

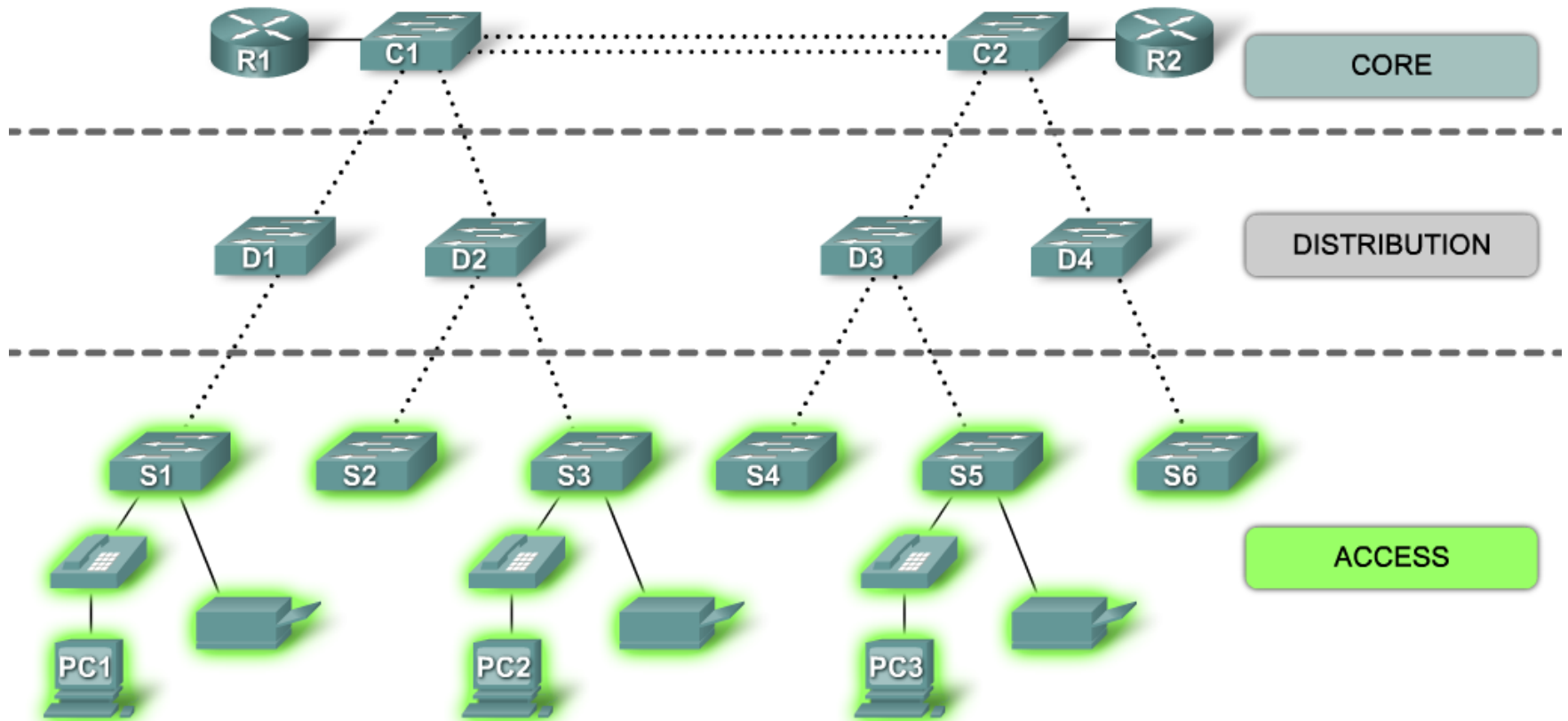
MODÉLISATION HIÉRARCHIQUE DU RÉSEAU

Pourquoi et comment hiérarchiser ?

Construire un réseaux ?

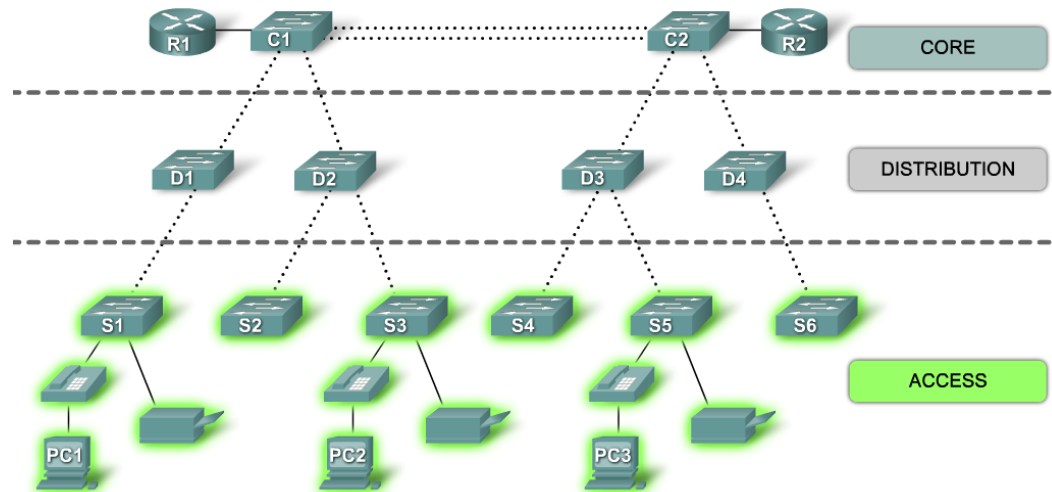
- Un réseau n'est pas la simple accumulation de switch et routeur !
- Il faut l'organiser, le hiérarchiser
 - Pour simplifier son administration
 - Pour isoler rapidement les problèmes
 - Pour rendre modulable le réseau et pour pouvoir facilement l'agrandir
- Un réseau d'entreprise est donc découpé suivant un modèle en 3 couches
 - Access Layer
 - Distribution Layer
 - Core Layer
- Chaque couche va avoir des fonctionnalités particulières

Access Layer

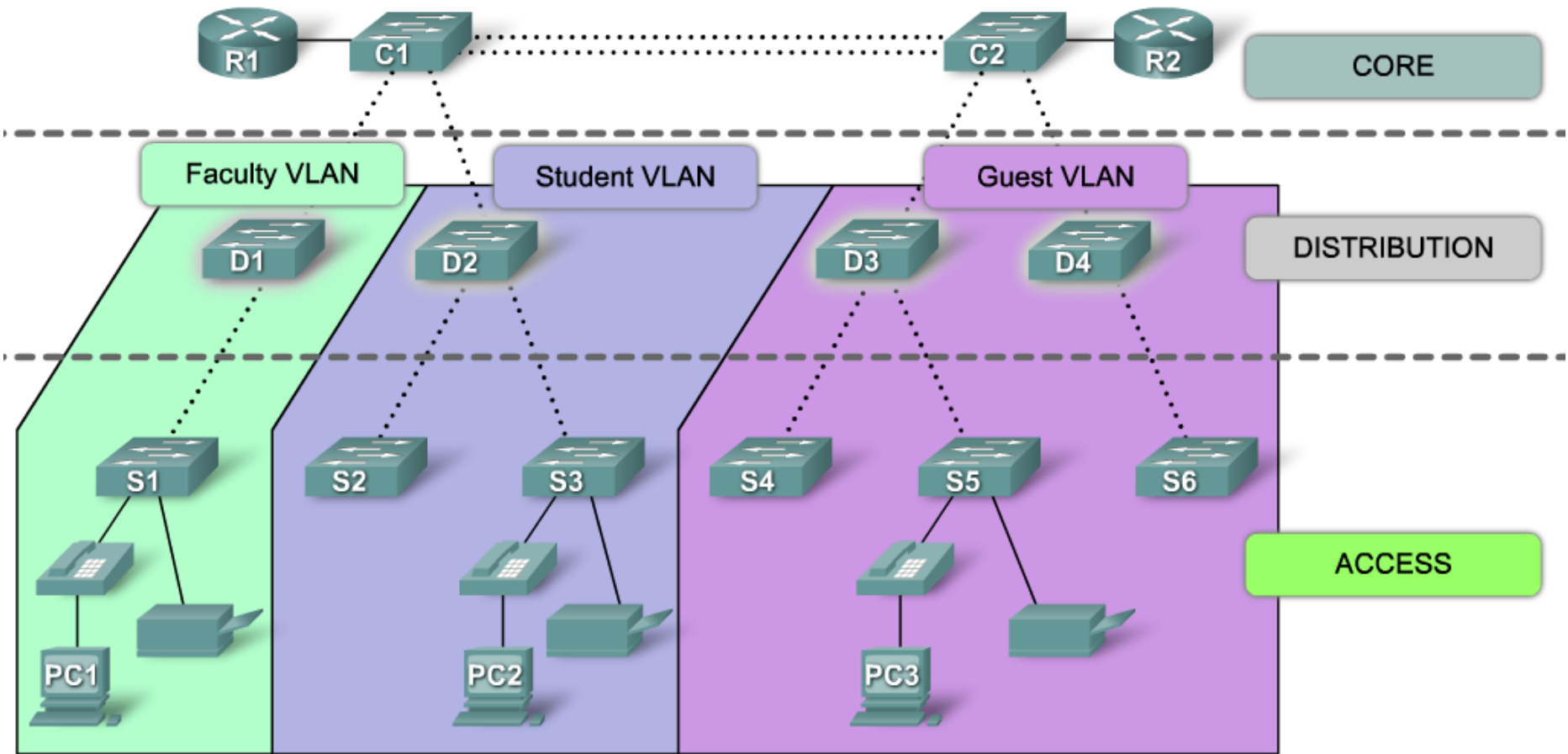


Rôle de l'Access Layer

- Attribution des VLANs
- Sécurité des ports

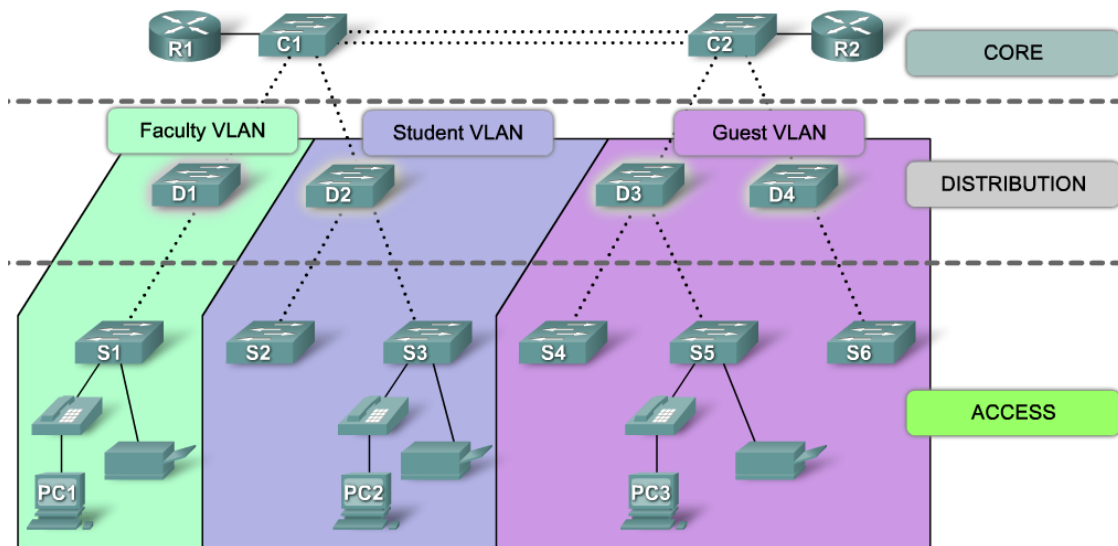


Distribution Layer



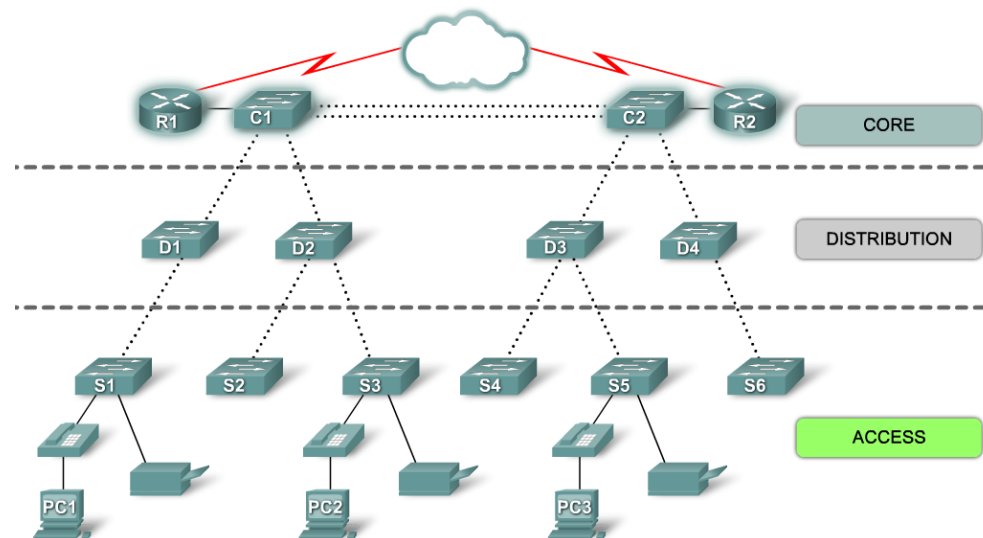
Rôle du Distribution Layer

- Limiter les zones de broadcast
- Transférer les paquets entre VLAN
- Filtrer l'accès entre certains VLAN



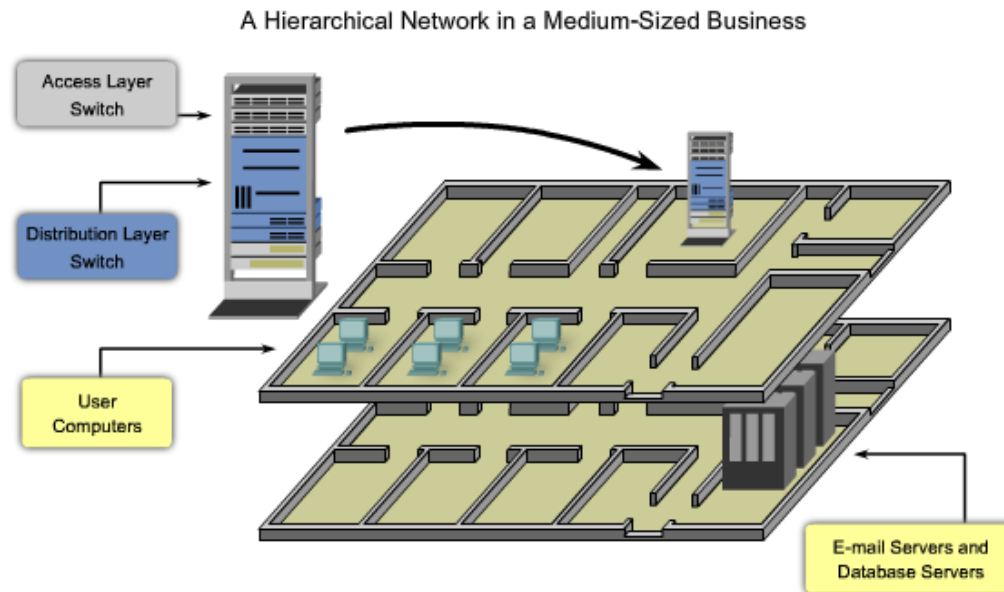
Rôle du Core Layer

- C'est le cœur du réseau
- Doit transférer les données le plus rapidement possible
- Apporte la connexion à Internet ou aux autres réseaux de la société via un MAN ou WAN



Représentation physique

- Généralement, une salle de brassage par étage
- Serveur dans une salle spécialisée
- Tous les étages reliés au core layer

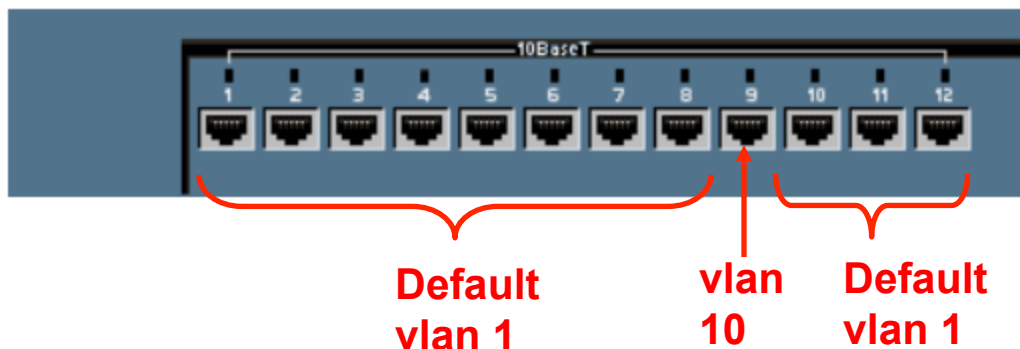


Avantages d'une architecture hiérarchique

- Scalabilité
 - Pouvoir faire des agrandissements du réseau simplement
- Redondance
 - Les services doivent être opérationnel 24/24
 - Exemple : pour la ToIP, on doit avoir une fiabilité de 99,999%, soit 5 min par an d'interruption de service
- Performance
 - Eviter les goulots d'étranglement
- Sécurité
 - Sécurisation des données et des accès au plus près de la source
- Administration simplifiée
- Maintenance facilité en raison de la modularité du réseau

VLANS (VIRTUAL LANS)

Introduction aux VLAN

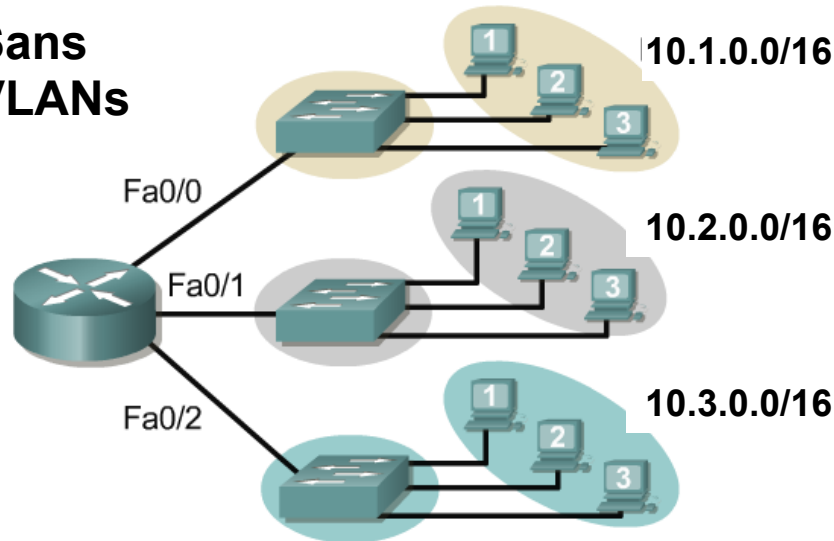


- **Les VLANs offrent la possibilité de segmenter les réseaux en domaines**
- VLAN = Sous-réseau
- Les VLANs aident à organiser les réseaux selon :
 - Localisation Physique (Exemple : Bâtiment)
 - Organisation (Exemple : Dept. Marketing)
 - Fonction (Exemple : Personnel)

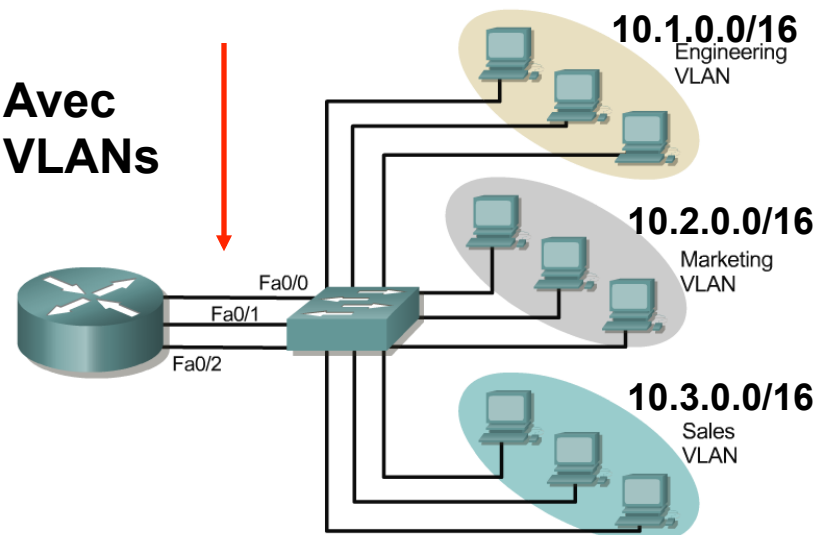
Introduction aux VLAN

Un lien par VLAN ou un lien Trunk

Sans VLANs

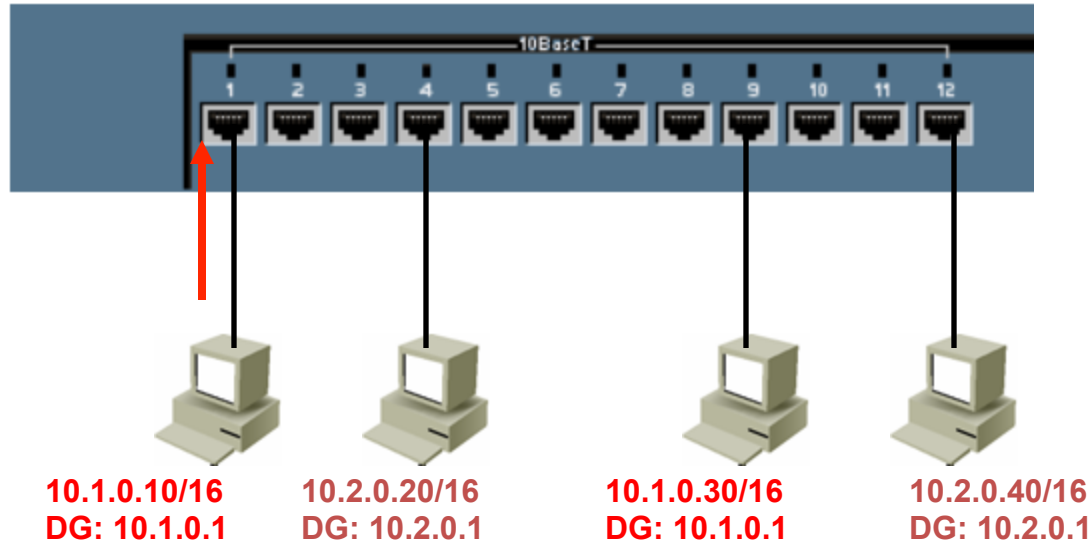


Avec VLANs



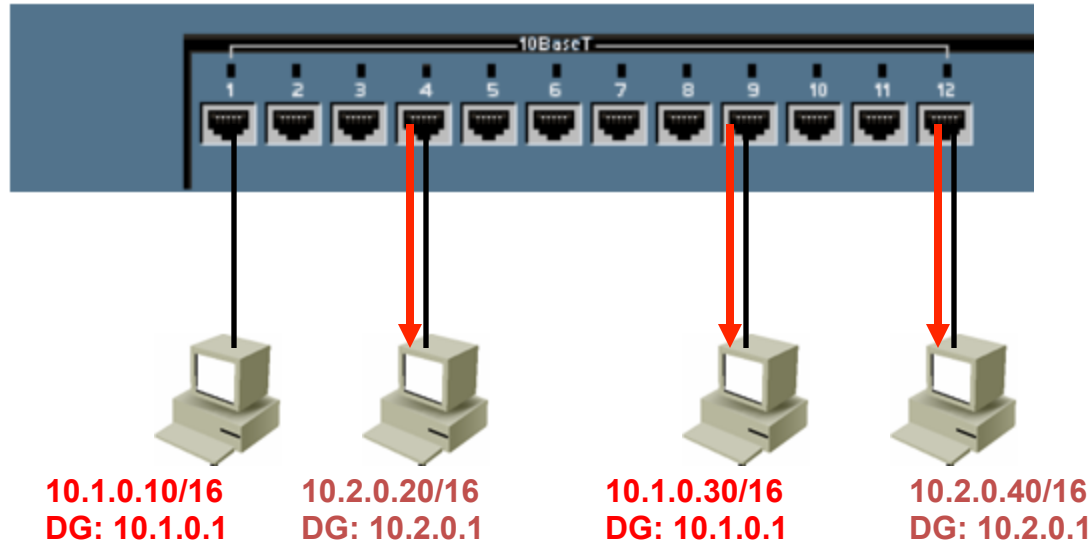
- Les VLANs créent des domaines qui autrefois demandaient l'usage d'un routeur
- Les VLANs aident la gestion du réseau (sécurité, scalabilité, administration)

Scénario sans VLANs



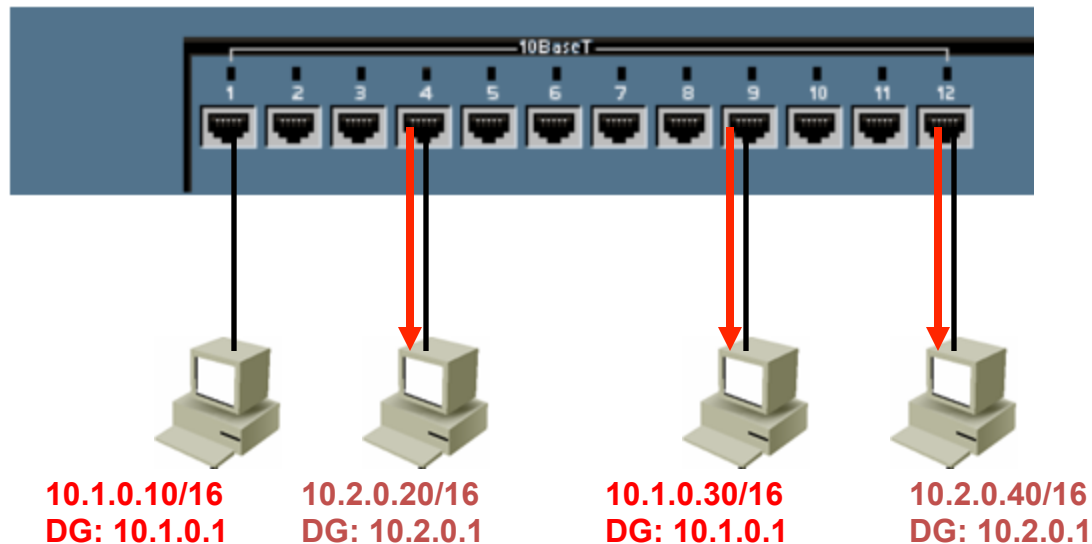
- Diffusions de couche 2 (Broadcasts)
 - Qu'est-ce que se passe lorsque 10.1.0.10 envoie une requête ARP pour 10.1.0.30 ?

Scénario sans VLANs



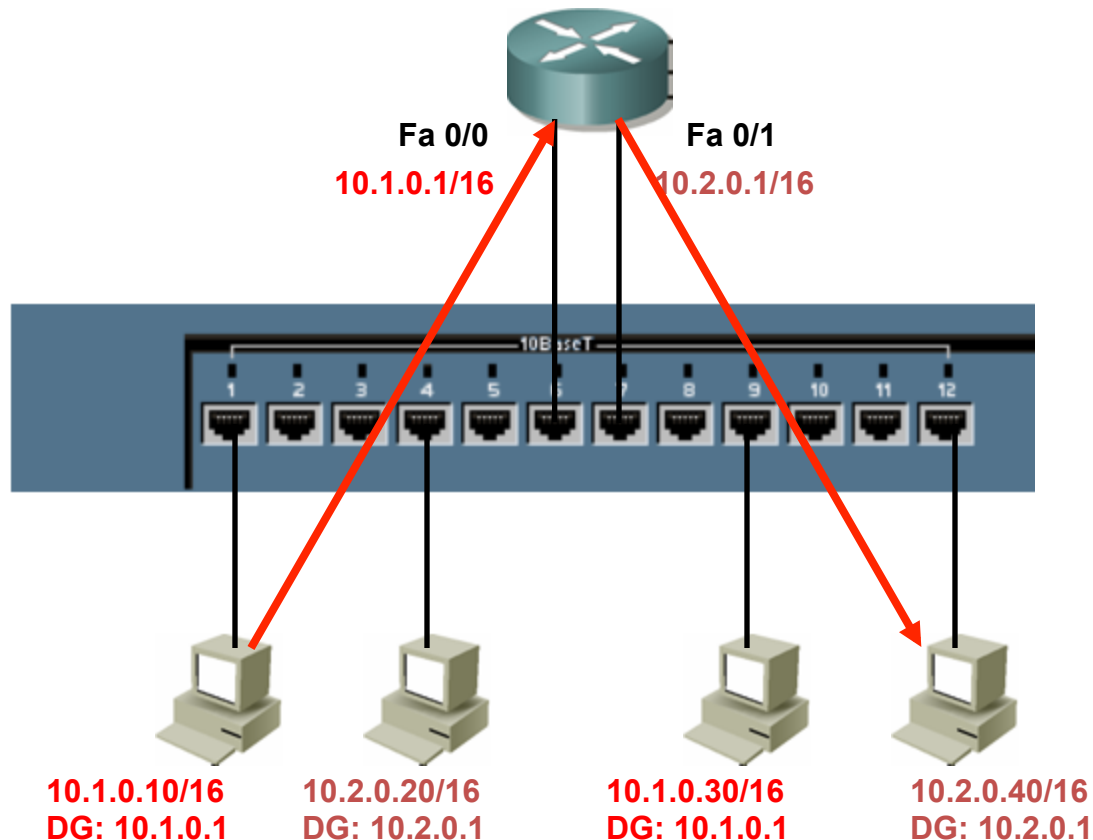
- Diffusion couche 2
 - Le switch "inonde" tous les ports
 - Toutes machines reçoivent le broadcast, même celles d'un réseau différent
 - Les diffusions de couche 2 devraient être limitées à ce sous-réseau

Scénario sans VLANs



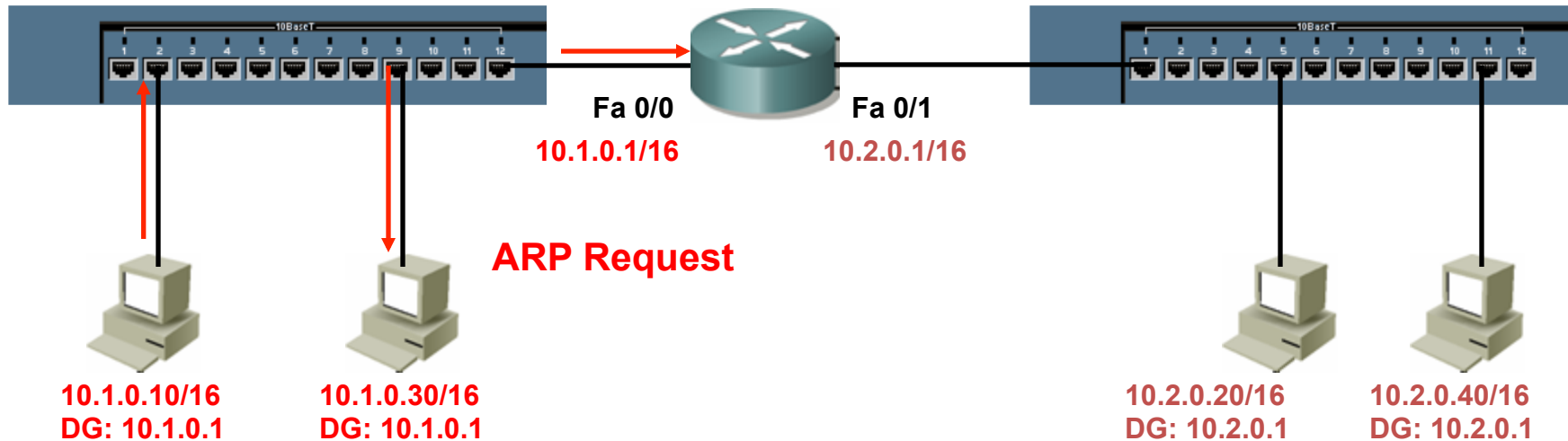
- Messages unicast pour des destinataires couche 2 inconnus
 - C'est la même situation qu'avec les diffusions
- Déjà, ce scénario n'est pas correct
 - Deux sous-réseaux doivent être reliés par un routeur, pas un switch !

Scénario sans VLANs



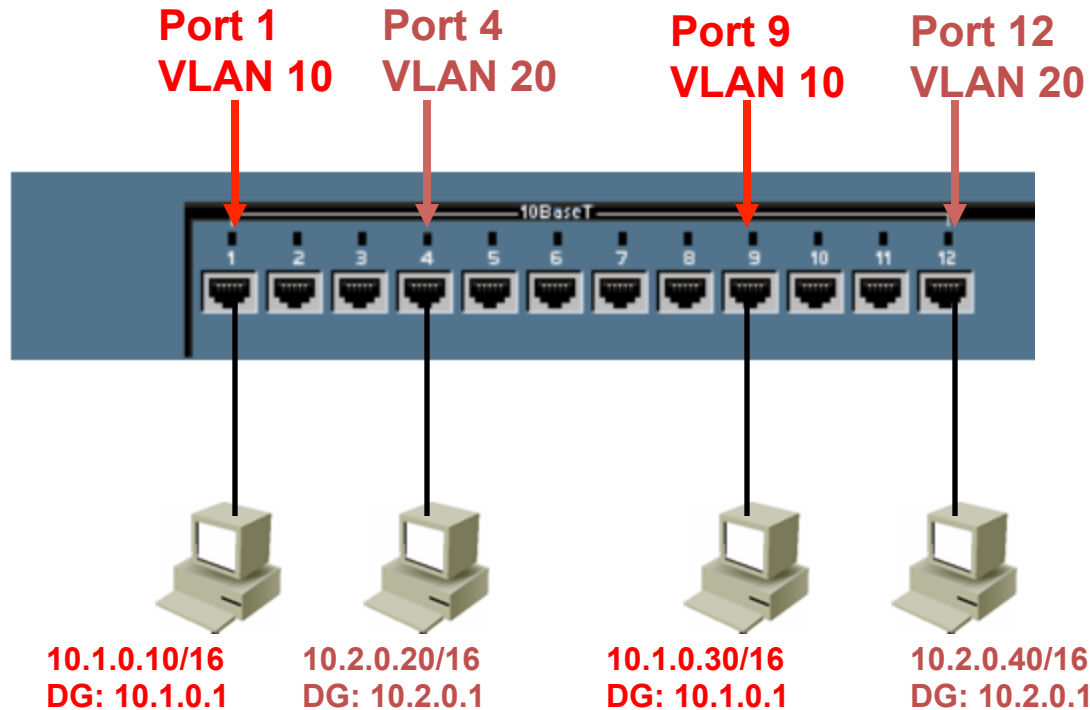
- Un routeur est le seul équipement vraiment "autorisé" à relier deux sous-réseaux
 - Il faut quand même séparer le trafic qui passe par ce switch

Solution traditionnelle



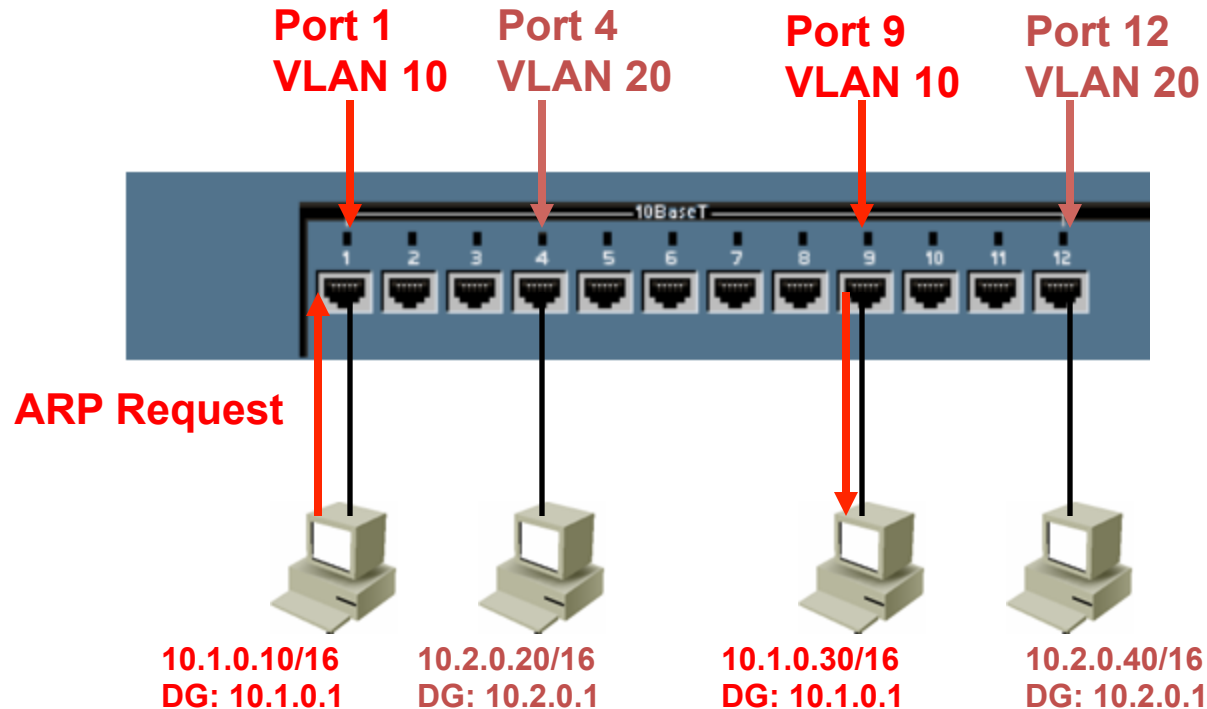
- La solution traditionnelle consistait à concentrer les équipements des réseaux sur des switches différents
- C'est une solution "sûre" (pour la diffusion couche 2) mais n'est pas bien scalable

Utilisation de VLANs



- Un **VLAN** est un **domaine de diffusion** crée par un ou plusieurs switches
- Les VLANs sont attribués par le switch et correspondent aux différents réseaux
- Chaque port d'un switch peut être assigné à un VLAN différent

Utilisation des VLAN

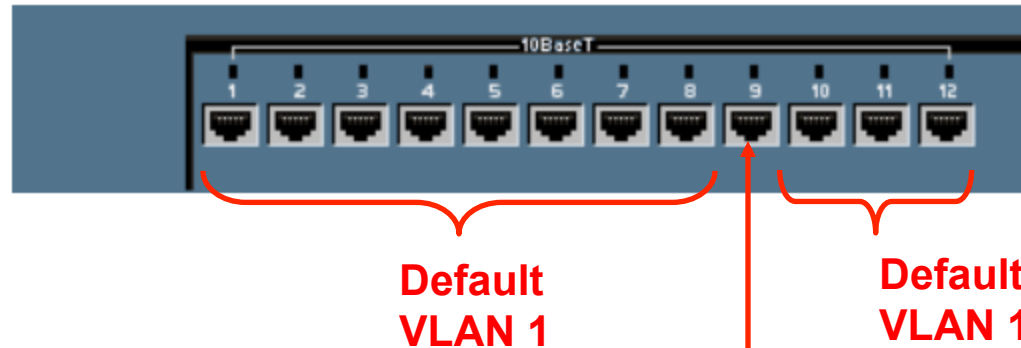


- Les ports appartenant au même VLAN partagent le même domaine de diffusion
- Les ports dans des VLANs différents sont séparés

Attribution des VLANs

- Deux méthodes peuvent être utilisés
 - Attribution statique
 - Chaque port est attribué à un VLAN
 - N'importe quel équipement connecté à ce port "rentre" dans le domaine de diffusion de ce VLAN
 - Attribution dynamique
 - Le switch consulte un tableau avec les adresses MAC des équipements et identifie le VLAN auquel un équipement doit appartenir
 - Procédure très rare (car bien plus complexe)

Configuration de VLANs Statiques

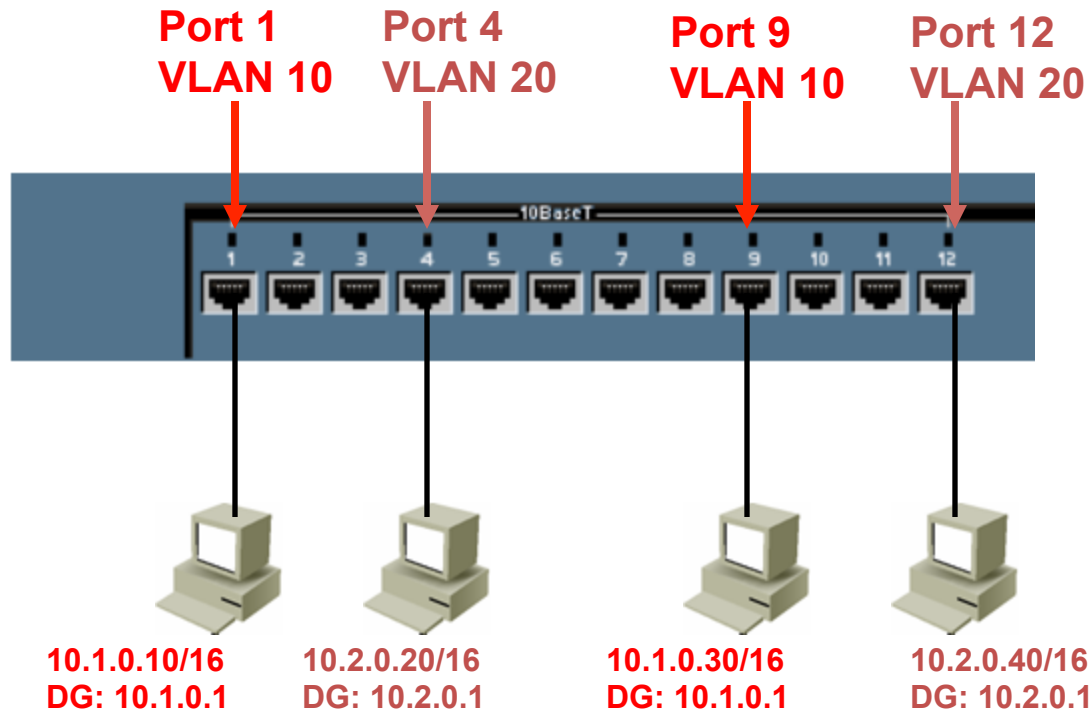


```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
```

**VLAN 10
Configuré**

- Les VLANs statiques se basent sur le port
- Lorsqu'un équipement se connecte, il est automatiquement annexé à ce VLAN
- Un switch "neuf" a tous les ports préconfigurés pour le **VLAN default**
- Dans les switches CISCO, c'est le VLAN 1

Opération des VLANs

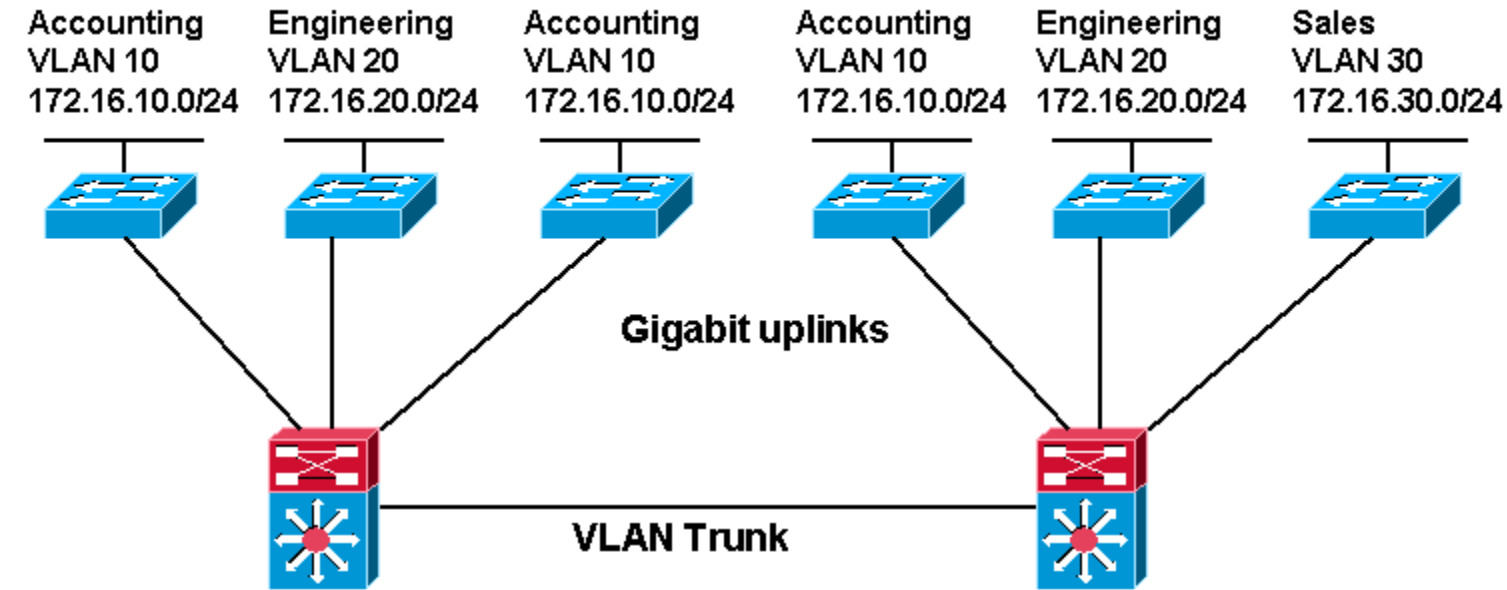


- Si les VLANs sont attribués suivant les ports, il faut encore configurer les adresses IP
- Une machine doit être configurée avec la plage d'adresses IP correspondant à son VLAN
 - VLAN = Sous-réseau

Organisation des VLANs

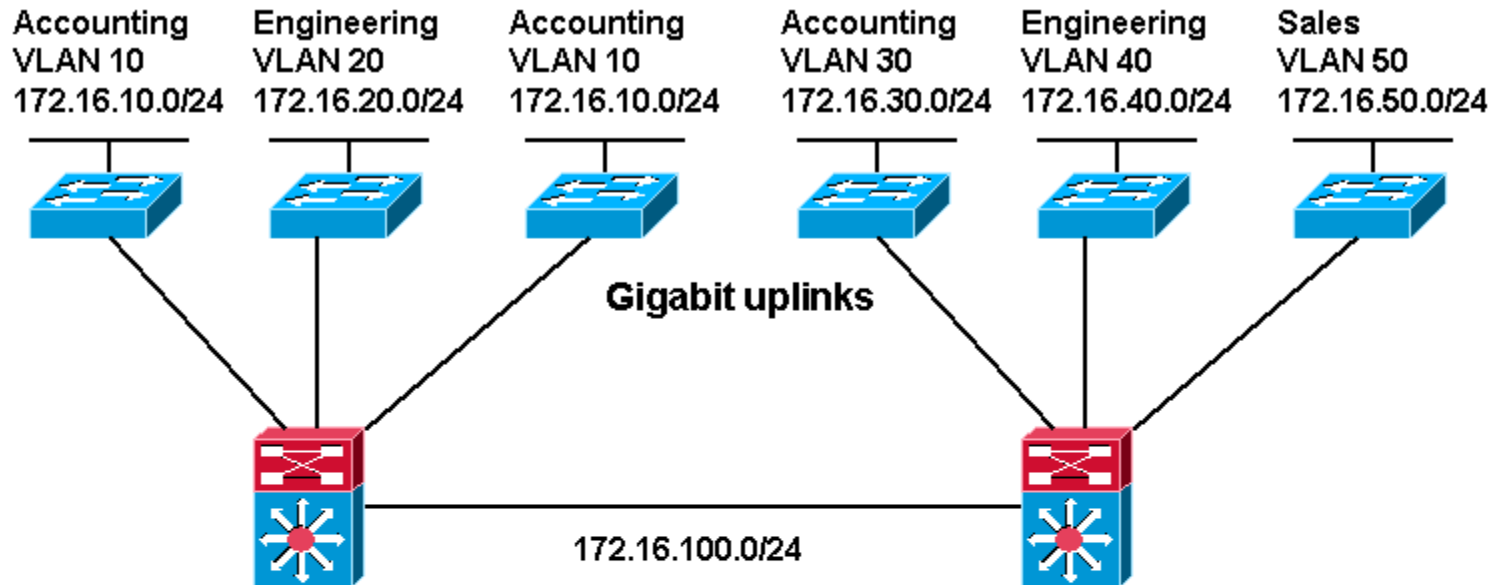
- Les VLANs sont normalement organisés selon deux modèles
 - "End-to-End" ou "Campus-wide"
 - L'organisation la plus "ancienne"
 - Géographique ou Local
 - L'organisation recommandée aujourd'hui

VLANs End-to-End ou Campus-wide



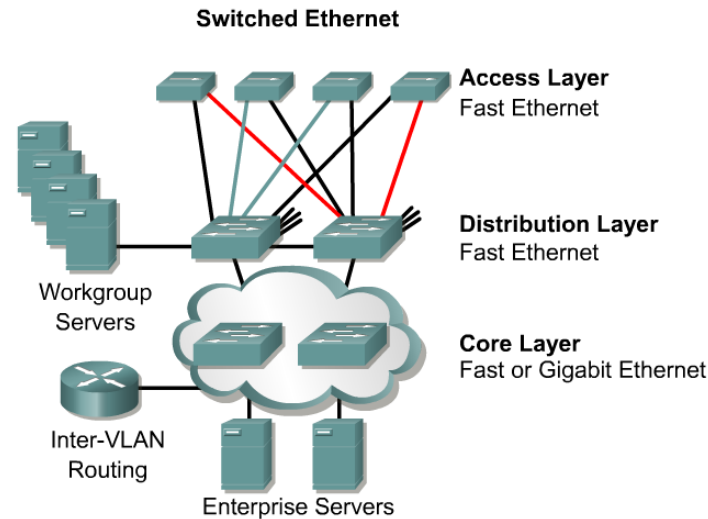
- Les VLANs sont basés sur la fonctionnalité
- Modèle "VLAN un peu partout"
- Problème de scalabilité

VLAN Géographique ou Local



- Modèle basé sur la localisation physique
- Des VLANs dédiés à chaque switch "d'accès"

Règles du 80/20 et 20/80



- Originellement, les réseaux étaient prévus pour gérer **80 percent du trafic à l'intérieur du VLAN**
 - Imprimantes, serveurs, collègues
- C'est la **règle 80/20**
- Problème :
 - Aujourd'hui, le trafic est plutôt inversé : 20% se fait en local, et 80% vient de l'extérieur (Internet)
 - Ceci rend les réseaux "campus" trop difficiles à gérer

Exercice 1

- Examiner le fonctionnement d'un réseau avec des VLANs

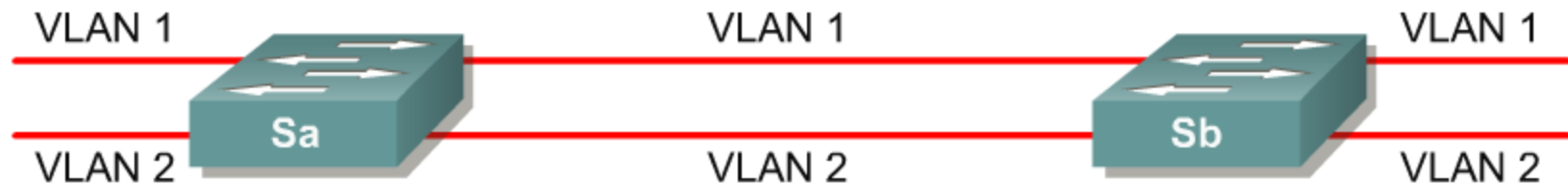
Exercice 2

- Configurer un réseau avec des VLANs

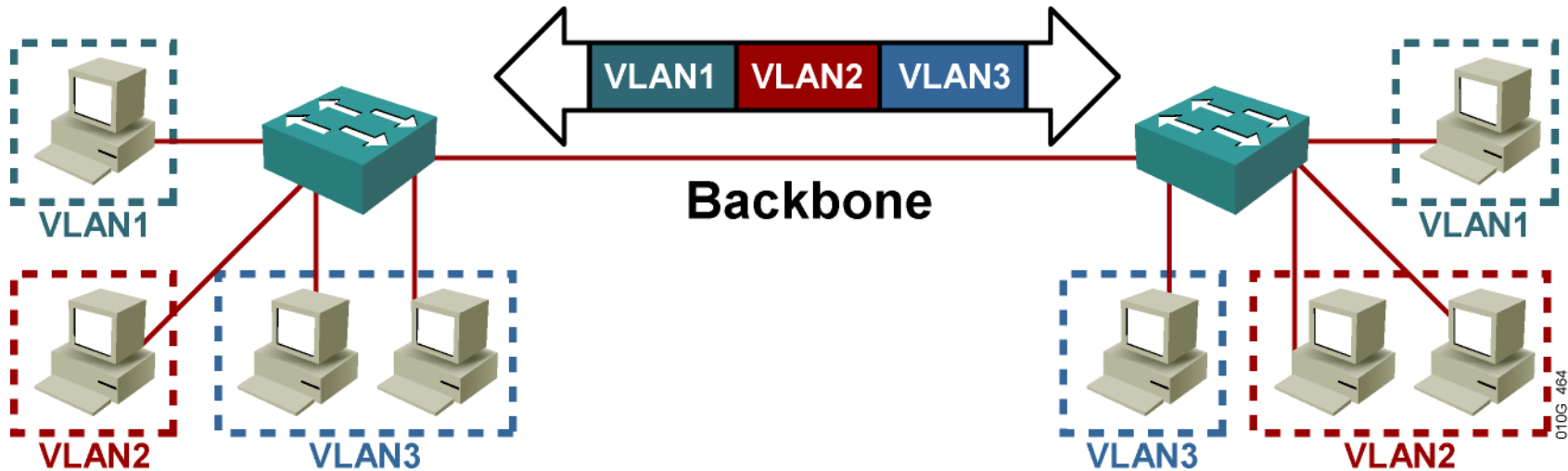
VLAN TRUNKING

Transporter plusieurs VLAN ?

- L'un des problèmes de la configuration "Campus" est qu'il faut transporter plusieurs VLAN à travers deux ou plus switches
 - Comment le faire sans utiliser un câble par VLAN ?

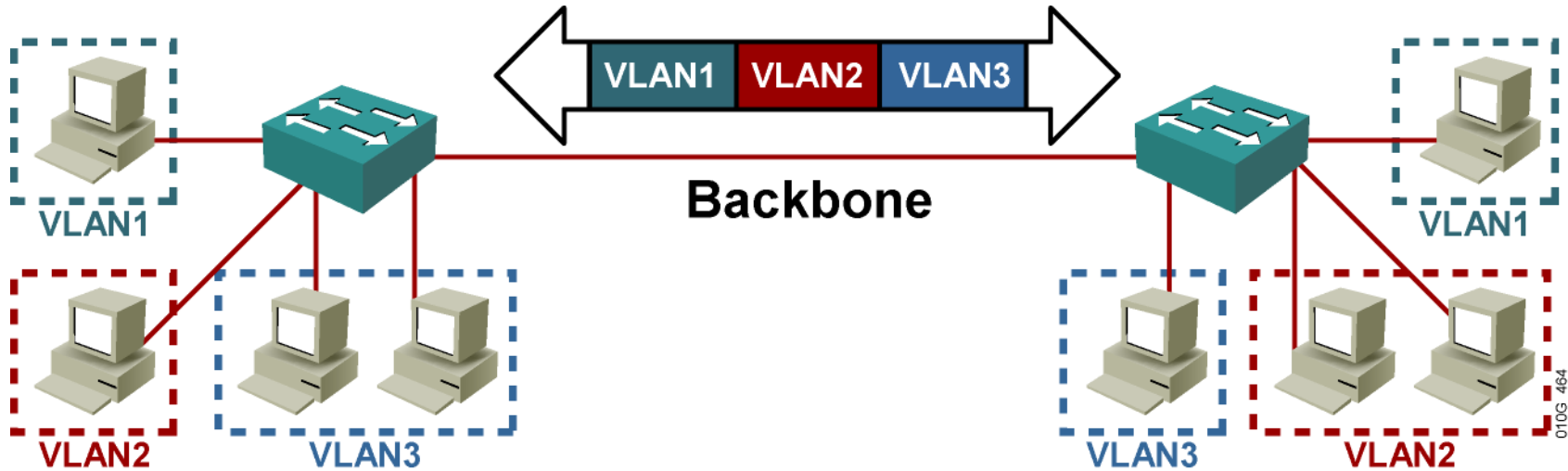


La solution : VLAN Tagging



- Le **VLAN Tagging** est utilisé pour permettre le passage de plusieurs VLAN à travers un seul lien
- **Lien "Trunk"** : lorsque les paquets sont reçus par le switch, il les attribue un identifiant unique qui correspond à son VLAN
- Les paquets de plusieurs VLAN sont ainsi transmis sur le même lien

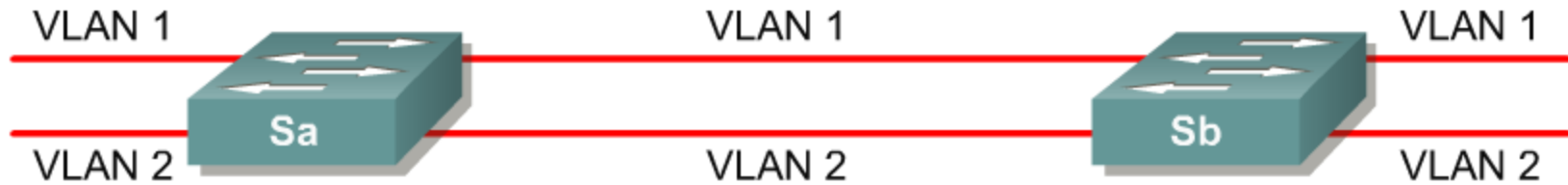
VLAN Tagging



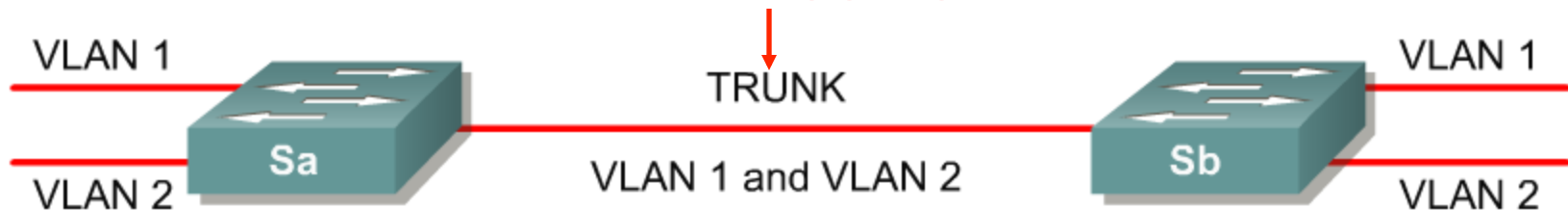
- Le paquet est forwardé selon son tag et son adresse MAC
- En arrivant au switch de destination, le tag est retiré et le paquet est envoyé au destinataire

VLAN Tagging

Sans VLAN Tagging



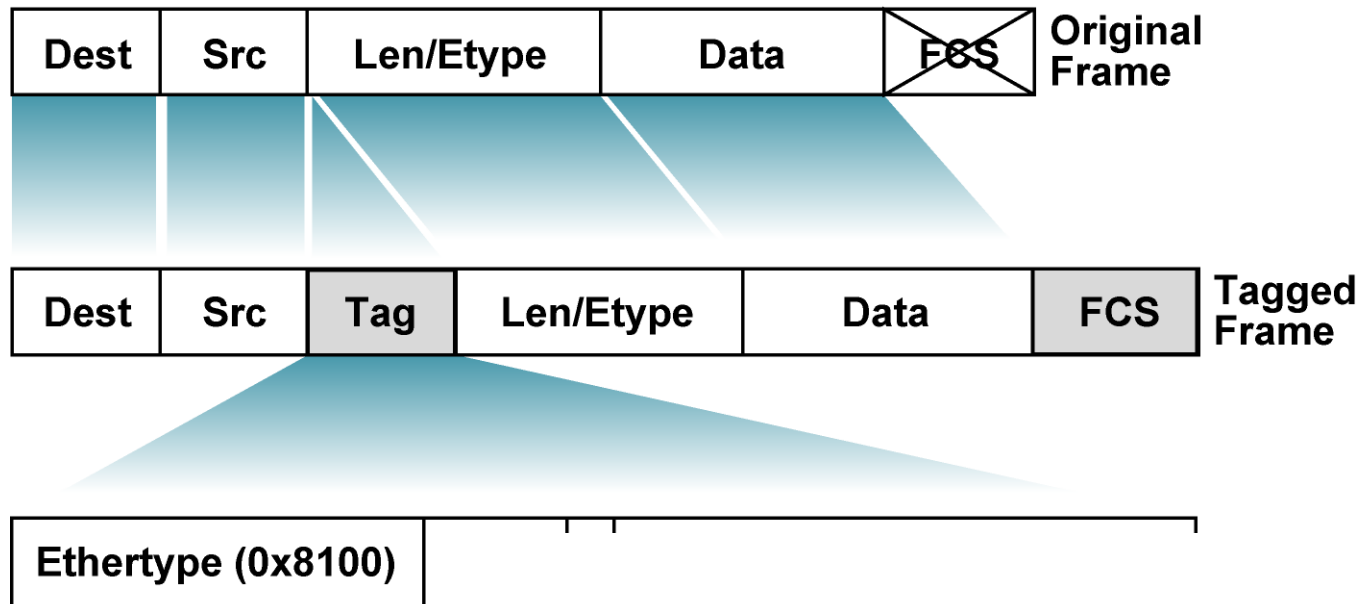
VLAN Tagging



- Le VLAN Tagging permet une meilleure utilisation des liens

802.1Q

- Le VLAN Tagging est fait grâce à une modification de l'entête Ethernet
- La norme IEEE 802.1Q inclut le tag juste après les champs MAC destination et MAC source



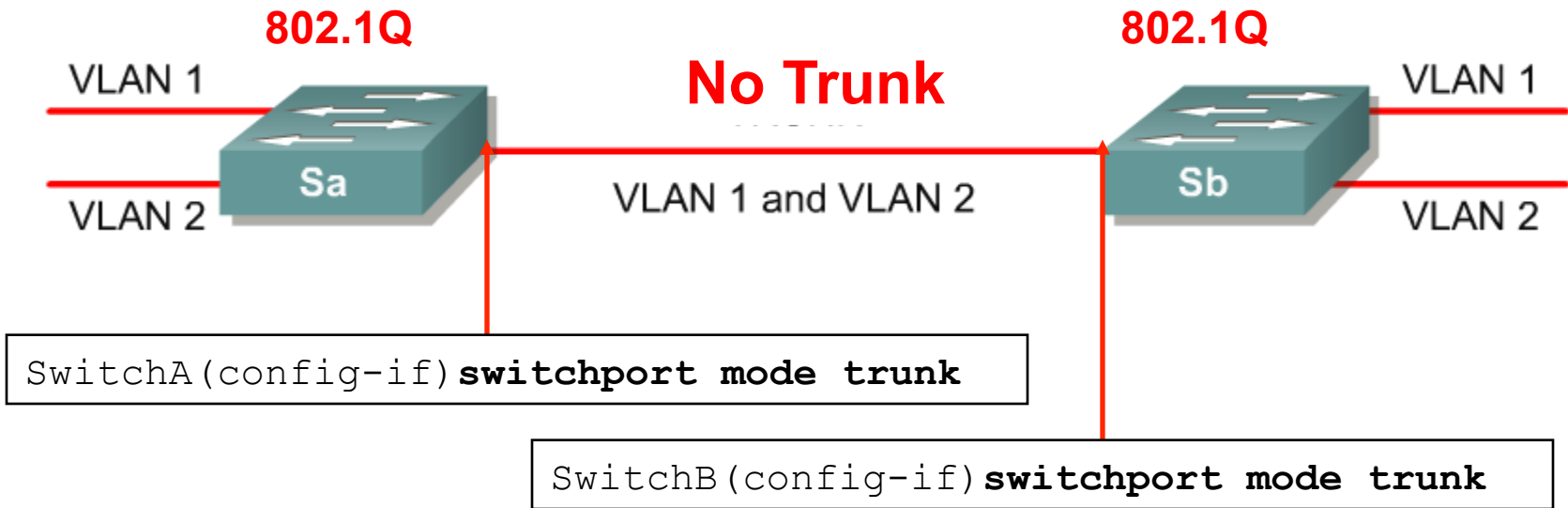
Configuration du mode Trunking

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed          Set allowed VLAN characteristics when
                  interface is in trunking mode
encapsulation    Set trunking encapsulation when interface
                  is in trunking mode
native           Set trunking native characteristics when
                  interface is in trunking mode
pruning          Set pruning VLAN characteristics when
                  interface is in trunking mode

Switch(config-if)#switchport trunk encap ?
dot1q            Interface uses only 801.1q trunking encapsulation
                  when trunking
```

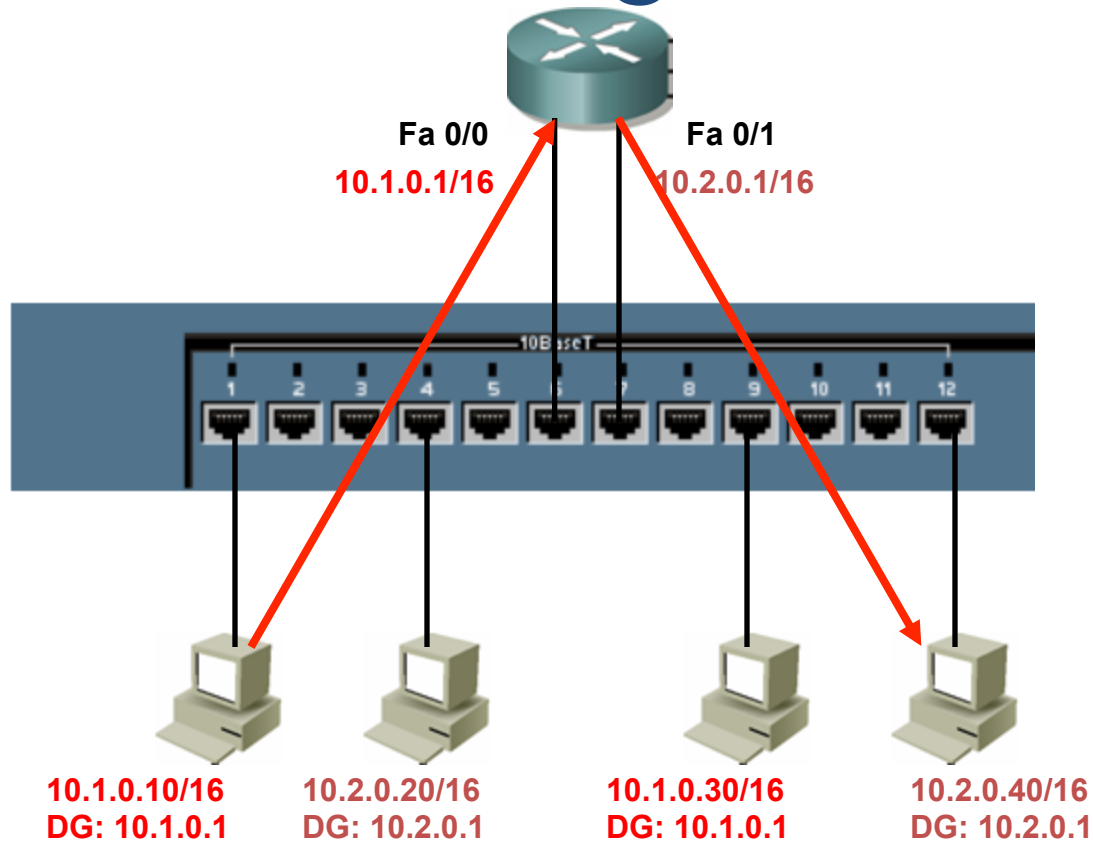
- En ligne de commande, il faut entrer ces deux commandes, dans la configuration de l'interface
 - Switchport mode trunk
 - Switchport trunk encapsulation dot1q

Configuration du mode Trunking



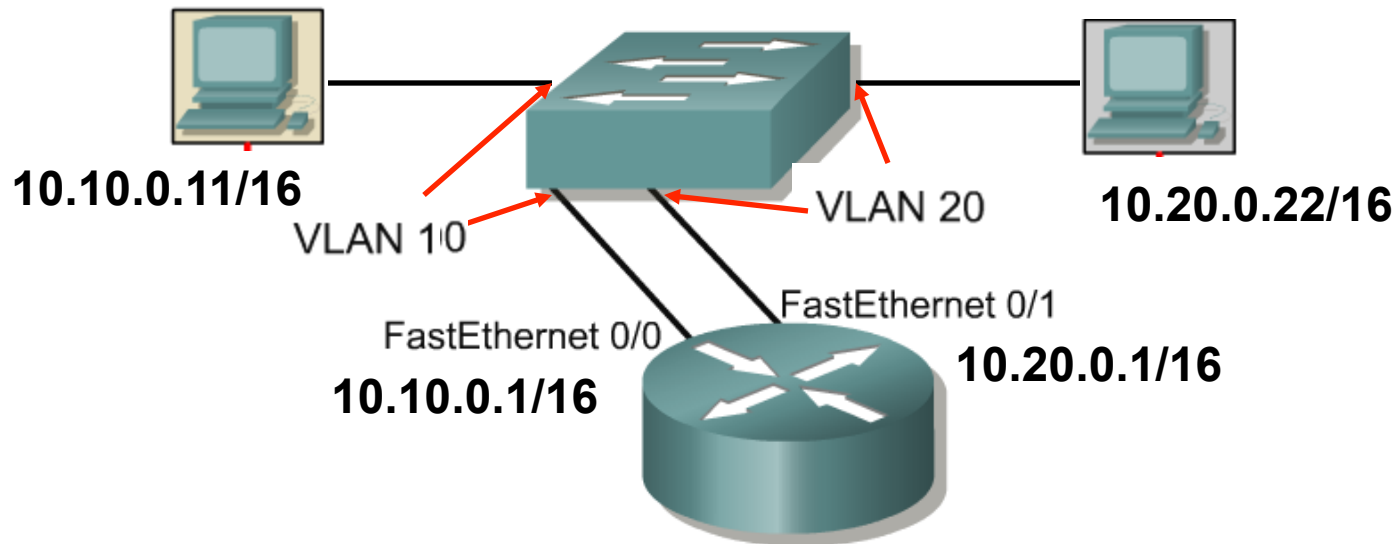
ROUTAGE INTER-VLAN

Le routage Inter-VLAN



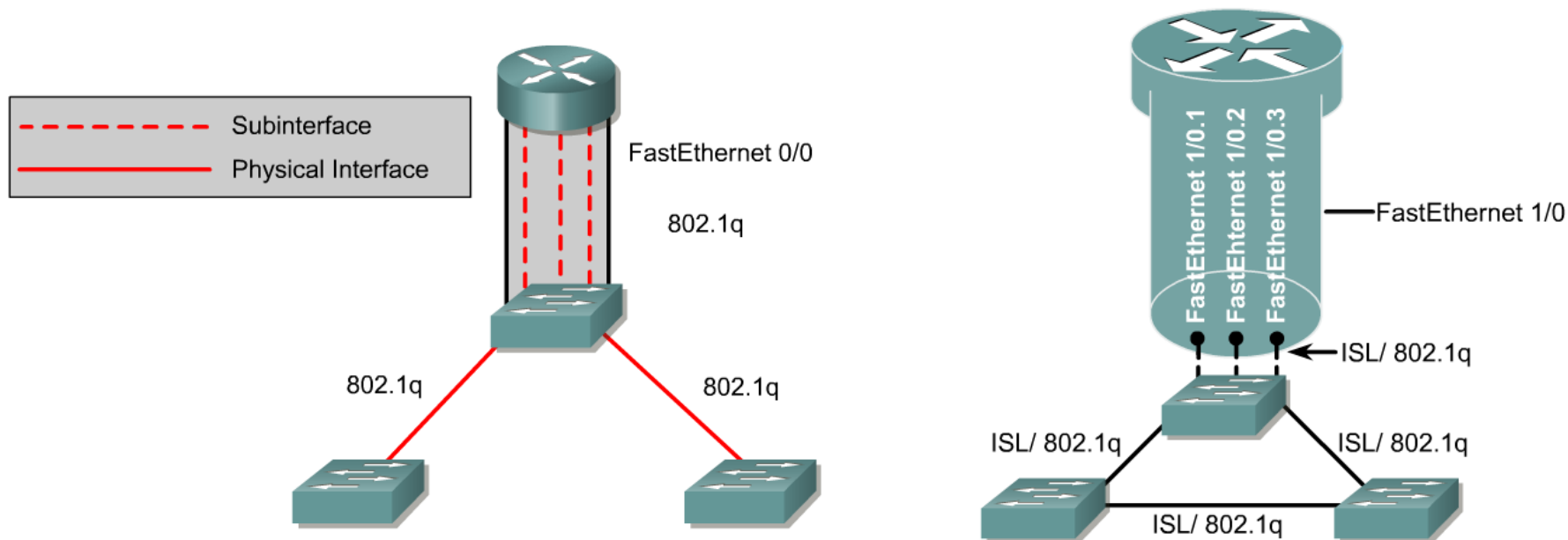
- Lorsqu'une machine doit communiquer avec une machine d'un autre réseau, il faut passer par un routeur
- Sans un équipement de routage, la connexion est impossible

Routage Inter-VLAN – Sans liens trunk



- Une option est d'utiliser un lien pour chaque VLAN, mais cette solution ne passe pas bien à l'échelle

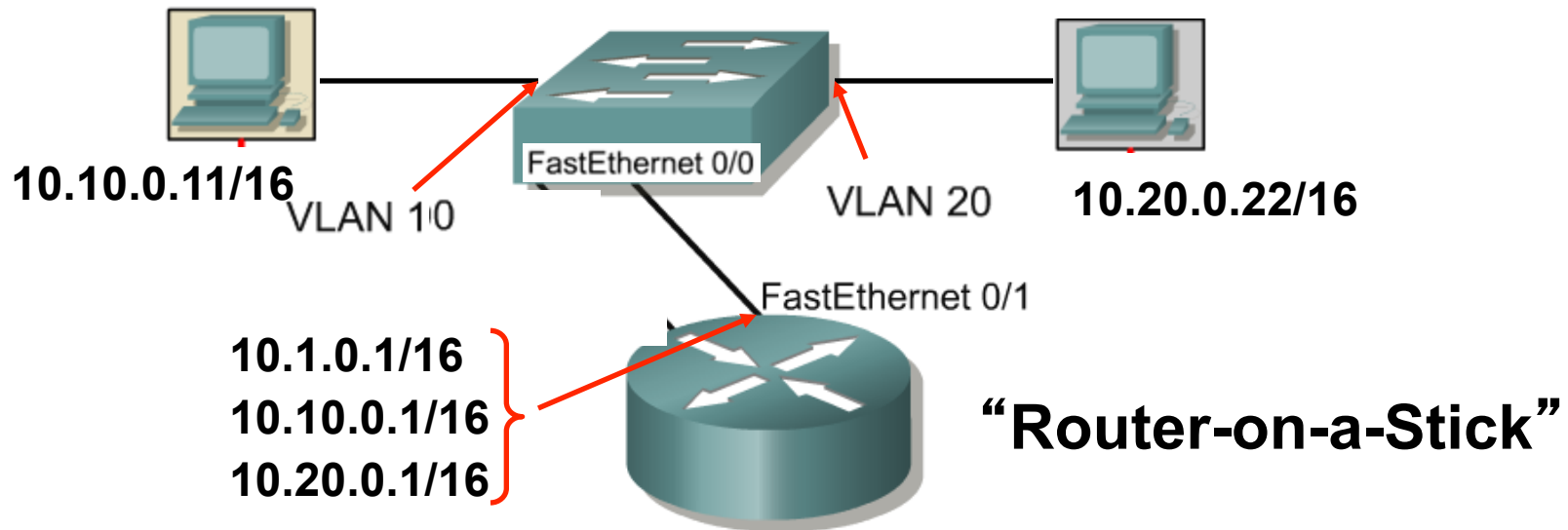
Interfaces physiques et logiques



- Dans les équipements réseau, il est possible de sous-diviser des interfaces physiques en plusieurs interfaces logiques

```
Rtr (config) #interface fastethernet  
port/interface.subinterface
```

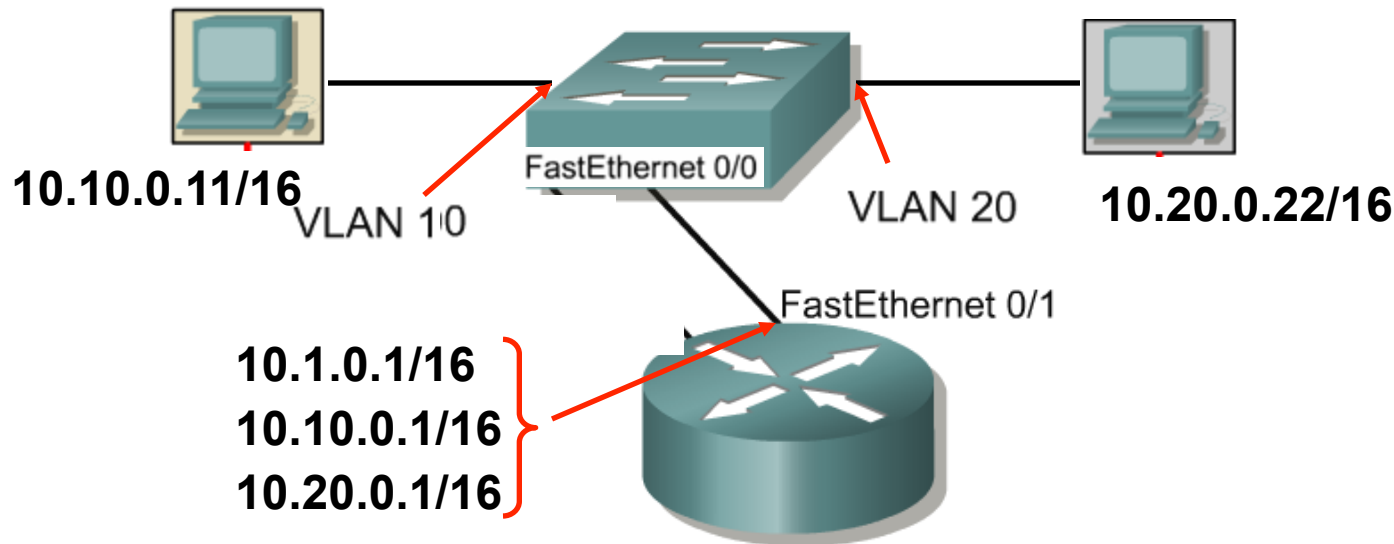

Routing Inter-VLAN – Avec trunk



```
Rtr(config)#interface fastethernet 0/1.1
Rtr(config-subif)#description VLAN 1
Rtr(config-subif)#encapsulation dot1q 1
Rtr(config-subif)#ip address 10.1.0.1 255.255.0.0
```

- Grâce aux sous-interfaces, un seul lien peut être utilisé pour relier plusieurs sous-réseaux

Routage Inter-VLAN – Avec trunk

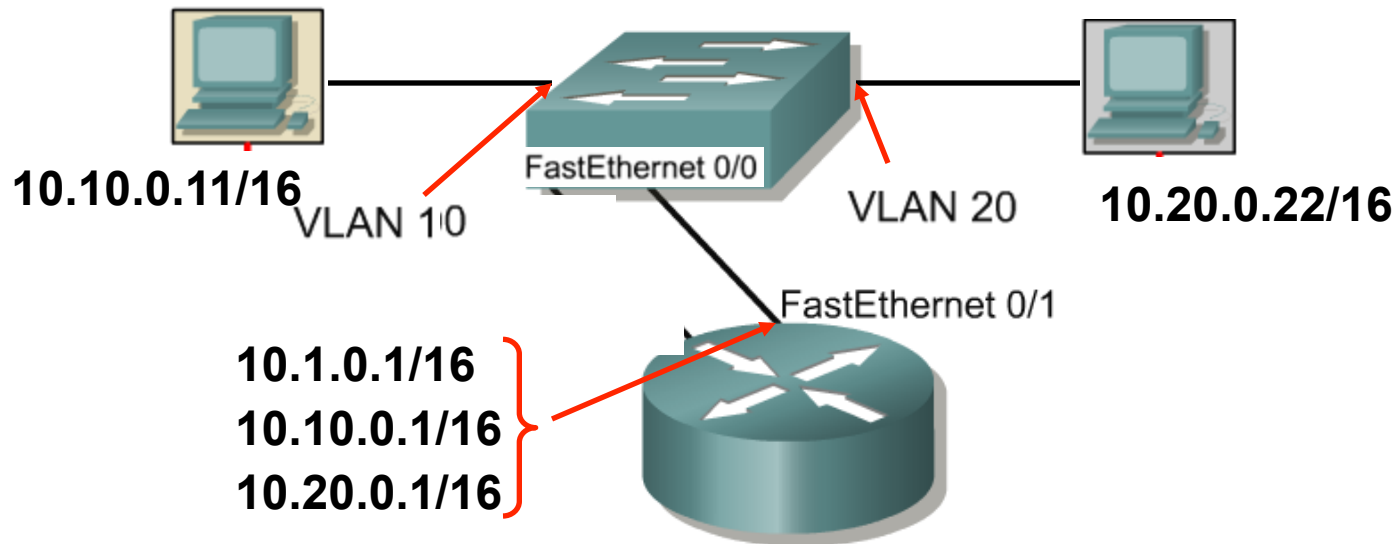


```

Rtr(config)#interface fastethernet 0/1.10
Rtr(config-subif)#description Management VLAN 10
Rtr(config-subif)#encapsulation dot1q 10
Rtr(config-subif)#ip address 10.10.0.1 255.255.0.0

Rtr(config)#interface fastethernet 0/1.20
Rtr(config-subif)#description Management VLAN 20
Rtr(config-subif)#encapsulation dot1q 20
Rtr(config-subif)#ip address 10.20.0.1 255.255.0.0
    
```

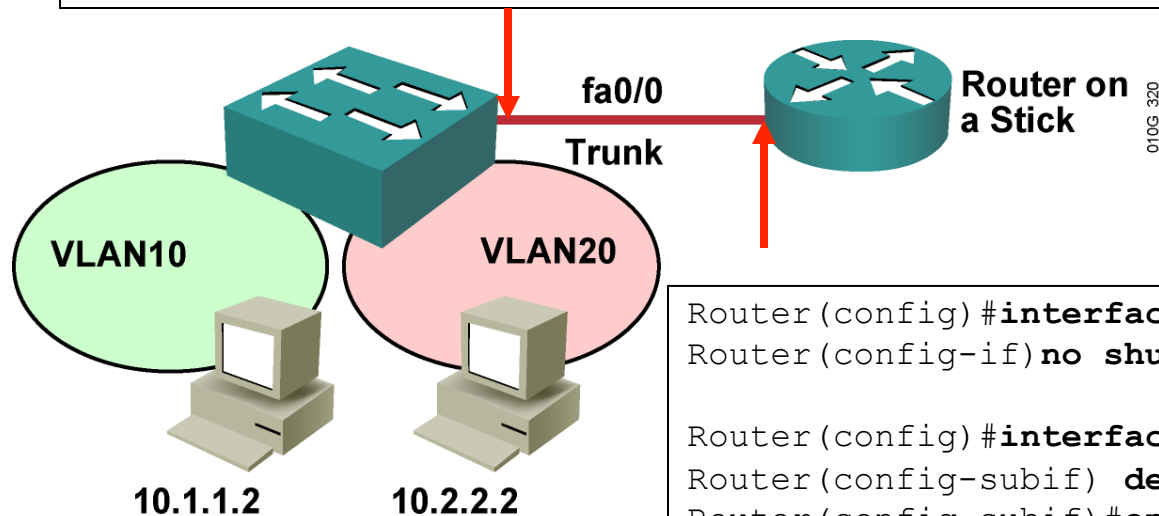
Routage Inter-VLAN – Avec trunk



```
switch(config)#interface FastEthernet 0/0
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```

Routage Inter-VLAN – Avec trunk

```
switch(config)#interface FastEthernet 0/0
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```



```
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown

Router(config)#interface FastEthernet 0/0.1
Router(config-subif) description VLAN 1
Router(config-subif)#encapsulation dot1Q 1 native
Router(config-subif)#ip address 10.10.1.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.10
Router(config-subif) description VLAN 10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.10.10.1 255.255.255.0

Router(config)#interface FastEthernet 0/0.20
Router(config-subif)# description VLAN 20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.10.20.1 255.255.255.0
```

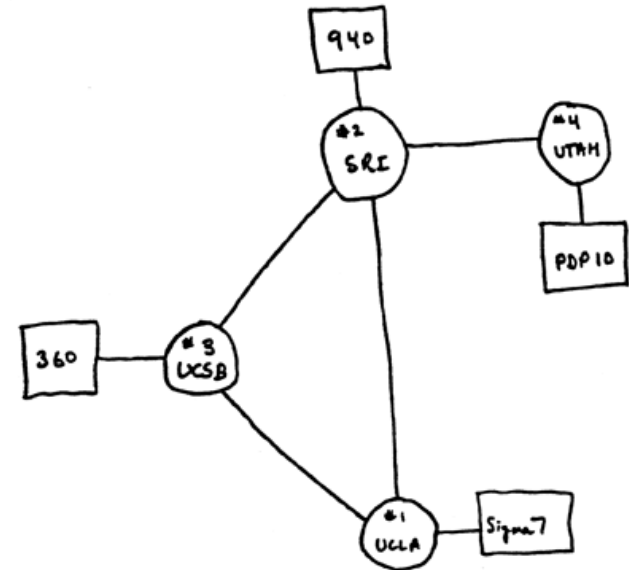
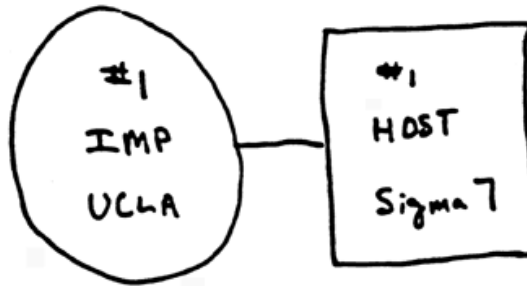
Exercice 3

- Faire du routage inter-VLAN

INTRODUCTION AU ROUTAGE

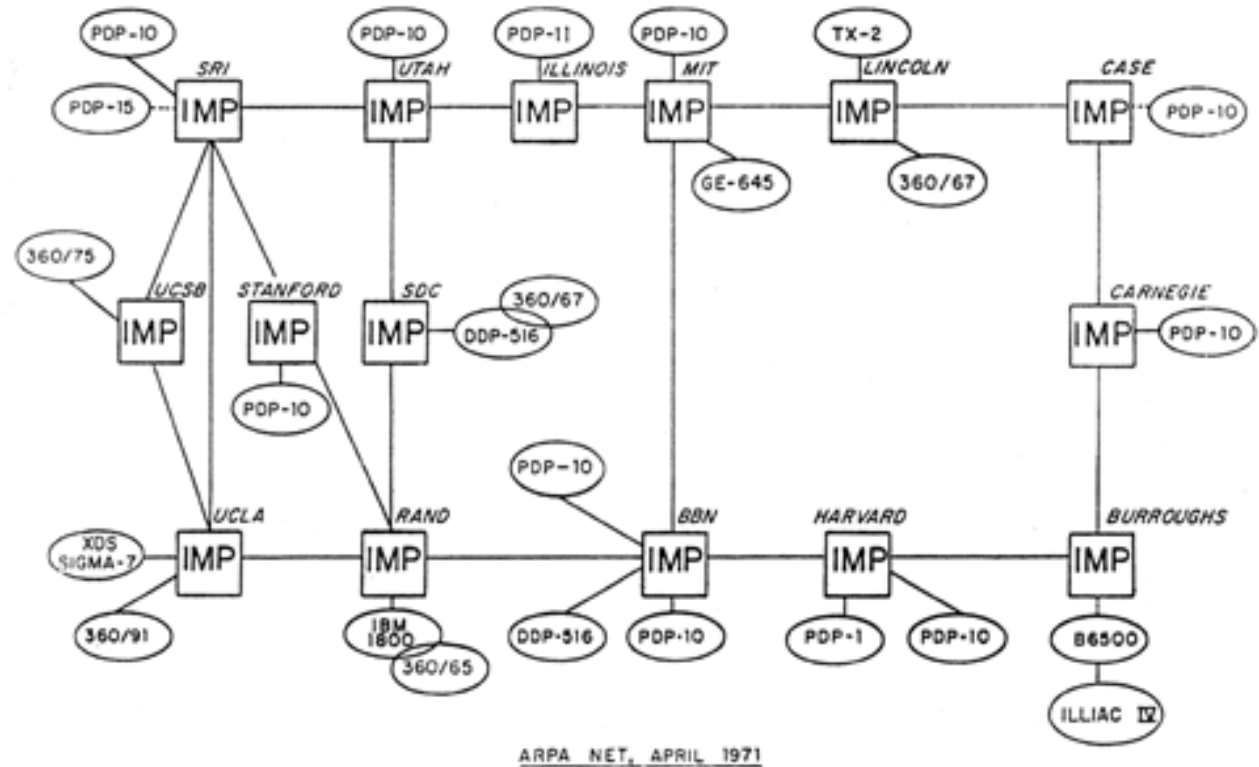
Histoire de l'Internet

• 1969



Histoire de l'Internet

- 1971

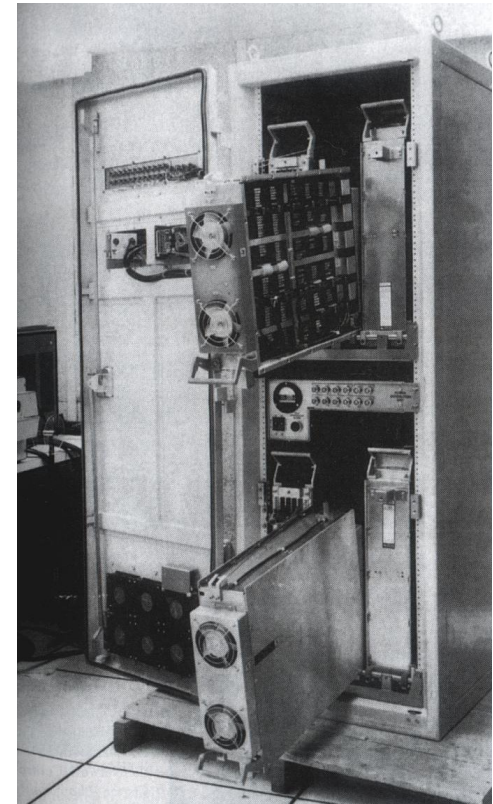


Les Routeurs sont des Ordinateurs



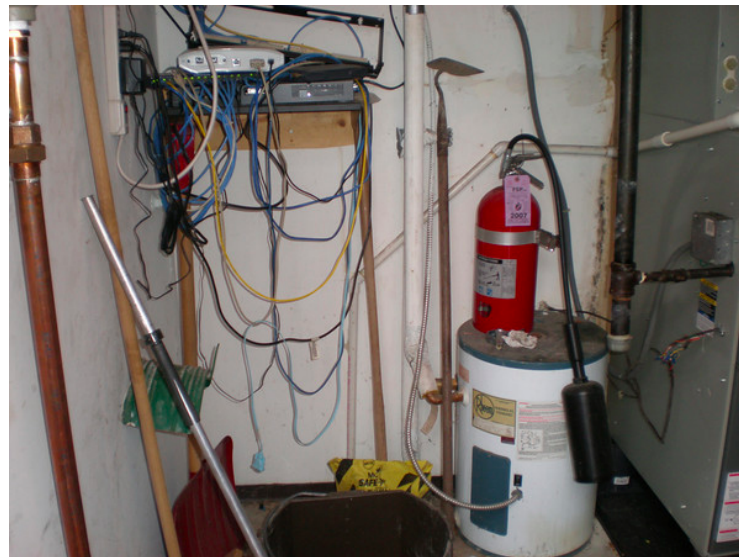
Leonard Kleinrock et le premier IMP

- **Un routeur est un ordinateur**
- Le premier routeur (ARPANET) :
 - IMP (Interface Message Processor)
 - Honeywell 516 minicomputer
 - 30 août 1969

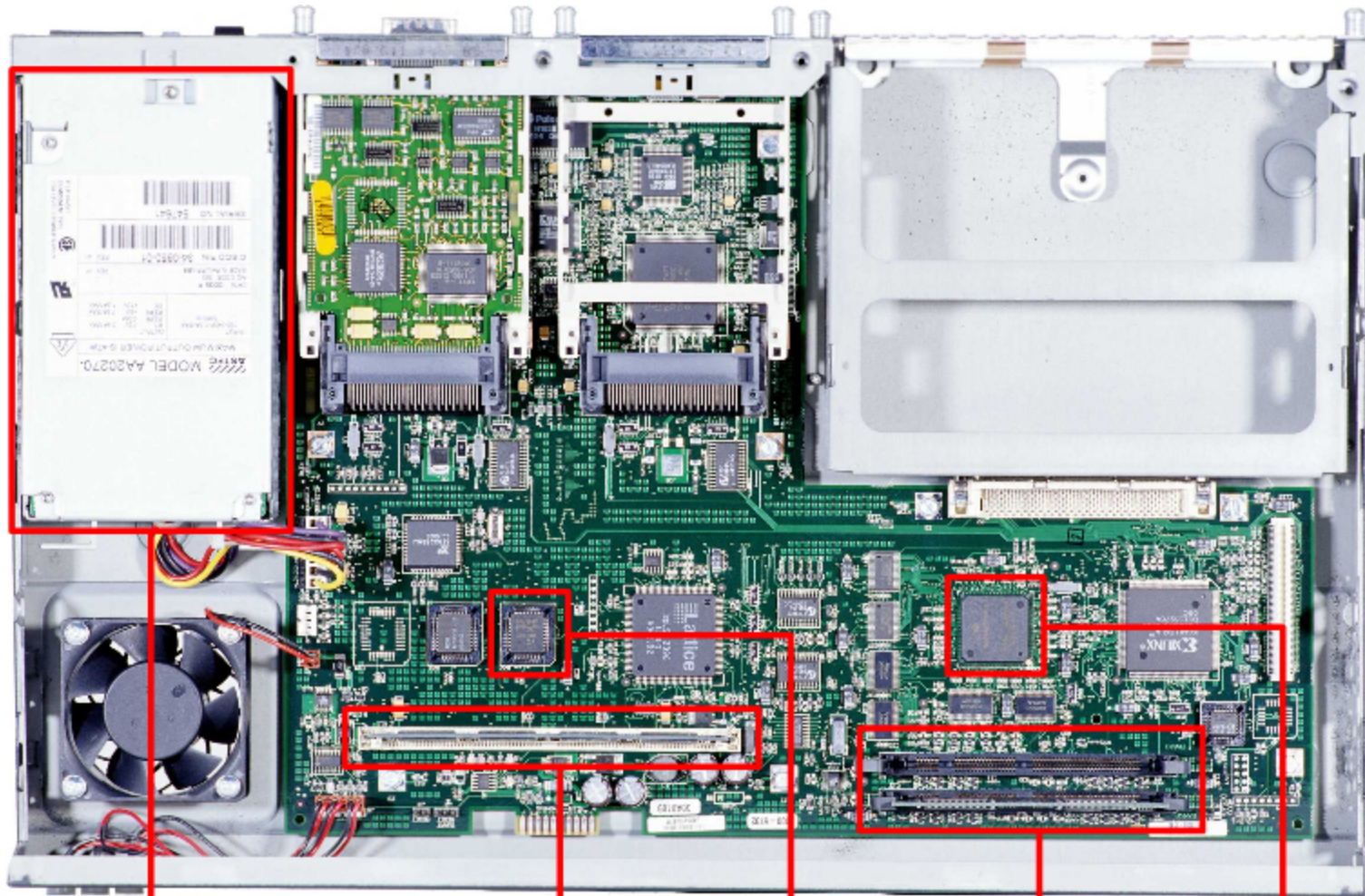


Gateways - Passerelles

- Pendant des années les fonctions d'un routeur ont été assurées par des ordinateurs "classiques"
 - Le plus souvent, des machines "sans clavier ni écran" cachées dans une armoire
- Ce n'est qu'à la fin des années 80 que des machines dédiées ont été développées
 - Ces machines restent très proches d'un PC, c'est surtout le système d'exploitation qui est adapté au processus de routage
 - Juniper (version Unix très spécialisée)
 - IOS (système propriétaire CISCO)
 - Zebra/Quagga (paquet Linux)



Caractéristiques physiques



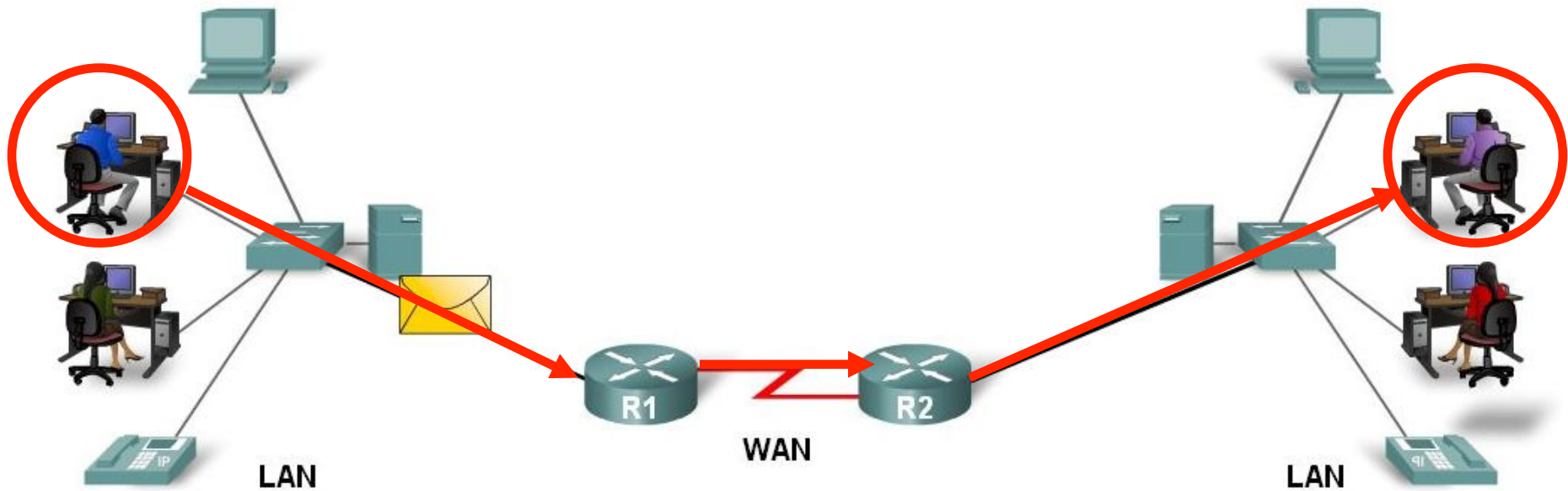
Power Supply

Flash SIMM

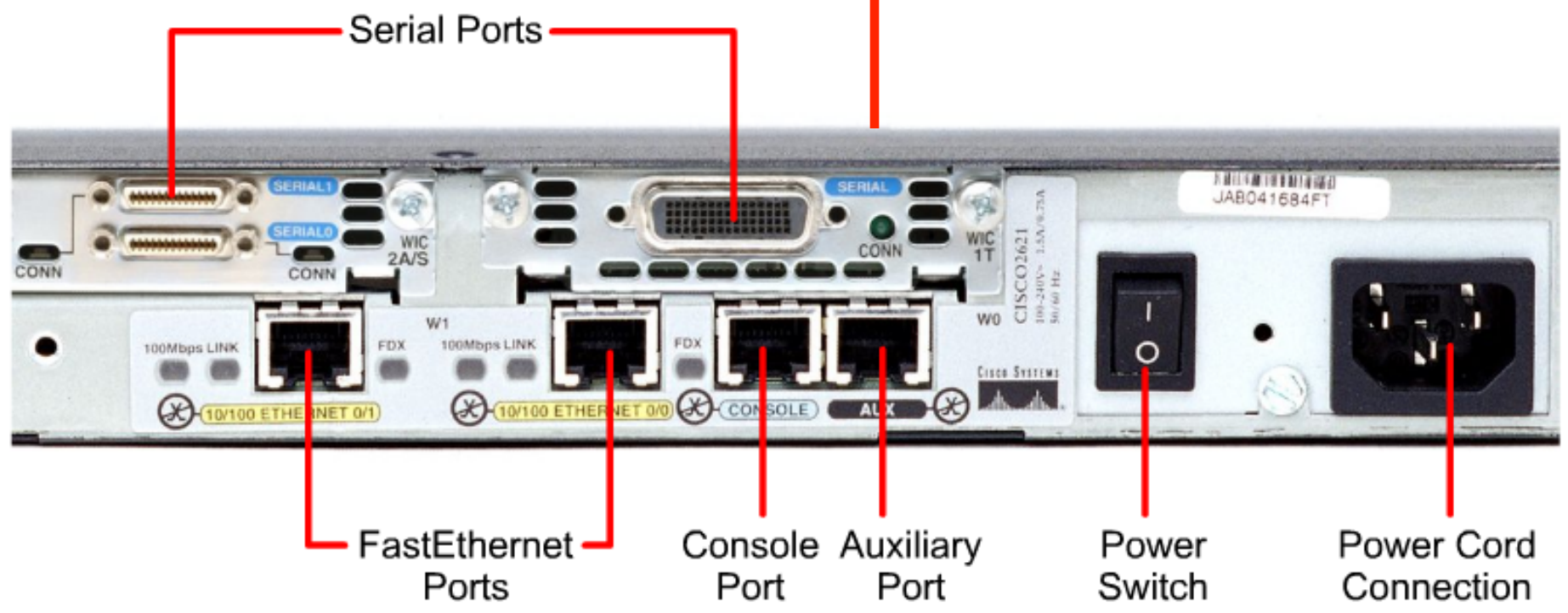
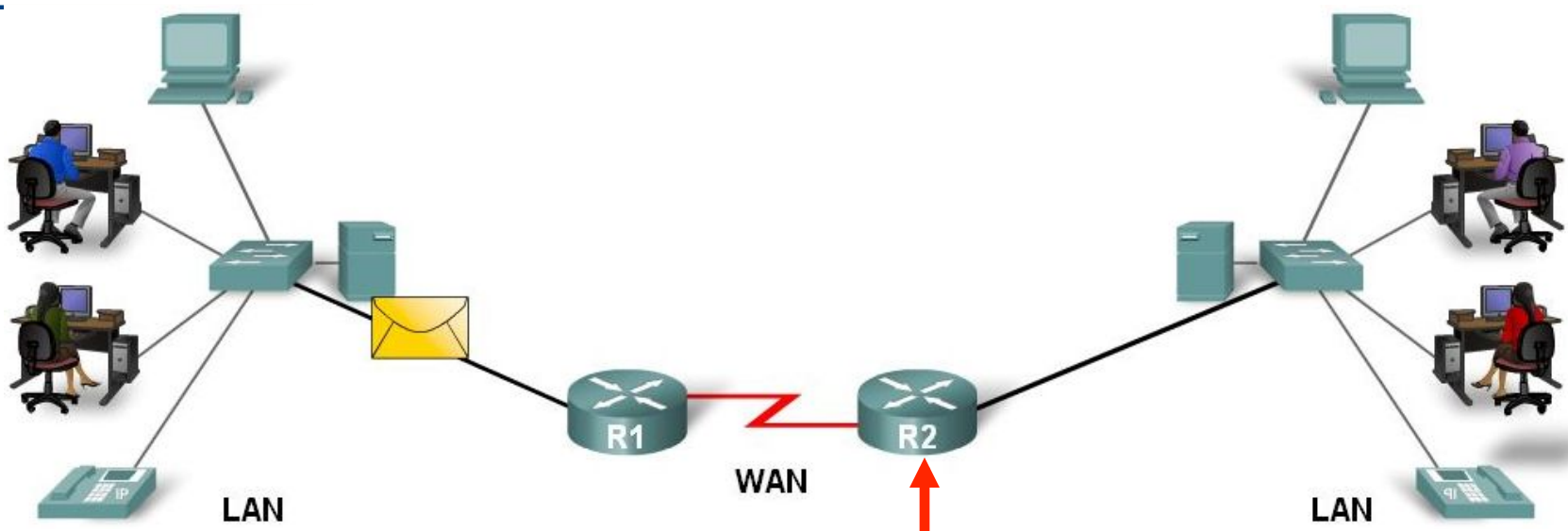
Boot ROM

RAM DIMMs

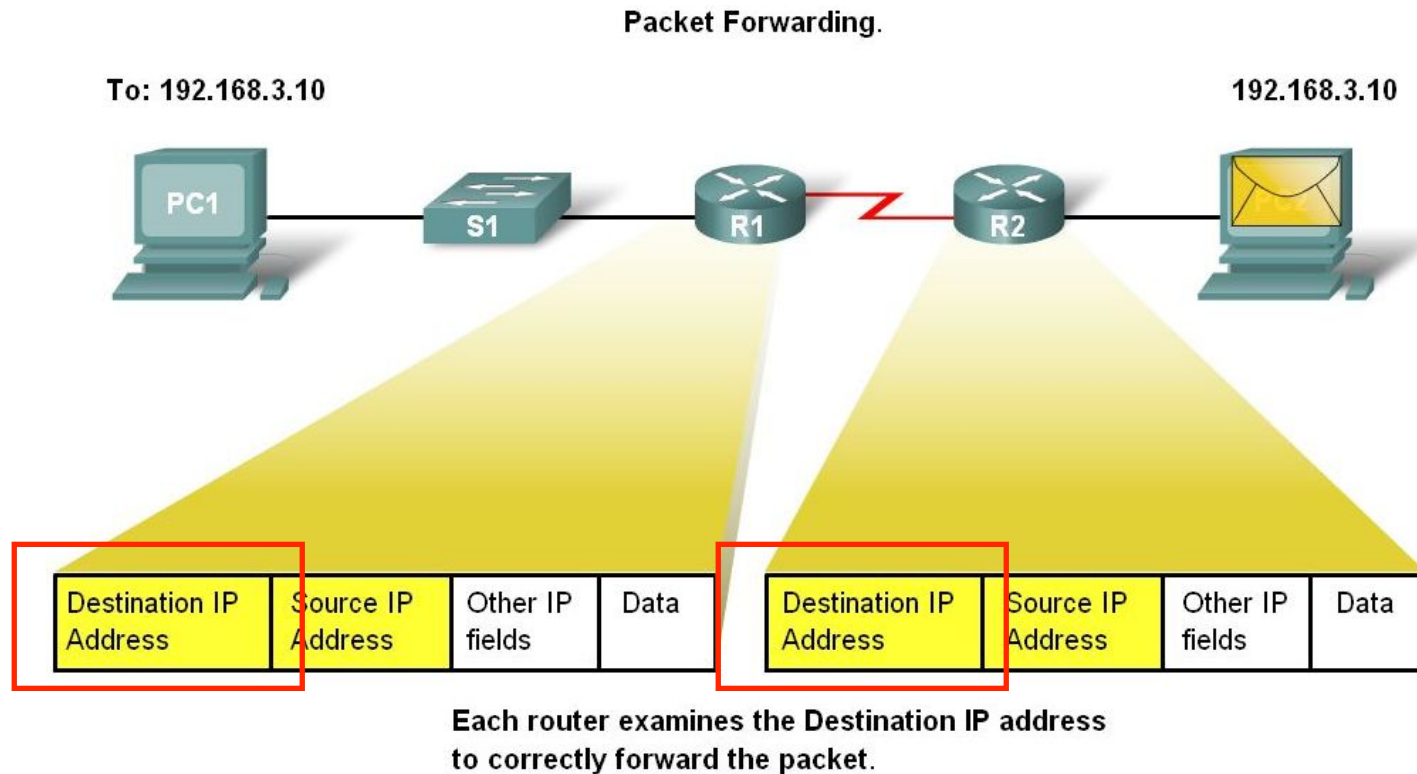
CPU



- Les routeurs transfèrent les paquets (**packet switching**) :
 - De la source jusqu'à la destination finale
 - Sélection du meilleur chemin (best path)
- Un routeur connecte plusieurs réseaux :
 - Interfaces dans des réseaux IP différents



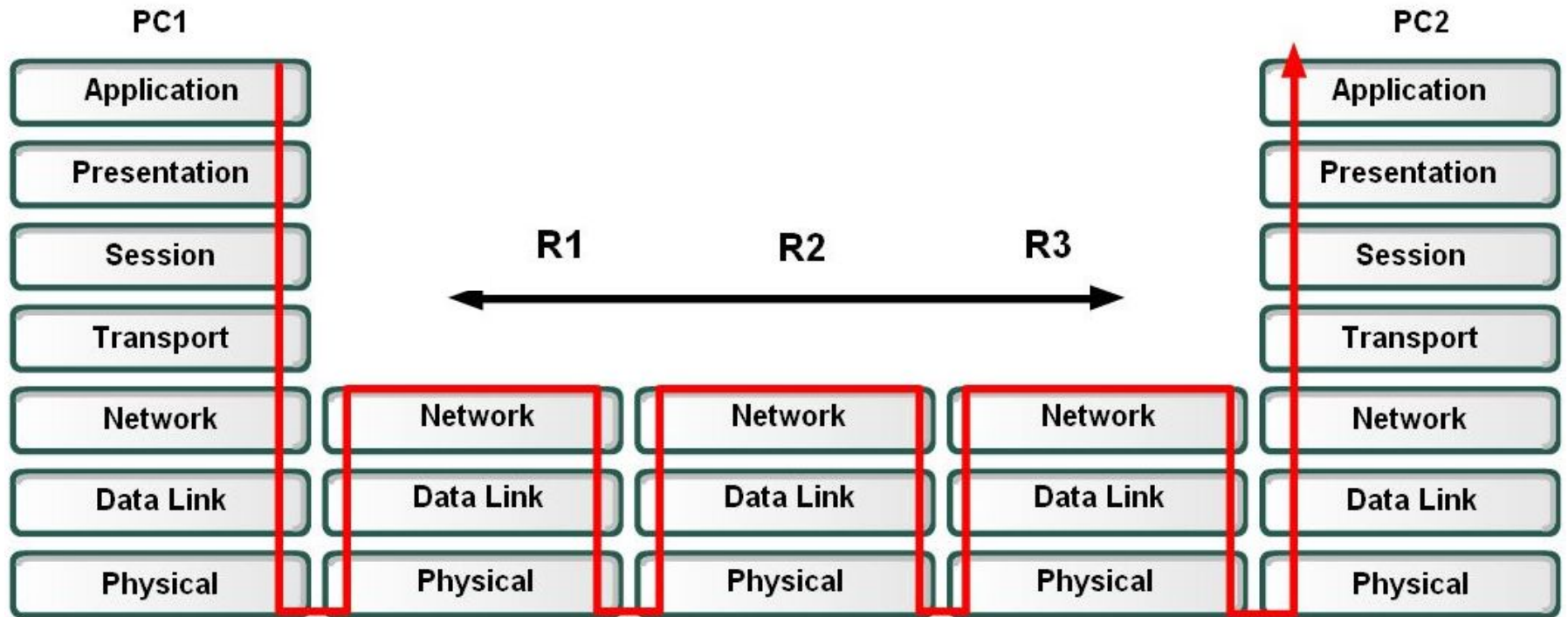
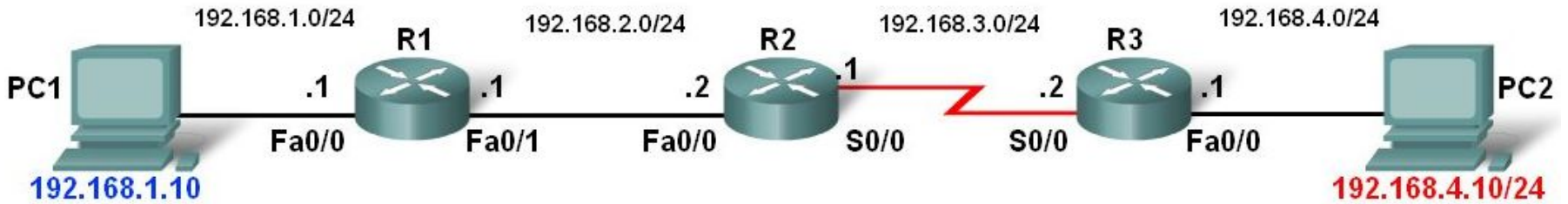
Les routeurs et la couche 3



- **Un routeur est un dispositif de couche 3** car il utilise l'information de couche 3 (adresse IP) pour prendre ses décisions (le **routing**)

Les Routeurs opèrent dans les couches 1, 2, et 3

Router Operates at Layers 1, 2, and 3



Rappel : trame Ethernet

Field Length in Bytes

Ethernet					
8	6	6	2	46-1500	4
Preamble	Destination Address	Source Address	Type	Data	FCS

Byte 1		Byte 2		Byte 3		Byte 4	
Ver.	IHL	Service Type		Packet Length			
Identification				Flag	Frag. Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options						Padding	

- Adresses de couche 2 : liaisons à l'intérieurs d'un réseau local (segment)
 - Modifiés à chaque segment traversé
- Adresses de couche 3 :
 - Adresse IP source et destination
 - Ne changent jamais (sauf si un NAT est utilisé)

Introduction à la table de routage

- ▶ La table de routage contient des relations "réseau-passerelle"
- ▶ La passerelle ("next hop") est l'adresse IP du prochain routeur
- ▶ La table peut aussi contenir la référence aux interfaces de sortie
- ▶ La table de routage est un fichier en mémoire RAM qui est utilisé pour stocker des informations relatives à :
 - ▶ Les réseaux directement connectés et réseaux distants
 - ▶ Les routes statiques et dynamiques

```
R1# show ip route
```

```
<output omitted>
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
C    192.168.2.0/24 is directly connected, Serial10/0/0
```

Introduction à la table de routage

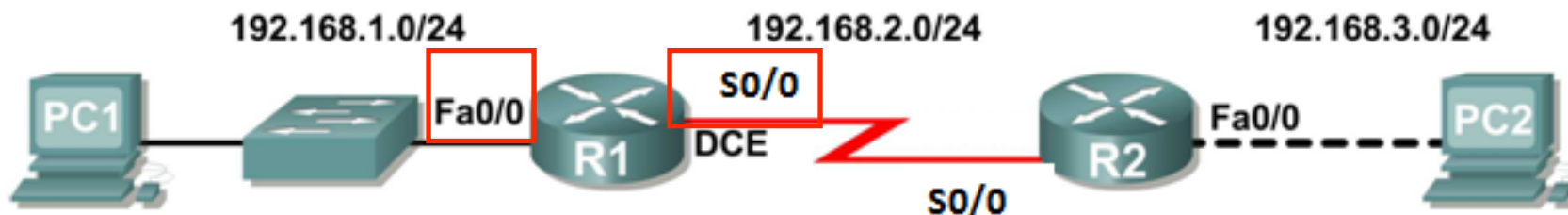
- Les réseaux directement connectés sont TOUJOURS renseignés dès l'activation de l'interface
- Un réseau directement connecté est associé à une interface "de sortie" (exit interface)

```
R1# show ip route
```

```
<output omitted>
```

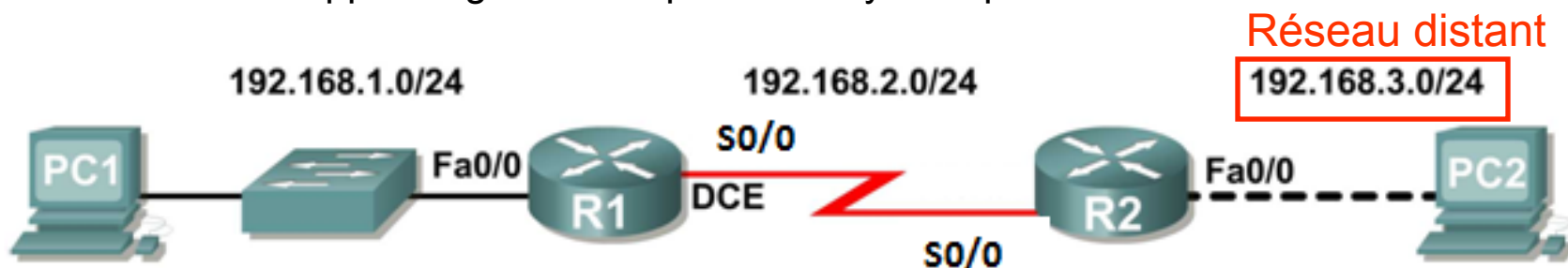
```
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0
```

Interface associée



Introduction à la table de routage

- Un **réseau distant** est un réseau qui n'est pas directement connecté au routeur
- Un réseau distant ne peut être accédé qu'en traversant d'autres routeurs
- Un réseau distant n'est pas automatiquement rajouté à la table de routage. Pour cela il faut :
 - Des routes statiques
 - Des routes apprises grâce à un protocole dynamique



```
R1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP,
```

```
C    192.168.1.0 is directly connected, FastEthernet0/0
```

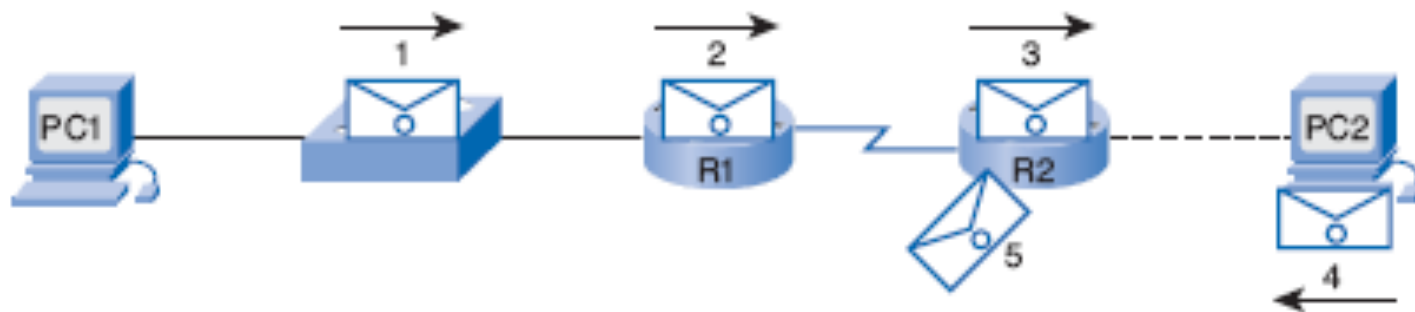
```
C    192.168.2.0 is directly connected, Serial0/0/0
```

```
S    192.168.3.0 [1/0] via 192.168.2.2
```

Les règles d'une table de routage

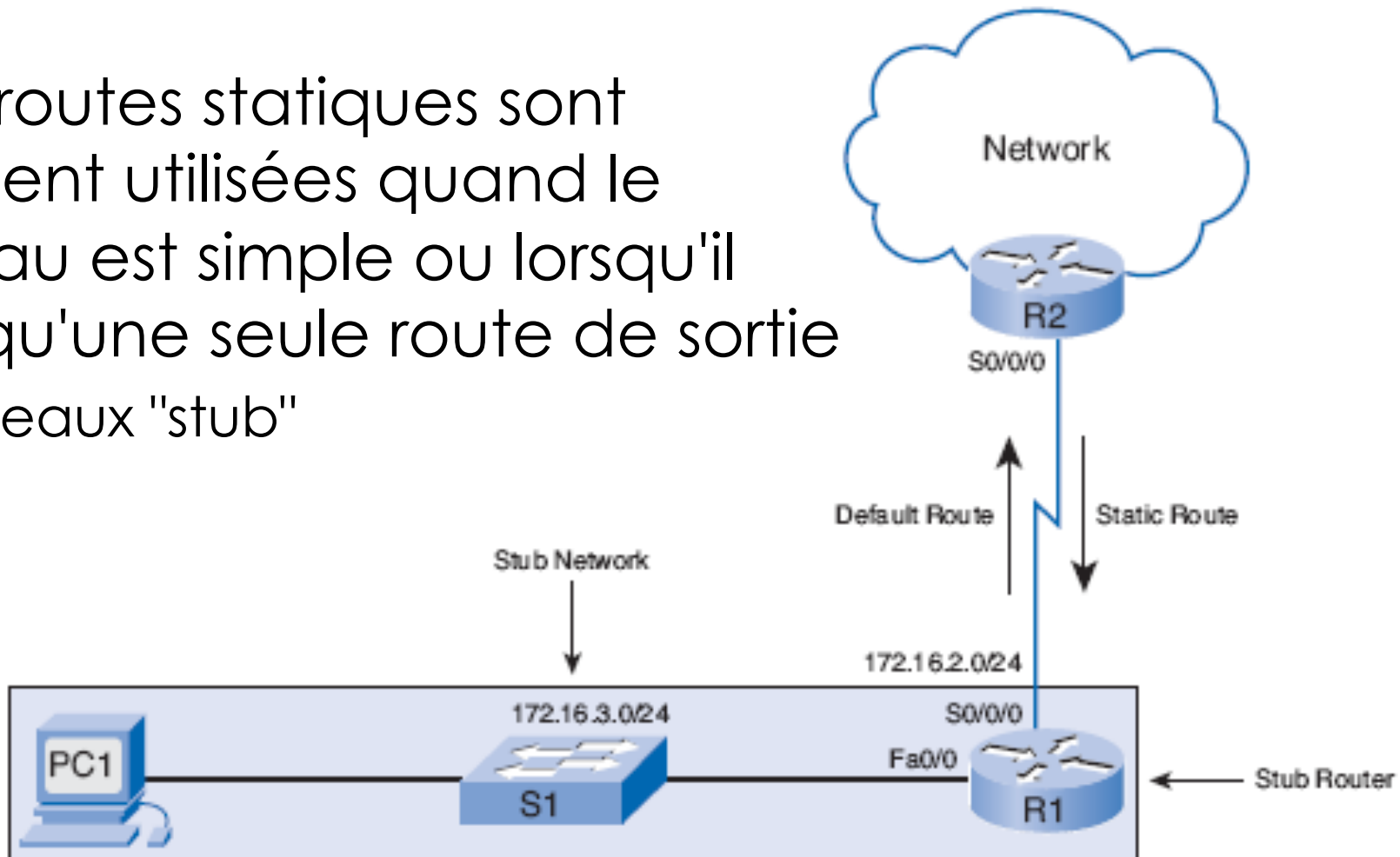
- ▶ Le fonctionnement des tables de routage suit certaines règles :
 1. Chaque routeur décide indépendamment sur le routage des paquets, grâce aux informations contenues dans sa propre table de routage.
 2. Le fait qu'un routeur détient une information dans sa table de routage ne veut pas dire que les autres routeurs la détiennent aussi.
 3. L'information du chemin de routage entre un réseau A et

est min



Utilisation des routes statiques

- ▶ Des routes statiques sont souvent utilisées quand le réseau est simple ou lorsqu'il n'a qu'une seule route de sortie
- ▶ Réseaux "stub"



La commande ip route

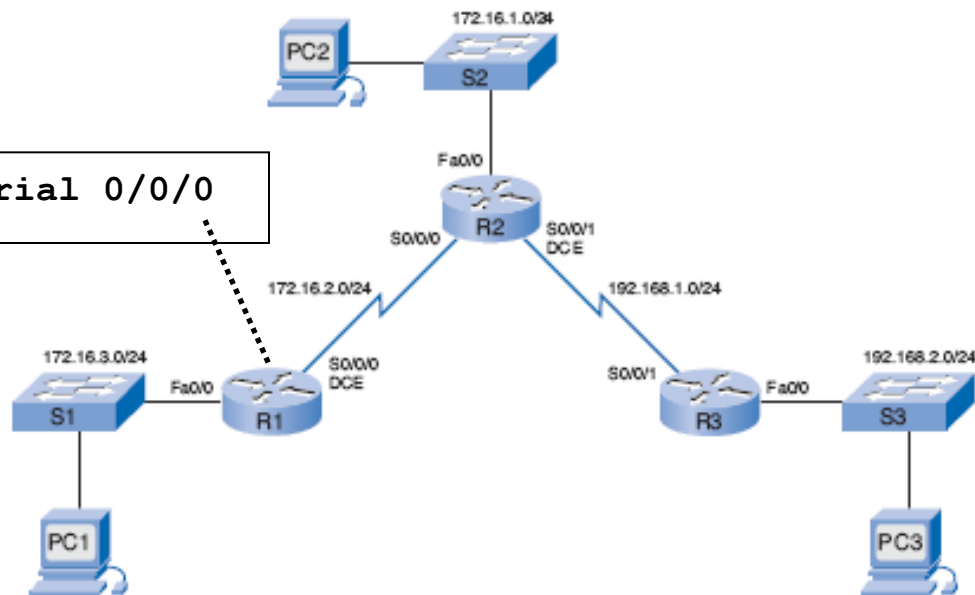
- ▶ La commande pour configurer une route statique est **ip route**
- ▶ **ip route** *réseau masque passerelle*

```
R1# debug ip routing
R1# conf t
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
       172.16.0.0/24 is subnetted, 3 subnets
S      172.16.1.0 [1/0] via 172.16.2.2
C      172.16.2.0 is directly connected, Serial0/0/0
C      172.16.3.0 is directly connected, FastEthernet0/0
```

Configurer une route statique défaut

- ▶ R1 est un routeur stub connecté uniquement à R2
- ▶ R1 ne requiert aucune information supplémentaire pour accéder aux réseaux de R3
- ▶ Actuellement R1 contient trois routes statiques qui partagent :
 - ▶ L'interface de sortie Serial 0/0/0
 - ▶ La passerelle vers R2

```
R1(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```



Exercice 4

- Configurer le routage statique sur des routeurs