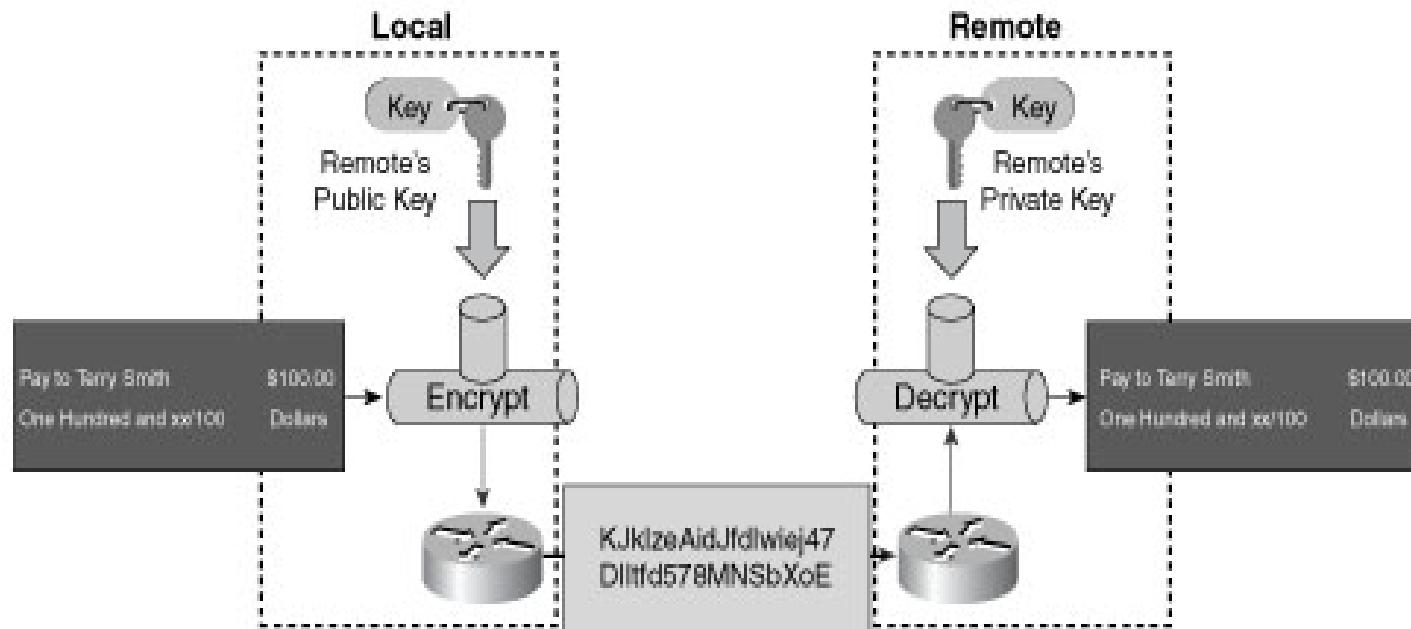
Authentification & intégrité



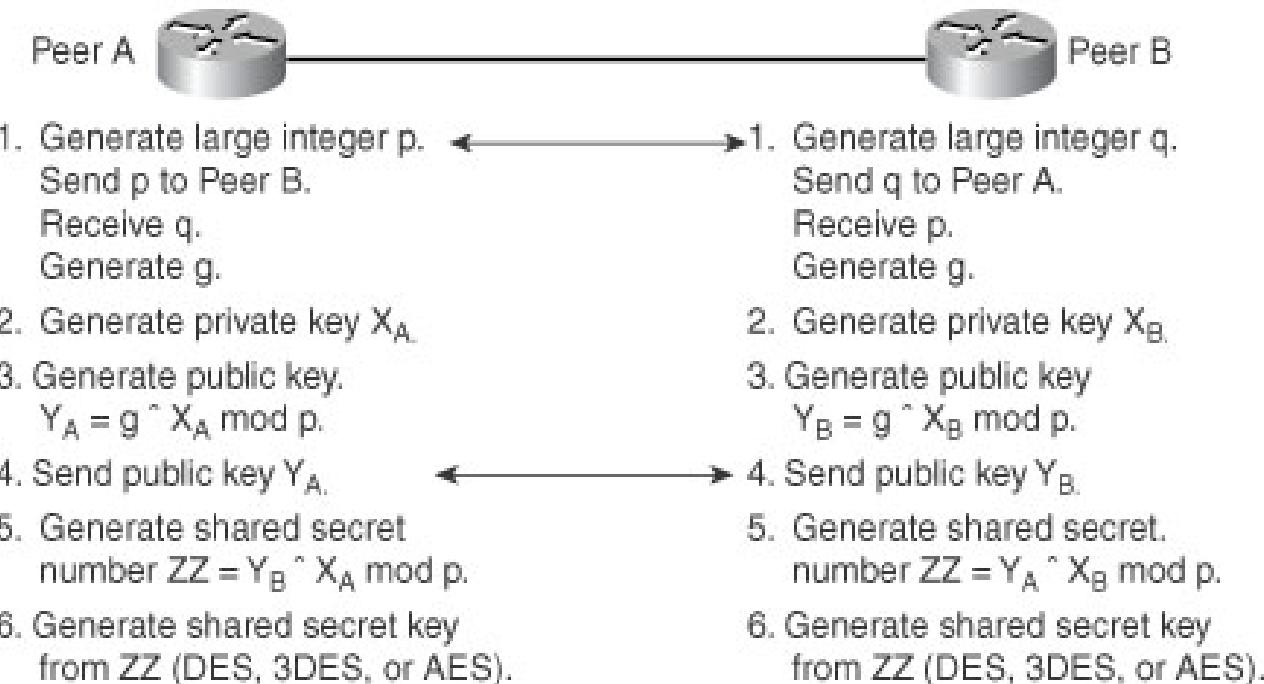
Confidentialité



RSA : clés asymétriques



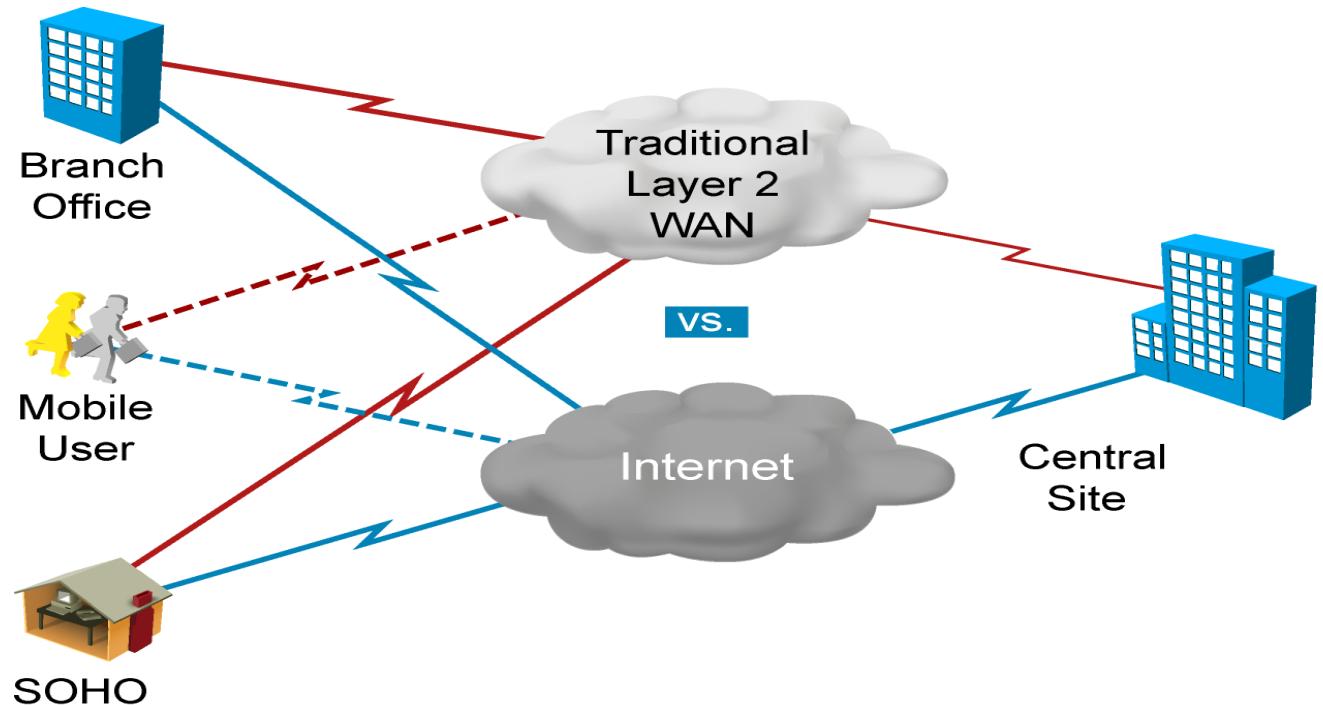
Diffie-Hellman



VPN

Qu'est-ce qu'un VPN

- Un réseau privé qui s'appuie sur un réseau public partagé
Il y a 2 types de VPN :
 - Le modèle opérateur
 - Le modèle Internet tunnel



Besoins d'un VPN

- Confidentialité
 - Chiffrement 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

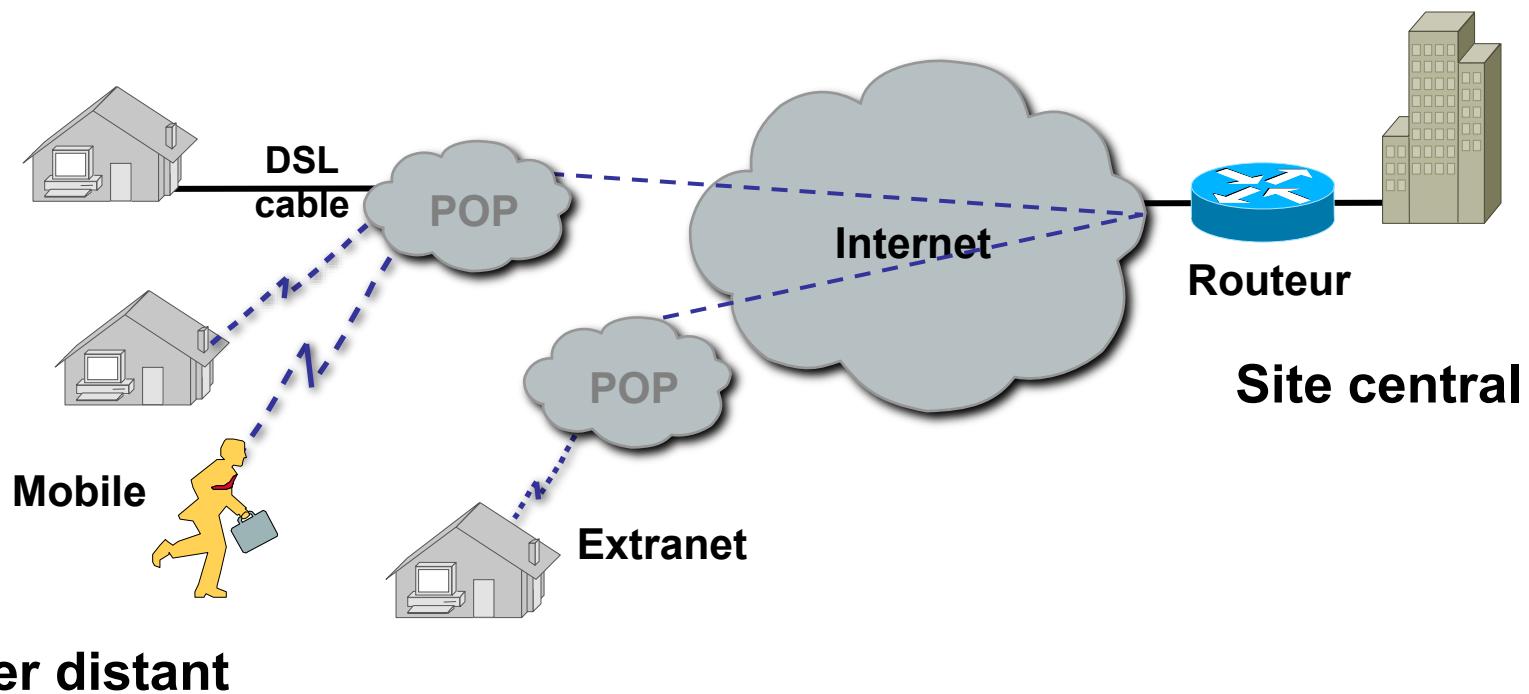
Introduction aux algorithmes

- 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

- Il sont classifiés de 3 types :
 - Remote access VPN
 - Site to site VPN
 - Host to host VPN

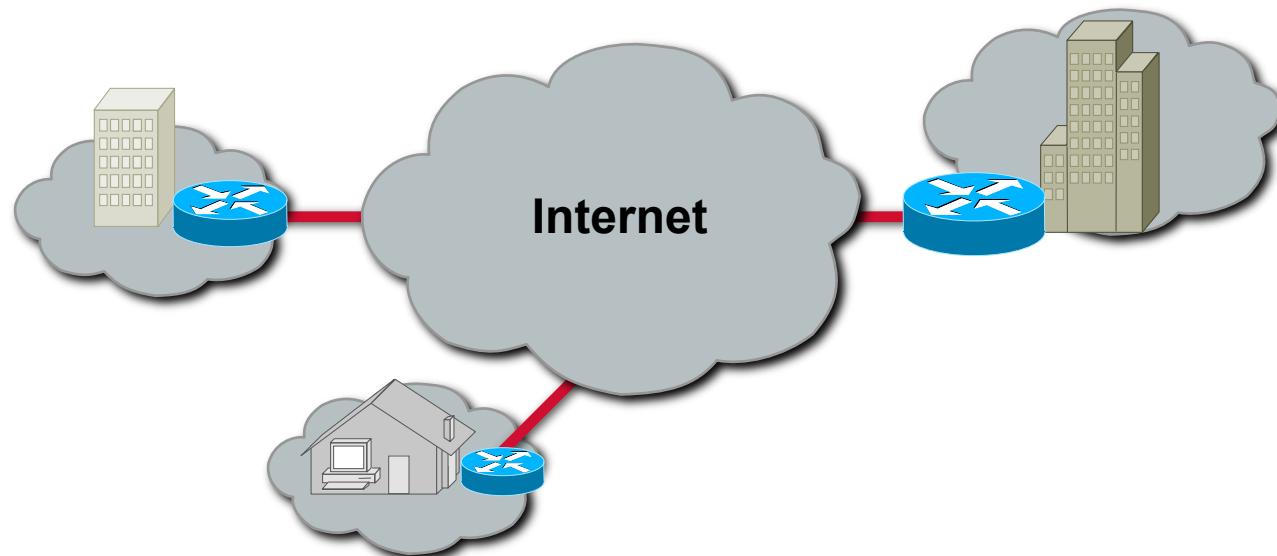
Remote access VPN

- Easy VPN nécessite un logiciel client
- Pour SSL, un navigateur suffit



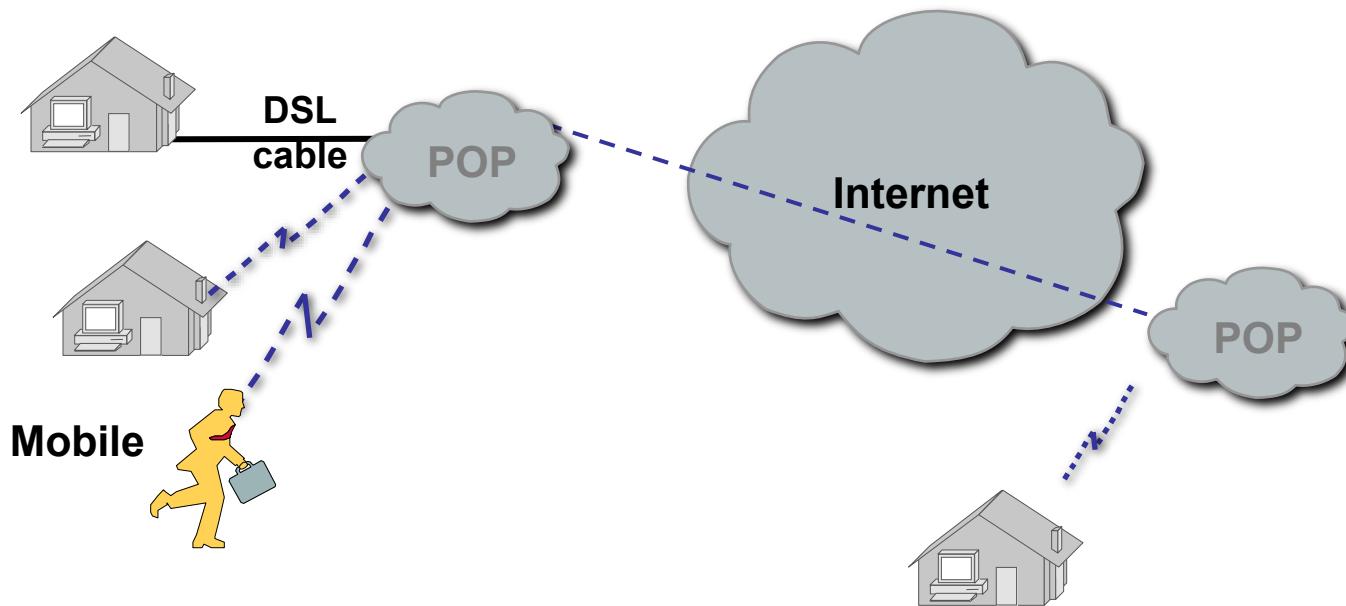
Site to site VPN

- Extension du LAN sur le WAN



Host to host VPN

- VPN de hôte à hôte



VPN IP Sec en deux phases

- Phase 1 : ISAKMP
 - mise en place d'un premier tunnel = SA
 - bidirectionnel
 - sécurise la phase 2
- Phase 2 : IPSec
 - mise en place de deux nouveaux tunnels = SA
 - unidirectionnels
 - sécurise l'échange des données

Différentes types d'attaque

- Reconnaissance
 - Scan des ports, social engineering
- Accès non autorisé
 - Brute force, mot de passe faible, attaque interne, escalader les privilèges
- Déni de service
 - Attaques SYN, saturation de la table des adresses mac
- Man in the middle
 - Faire appel à des certificats
- Code malicieux
 - Eduquer les usagers : user awareness

Le Wifi

Les fondamentaux

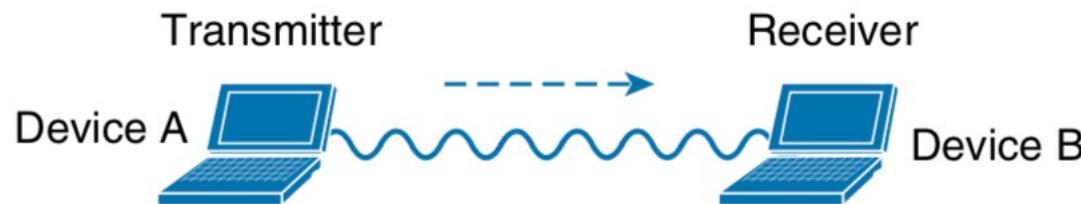
Topologies WiFi

Les échanges en WiFi

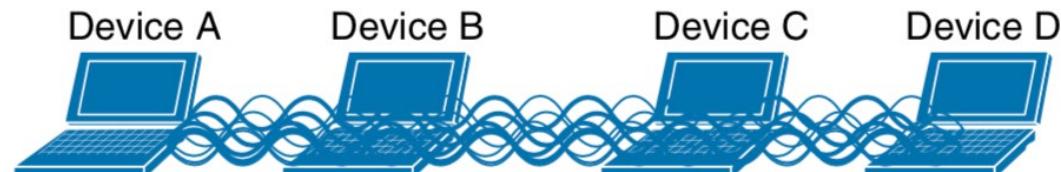
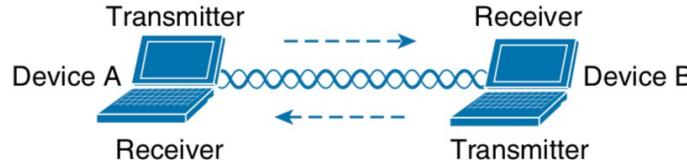
- Principes :
 - les données sont transmises via des **fréquences** radio
 - les équipements peuvent être fixes ou **mobiles**
 - assurer une zone de « couverture »
 - plusieurs équipements **partagent** le médium et la bande passante correspondante
- Changement de standard :
 - réseaux cablés => IEEE 802.3
 - réseaux wifi => IEEE **802.11**

Fréquence radio

- Communication entre un **émetteur** et un **récepteur** :
 - si la communication n'avait lieu que dans un seul sens, alors l'émetteur pourrait communiquer autant qu'il veut et quand il veut :



- En réalité, la communication est **bidirectionnelle**, et entre de **nombreux** équipements :
 - il faut donc gérer un ordre de passage pour éviter les collisions, appelées « interférences » :



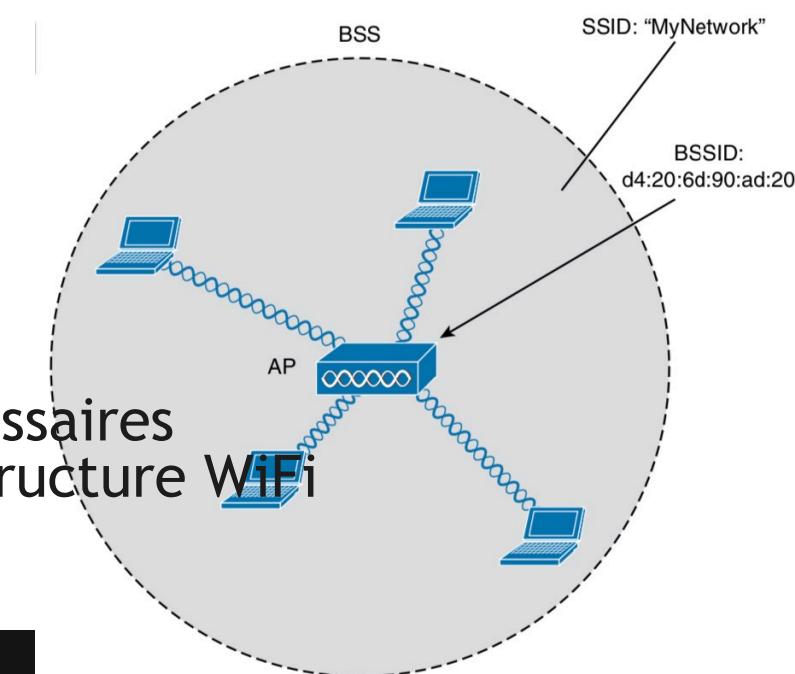
- Pour éviter les interférences :
 - Mode « **half duplex** »
 - aucun équipement ne peut émettre et recevoir en même temps
 - A chaque instant, **un seul** équipement peut communiquer
 - les équipements se partagent le temps d'accès au Wifi « airtime »
 - avant d'émettre un signal, il doit vérifier que le canal est **libre**

Les topologies WiFi

- BSS
 - Basic Service Set
- ESS
 - Extended Service Set
- IBSS
 - Independent Basic Service Set

BSS : « Basic Service Set »

- Ensemble d'équipements
 - connectés à un même point d'accès, « **Access Point** » AP
 - utilisent le même **canal**
 - répartis dans une zone géographique où le signal est disponible : **BSA**, « **Basic Service Area** », « **Cell** »
 - sa forme dépend de l'antenne utilisée et des objets de l'environnement qui pourraient affecter la force du signal
- Mode « **infrastructure** » :
 - l'AP offre les services nécessaires pour constituer une infrastructure WiFi

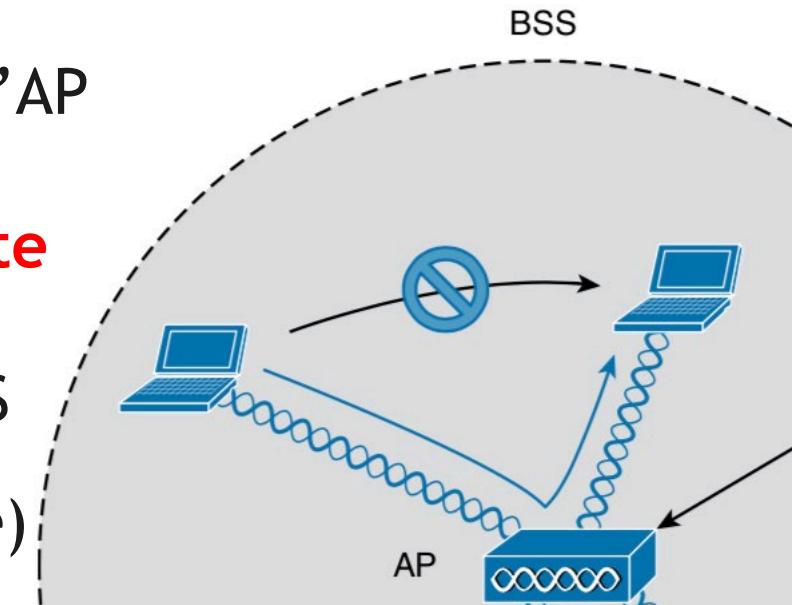


AP : « Access Point »

- Le point de contact unique permettant de se connecter au réseau sur ce BSS
- Rôles :
 - Il **annonce** la présence du BSS
 - via son **BSSID**
 - Basic Service Set ID
 - adresse MAC qui identifie de manière unique l'AP
 - exemple : **0102:0102:0102**
 - via un **SSID**
 - Service Set ID
 - chaîne alphanumérique qui identifie de manière non unique le service proposé
 - exemple : **MonReseau**

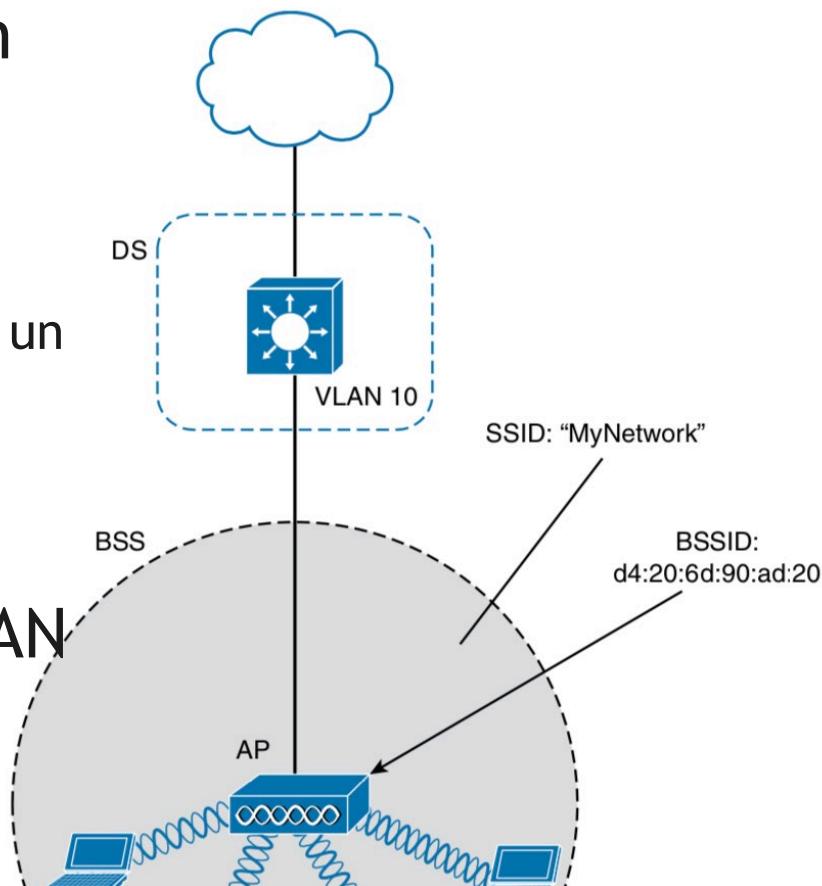
Mode de fonctionnement

- L'équipement envoie une requête pour **s'associer** au point d'accès.
- Si l'AP accepte la requête :
 - l'équipement devient un client : station 802.11, **STA**
- Pour garder le contrôle sur le BSS, toutes les communications doivent alors passer par l'AP
 - en utilisant l'adresse MAC de l'AP en source ou destination
 - **aucune communication directe** entre deux STA
 - tous les clients d'un même BSS peuvent alors écouter les conversations (sauf si cryptage)



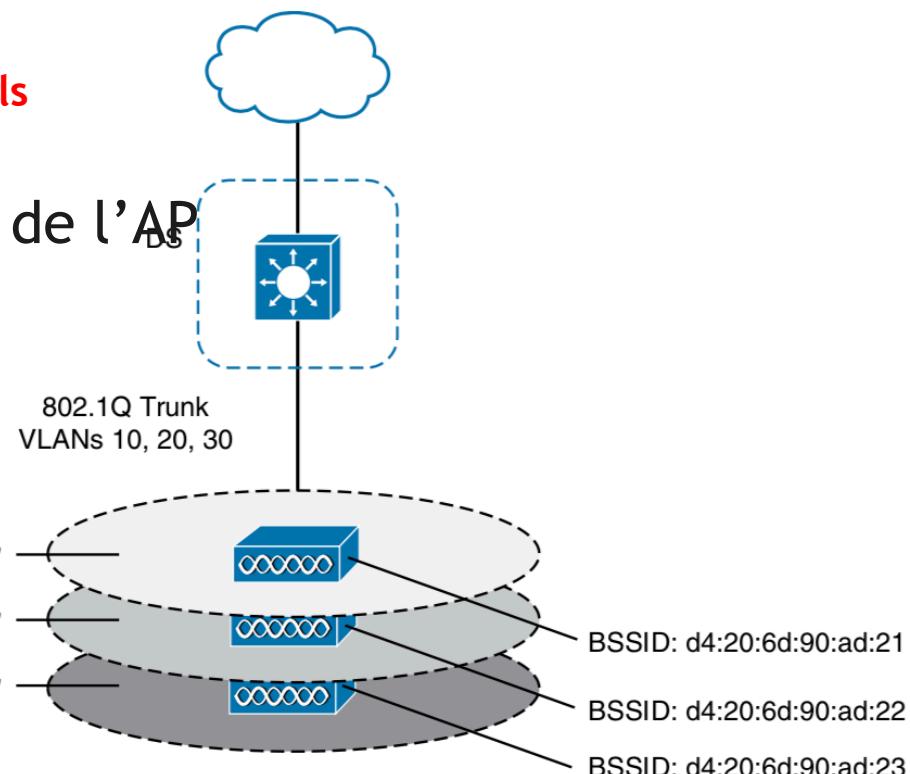
DS : « Distribution System »

- Les équipements ont besoin de communiquer en dehors de leur BSS :
 - l'AP a donc une connection **cablée** Ethernet : DS
- L'AP est donc un **pont** entre un VLAN et un SSID
 - les stations qui lui sont associées vont apparaître comme appartenant au VLAN de l'AP



Trunk

- Un même AP peut associer **plusieurs SSID** à plusieurs VLANs :
 - la connection avec le switch d'accès est alors en trunk 802.1Q
- L'AP apparaît comme **plusieurs APs virtuels**
 - les BSSID sont construits en incrémentant l'adresse MAC de l'AP
- Tous les BSS partagent la même couverture géographique :
 - même émetteur, receveur,
 - même antenne, canal
 - **même BSA**



ESS : « Extended Service Set »

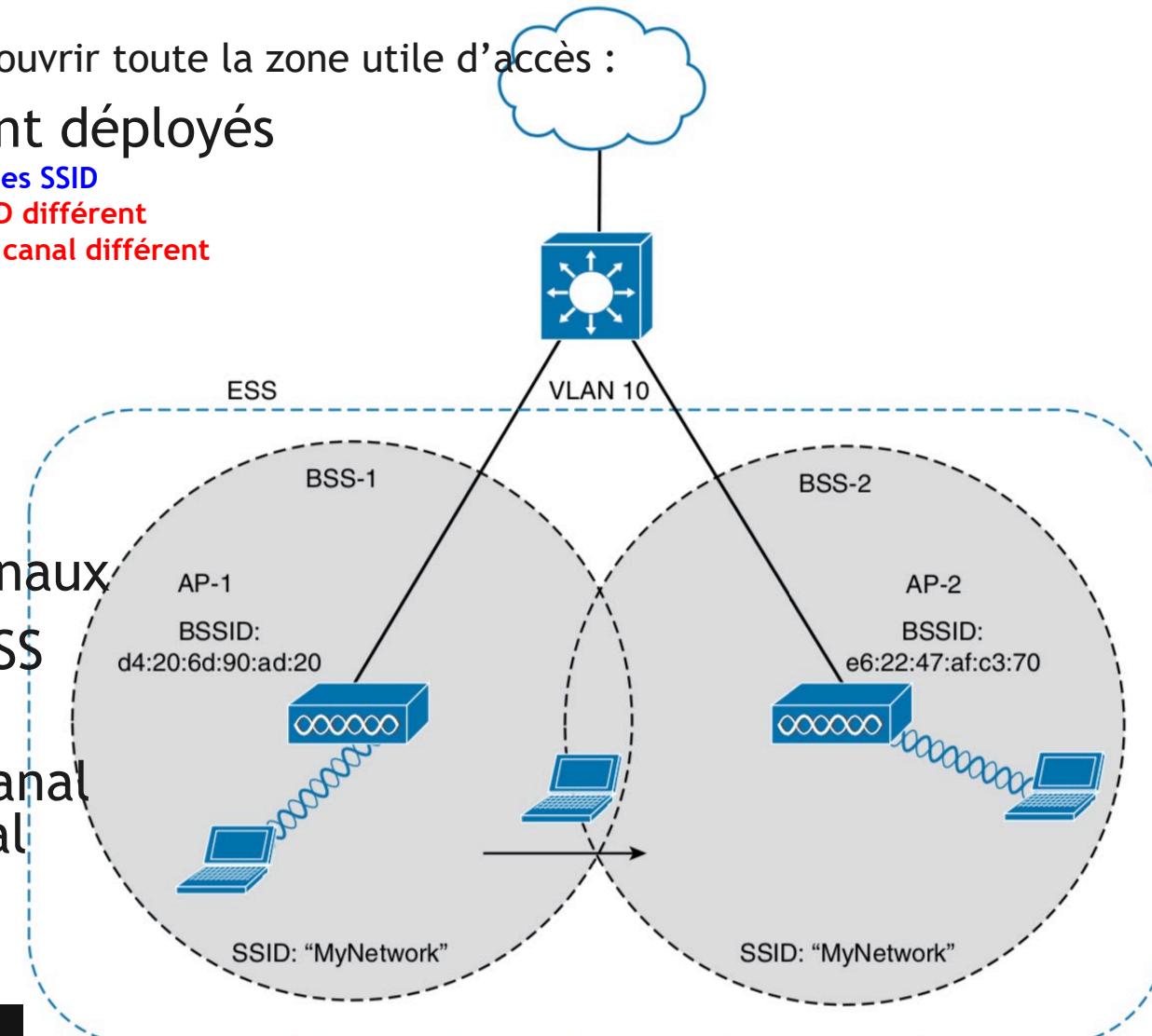
- Un seul AP ne peut pas couvrir toute la zone utile d'accès :

- plusieurs AP sont déployés

- ils annoncent **les mêmes SSID**
 - ils ont chacun **un BSSID différent**
 - ils utilisent chacun **un canal différent**

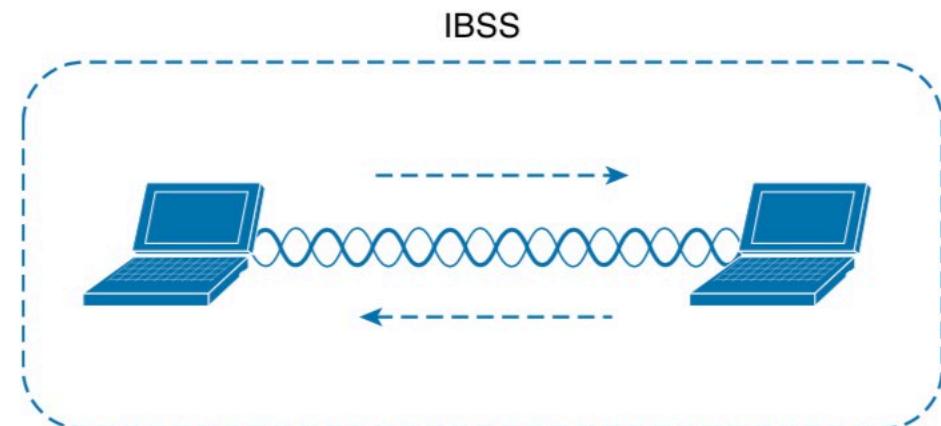
- Les clients se déplacent et restent connectés :
« **roaming** » :

- re-connection automatique via scan des canaux
 - passage d'un BSS à un autre BSS
 - passage d'un canal à un autre canal



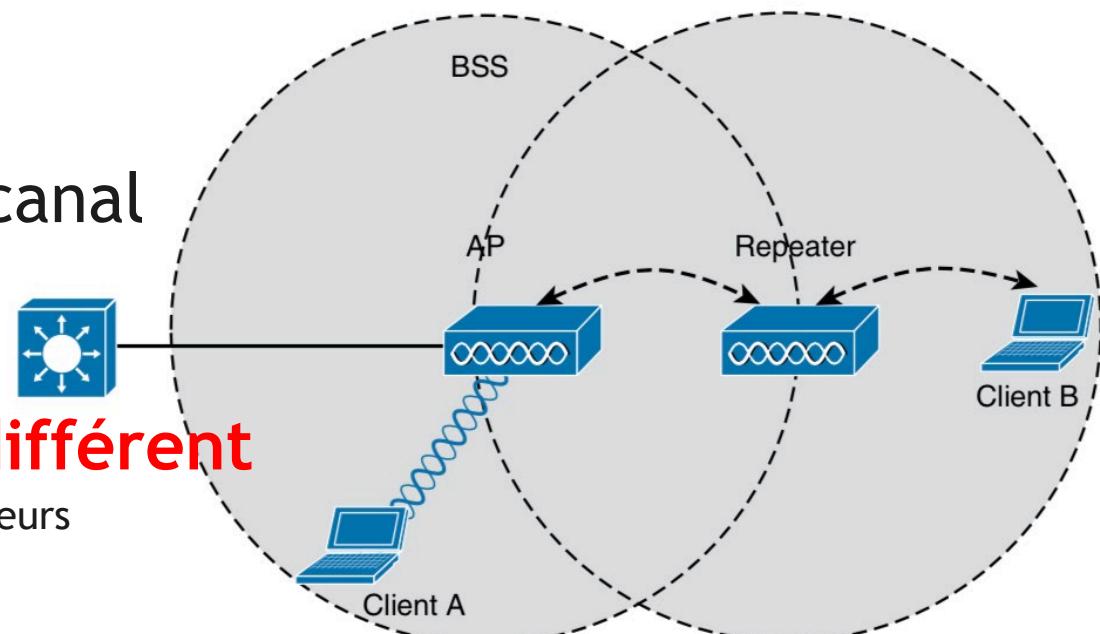
IBSS : « Independent BSS »

- Exemple :
 - 2 personnes souhaitent échanger des documents électroniques sans s'authentifier sur un réseau WiFi
 - une imprimante permet de lancer des impressions en Wifi sans déployer un AP
- IBSS, ou « **ad hoc** »
 - un équipement prend la main et annonce un BSS, comme s'il était un AP
 - max 8 ou 10 équipements



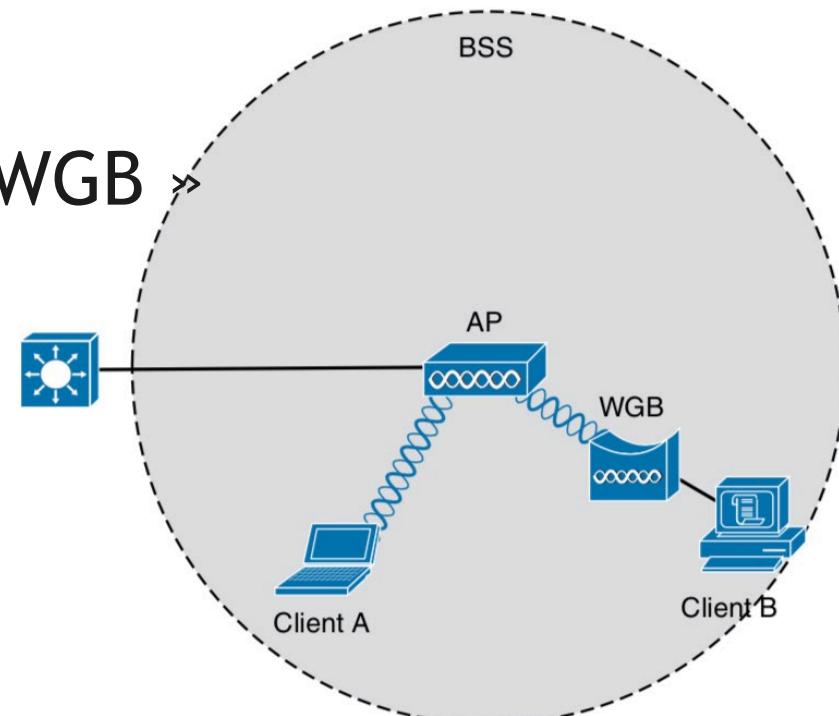
Le répéteur

- Comment étendre la couverture géographique si on ne peut pas rajouter d'AP (limitation de la longueur du câble Ethernet) ?
 - déployer un AP en mode « repeater »
 - il doit être positionné dans la zone de couverture de l'AP initial
- Deux options :
 - utiliser le même canal
 - bande passante réduite
 - utiliser un canal différent
 - nécessite 2 paires d'émetteurs -récepteur sur le répéteur



WGB : « Workgroup bridge »

- Pour un host n'ayant pas de carte Wifi :
 - Le WGB est un **adaptateur** réseau Wifi
- Deux options :
 - uWGB, « universal WGB
 - 1 seul équipement peut se connecter au Wifi
 - WBG :
 - plusieurs équipements peuvent se connecter
 - propriétaire Cisco



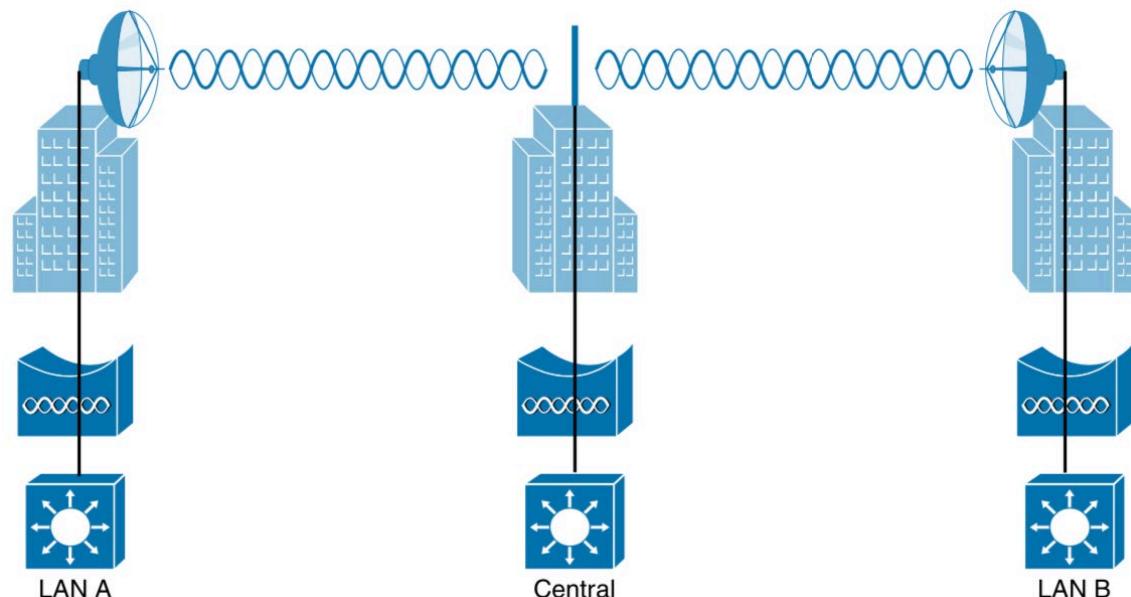
Outdoor bridge : point-to-point

- Pour connecter **2 LANs** entre eux :
 - entre 2 bâtiments
 - entre 2 villes
- Déployer 2 APs :
 - en mode bridge
 - **antenne** spécifique qui oriente le signal sur **une** direction



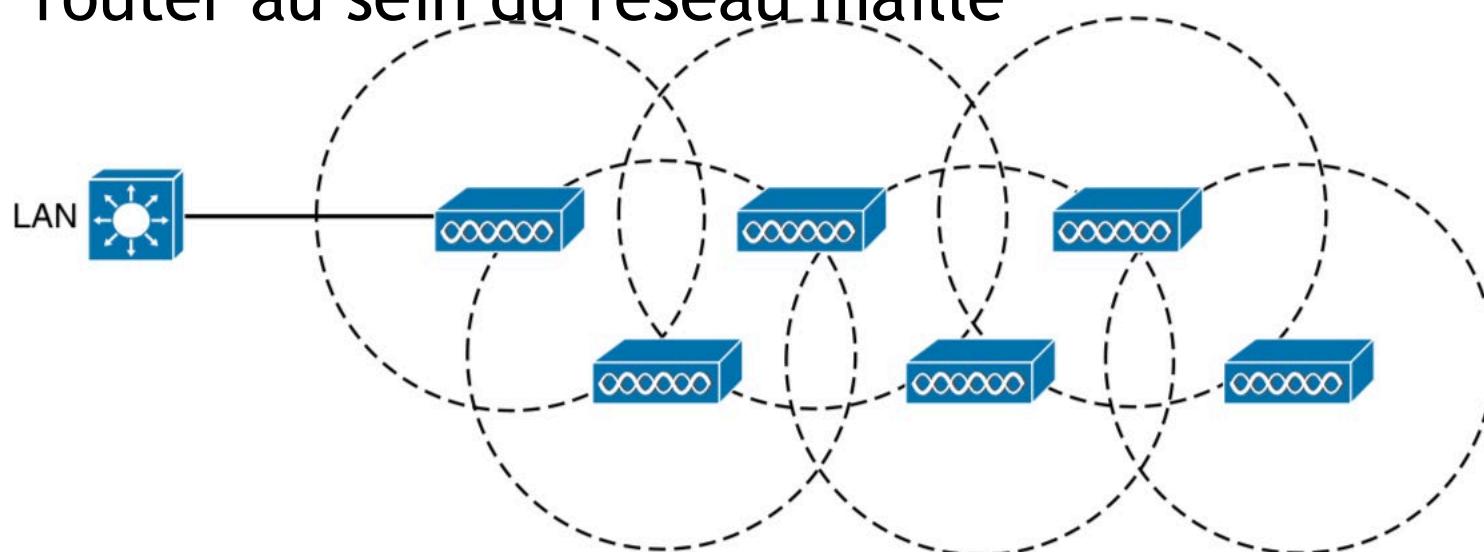
Outdoor bridge : point-to-multipoint

- Pour connecter un site central à plusieurs sites distants
- Sur le site **central** :
 - utiliser une antenne **omnidirectionnelle**
 - transmet le signal de manière égale sur toutes les directions
- Sur les sites **distant** :
 - utiliser une antenne **directionnelle**
 - qui pointe vers le site central



Topologie « Mesh »

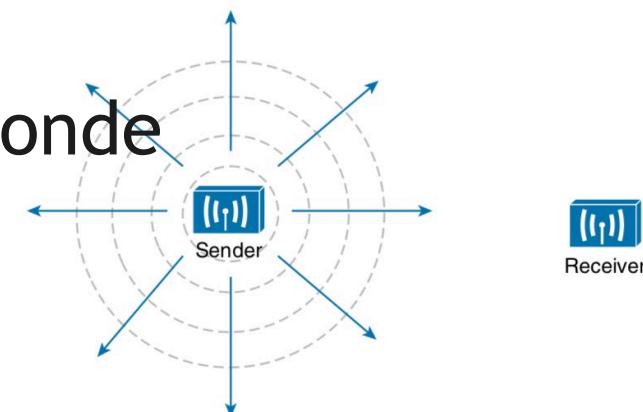
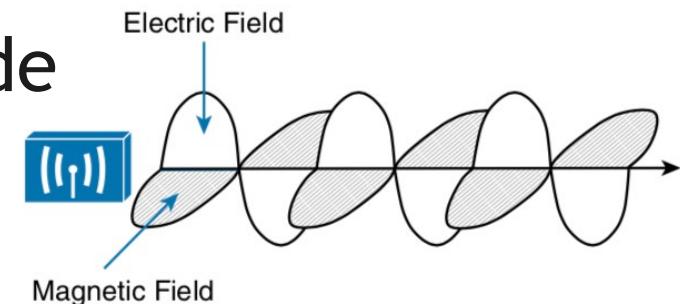
- Pour couvrir une grande zone géographique, sans accès Ethernet câblé
 - Plusieurs AP **bridgés en série**
 - Chaque AP utilise **un canal différent**
 - Un protocole de routage spécifique permet de router au sein du réseau maillé



Les fréquences radio

Fondamentaux

- Pour envoyer un message dans l'air :
 - une **antenne** génère une onde
 - l'onde = signal électromagnétique
 - son déplacement n'est pas rectiligne
 - uniforme dans toutes les directions
 - le **récepteur** re-traduit cette onde en signal électrique

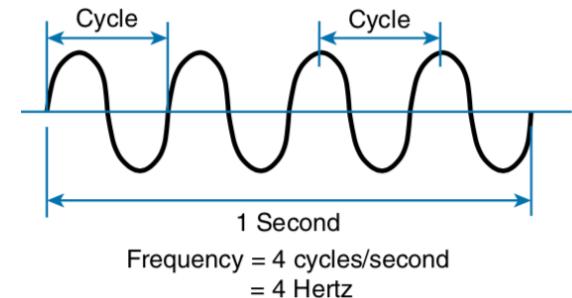


Caractéristiques d'une onde

- Durée d'un cycle, en secondes

- Fréquence, en Hertz (Hz)

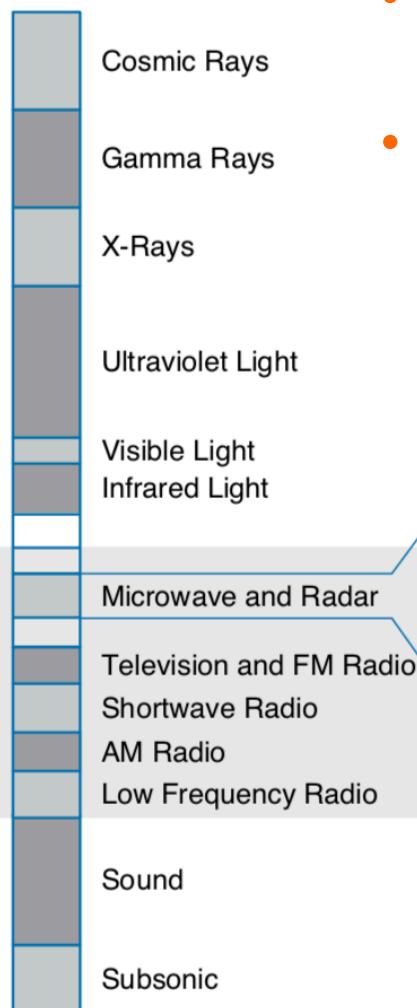
- nombre de cycles par seconde



Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz

Les ondes radio

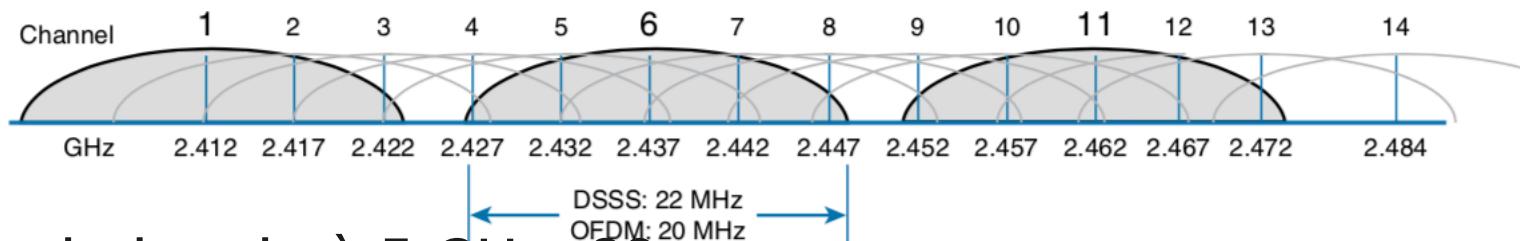
Frequency (Hz)	Frequency Notation
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	
10^{11}	100 GHz
10^{10}	10 GHz
10^9	1 GHz
10^8	100 MHz
10^7	10 MHz
10^6	1 MHz
10^5	100 kHz
10^4	10 kHz
10^3	1 kHz
10^2	100 Hz
10^1	10 Hz
0	0 Hz



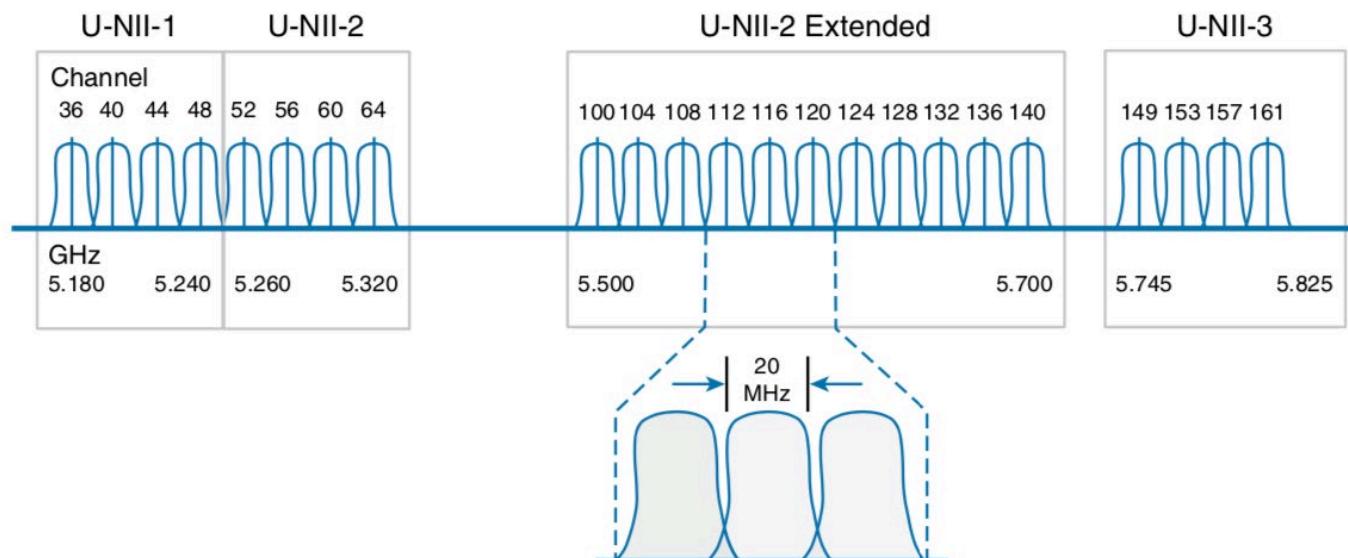
- Fréquence des ondes radio : de 3 kHz à 300 GHz
- Deux bandes pour le Wifi :
 - bande à 2,4 GHz :**
 - de 2,4 à 2,4835 GHz
 - bande à 5 GHz :**
 - de 5,15 à 5,825 GHz

Le canal

- Chaque bande de fréquence est divisée en canaux :
 - pour la bande à 2,4 GHz, 14 canaux **avec recouvrement** :



- pour la bande à 5 GHz, 23 canaux **sans recouvrement** :



Amendements à 802.11

Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2021 will operate on other bands too, as they become available

Choix de la bande et du canal

- Station :
 - choisit la bande qui présente le meilleur débit
- AP :
 - « **dual-band** », 2 antennes, une dans chaque bande :
 - permet d'offrir certains BSS en 2,4 GHz et d'autres BSS en 5 GHz
 - « **dual-radio** », 2 antennes dans la même bande :
 - permet d'offrir des BSS dans 2 canaux différents
 - pour augmenter la densité des stations
- Comparatif 2,4 GHz **vs** 5 GHz :
 - **2,4 GHz** :
 - plus grande étendue géographique
 - meilleur pénétration à travers les murs et objets
 - **5 GHz** :
 - davantage de canaux disponibles :
 - moins de clients connectés au même canal
- Sur un même AP :
 - chaque station peut utiliser un amendement différent



Quiz

Quiz

Wired Ethernet and Wi-Fi are based on which **two IEEE standards**, respectively?

- a. 802.1, 802.3
- b. 802.3, 802.1
- c. 802.3, 802.11
- d. 802.11, 802.3



Quiz

Devices using a wireless LAN must operate in which one of the following modes?

- 
- a. Round-robin access
 - b. Half duplex
 - c. Full duplex
 - d. None of these answers

Quiz

An **access point** is set up to offer wireless coverage in an office.

Which one of the following is the correct 802.11 term for the resulting **standalone network**?

- a. BSA
- b. BSD
- c. BSS
- d. IBSS



Quiz

Which one of the following is used to uniquely identify an AP and the basic service set it maintains with its associated wireless clients?

- a. SSID
-  b. BSSID
- c. Ethernet MAC address
- d. Radio MAC address

Quiz

Which one of the following can be used to provide wireless connectivity to a non wireless device?

- 
- a. Wireless repeater
 - b. Workgroup bridge
 - c. Transparent bridge
 - d. Adaptive bridge

Quiz

Which of the following are **frequency bands** commonly used for Wi-Fi?

- a. 2.4 kHz
- b. 2.4 MHz
- c. 5 MHz
- d. 2.4 GHz
- e. 5 GHz

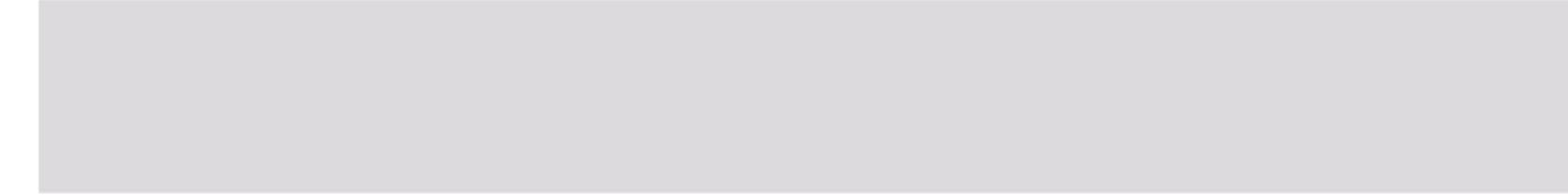


Quiz

Which of the following are considered to be **nonoverlapping channels**? (select two)

- a. Channels 1, 2, and 3 in the 2.4-GHz band
- b. Channels 1, 5, and 10 in the 2.4-GHz band
- c. Channels 1, 6, and 11 in the 2.4-GHz band
- d. Channels 40, 44, and 48 in the 5-GHz band





Architectures Wifi

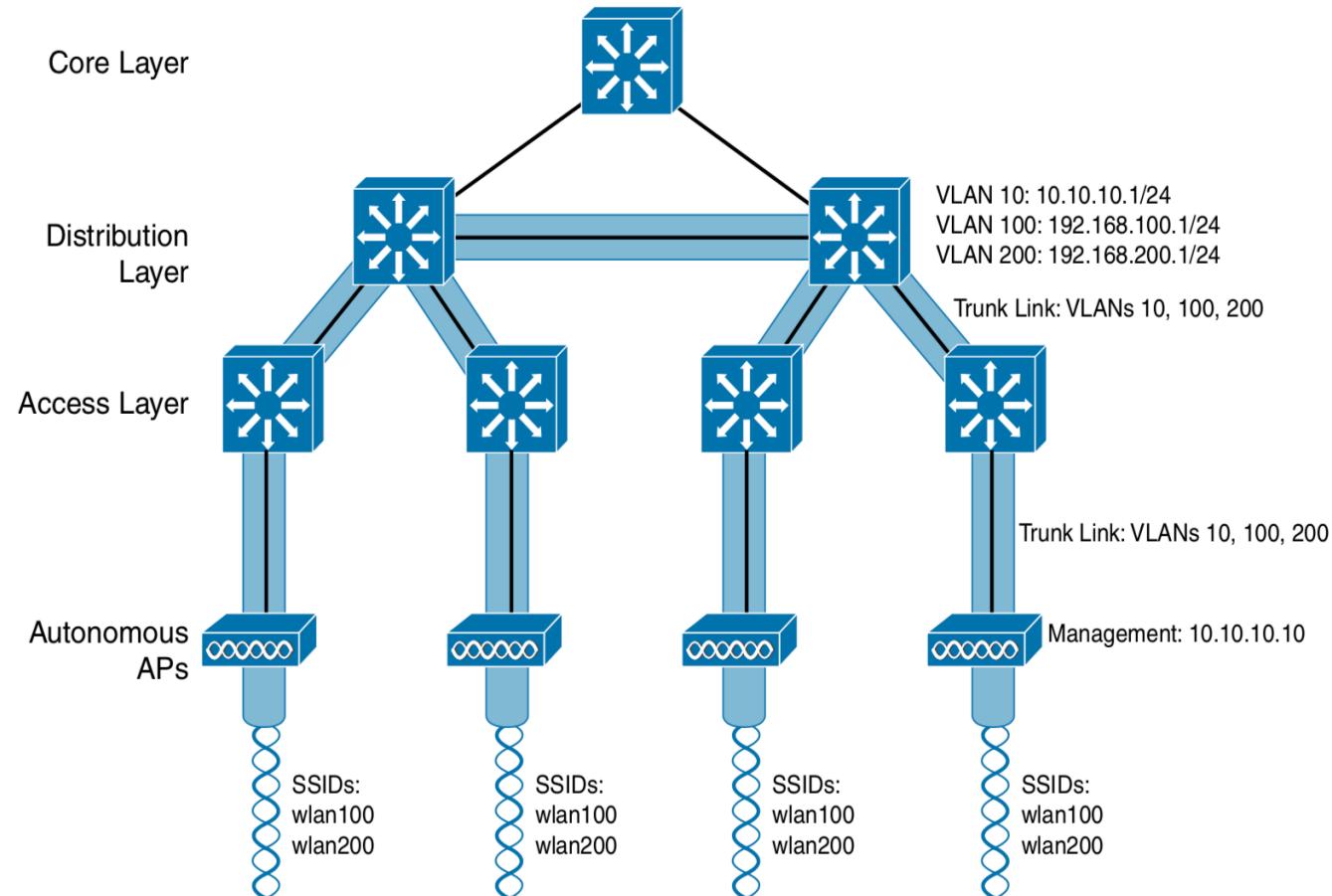
Trois architectures

- Autonomous AP
- Cloud-based AP
- Split-MAC

Architecture AP autonome

- L'AP est autonome :
 - il est directement connecté au réseau **câlé**
- Pour permettre le **roaming** à travers l'ensemble du réseau, sans que les stations n'aient besoin de changer d'IP :
 - **Tous** les SSID et **tous** les VLANs doivent être configurés sur tous les AP
 - **Tous** les trunk doivent permettre ces VLANs, jusqu'à chaque AP
- Architecture complexe à maintenir

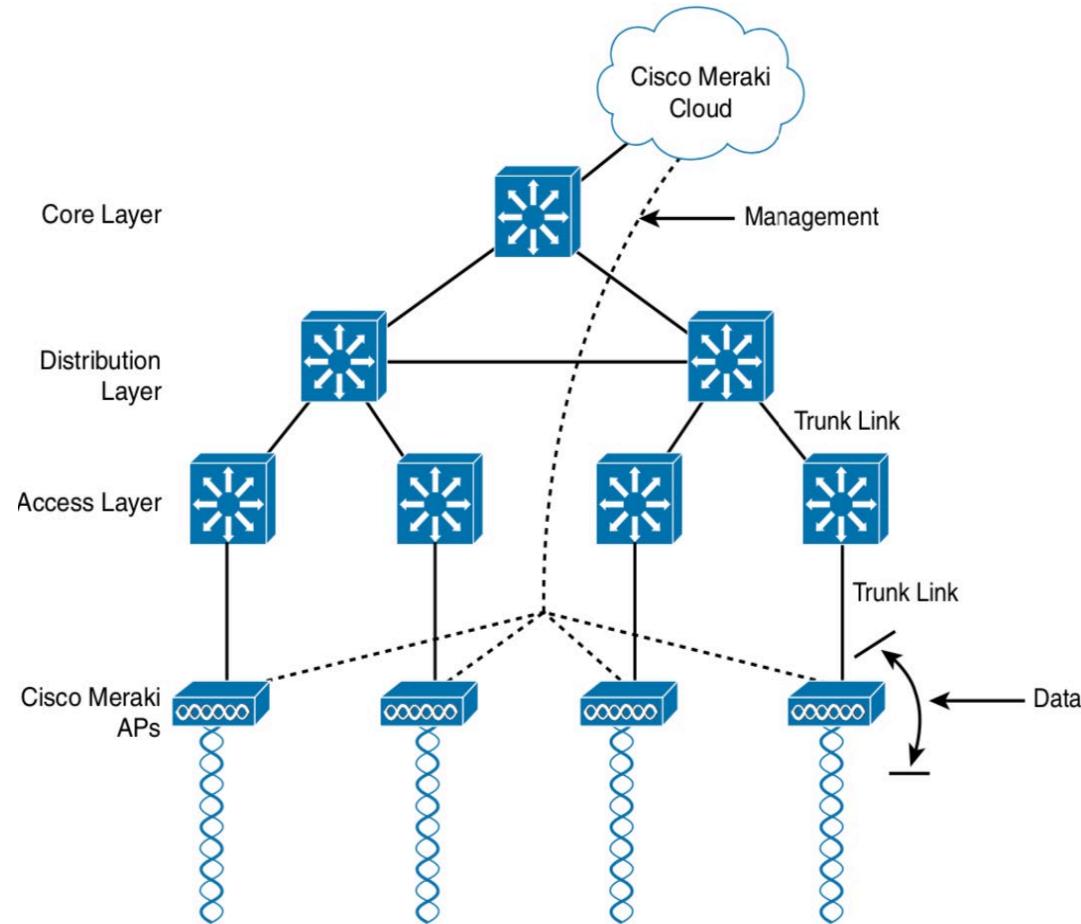
Exemple



Architecture cloud-based

- Management des AP :
 - depuis un cloud
 - exemple : Cisco Meraki
 - permet également de monitorer les AP
 - configuration & optimisation automatiques :
 - canal de transmission WiFi
 - puissance

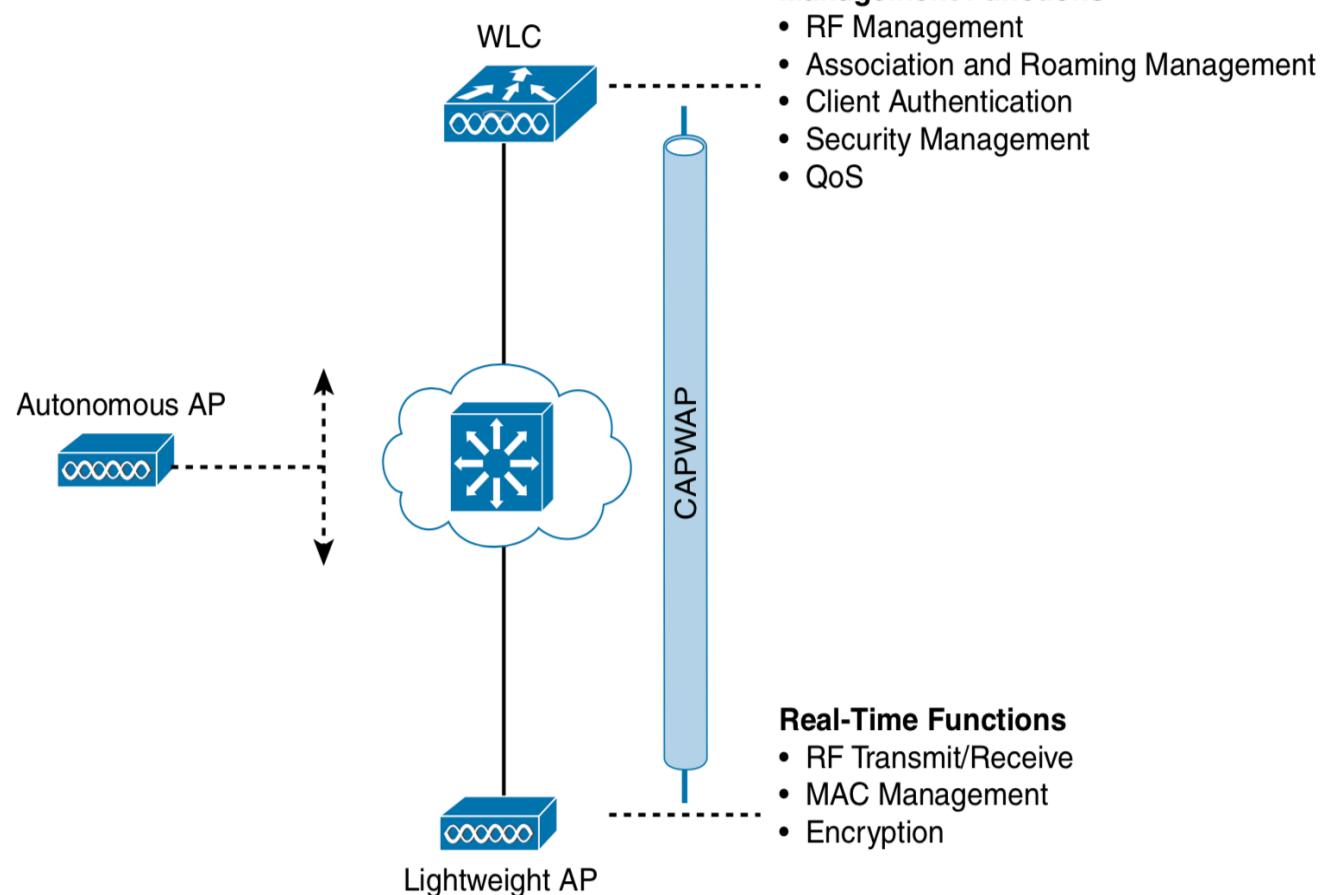
Exemple



Architecture Split-MAC

- Centraliser certaines fonctionnalités des APs
 - management des canaux
 - management de la sécurité, du roaming, de la QoS
- Split MAC « Media Access Control » (couche 2) :
 - **WLC** : « WireLessController »
 - AP « **lightweight** »
 - totalement dépendant du WLC pour :
 - authentifier les utilisateurs
 - obtenir un canal et la puissance d'émission
 - récupérer les polices de sécurité

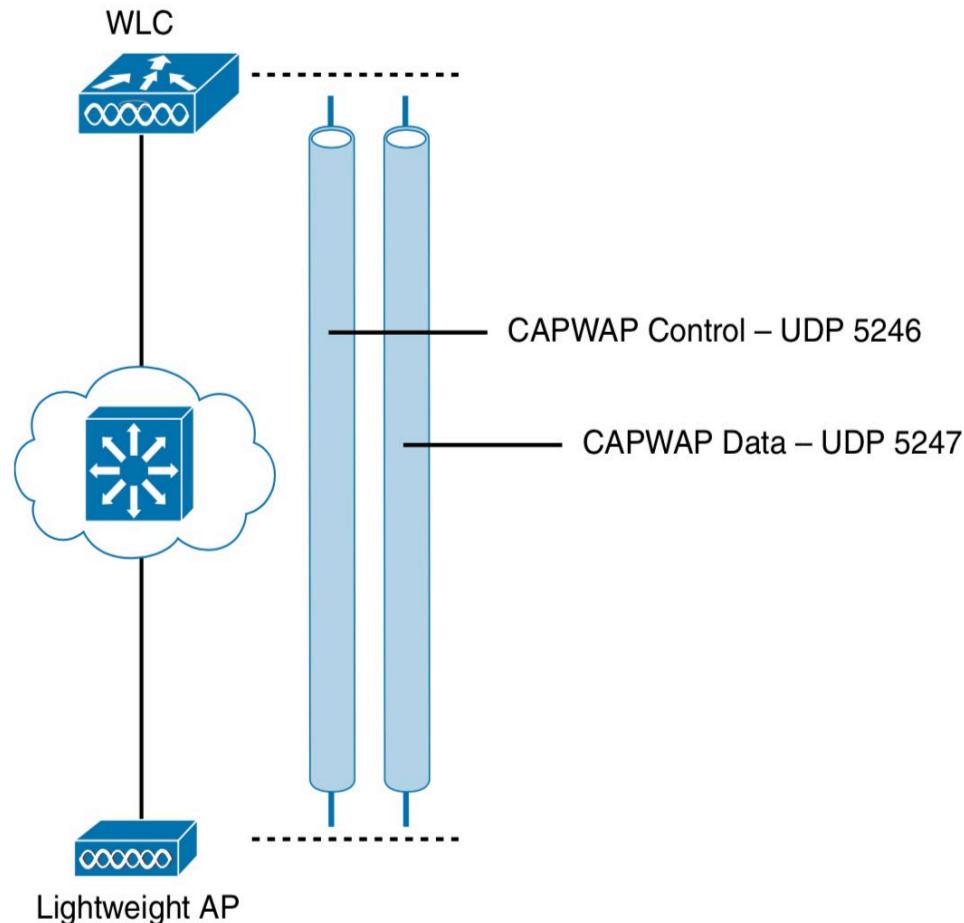
AP autonome vs lightweight



CAPWAP

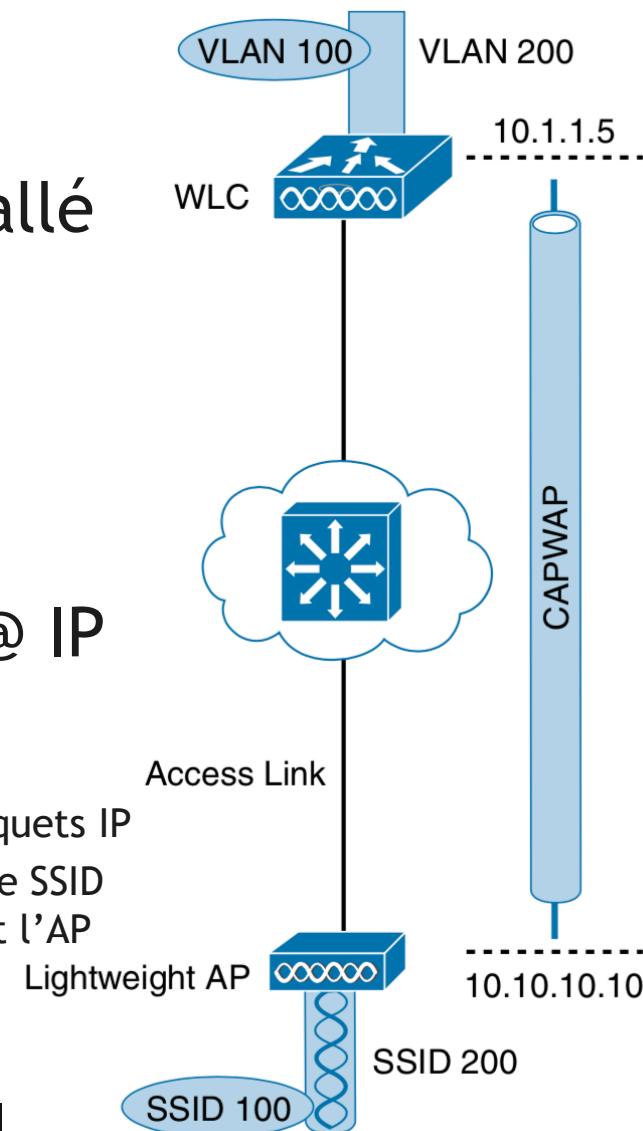
- Communication entre AP et WLC :
 - tunnel CAPWAP
 - « **Control and Provisioning of Wireless AP** »
 - architecture :
 - soit dans le même VLAN
 - soit dans 2 subnets différents
 - deux tunnels :
 - trafic de **contrôle** :
 - » pour configurer l'AP
 - » chiffré et authentifié
 - trafic de **données** :
 - » chiffrage DTLS en option

CAPWAP control vs data



Avantages du WLC

- Authentification :
 - Certificat digital **X.509** pré-installé sur chaque équipement
 - évite AP non autorisés
- Tunneling :
 - L'AP et le WLC ont chacun une @ IP
 - **Pas de trunk nécessaire**
 - les trames sont encapsulées et routées dans des paquets IP
 - Exemple du schéma : le VLAN 100 est étendu dans le SSID 100 sans que ce VLAN soit configuré entre le WLC et l'AP



Avantages du WLC

- **Dynamic channel assignment:** The WLC can automatically **choose and configure the RF channel** used by each AP, based on other active access points in the area.
- **Transmit power optimization:** The WLC can automatically **set the transmit power** of each AP based on the coverage area needed.
- **Self-healing wireless coverage:** **If an AP radio dies**, the coverage hole can be “healed” by turning up the transmit power of surrounding APs automatically.
- **Dynamic client load balancing:** If two or more APs are positioned to cover the same geographic area, the WLC can associate clients with the least used AP. This **distributes the client load across the APs**.
- **RF monitoring:** The WLC manages each AP so that **it scans channels to monitor the RF usage**. By listening to a channel, the WLC can remotely gather information about RF interference, noise, signals from neighboring APs, and signals from rogue APs or ad hoc clients.
- **Security management:** The WLC can **authenticate** clients from a central service and can require wireless clients to obtain an IP address from a **trusted DHCP server** before allowing them to associate and access the WLAN.
- **Wireless intrusion protection system:** Leveraging its central location, the WLC can **monitor client data** to detect and prevent malicious activity.

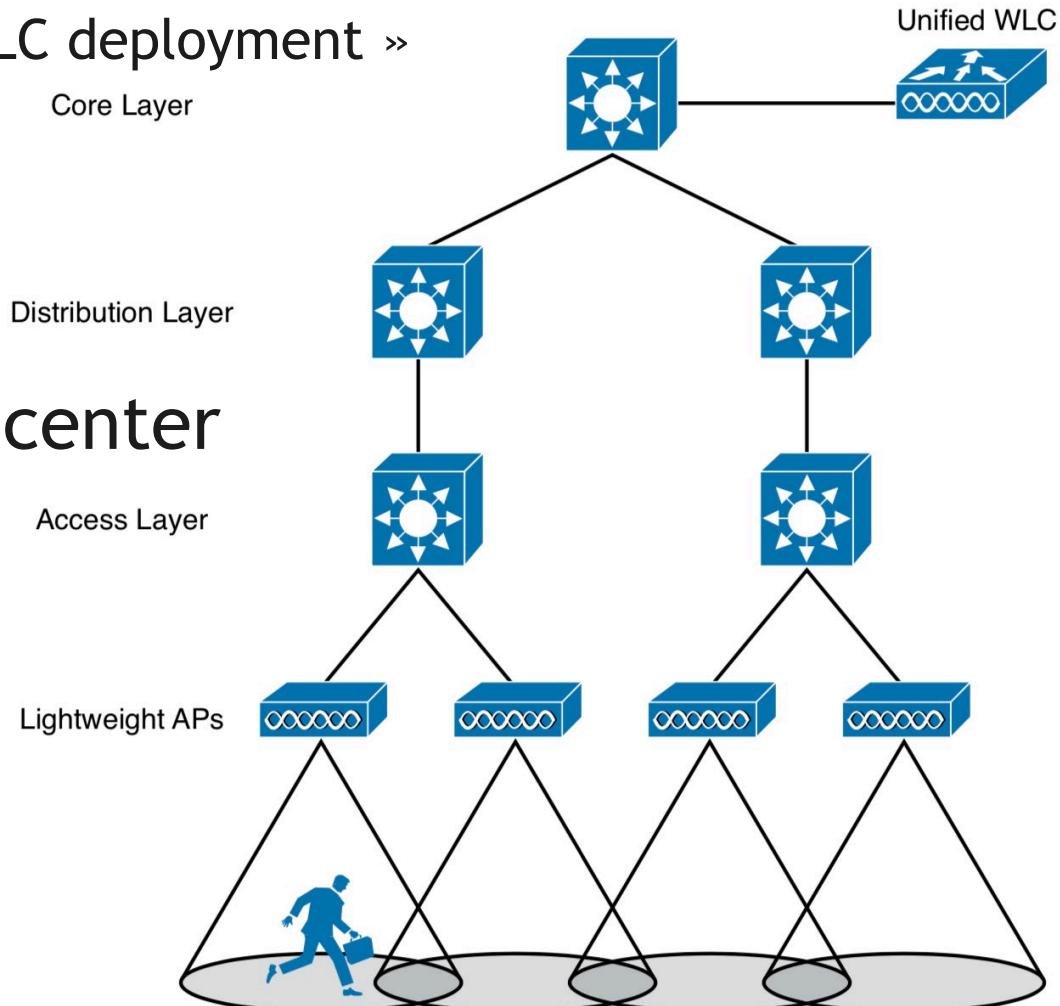
Positionnement du WLC

Option 1

- « **Unified / centralized** WLC deployment »

- les utilisateurs accèdent essentiellement à internet / data center

- max. 6000 APs



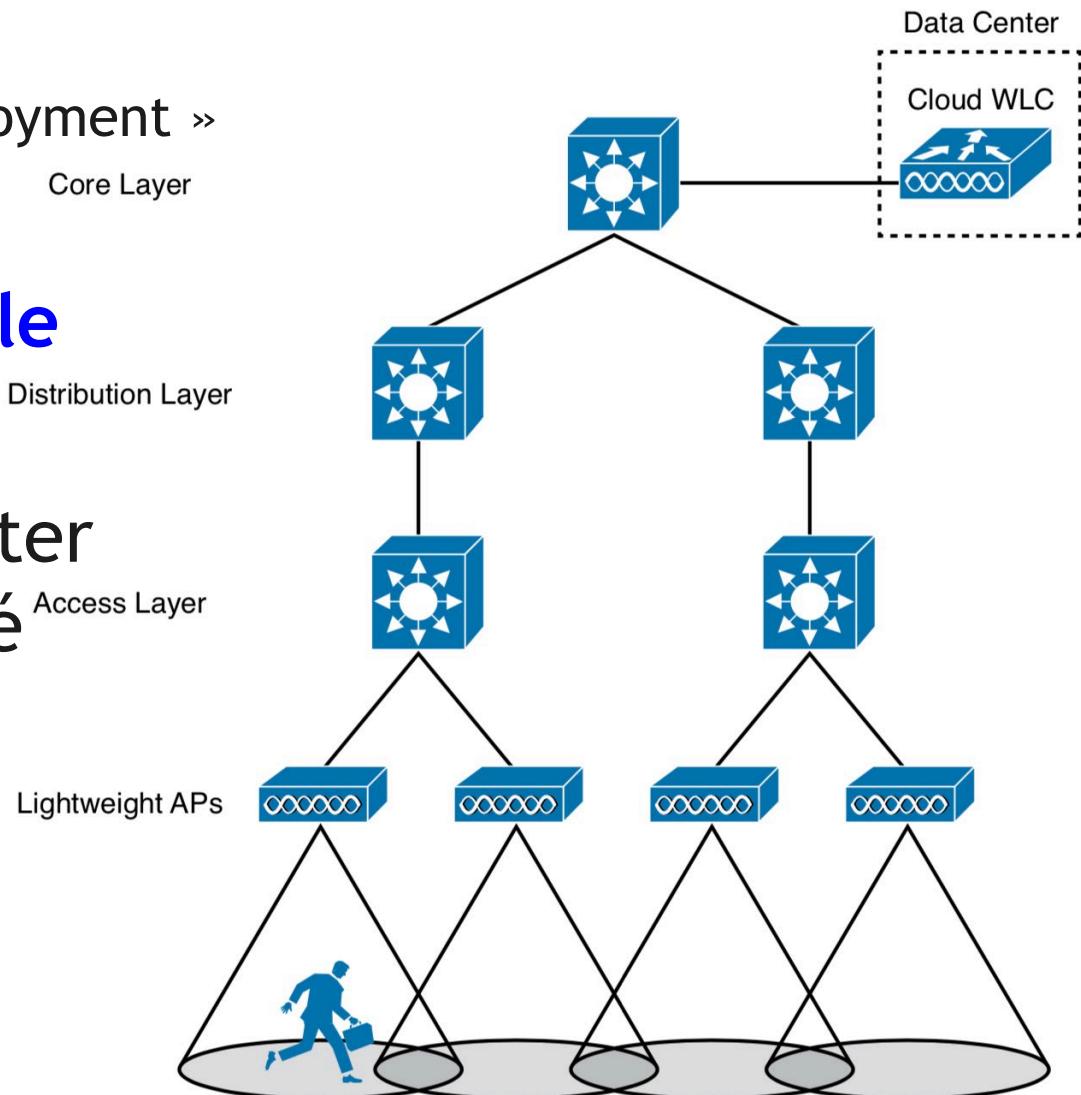
Option 2

- « **Cloud-based WLC deployment** »

- WLC dans une **machine virtuelle**

- dans le data center ou un cloud privé

- max. 3000 APs

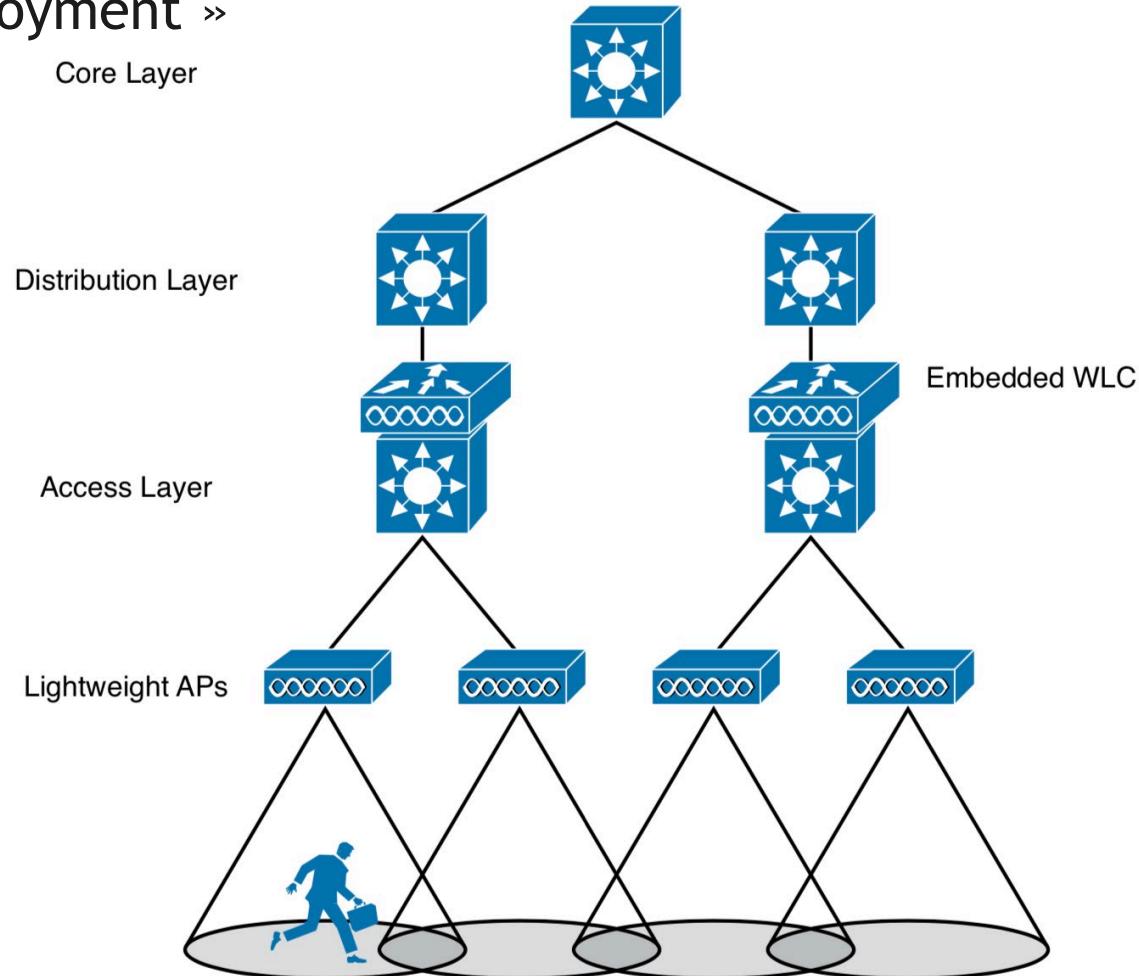


Option 3

- « **Embedded WLC deployment** »

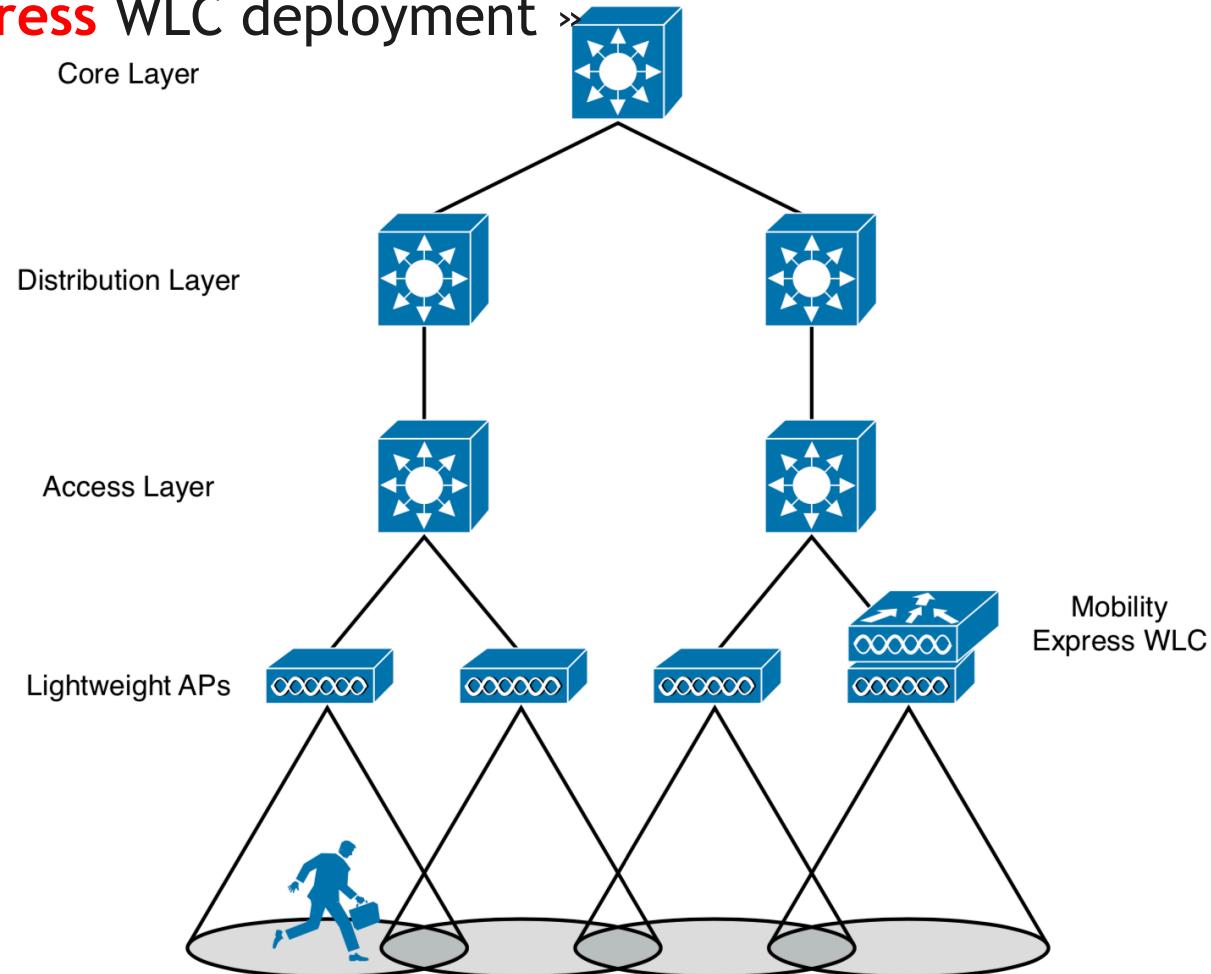
- WLC intégré dans un **switch**

- max. 200 APs



Option 4

- « **Cisco Mobility Express** WLC deployment »



- max. 100 APs

Bilan des 4 options

Deployment Model	WLC Location (DC, Access, Central, AP)	APs Supported	Clients Supported
Unified	Central	6000	64,000
Cloud	DC	3000	32,000
Embedded	Access	200	4000
Mobility Express	Other	100	2000

Modes de l'AP lightweight

Mode par défaut

- **L'image** chargée sur l'AP détermine s'il fonctionne en mode autonome ou lightweight.
 - Si lightweight, alors le WLC permet de configurer l'AP dans différents modes.
- Mode par défaut : « **Local** » :
 - l'AP utilise un canal pour offrir un ou plusieurs BSS
 - lorsqu'il n'a rien à transmettre, l'AP **scan** les autres canaux :
 - pour mesurer le bruit & les interférences
 - pour détecter les AP illicites

Autres modes

- **Monitor:**
 - **Récepteur** actif en continu, afin de déterminer la position des stations, détecter les intrusion et les AP illicites.
- **FlexConnect:**
 - **Dépanne** un autre AP dont le WLC est down.
- **Sniffer:**
 - Transmet le trafic sniffé à un poste équipé d'un **analyseur** de trafic.
- **Rogue detector:**
 - Déetecte les AP **illicites**= ceux dont l'adresse MAC apparaît à la fois sur le réseau WiFi et le réseau cablé.
- **Bridge:**
 - **Pont** dédié entre 2 subnets sur 2 réseaux distant (point-to-point / point-to-multipoint)
- **SE-Connect « Spectrum Expert » :**
 - Récepteur actif en continu, sur tous les canaux, afin de détecter les sources **d'interférence** (analyse de spectre)



Quiz

Quiz

Which one of the following terms best describes a Cisco wireless access point that operates in a **standalone, independent manner**?

- 
- a. Autonomous AP
 - b. Independent AP
 - c. Lightweight AP
 - d. Embedded AP

Quiz

The Cisco **Meraki** cloud-based APs are most accurately described by which one of the following statements?

- 
- a. Autonomous APs joined to a WLC
 - b. Autonomous APs centrally managed
 - c. Lightweight APs joined to a WLC
 - d. Lightweight APs centrally managed

Quiz

A **lightweight access point** is said to participate in which one of the following architectures?

- a. Light-MAC
- b. Tunnel-MAC
- c. Split-MAC
- d. Big-MAC



Quiz

How does a **lightweight access point communicate with a wireless LAN controller?**

- 
- a. Through an IPsec tunnel
 - b. Through a CAPWAP tunnel
 - c. Through a GRE tunnel
 - d. Directly over Layer 2

Quiz

Which one of the following is **not** needed for a **lightweight AP** in default **local** mode to be able to support **three SSIDs** that are bound to **three VLANs**?

- 
- a. A trunk link carrying three VLANs
 - b. An access link bound to a single VLAN
 - c. A WLC connected to three VLANs
 - d. A CAPWAP tunnel to a WLC

Quiz

Which one of the following WLC deployment models would be best for a large enterprise with around 3500 lightweight APs?

- 
- a. Cisco Mobility Express
 - b. Embedded
 - c. Unified
 - d. Cloud-based

Quiz

If a lightweight AP provides at least one BSS for wireless clients, which one of the following modes does it use?



- a. Local
- b. Normal
- c. Monitor
- d. Client

Quiz

Regarding **lightweight AP modes**, which one of the following is **true**?

- a. An AP can operate in multiple modes at the same time.
- b. An AP has only one possible mode of operation.
- c. The Run mode is the default mode.
- d. The SE-Connect mode is used for spectrum analysis.

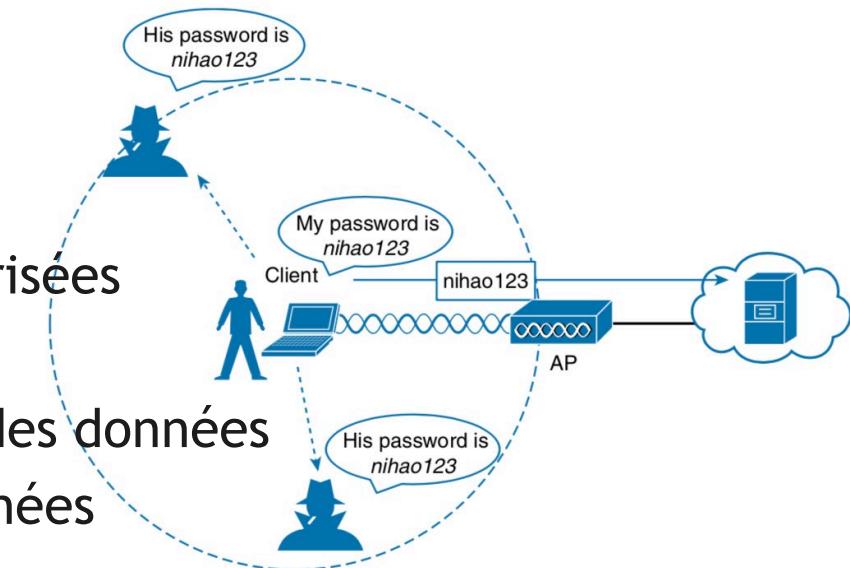


La sécurité du WiFi

Pourquoi faire ?

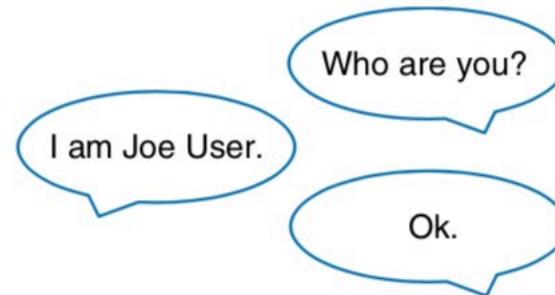
- Risques :
 - Les données échangées en WiFi sont entendues par toute station localisée dans le même BSA.
 - Une station non autorisée se connecte à l'AP.
 - Une station s'associe à un AP non autorisé

- Quatre objectifs de la sécurité :
 - Identifier les **stations** autorisées
 - Identifier les **AP** autorisés
 - Assurer **la confidentialité** des données
 - Assurer **l'intégrité** des données

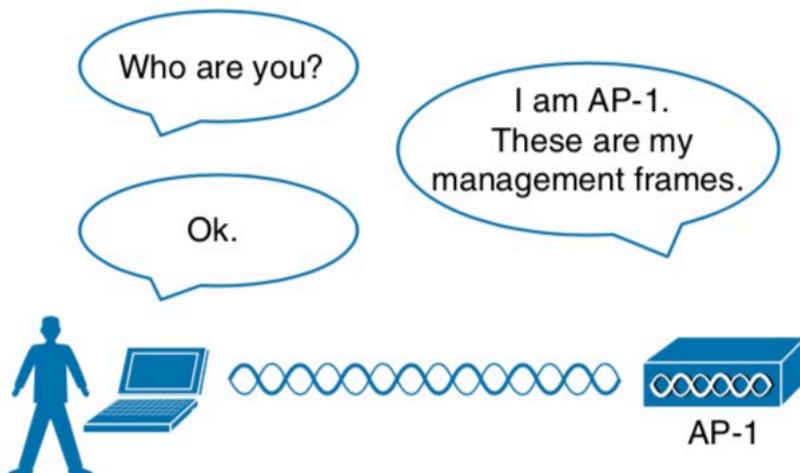


Authentification

- Authentifier la station :

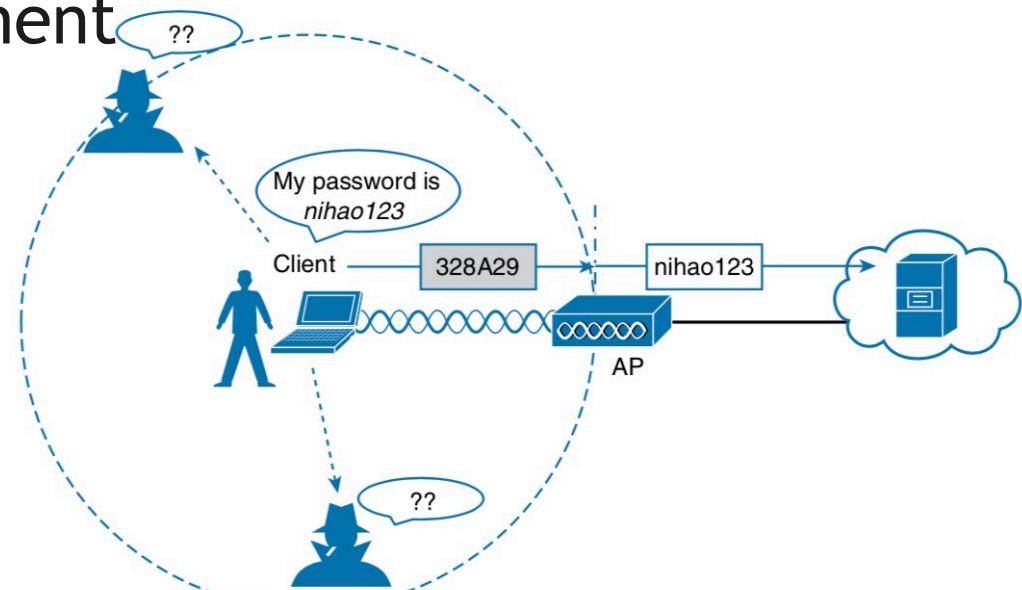


- Authentifier l'AP :



Confidentialité

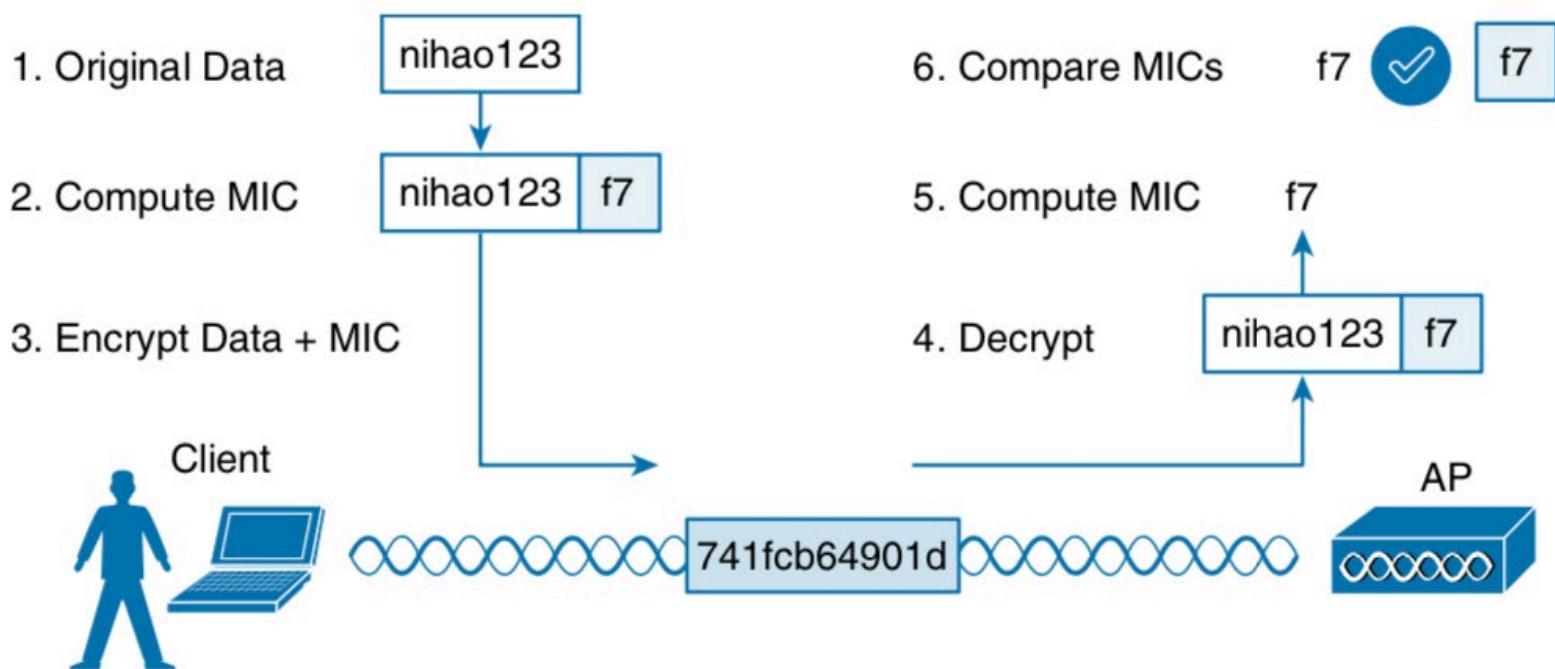
- Chaque association entre l'AP et une station aura sa propre clef de chiffrement :
 - **clef unique**
négociée secrètement



- L'AP peut aussi utiliser une **clef de groupe**, pour communiquer avec toutes les stations de sa cellule.

Intégrité

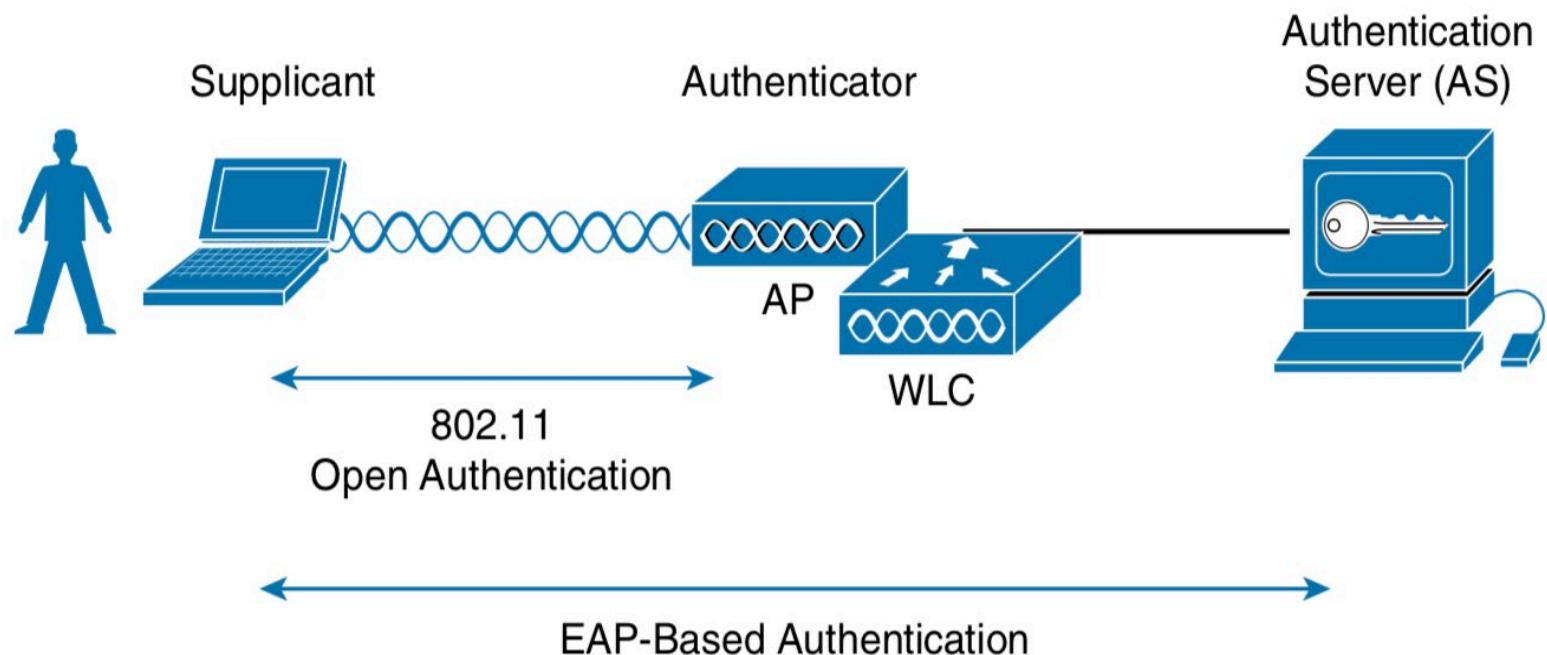
- Sur réception d'un trame :
 - **MIC**, « Message integrity check »



3 modes d'authentification

- **OPEN** :
 - aucune vérification basée sur identifiant
 - vérification de l'utilisation du protocole 802.11
 - utilité : dans les lieux **publics**
 - le client doit ouvrir un navigateur pour accepter les termes du contrats (et éventuellement s'authentifier)
- **WEP**, « Wired equivalent privacy » :
 1. **authentification des stations (challenge)** :
 - seules celles connaissant la clef **commune** peuvent s'associer à l'AP
 2. **chiffrement des données, algorithme RC4** (clef de 40 / 104 bits)
 - un 1ère clef commune utilisée par l'AP et toutes les stations
 - elle permet de générer une clef spécifique pour chaque station
 - **déprécié depuis 2004**
- **EAP**, « Extensible Authentication Protocol » :
 - collabore avec **802.1X** :
 - limitation de l'accès au réseau jusqu'à authentification complète
 - les stations peuvent s'associer à l'AP, mais ne peuvent envoyer de données

Rôle 802.1x



4 options EAP/802.1x

- **LEAP**, « Lightweight EAP » :
 - propriétaire Cisco, **déprécié**
 - authentification mutuelle :
 - challenges basés sur username / password
 - chiffrement via des clefs WEP dynamiques
- **EAP FAST**, « EAP Flexible Authentication by Secure Tunneling » :
 - étapes :
 - le server RADIUS (SA) génère une clef PAC « Protected Access Credential »
 - le SA envoie le PAC au supplicant
 - le SA et le supplicant s'authentifient mutuellement (« outer authentication »)
 - ils montent un tunnel TLS entre eux
 - l'utilisateur final est authentifié via ce tunnel (« inner authentication »)
- **PEAP**, « Protected EAP » :
 - EAP-FAST + **certificat digital côté SA** (« outer auth »)
- **EAP-TLS**, « EAP Transport Layer Security » :
 - PEAP + **certificat digital côté client**
 - le tunnel TLS permet d'échanger les clefs de chiffrement

3 modes de confidentialité & intégrité

- **TKIP**, « Temporal Key Integrity Protocol » :
 - WEP + MIC + Timestamp
 - **déprécié en 2012**
- **CCMP**, « Counter/CBC-MAC Protocol » :
 - chiffrement AES
 - intégrité CBC-MAC
 - opérations effectuées en hardware
- **GCMP**, « Galois/Counter Mode Protocol » :
 - chiffrement AES
 - intégrité G-MAC
 - le plus sécurisé

Bilan des protocoles

Security Mechanism	Type	Type Expansion	Credentials Used
Authentication Methods	Open	Open Authentication	None, other than 802.11 protocol
	WEP	Wired Equivalent Privacy	Static WEP keys
	802.1x/EAP (Extensible Authentication Protocol)	LEAP	Lightweight EAP
	EAP-FAST	EAP Flexible Authentication by Secure Tunneling	Uses protected access credential (PAC)
		PEAP	AS authenticated by digital certificate
	EAP-TLS	EAP Transport Layer Security	Client and AS authenticated by digital certificate
Privacy & Integrity Methods	TKIP	Temporal Key Integrity Protocol	N/A
	CCMP	Counter/CBC-MAC Protocol	N/A
	GCMP	Galois/Counter Mode Protocol	N/A

WPA

- Comment configurer un WLAN ?
 - quels protocoles sélectionner ?
 - quels protocoles sont compatibles ?
- **Certifications WPA**, « Wi-Fi Protected Access »
 - définies par l'Alliance Wi-Fi
 - choisir des équipements qui ont la même version
 - trois versions :
 - 2003 : **WPA** : TKIP
 - 2006 : **WPA2** : CCMP
 - 2018 : **WPA3** : GCMP + PMP « Protected management frames »

Bilan des certifications

Authentication and Encryption Feature Support	WPA	WPA2	WPA3
Authentication with Pre-Shared Keys?	Yes	Yes	Yes
Authentication with 802.1x?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	No	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

PSK vs 802.1x

- PSK, « **Personal mode** » :
 - la même clef doit être configurée sur toutes les stations et sur l'AP
 - simple à déployer
 - seule WPA3 pleinement sécurisé
- 802.1x, « **Enterprise mode** » :
 - déployer EAP
 - plus complexe



Quiz

Quiz

Which of the following are necessary components of a **secure** wireless connection? (Choose all that apply.)

- a. Encryption
- b. MIC
- c. Authentication
- d. All of these answers are correct.



Quiz

Which one of the following is used to protect the **integrity** of data in a wireless frame?

- a. WIPS
- b. WEP
- c. MIC
- d. EAP



Quiz

Which one of the following is a wireless **encryption** method that has been found to be vulnerable and is **not recommended** for use?

- a. AES
- b. WPA
- c. EAP
- d. WEP



Quiz

Which one of the following is used as the **authentication** framework when **802.1x** is used on a WLAN?

- a. Open authentication
- b. WEP
- c. EAP
- d. WPA



Quiz

Suppose you would like to select a method to protect the **privacy and integrity** of wireless data.

Which one of the following methods should you avoid because it has been **deprecated** ?

- 
- a. TKIP
 - b. CCMP
 - c. GCMP
 - d. EAP

Quiz

Which one of the following is the data encryption and integrity method used by **WPA2**?

- a. WEP
- b. TKIP
- c. CCMP
- d. WPA



Quiz

The Wi-Fi Alliance offers which of the following **certification** for wireless devices that **correctly** implements security standards?

- a. WEP
- b. WPA2
- c. 802.11
- d. AES



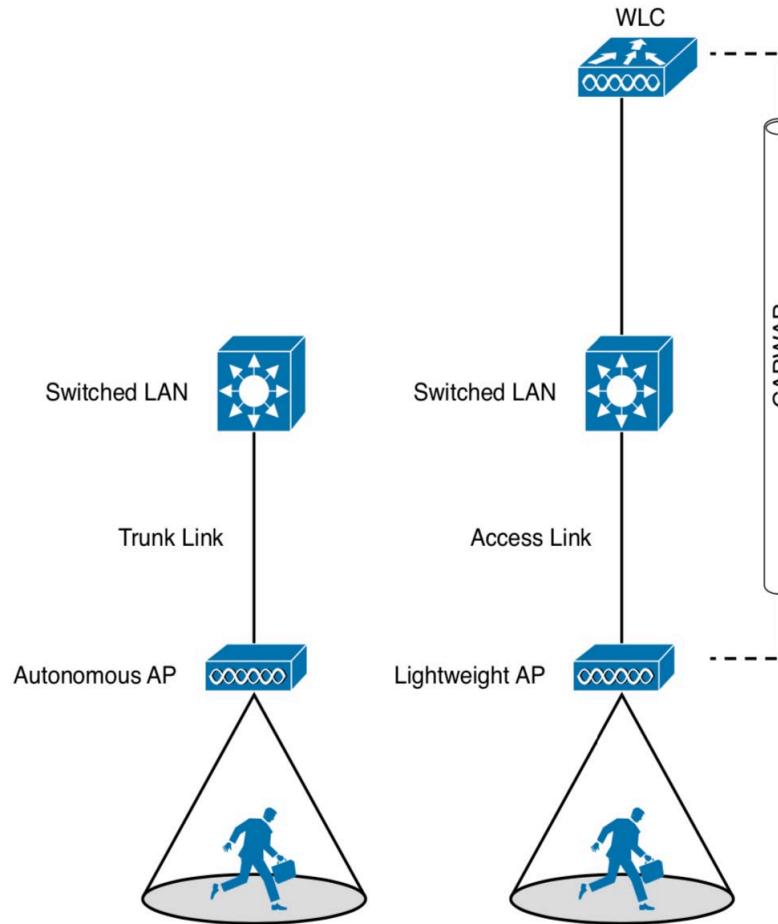
Quiz

A **pre-shared key** is used in which of the following wireless security configurations? (Choose all that apply.)

-  a. WPA2 personal mode
-  b. WPA2 enterprise mode
-  c. WPA3 personal mode
- d. WPA3 enterprise mode

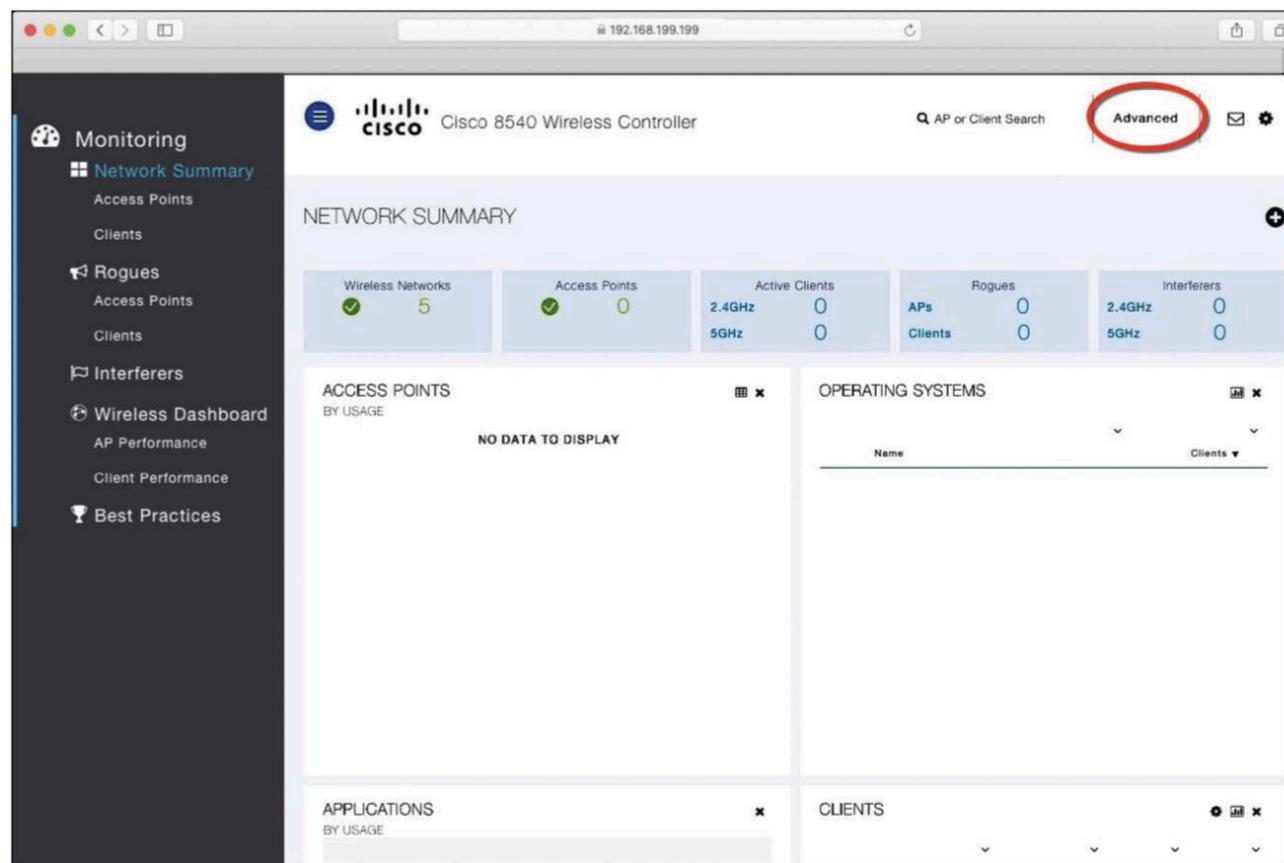
Configurer un WLC

Connection de l'AP au réseau



Management du WLC

- GUI, interface web :



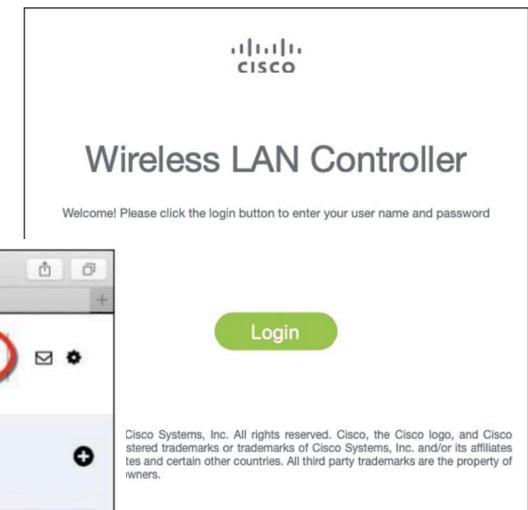
The screenshot shows the Cisco 8540 Wireless Controller's Network Summary page. The left sidebar has a dark theme with the following menu items:

- Monitoring
- Network Summary
- Access Points
- Clients
- Rogues
- Access Points
- Clients
- Interferers
- Wireless Dashboard
- AP Performance
- Client Performance
- Best Practices

The main content area displays network statistics:

Wireless Networks	Access Points	Active Clients	Rogues	Interferers
5	0	2.4GHz: 0 5GHz: 0	0	2.4GHz: 0 5GHz: 0
			APs: 0 Clients: 0	

Below this are sections for ACCESS POINTS BY USAGE (No data to display) and OPERATING SYSTEMS (with a table header for Name and Clients).



The screenshot shows the Cisco Wireless LAN Controller's login page. It features a Cisco logo at the top right, a "Login" button in the center, and a welcome message: "Welcome! Please click the login button to enter your user name and password". At the bottom, there is a copyright notice: "Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco stored trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates and certain other countries. All third party trademarks are the property of their owners."

Interface avancée

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping | Logout | Refresh

Home

Monitor

Summary

Access Points Cisco CleanAir Statistics CDP Rogues Redundancy Clients Sleeping Clients Multicast Applications Lync Local Profiling

6000 Access Points Supported

CISCO Cisco 8540 Wireless Controller

10 GbE Port 4 Port 3 Port 2 Port 1 Pwr OK

4 3 2 1

Mgnt IOIOI SP2x RP2x ICI PSU

Controller Summary

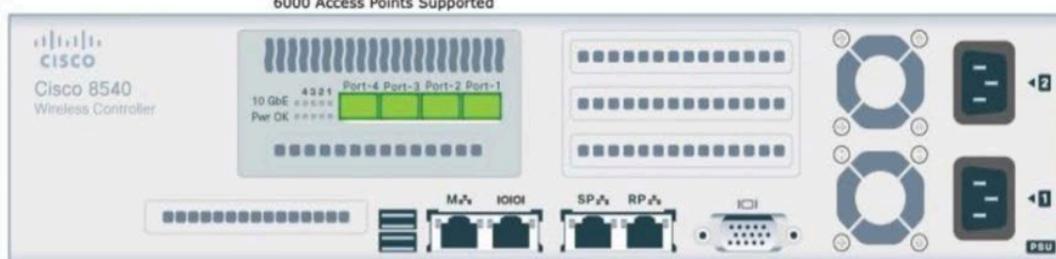
Management IP Address	192.168.199.199, ::/128
Service Port IP Address	192.168.1.1, ::/128
Software Version	8.5.140.0
Emergency Image Version	8.2.166.0
System Name	wlc
Up Time	7 days, 1 hours, 56 minutes
System Time	Wed Apr 17 15:13:51 2019

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Session Timeout

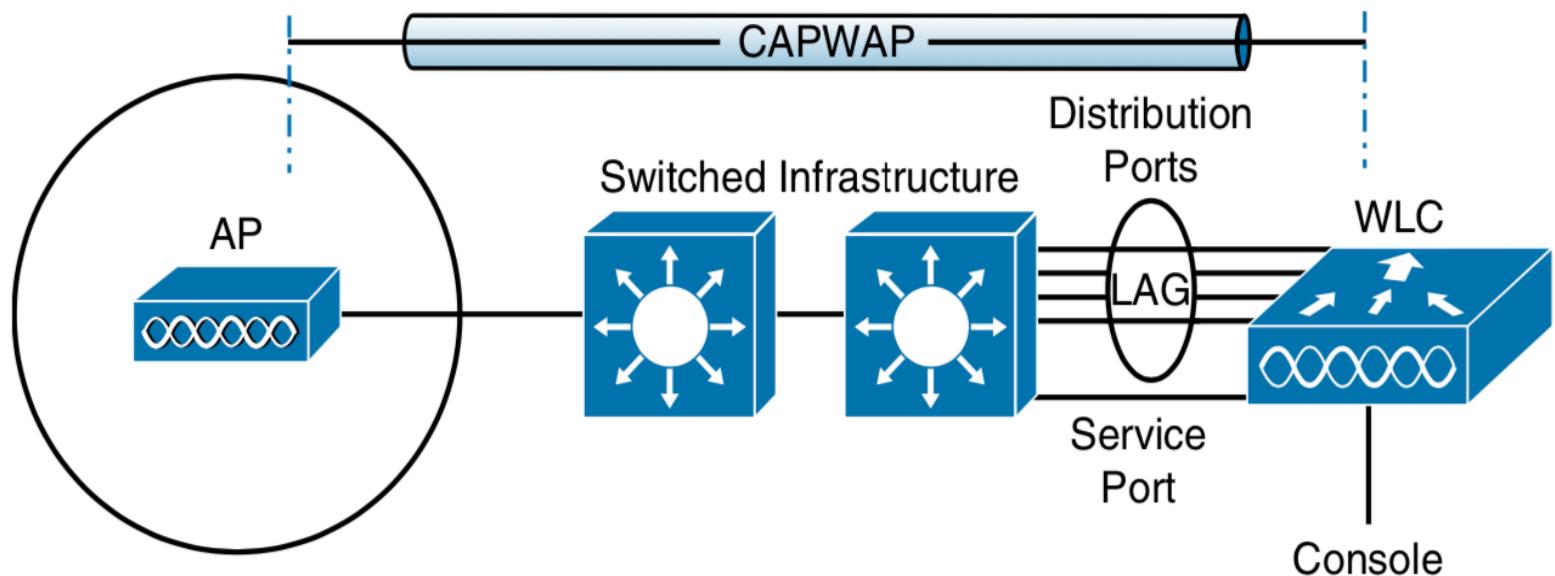
Top WLANs



WLC : port **vs** interface

- « **Port** », connection physique :
 - **Console**
 - management out-of-band, asynchrone
 - **Service**
 - management out-of-band, connecté à un port accès de switch
 - **Distribution**
 - pour le trafic vers les AP, connecté à un port trunk de switch
 - option 1 : paire redondante
 - option 2 : **LAG** « Ling Aggregation Group » (mode static côté switch)
 - **Redondant**
 - pour Haute Disponibilité, connecté à un autre WLC
- « **Interface** », connection logique :
 - interface de couche 3 associée à chaque VLAN

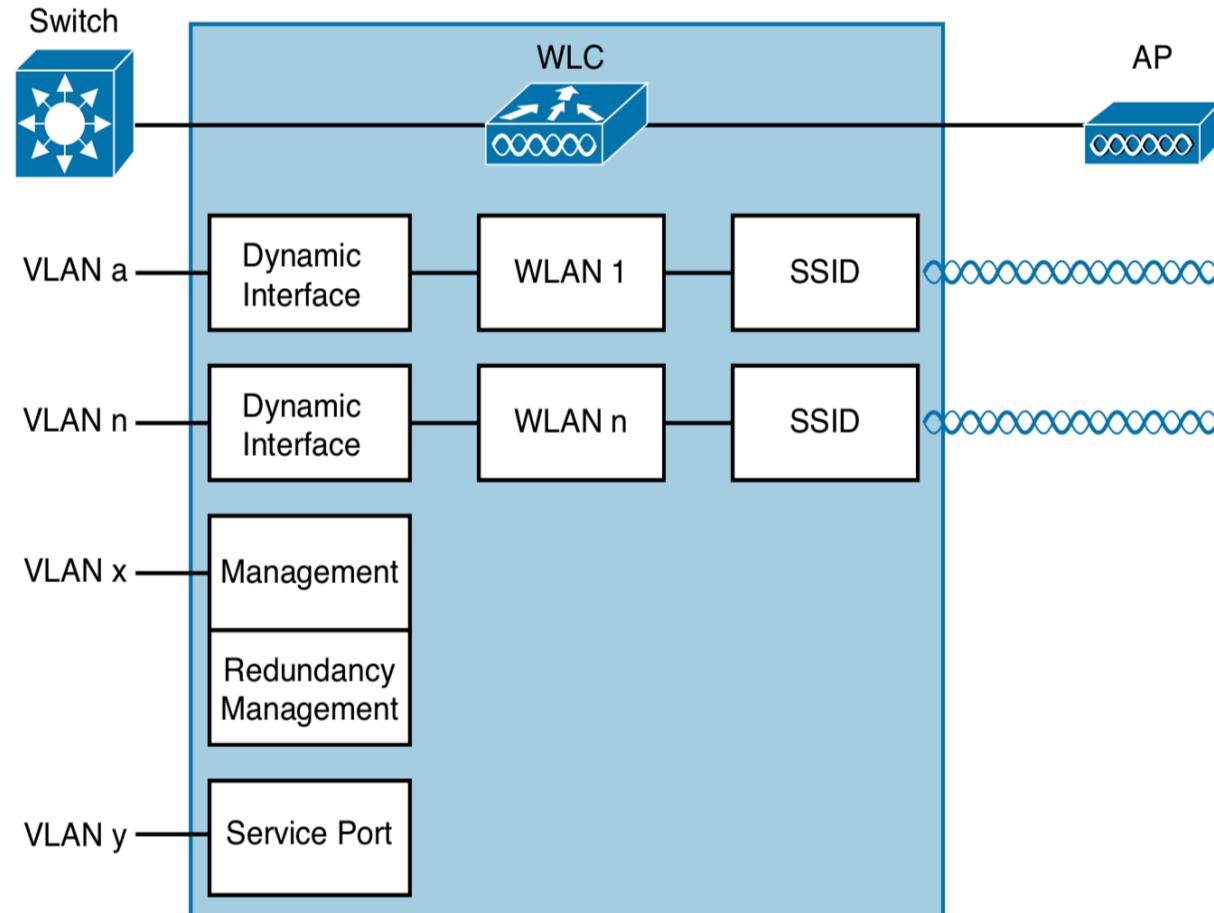
Ports d'un WLC



Interfaces d'un WLC

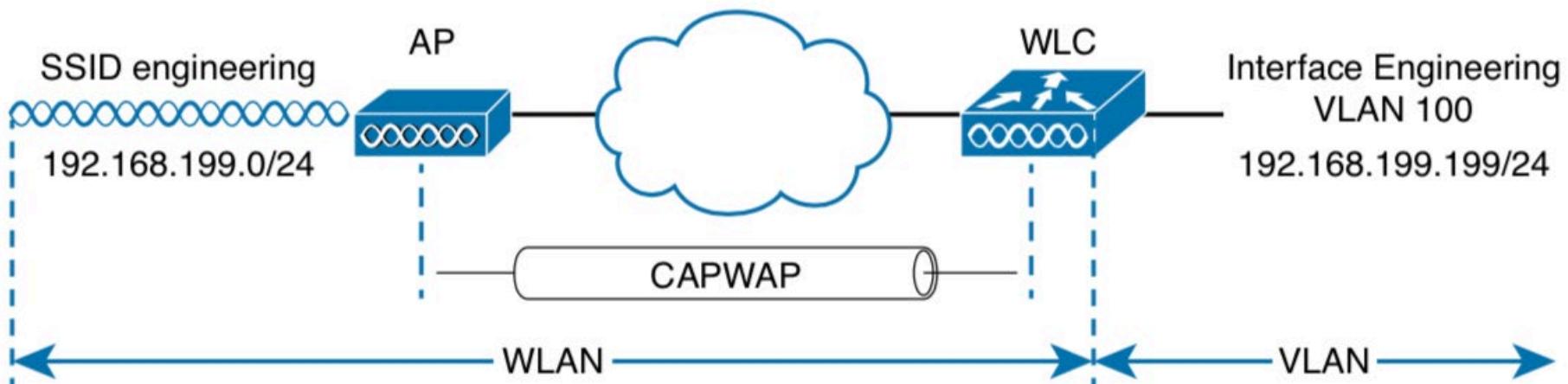
- Interface **logique** :
 - avec une adresse IP, un masque, une passerelle par défaut
 - associée
 - à un serveur DHCP
 - à un port physique
 - à un n° de VLAN
 - types :
 - **dynamique**
 - pour connecter un VLAN à un WLAN
 - **service**
 - associée au port de service
 - **management**
 - pour le trafic de management
 - terminaison des tunnels CAPWAP

Interfaces d'un WLC



VLAN vs WLAN

- L'AP annonce un **SSID**
- Le WLC est connecté à un **VLAN**
- Pour relier le SSID avec le VLAN :
 - un **WLAN** doit être configuré sur le WLC



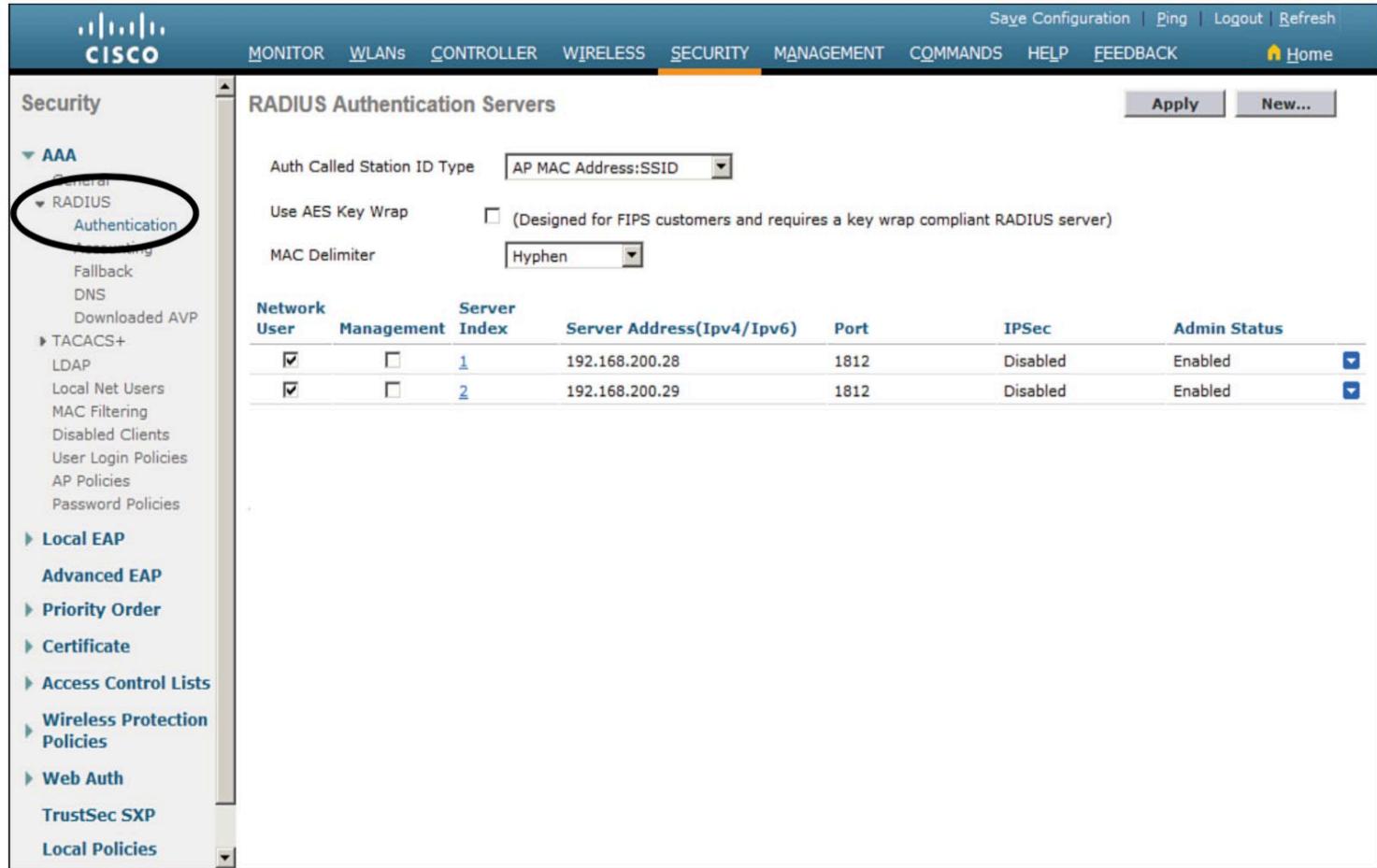
Bonne pratique

- Ségrégation du trafic entre chaque WLAN
 - routage inter-WLAN par un équipement niveau 3 sur réseau câblé
- Configuration :
 - max 512 WLAN / WLC
 - max 16 WLAN / AP
- Bonne pratique :
 - **3 ou 5 WLAN / AP**
 - sinon **saturation** du canal
 - par l'envoi des annonces « **beacons** »
 - toutes les 100 ms
 - pour chaque WLAN

Configuration en 3 étapes

- Configurer **le serveur Radius** (si WPA2-enterprise ou WPA3-enterprise) :
 - @ IP, mot de passe, n° de port
- Configurer **l'interface dynamique** :
 - nom, n° de VLAN
 - @ IP, masque, passerelle, @ de serveur DHCP
- Configurer **le WLAN** :
 - nom, SSID, interface associée,
 - police de sécurité

Etape 1 : radius



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the **SECURITY** tab. On the left, the **AAA** menu is expanded, showing **RADIUS Authentication** selected. This section is highlighted with a red oval. The main pane displays the **RADIUS Authentication Servers** configuration.

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	192.168.200.28	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	192.168.200.29	1812	Disabled	Enabled

Etape 1 : radius

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

RADIUS Authentication Servers > New

< Back Apply

Server Index (Priority)	3
Server IP Address(Ipv4/Ipv6)	192.168.200.30
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Disabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP
- Local Policies

Etape 2 : interface dynamique

CISCO MONITOR WLAN **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration | Ping | Logout | Refresh Home

Controller

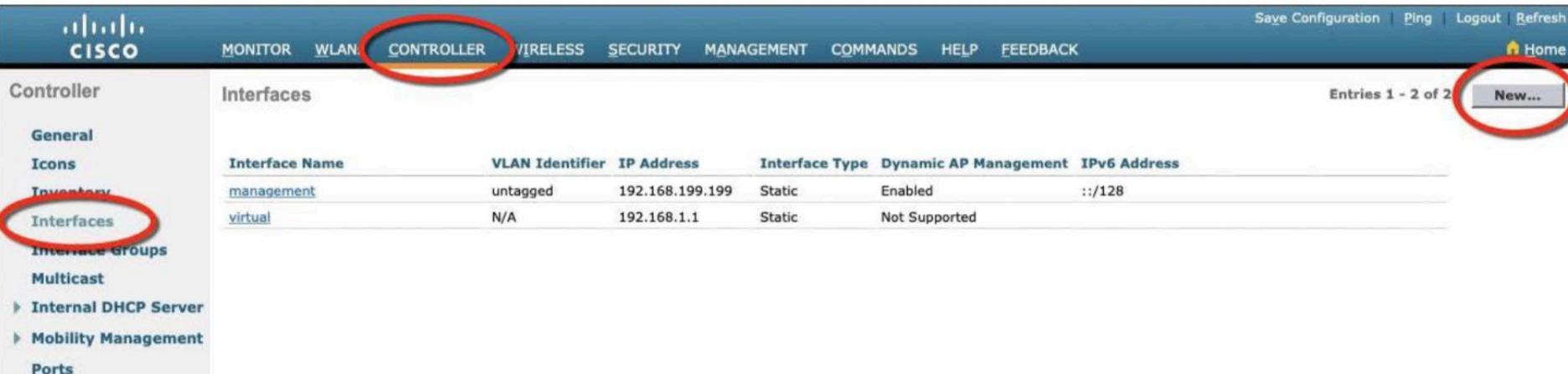
- General
- Icons
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- Internal DHCP Server
- Mobility Management
- Ports

Interfaces

Entries 1 - 2 of 2

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.199.199	Static	Enabled	::/128
virtual	N/A	192.168.1.1	Static	Not Supported	

New...



CISCO MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration | Ping | Logout | Refresh Home

Controller

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Internal DHCP Server
- Mobility Management
- Ports

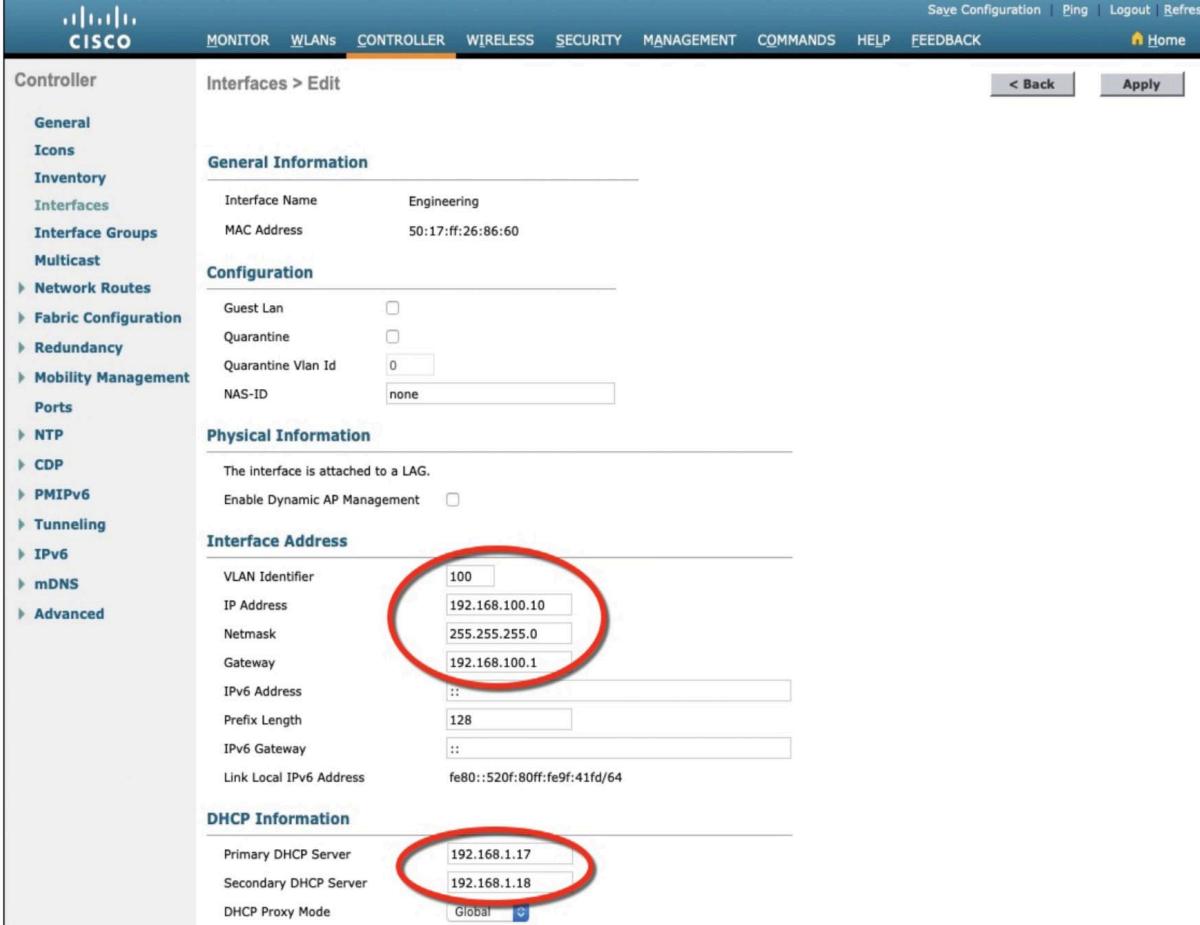
Interfaces > New

< Back Apply

Interface Name	Engineering
VLAN Id	100



Etape 2 : interface dynamique



The screenshot shows the 'Interfaces > Edit' page for the 'Engineering' interface. The left sidebar lists various interface-related options. The main configuration area is divided into sections: General Information, Configuration, Physical Information, Interface Address, and DHCP Information.

General Information:

- Interface Name: Engineering
- MAC Address: 50:17:ff:26:86:60

Configuration:

- Guest Lan:
- Quarantine:
- Quarantine Vlan Id: 0
- NAS-ID: none

Physical Information:

The interface is attached to a LAG.

Enable Dynamic AP Management:

Interface Address:

VLAN Identifier	100
IP Address	192.168.100.10
Netmask	255.255.255.0
Gateway	192.168.100.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::520f:80ff:fe9f:41fd/64

DHCP Information:

Primary DHCP Server	192.168.1.17
Secondary DHCP Server	192.168.1.18
DHCP Proxy Mode	Global

Etape 3 : WLAN



Save Configuration | Ping | Logout | Refresh

Home

WLANS

WLANS

WLANS

Advanced

WLANS

WLANS

Entries 0 - 0 of 0

Create New Go



Save Co

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS

WLANS

WLANS

Advanced

WLANS

WLANS > New

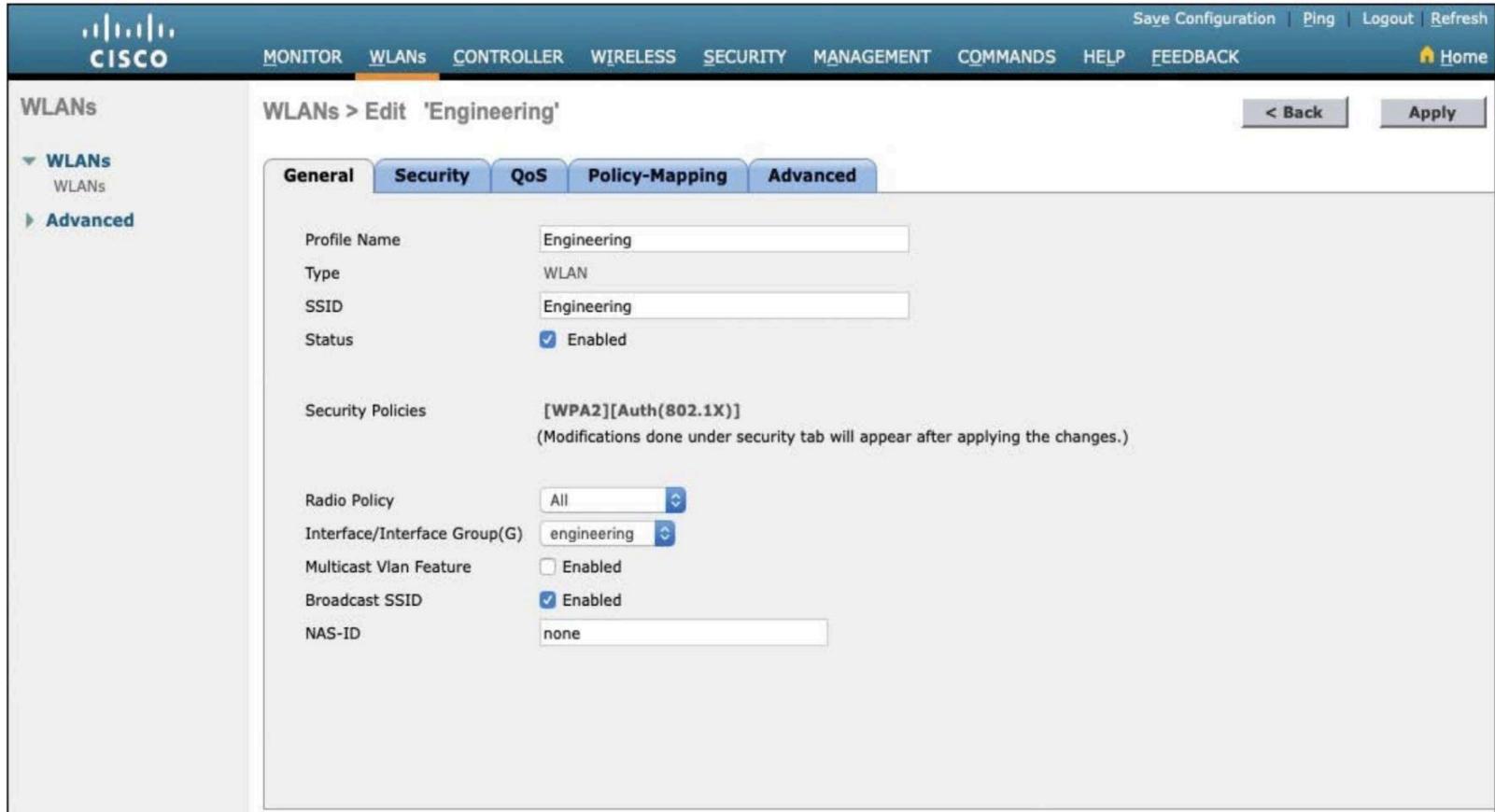
Type: WLAN

Profile Name: Engineering

SSID: Engineering

ID: 1

Etape 3 : WLAN, onglet « General »



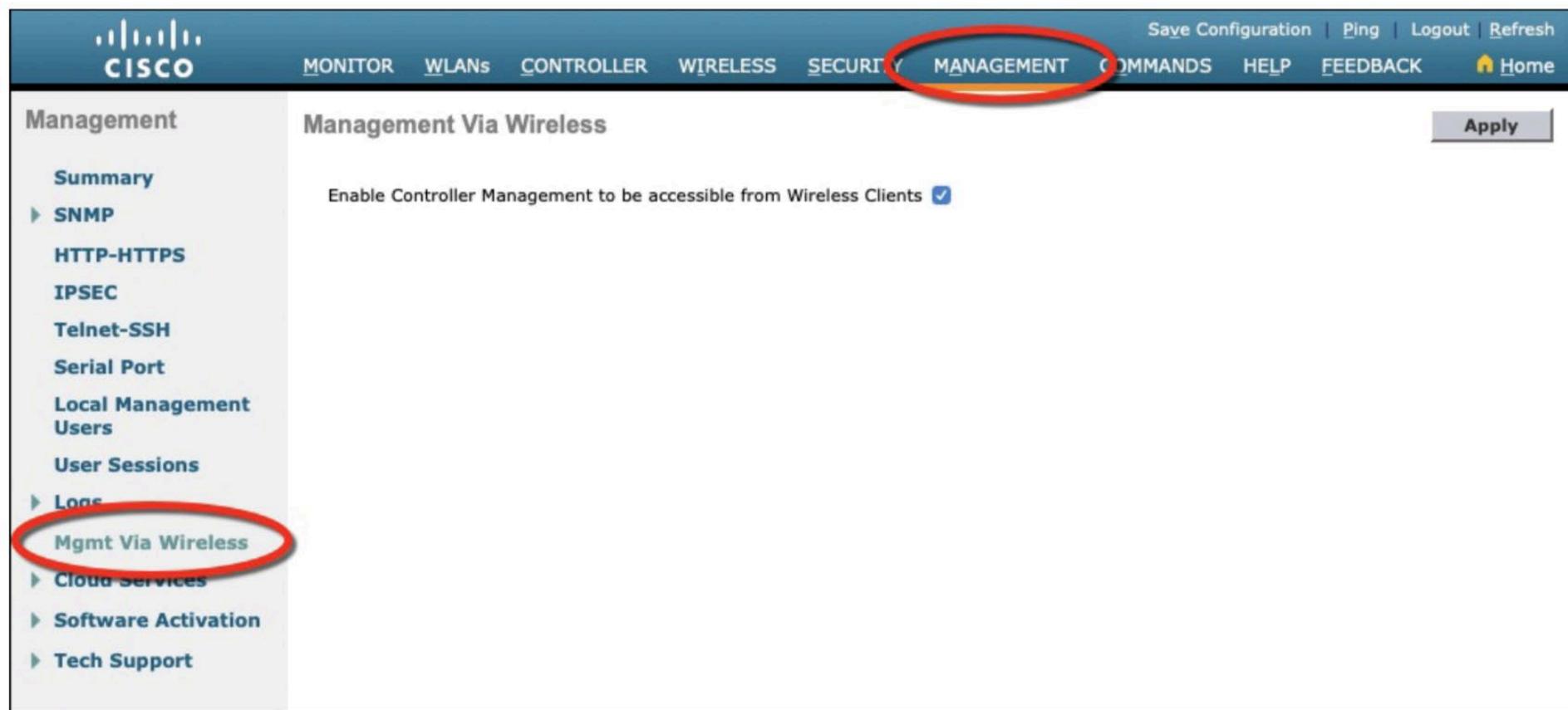
The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs (which is highlighted), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK, and options to Save Configuration, Ping, Logout, and Refresh. The left sidebar has a tree view with WLANS selected, under which WLANS and Advanced are listed. The main content area shows the 'WLANS > Edit 'Engineering'' screen. The 'General' tab is active, while Security, QoS, Policy-Mapping, and Advanced tabs are visible. The configuration fields include:

Profile Name	Engineering
Type	WLAN
SSID	Engineering
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	engineering
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

Buttons for < Back and Apply are located at the top right of the main content area.

Management

- Par défaut, autorisé seulement depuis le réseau câblé
- Pour autoriser depuis le réseau WiFi :



The screenshot shows a Cisco management interface. At the top, there's a navigation bar with links: MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT (which is highlighted with a red oval), COMMANDS, HELP, FEEDBACK, and a Home link. Below the navigation bar, the main content area has a sidebar on the left with various management options like Summary, SNMP, HTTP-HTTPS, IPSEC, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless (also highlighted with a red oval), Cloud Services, Software Activation, and Tech Support. The main panel displays "Management Via Wireless" and a checkbox for "Enable Controller Management to be accessible from Wireless Clients" which is checked. There's also an "Apply" button at the bottom right of the main panel.



Quiz

Quiz

Suppose you need to connect a **lightweight AP** to a network.

Which one of the following link types would be necessary?



- a. Access mode link
- b. Trunk mode link
- c. LAG mode link
- d. EtherChannel link

Quiz

An **autonomous AP** will be configured to support three WLANs that correspond to three VLANs.

The AP will connect to the network over which one of the following?

- a. Access mode link
- b. Trunk mode link
- c. LAG mode link
- d. EtherChannel link



Quiz

Suppose you would like to **connect** to a WLC to configure a new WLAN on it.

Which one of the following is a valid method to use?

- a. SSH
- b. HTTPS
- c. HTTP
- d. All of these answers are correct.



Quiz

Which one of the following correctly describes the single logical link formed by **bundling** all of a controller's **distribution system** ports together?

- a. PHY
- b. DSP
- c. LAG
- d. GEC



Quiz

Which one of the following controller interfaces maps a WLAN to a VLAN?

- 
- a. Bridge interface
 - b. Virtual interface
 - c. WLAN interface
 - d. Dynamic interface

Quiz

Which two of the following items are bound together when a new WLAN is created?

- a. VLAN
- b. AP
- c. Controller interface
- d. SSID



Quiz

What is the **maximum number of WLANs** you can configure on a Cisco wireless controller?

- a. 8
- b. 16
- c. 512
- d. 1024



Quiz

Which of the following parameters are necessary when **creating a new WLAN** with the controller GUI? (Choose all that apply.)

-  a. SSID
-  b. VLAN number
-  c. Interface
- d. BSSID
- e. IP subnet

Félicitations

Vous avez suivi avec succès
cette formation