

# Switching & Routing

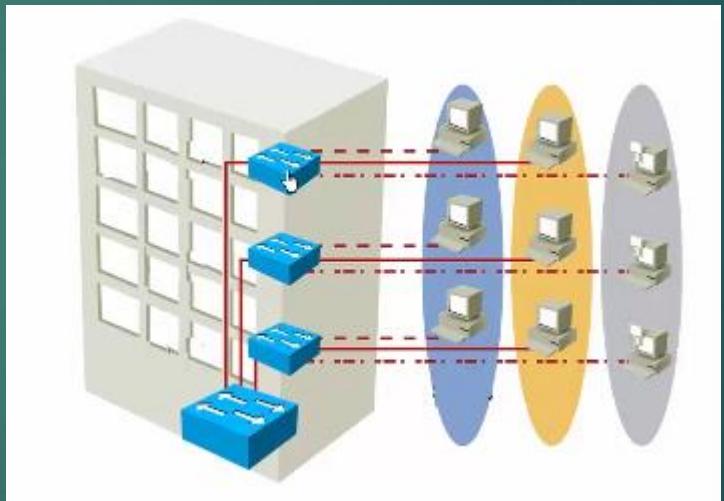
PRÉSENTÉ PAR : **KATAKPE KOSSI KUMA** ÉTUDIANT CHERCHEUR À  
L'INSTITUT DE MATHÉMATIQUES ET DE SCIENCES PHYSIQUES  
(IMSP) DE L'UNIVERSITÉ D'ABOMEY CALAVI (UAC), CONTACTS:  
[KOSSI.KATAKPE@IMSP-UAC.ORG](mailto:KOSSI.KATAKPE@IMSP-UAC.ORG), [KOSSI.KATAKPE@GMAIL.COM](mailto:KOSSI.KATAKPE@GMAIL.COM)

# Partie I

## Switching

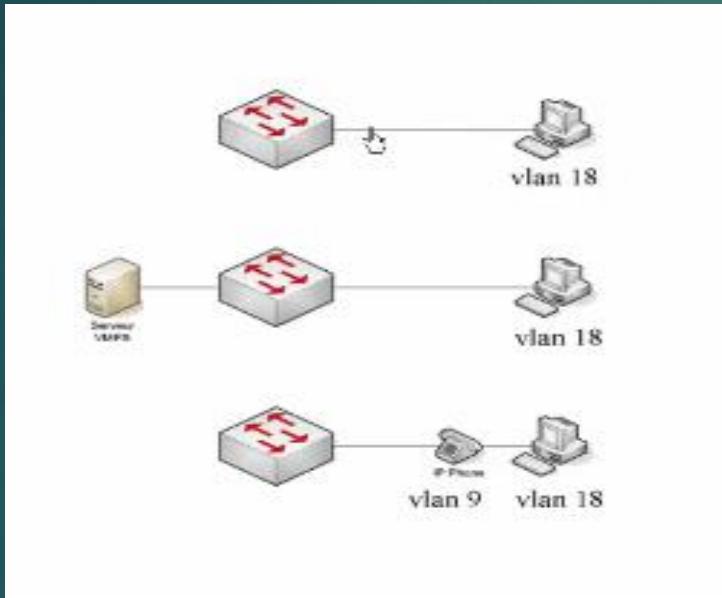
# Introduction aux VLANs

- ▶ Définition
  - VLAN
    - Virtual Local Area Network
- ▶ Avantages
  - Segmentation
  - Flexibilité
  - Sécurité



# VLAN

- ▶ Appartenance à un VLAN



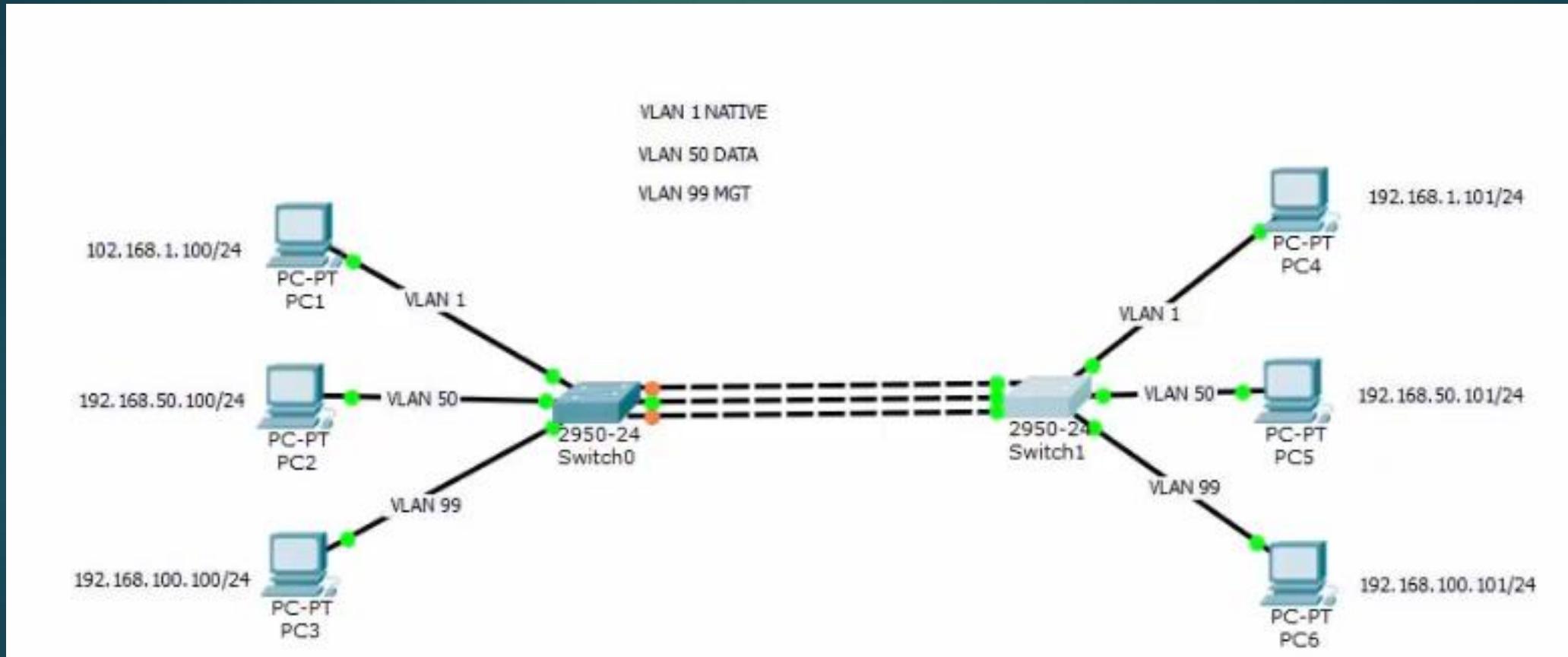
- ▶ Serveur Tacacs ou radius
- ▶ Authentification 802.1x

# Les différentes utilisations de VLAN

- ▶ Le nombre maximum de VLAN que l'on peut créer dépend du type de Switch (64, 128, 1024, 4096)
- ▶ Le VLAN 1 est créé par défaut et tous les ports du Switch appartiennent à ce VLAN
- ▶ Il faut d'abord créer l'identifiant du VLAN puis attribuer des ports à ce VLAN
- ▶ On peut donner un nom à un VLAN (optionnel), par exemple:
  - VLAN 1 – Management
  - VLAN 2 – Commerciaux
  - VLAN 3 – Voix
  - VLAN 4 – Finance
- ▶ VLAN = un domaine de broadcast; à un VLAN créé, on attribue un sous-réseau IP dédié.

# Configuration des VLANs

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024



# Configuration des VLANs

7

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

Rien de plus facile... créons le VLAN n°2 que l'on va nommer "finance"

```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name finance
SwitchX(config-vlan)#end
```

# Attribution d'un port dans un VLAN

- On identifie le port du Switch (par exemple l'interface FastEthernet 0/1) qui doit être dans le VLAN 2 précédemment créé:

```
SwitchX# configure terminal
SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport access vlan 2
SwitchX(config-if)# end
SwitchX# show vlan

VLAN Name                               Status      Ports
---- -----
1   default                             active     Fa0/2
2   finance                            active     Fa0/1
```

# Astuce

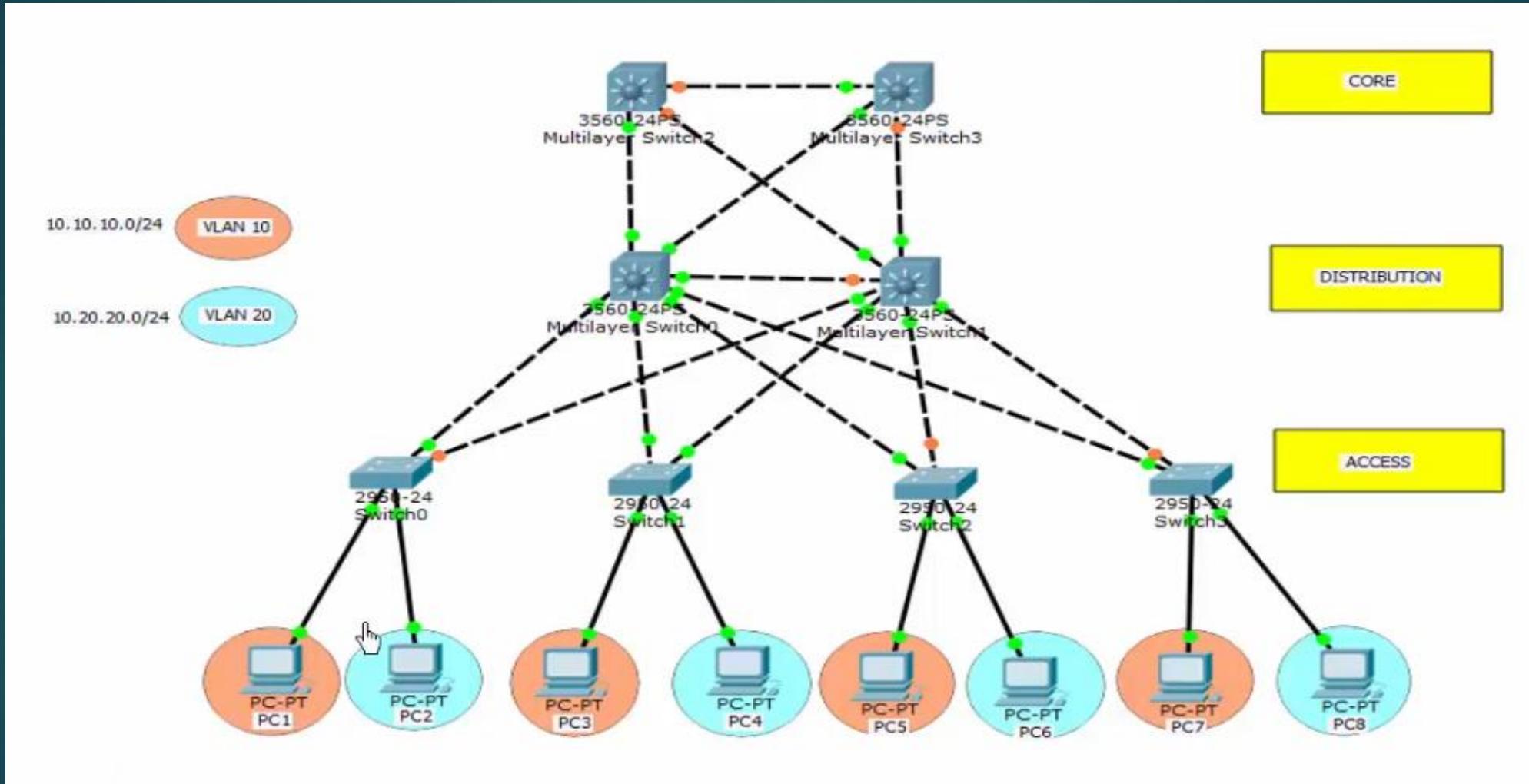
9

- ▶ Pour configurer plusieurs ports (exemple avec les ports 0/2 à 0/7) dans un VLQN; on peut utiliser la variable range pour configurer en une seule fois tous les ports:

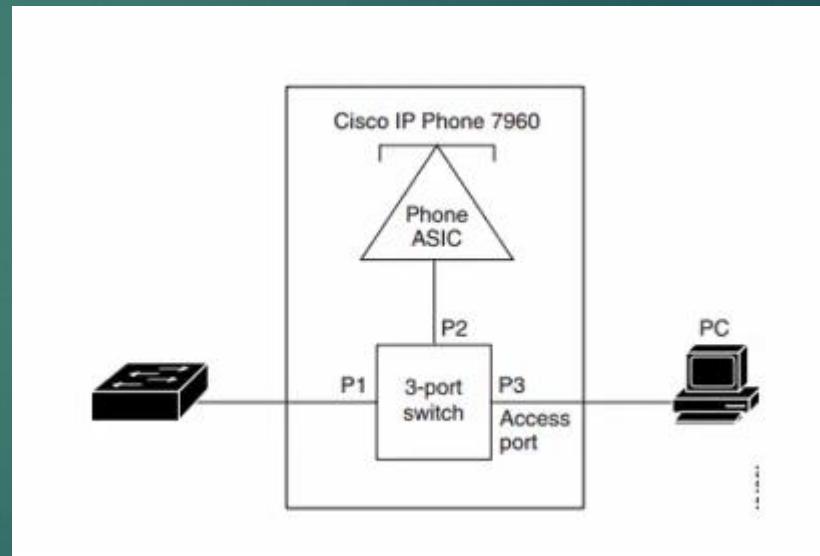
```
SwitchX# configure terminal
SwitchX(config)# interface range fastethernet 0/2 - 7
SwitchX(config-if)# switchport access vlan 2
SwitchX(config-if)# end
SwitchX# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1
2	finance	active	Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7

# VLAN Voice



# VLAN Voice



# Configuration d'un VLAN dédié à La téléphonie

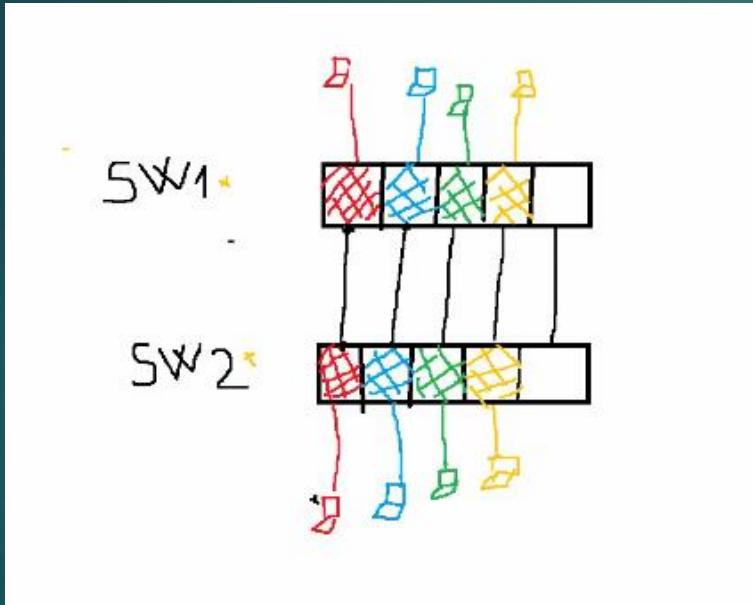
- ▶ Le protocole CDP doit préalablement être activé

```
2960-RG(config)#vlan 10
2960-RG(config-vlan)#name voip
2960-RG(config-vlan)#exit
2960-RG(config)#interface fastEthernet 0/1
2960-RG(config)#switchport voice vlan 10
```

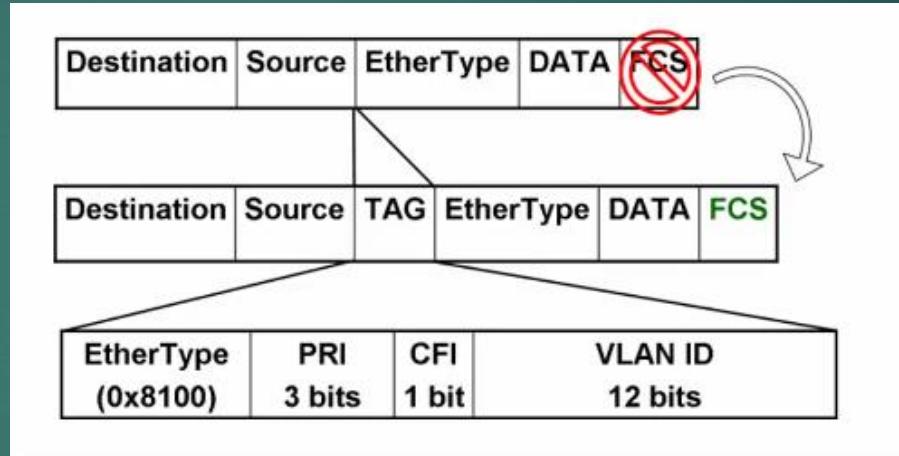
- ▶ Le Switch doit supporter la fonctionnalité POE (Power Over Ethernet)

# Trunk

► trunk



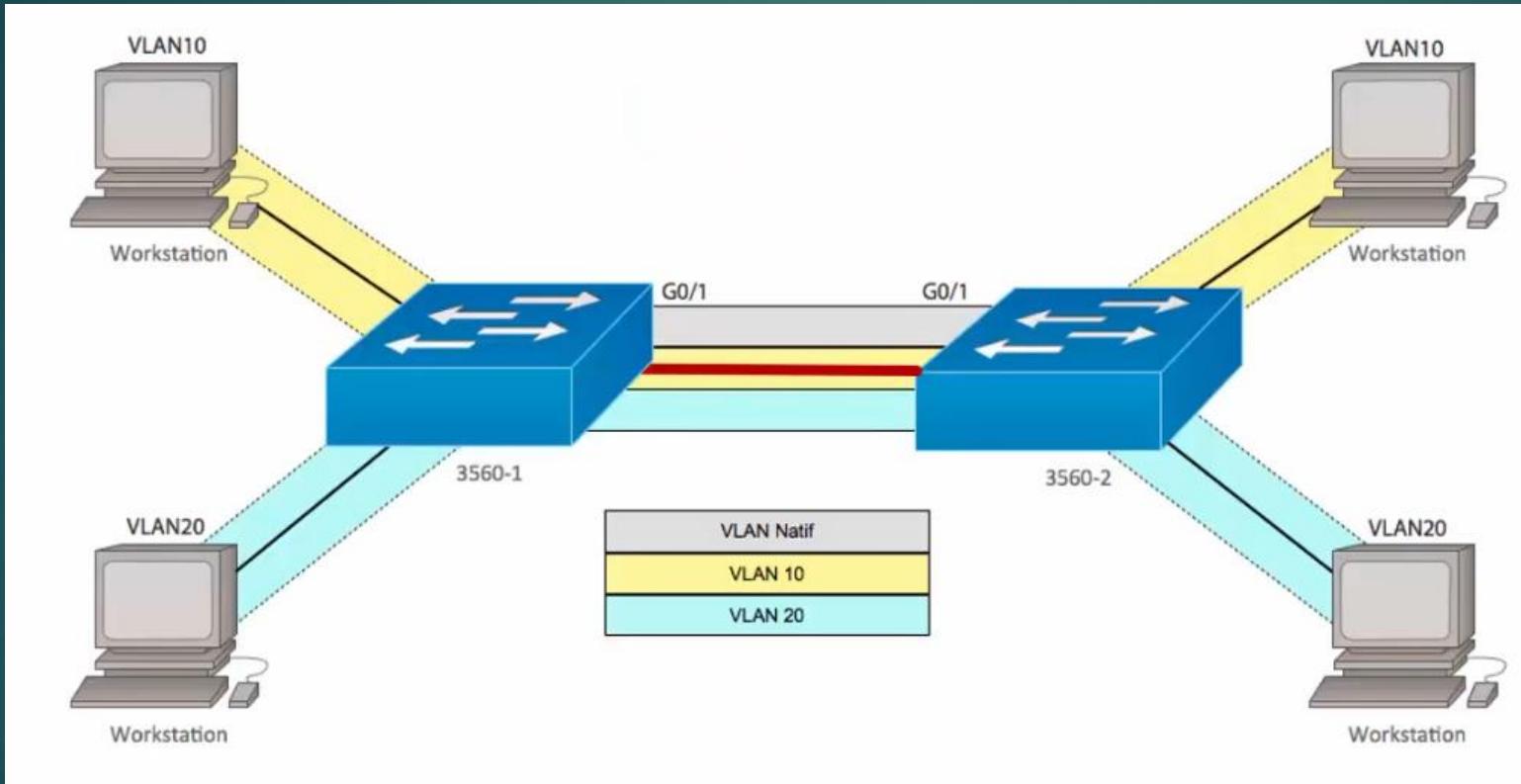
► Trunk 802.1Q



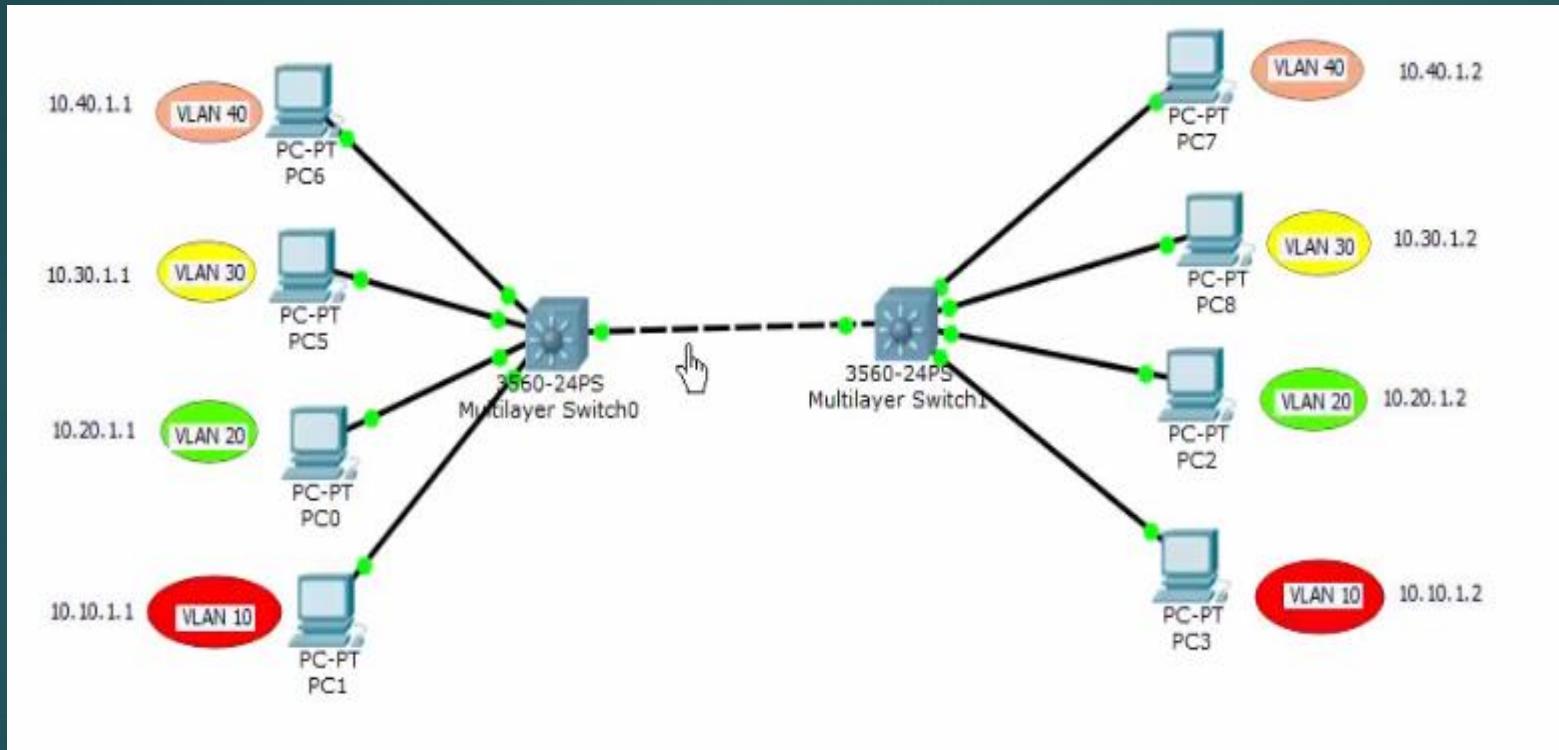
► ISL

Entête ISL 26 octets	Trame Ethernet Utilisateur 0 – 1500 octets	FCS 4 octets
-------------------------	---	-----------------

# Trunk: Limiter la propagation inutile des VLANs



# Configuration Trunk



# Configuration du Trunk

- ▶ La configuration à effectuer sur les ports des Switchs interconnectés entre eux :

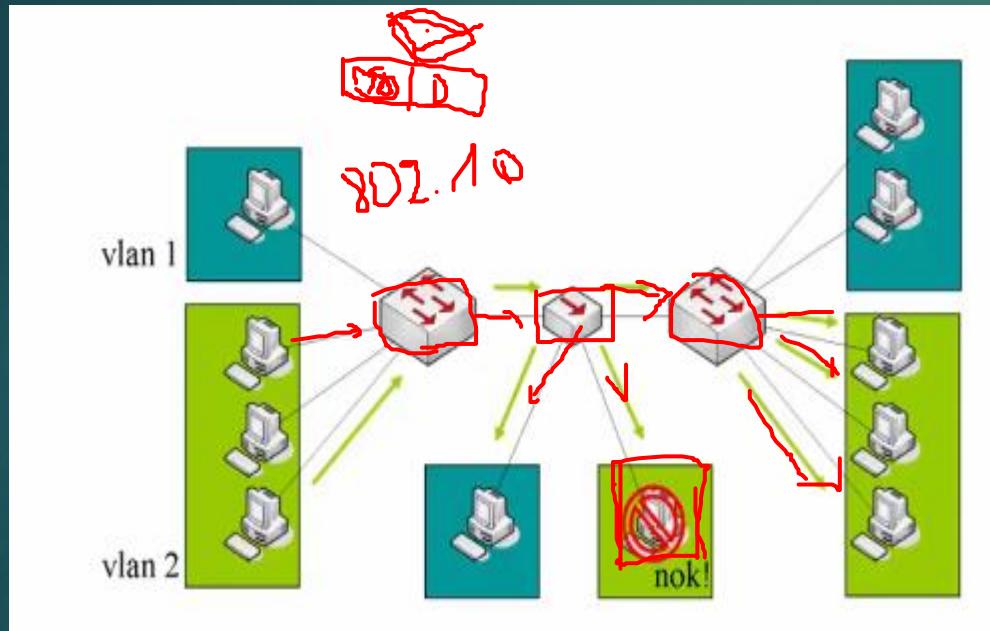
```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# shutdown
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
```

## ▶ Optimisation du Traffic

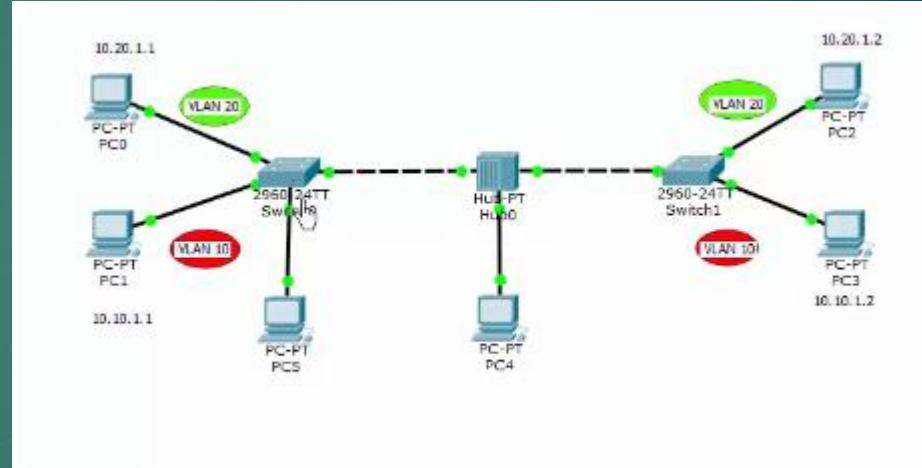
```
switch# configure terminal
switch(config)# interface FastEthernet 0/1
switch(config-if)# switchport trunk allowed vlan 5-15
switch(config-if)#
switch#
```

# VLAN Native

## ► Native

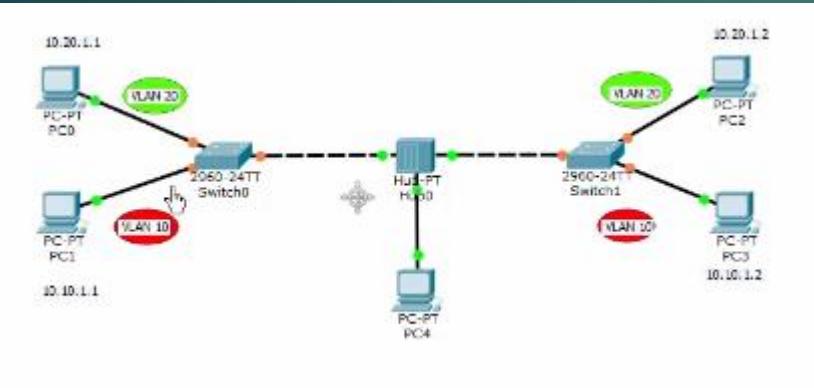


## ► Le VLAN native n'est pas tagué



# Configuration du VLAN native

## ► Native Vlan



## ► Configuration

```
3560-1#configure terminal
```



! Création d'un nouveau vlan spécifique

```
3560-1(config)#vlan 999
```

```
3560-1(config-vlan)#name NATIF
```

```
3560-1(config-vlan)#exit
```

# Configuration du Vlan native

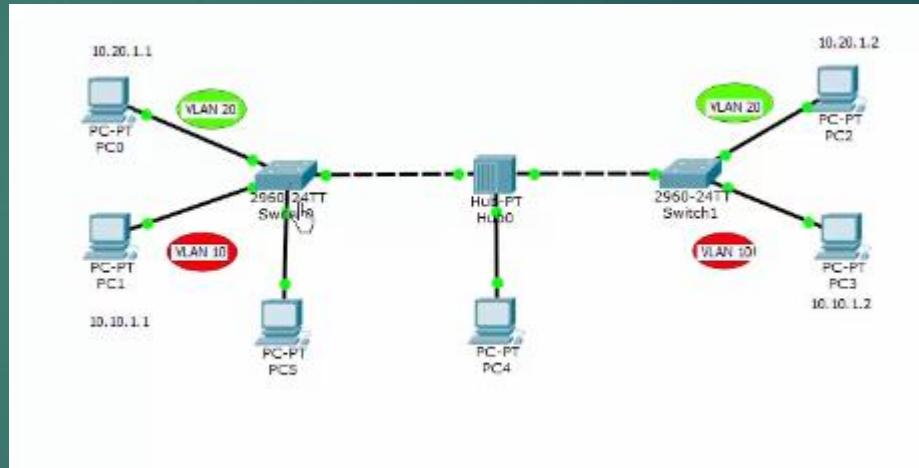
## ► Native

! Configuration du Vlan natif sur le trunk

```
3560-1(config)#interface  
gigabitEthernet 0/1
```

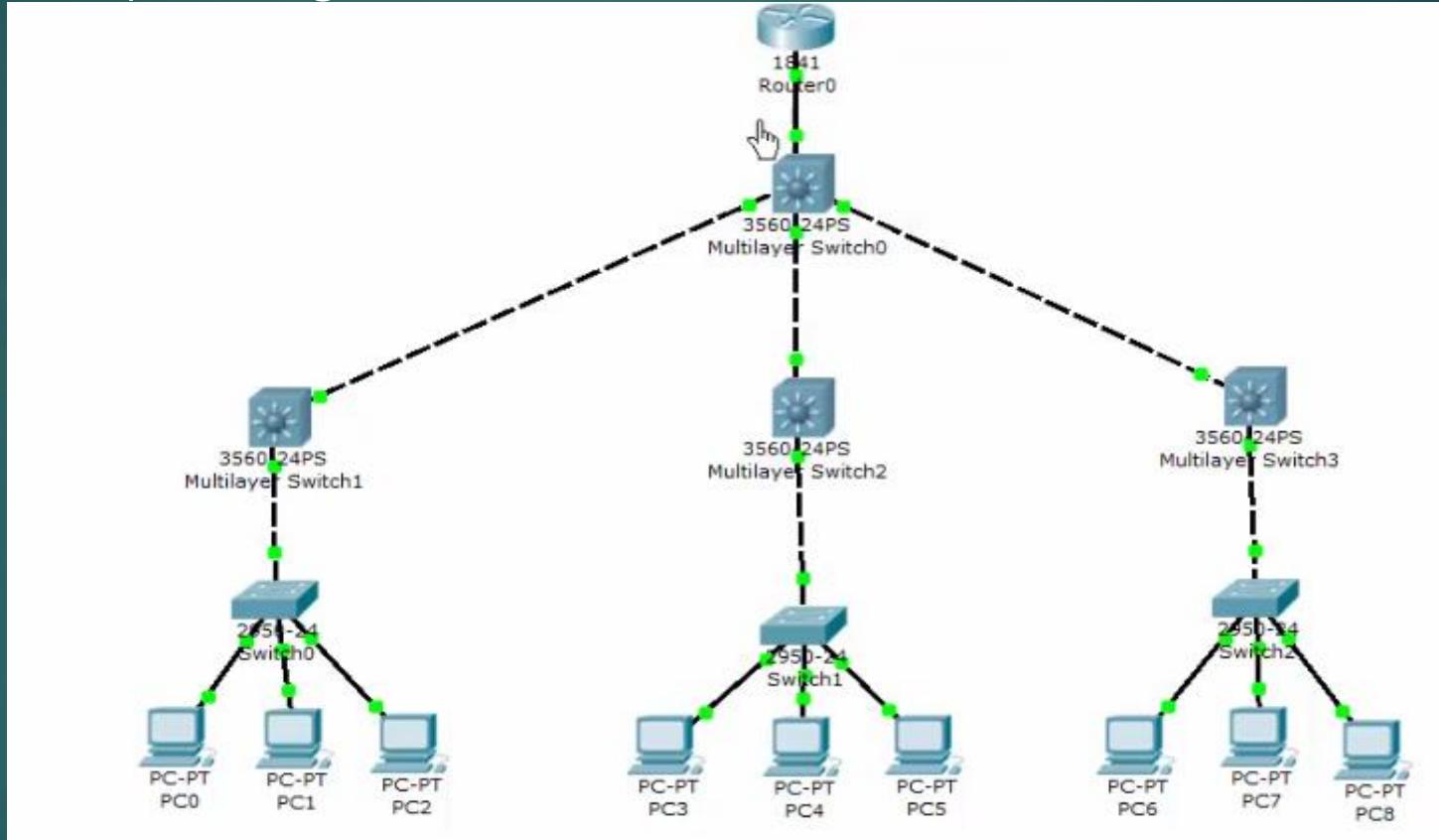
```
3560-1(config-if)#switchport  
trunk native vlan 999
```

```
3560-1(config-if) #
```



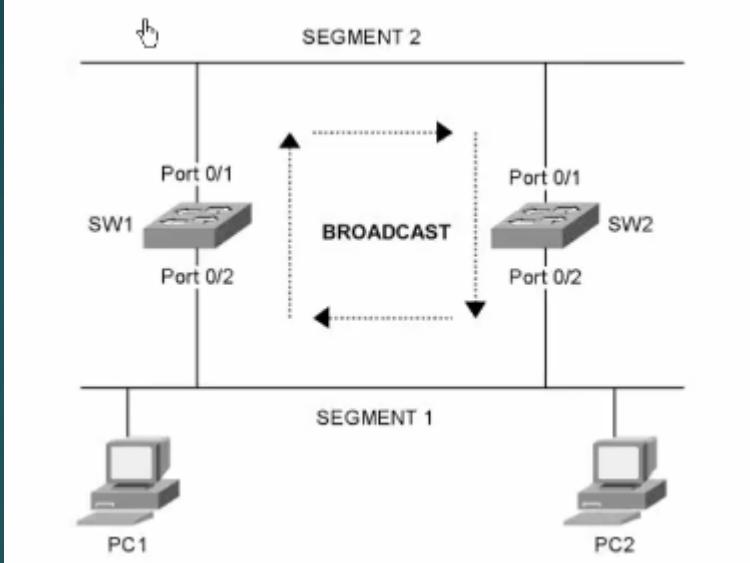
# Protocole Spanning Tree

## ► Spanning Tree

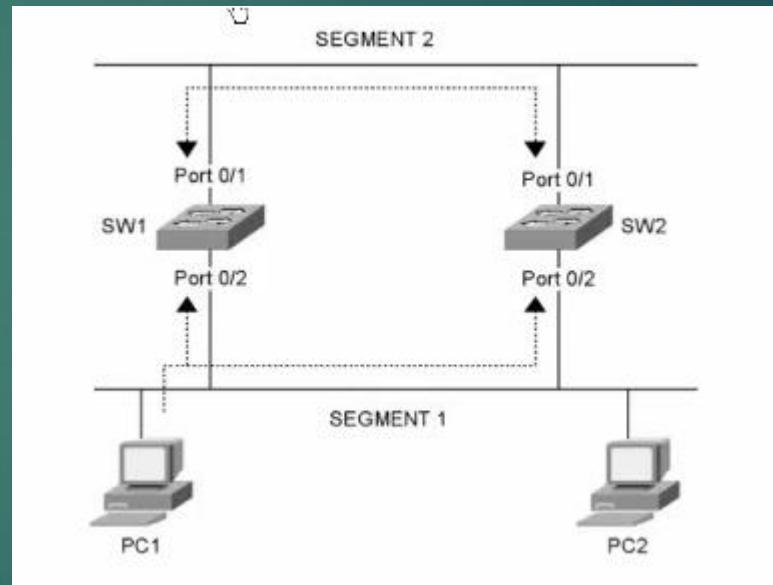


# Problématique

- ▶ Des tempêtes de diffusion (broadcast)

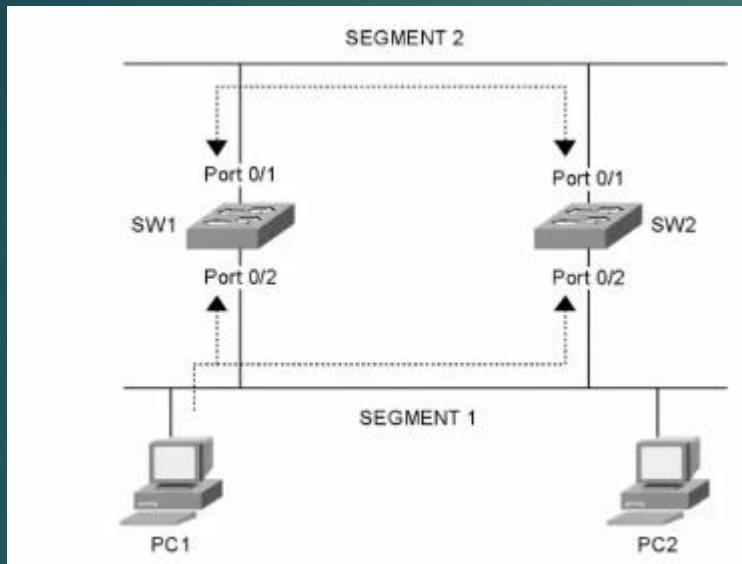


- ▶ Une instabilité de la table MAC

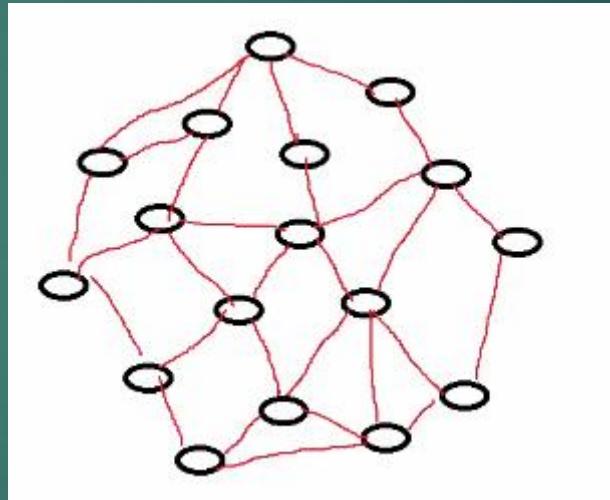


# Problématique

- ▶ Plusieurs copie de la même trame



- ▶ Introduction au protocole Spanning Tree (meilleur chemin)



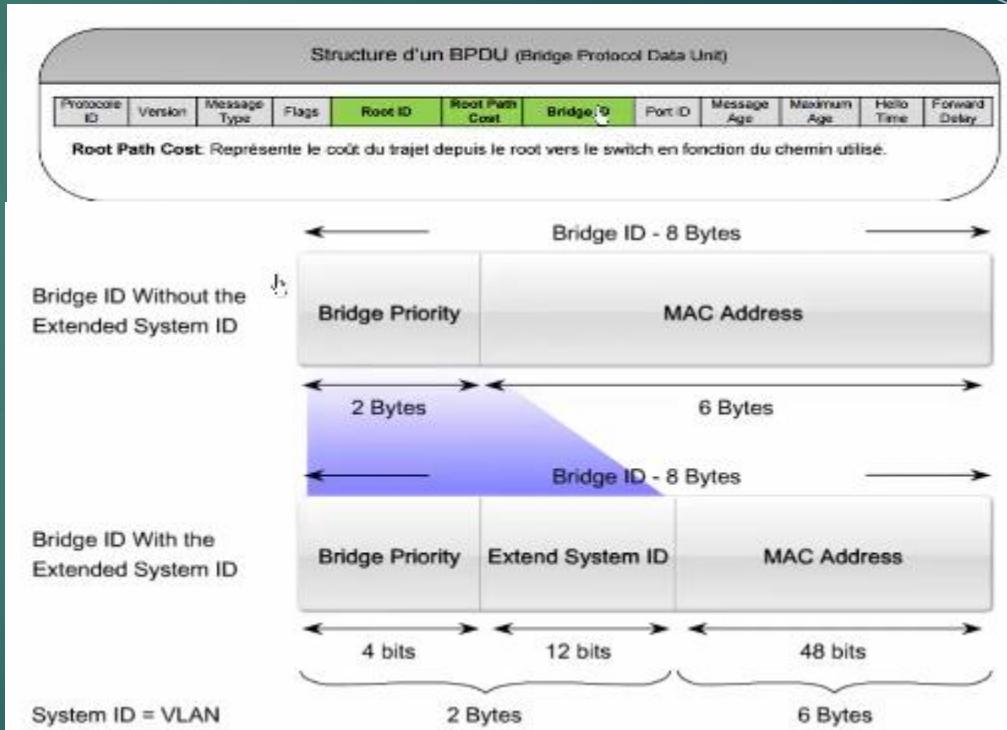
# Le protocole Spanning Tree

- ▶ Un protocole de couche 2
- ▶ IEEE 802.1D-2004
- ▶ Déetecte et désactive les boucles
- ▶ IEEE 802.1w Rapid Spanning Tree
- ▶ PVST+, PVRST+ (Cisco)
- ▶ Le fonctionnement du protocole Spanning Tree

# Root Bridge

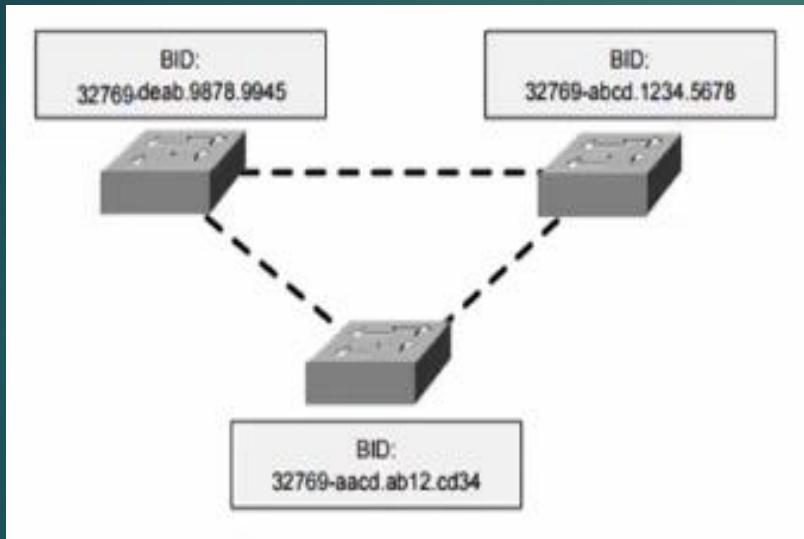
- ▶ Le Switch dont le Bridge ID est le plus petit remporte l'élection du Root Bridge
- ▶ Le BID est la concaténation d'une priorité comprise entre 1 et 65536, par défaut 32768, et de l'adresse MAC du Switch
- ▶ Un commutateur avec une priorité par défaut de 32768 et une adresse MAC 00:A0:C5:12:34:56 prendra L'ID 8000:00A0:C512:3456

## ► BPDU



# Port Root

## ► Port Root



## ► Les état Spanning Tree

- Etat « Blocking »
- Etat « Listening »
- Etat « Learning »
- Etat « Forwarding »
- Etat « Disabled »

## ► Ce qu'il faut retenir:

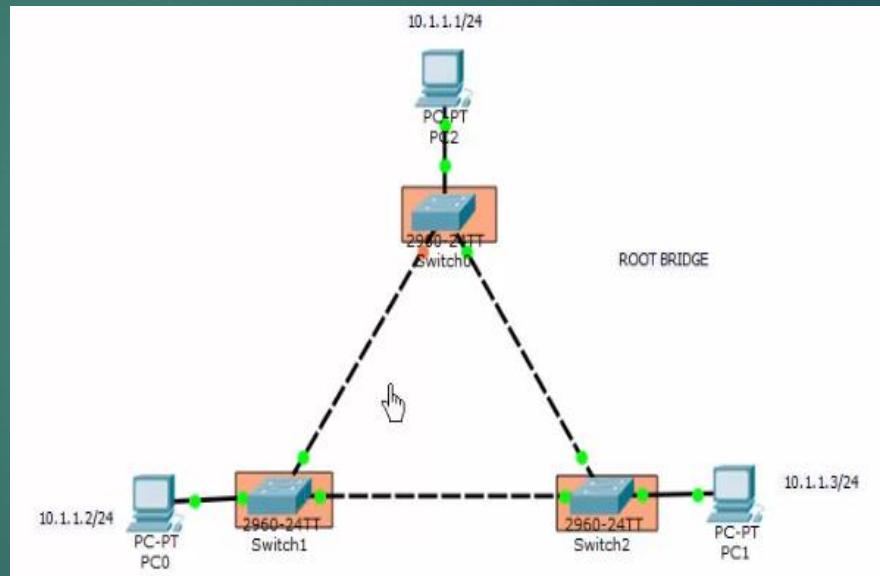
- 1 commutateur Root par réseau dont tous les ports sont Designated
- Un port Root par commutateur non Root
- 1 port Designated par domaine de collision (liaison) tous les autres ports sont Non-Designated

# Configuration du protocole Spanning Tree

## ▶ Introduction

- STP active par défaut
- Echange des BPDU
- Les processus Spanning Tree

## ▶ Configuration



# Atelier Spanning Tree

## ► Les commandes Spanning Tree

```
SW1#show spanning-tree vlan 1
```

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 24577  
Address 0013.c3ff.2580  
Cost 19  
Port 1 (FastEthernet0/1)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

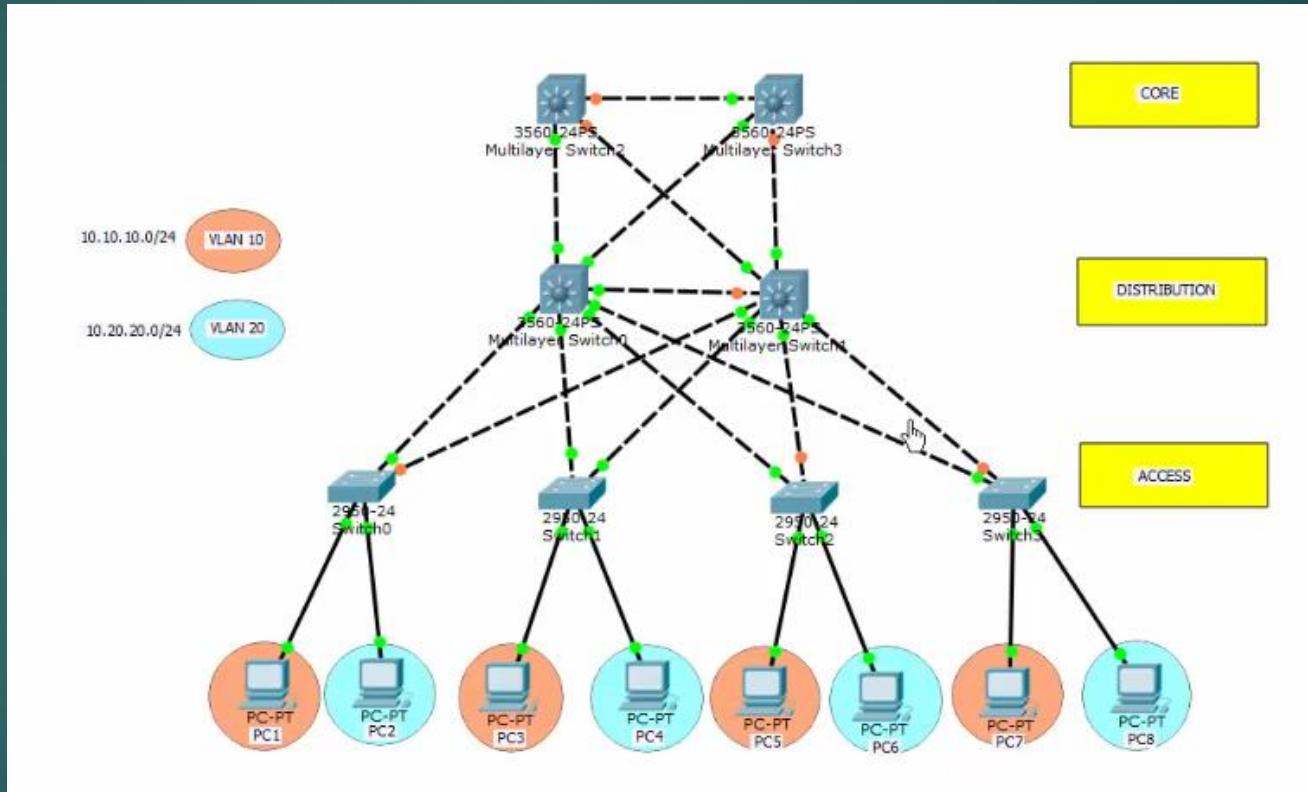
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)  
Address 0009.7cd5.1a40  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Alt	BLK	19	128.2	P2p

SW1#

# Optimisation Spanning Tree

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



# configuration et Optimisation du protocole Spanning Tree

- ▶ Pour voir les ports bloqués: **show Spanning Tree Vlan 1**

```
SW1 (config) #spanning-tree vlan 10 root primary
SW1 (config) #spanning-tree vlan 20 root primary
```

**Ou**

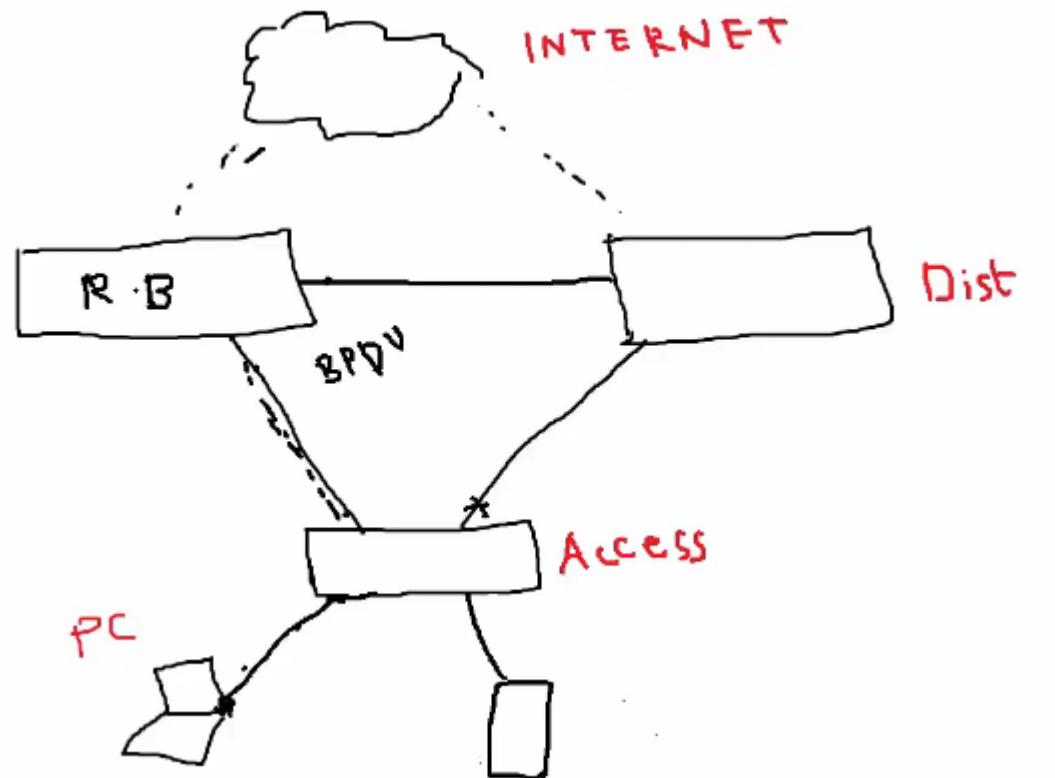
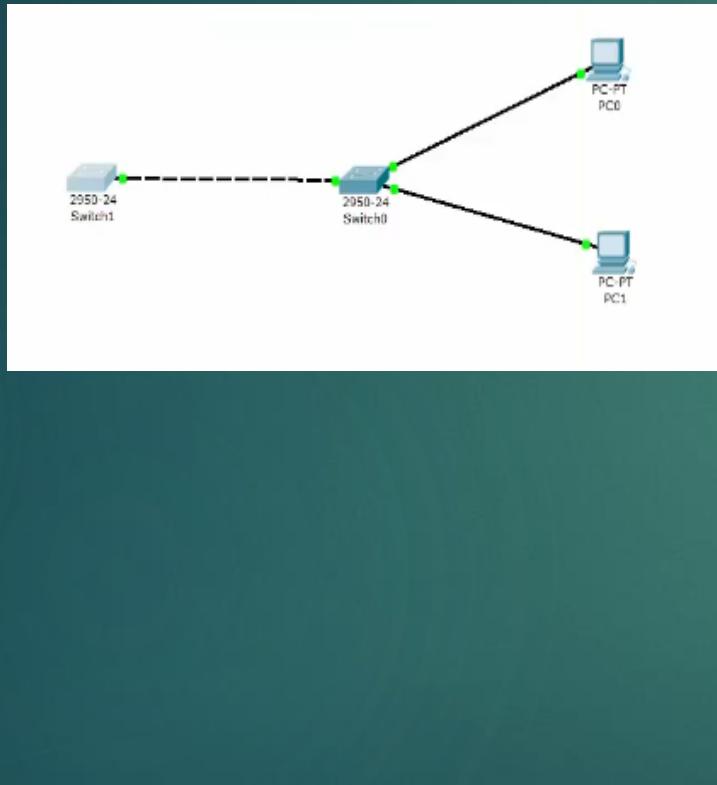
```
SW1 (config) #spanning-tree vlan x priority y
```

---

```
SW1 (config) #spanning-tree vlan 10 root secondary
SW1 (config) #spanning-tree vlan 20 root secondary
```

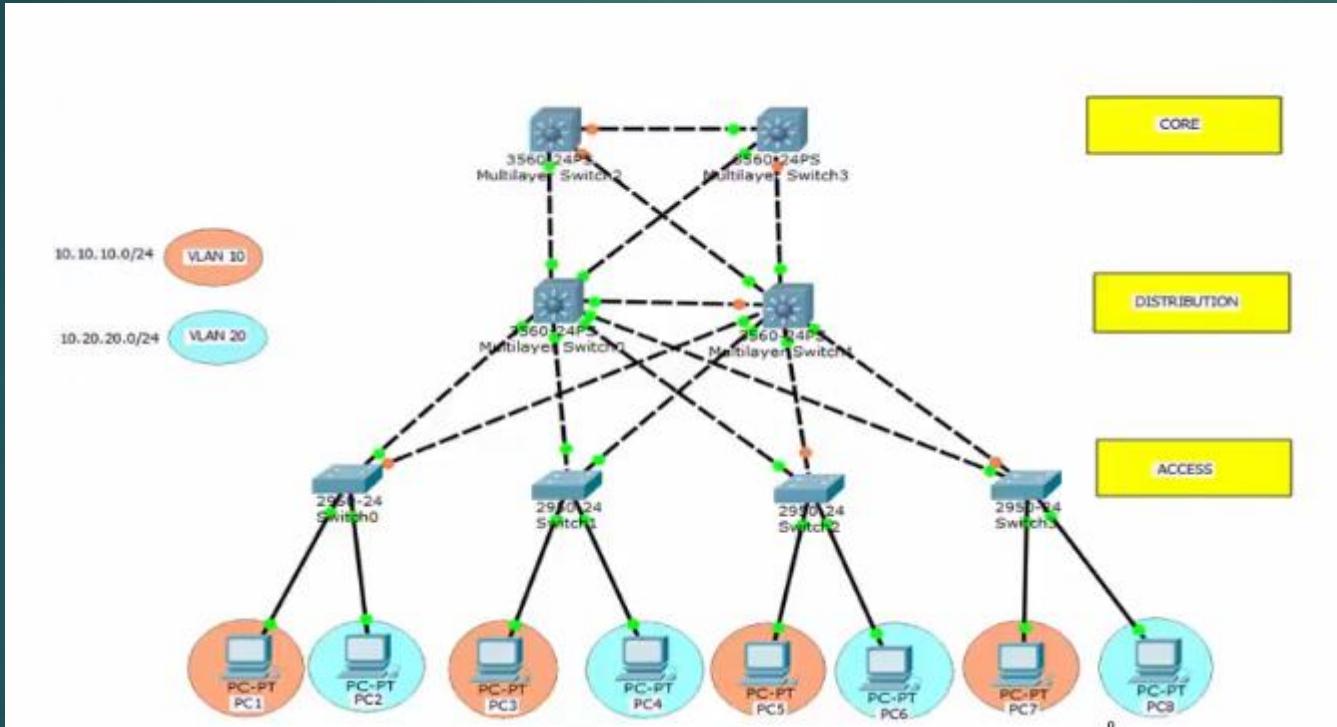
# Spanning Tree : Portfast

## ► Spanning-tree portfast



# BPDUs Guard

## ► Attaque de type Spanning Tree

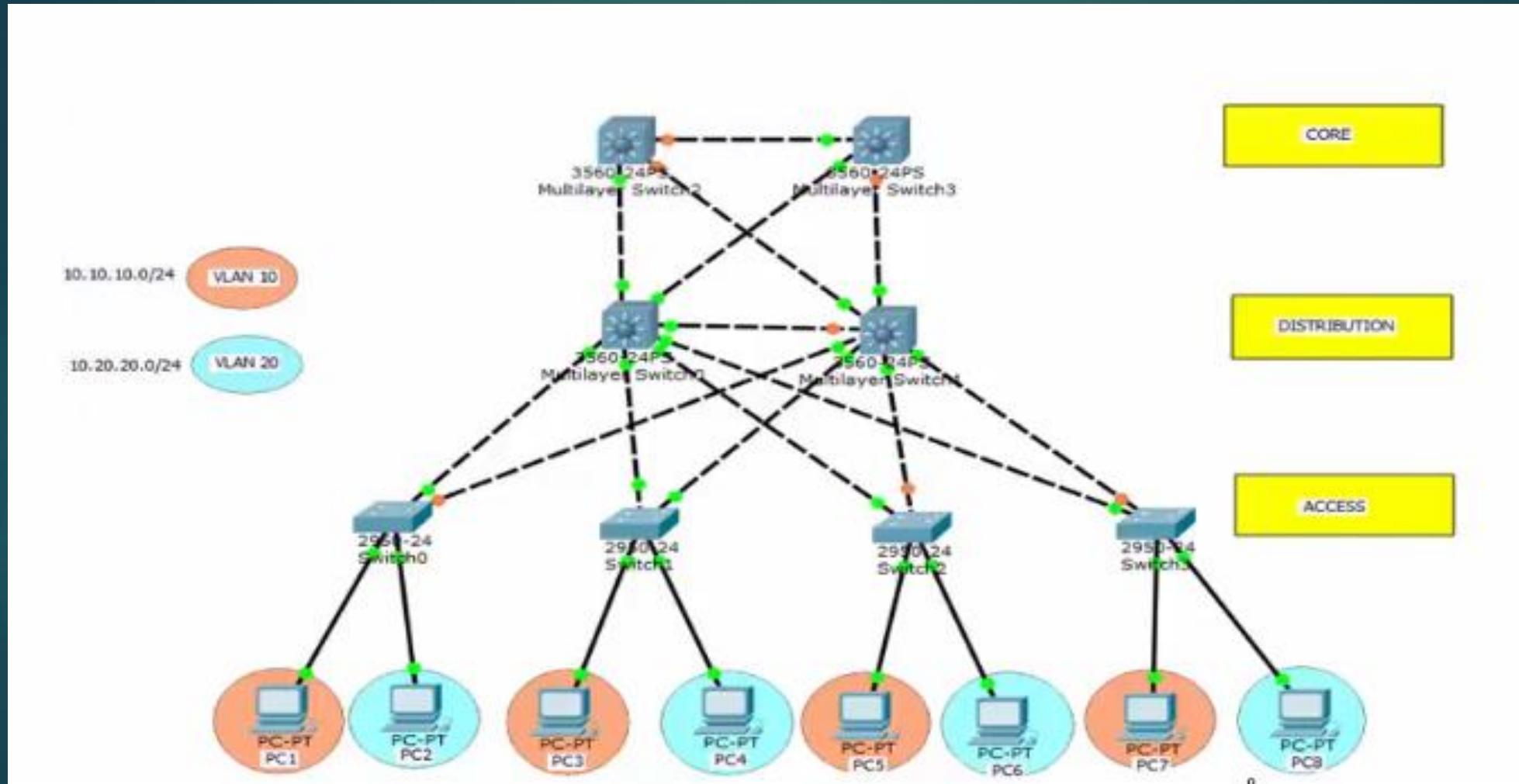


# BPDU Guard

```
SW1 (config) #interface FastEthernet 0/1
SW1 (config-if) #spanning-tree bpduguard enable
```

# Le RSTP 802.1w

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



- ▶ Fonctionnement du protocole RSTP
  - Election root bridge
  - Election root port
  - Election des ports bloqués
- ▶ Les rôles RSTP
  - Port Root
  - Port désigné
  - Port alternatif
  - Port Backup
- ▶ Les états Spanning Tree
  - Etat « discarding »
  - Etat « Learning »
  - Etat « Forwarding »
- ▶ Configuration PVRST+

```
switchX(config)#  
spanning-tree mode rapid-pvst  
  
Configuration PVRST+  
switchX#  
show spanning-tree vlan vlan# [detail]  
  
Verification de la configuration spanning-tree
```

# Le protocole Etherchannel

## ▶ Introduction

- Besoin d'une bande passante de plus en plus importante
- Une technique permettant l'agrégation de lien
- Permet également de faire l'équilibrage de charge sur les liens.

## ▶ Avantage de l'Etherchannel

- Augmentation de la bande passante
- Redondance
- C'est vu comme un seul lien par le protocole STP

## ▶ Fonctionnement de l'Etherchannel

- En forçant l'agrégation (mode ON)
- PAGP – Port Aggregation Protocol (Cisco)
- Auto
- Desirable
- LACP – Link Aggregation Control Protocol (802.3AD)
- Passive
- Active

# Load Balancing

- ▶ Sur les Switchs basiques, l'adresse Mac source et destination est utilisée.
- ▶ Certains équipements sont capables d'utiliser l'adresse IP ainsi que le port
- ▶ Par défaut c'est l'adresse MAC source qui est utilisée.
- ▶ Les bonnes pratiques
  - Utiliser les ports de même bande passante
  - Les ports qui composent l'agrégation, soient dans le même VLAN
  - Il n'est pas recommandé de faire du SPAN sur les ports d'une agrégation.

# Configuration Etherchannel

- ▶ Forcer l'agrégation de lien sur deux Switchs
- ▶ Configuration du port Channel avec le protocole LACP

```
Switch-1(config)#interface range fastEthernet 0/1 - 2
Switch-1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
```

```
Switch-2(config)#interface range fastEthernet 0/1 - 2
Switch-2(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
```

```
Switch-1(config)#interface range fastEthernet 0/1 - 2
Switch-1(config-if-range)#channel-protocol lacp
Switch-1(config-if-range)#channel-group 1 mode active
```

```
Switch-2(config)#interface range fastEthernet 0/1 - 2
Switch-2(config-if-range)#channel-protocol lacp
Switch-2(config-if-range)#channel-group 1 mode active
```

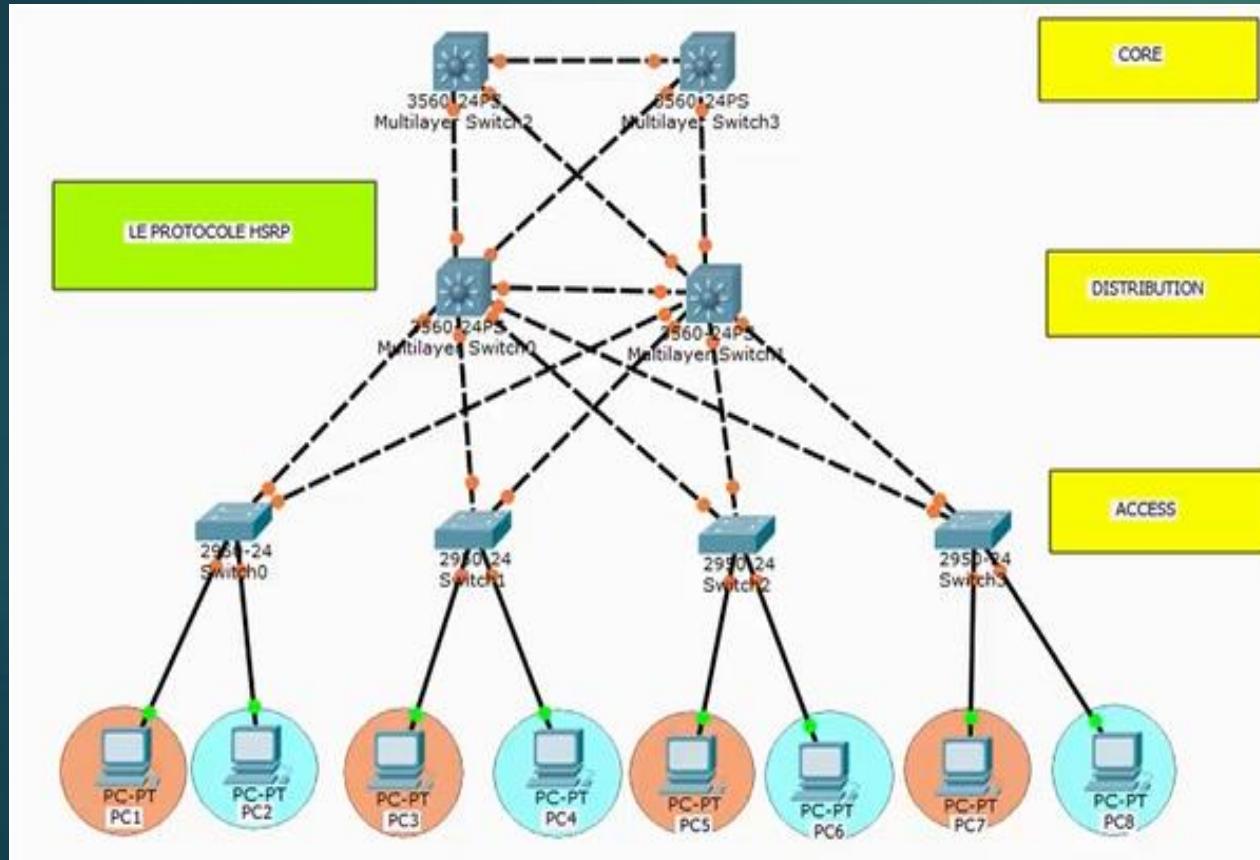
# Configuration Etherchannel

- ▶ Configuration de l'Etherchannel avec le protocole PAGP

```
SW1#config t
SW1(config)#interface range f0/1 - 2
SW1(config-if)#channel-group 5 mode desirable
SW1(config-if)#end
```

```
SW2#config t
SW2(config)#interface range f0/1 - 2
SW2(config-if)#channel-group 5 mode desirable
SW2(config-if)#end
```

# redondance de passerelle : HSRP Hot Standby Router Protocol



- ▶ Principe de fonctionnement
  - HSRP est un protocole Cisco permettant d'assurer la haute disponibilité de la passerelle du réseau
  - Le protocole HSRP peut être mis en place sur un routeur ou un Switch de niveau 3
  - Les rôles du protocole HSRP :
  - Active
  - Standby

# Principe de fonctionnement

- Le routeur actif est celui qui a la priorité la plus haute
- Le routeur standby est celui ayant la deuxième meilleure priorité
- Les autres routeurs sont en mode Listen
- En cas d'égalité sur la priorité, c'est le routeur avec la plus haute IP qui devient actif
- La priorité va de 0 à 255
- Le Hold Timer est de 10 secondes, soit 3\*le Hello Timer + 1 seconde
- Une IP virtuelle sera associée au groupe, et c'est le routeur actif qui va répondre sur cette IP
- Cette IP virtuelle est celle qui sera utilisée par les hôtes comme IP de Default Gateway
- Pour que les paquets soient envoyés au bon routeur, une adresse MAC virtuelle sera aussi créée
- Le routeur actif va répondre aux requêtes ARP sur l'IP virtuelle.

# Principe de fonctionnement

- ▶ Configuration du protocole HSRP
  - Configuration des SVI

Structure Adresse Mac HSRP		
00.00.0C	07.AC	XX
Cisco ID	HSRP ID	Standby Group ID

```
Switch-1(config)#interface vlan 10
Switch-1(config-if)#ip address 10.0.10.2 255.255.255.0
```



```
Switch-2(config)#interface vlan 10
Switch-2(config-if)#ip address 10.0.10.3 255.255.255.0
```

# Configuration du protocole HSRP

- ▶ Pour la configuration d'HSRP, nous devons choisir une IP virtuelle, et une priorité.

```
Switch-1(config-if)#standby 1 ip 10.0.10.1
Switch-1(config-if)#standby 1 priority 150
```

- ▶ Cette option permet au Switch actif de reprendre son rôle après une panne

```
Switch-2(config-if)#standby 1 ip 10.0.10.1
Switch-2(config-if)#standby 1 preempt
```

- ▶ Afin de rendre la bascule plus rapide, nous pouvons modifier les Timers HSRP:

```
Switch-1(config-if)#standby 1 timers msec 150 msec 600
```

# Le protocole VRRP: Protocole de Routage Virtuel Redondant

## ▶ Introduction

- VRRP est un protocole standard permettant d'assurer la haute disponibilité de la passerelle d'un réseau
- Master (Actif en HSRP)
- Backup (Standby en HSRP)
- Contrairement à HSRP, plusieurs peuvent avoir le rôle Backup

## ▶ Principe de fonctionnement

- Par défaut la priorité égale à 100
- Les messages VRRP sont envoyés sur l'IP de multicast 224.0.0.18
- L'adresse Mac virtuelle de la passerelle est 00-00-5E-00-01-XX
- Les Timers VRRP
  - Hello Timer = 1s
  - Dead Timer = (3\*Hello) + skew Timer
  - Skew Timer = (256-Priorité du Routeur)/256

# Principe de fonctionnement de VRRP

- ▶ En VRRP l'IP virtuelle peut être configurée directement sur l'interface du routeur Master.
- ▶ En HSRP il faut 3 IP : une pour R1, une pour R2, et une pour l'IP virtuelle
- ▶ En VRRP il n'en faut que 2 : une pour le Master (qui sera l'IP virtuelle) et une pour R2
- ▶ Par contre nous pouvons aussi utiliser 3 IP, à la manière d'HSRP

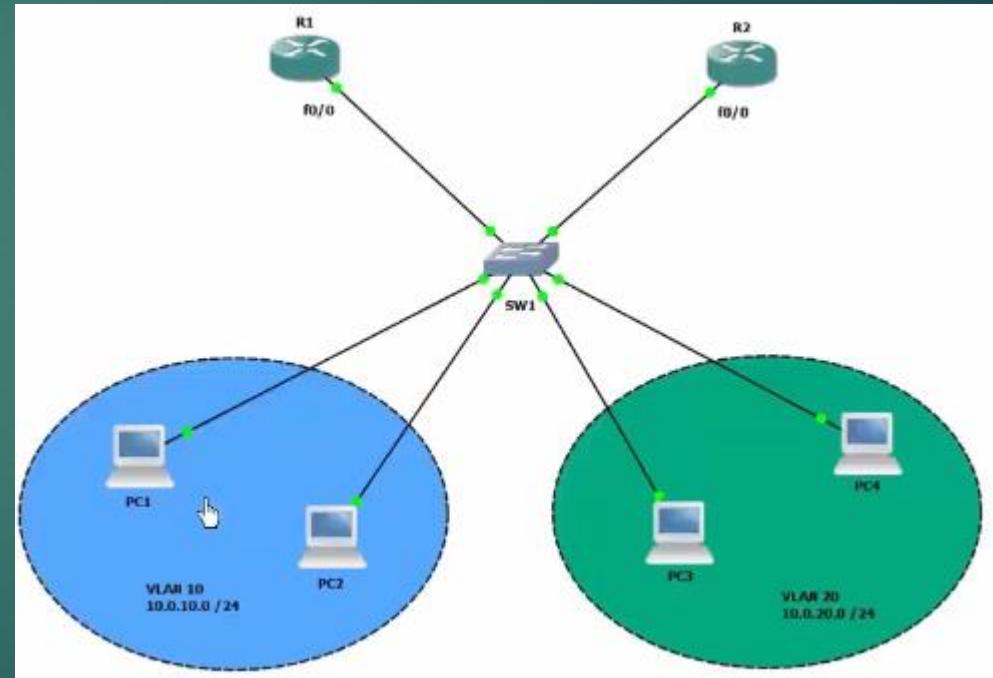
## ▶ Le protocole Global Load Balancing GLBP

### Introduction

- GLBP est un protocole Cisco permettant d'assurer la haute disponibilité de la passerelle d'un réseau
- L'avantage de GLBP est qu'il est capable de faire du Load Balancing
- En GLBP les routeurs peuvent avoir trois rôles :
  - AVG – Active Virtual Gateway
  - Standby AVG
  - AVF – Active Virtual Forwarders

# Le protocole GLBP Global Load balancing Protocol

- ▶ Principe du fonctionnement
  - L'AVG doit donc répondre aux requêtes ARP, de manière à repartir la charge entre les AVF
  - Le Standby AVG est le deuxième routeur avec la plus haute priorité. Il prendra la place de l'AVG en cas de panne de celui-ci
  - Les AVF sont les routeurs qui routent le trafic. Un AVG est aussi AVF
  - L'adresse de multicast utilisée est la suivante : 224.0.0.102

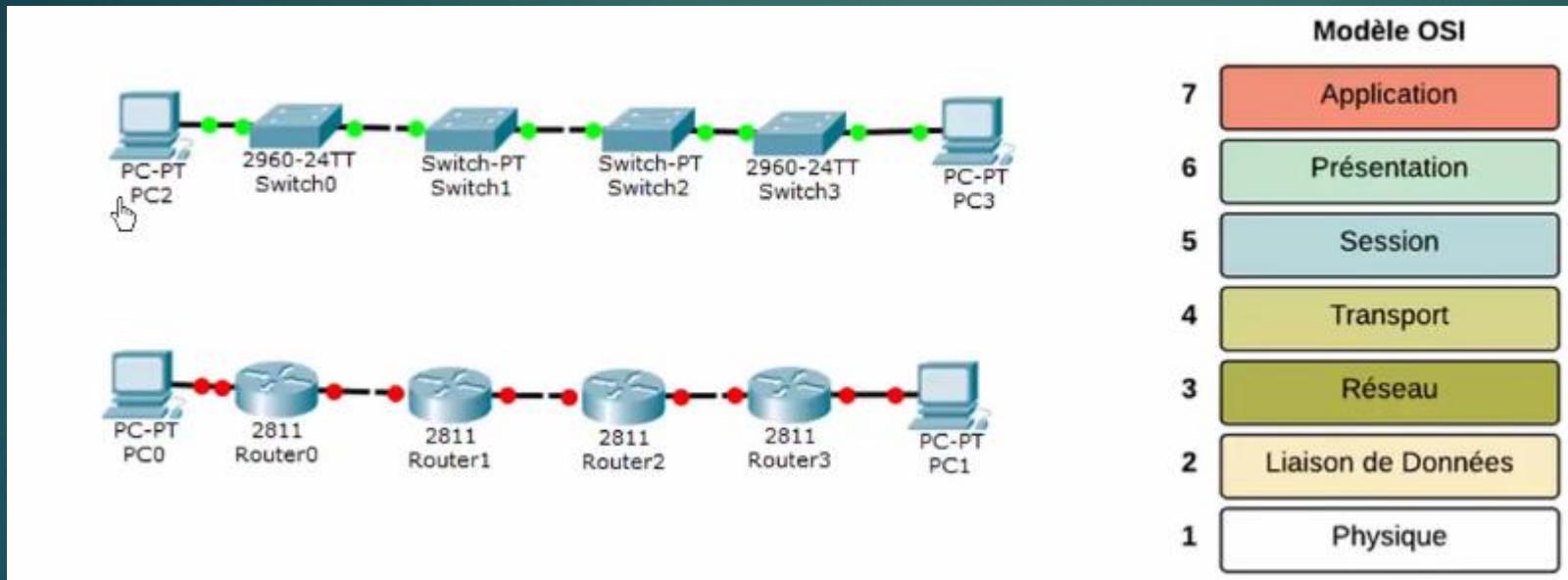


# Protocole GLBP

- ▶ Principe de fonctionnement
  - En GLBP il y a une IP virtuelle pour le groupe, et une adresse MAC par routeur
  - |            |          |           |
|------------|----------|-----------|
| 00.07.B4.0 | X.XX     | YY        |
| GLBP ID    | Group ID | Router ID |
  - L'adresse de Multicast utilisée est la suivante : 2240.0.102
- ▶ En GLBP, il existe 4 Timers :
  - Hello
  - Holdtime
  - Redirect time
  - Secondary holdtime

# Partie II : Routage

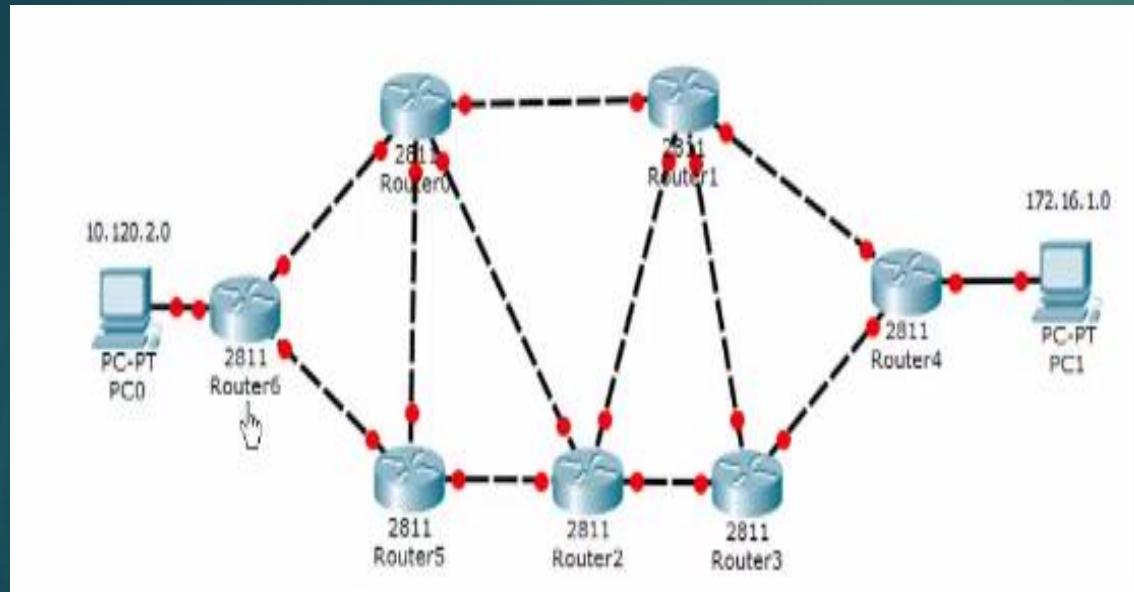
# Introduction au routage



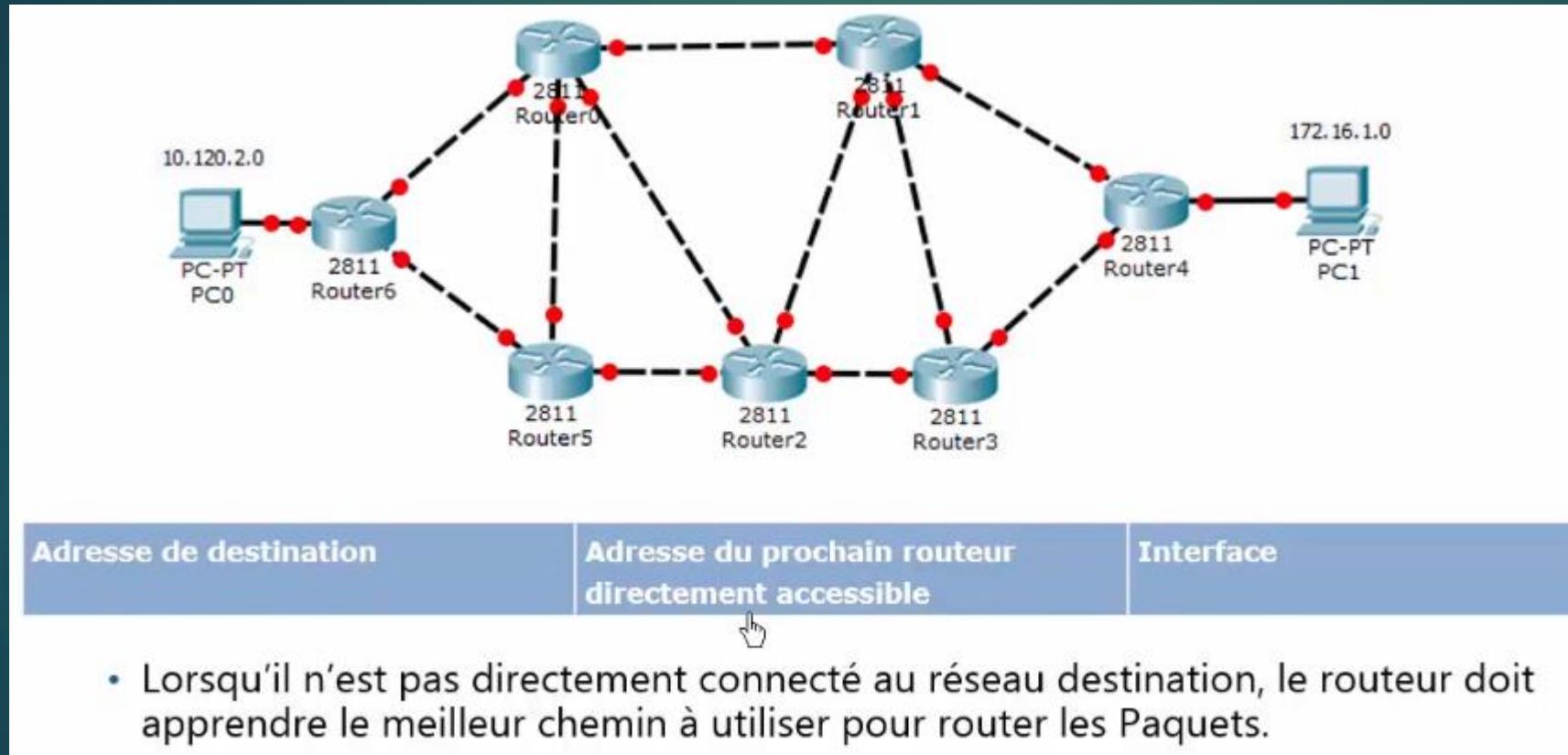
# Introduction au routage

▶ Pour router, un routeur doit :

- Connaitre l'adresse destination
- Identifier les sources d'informations sur le routage (autres routeurs)
- Découvrir les chemins possibles vers l'adresse destination
- Sélectionner le meilleur chemin
- Maintenir et vérifier les informations concernant le routage



# Introduction au routage



# Identifier le routage statique et le routage dynamique

## Route Statique

- Configurée (introduite dans la table de routage) manuellement par l'Administrateur.
- L'Administrateur Réseau doit mettre à jour les routes statiques manuellement en cas de changement

## Route Dynamique

- Ajustée automatiquement par le protocole de routage réseau.
- Le routeur apprend et maintient les routes dynamiques pour les destinations distantes en échangeant des mises à jour sur le routage avec les autres routeurs du *internetwork*.

# Introduction au routage

- ▶ Le protocole IGP et EGP
  - IGP (Interior Gateway Protocol) : protocole utilisé dans les systèmes autonomes
  - EGP (Exterior Gateway Protocol) : protocole permettant le routage entre différents systèmes autonomes
- ▶ Les protocoles vecteurs distance
  - Les protocoles distances vector s'échangent leur table de routage à l'aide d'update de routage. Ceux-ci contiennent les réseaux connus ainsi que leur masque si le protocole est Classless (qui comprend la notion de sous-réseaux).
  - La métrique d'un réseau est également transmise, elle représente la « distance » à laquelle se trouve le réseau

# Introduction au routage

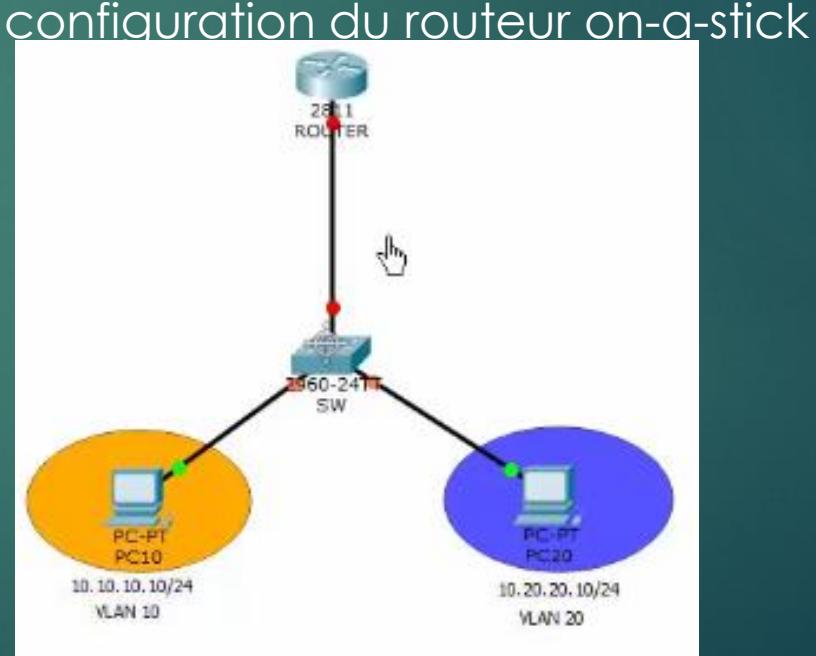
- ▶ Les protocoles vecteur distance
  - Si il existe plusieurs chemins pour une même destination, le protocole de routage utilise la meilleure métrique (la plus faible) pour choisir le chemin optimum
  - Le chemin optimum est alors intégré à la table de routage.
  - Exemple : le protocole RIP, le protocole IGRP

- ▶ Les protocoles état de liens
  - Les protocoles de routage **Link State** utilise l'algorithme **Shortest path First (SPF)**.
  - Cet Algorithme complexe permet une convergence rapide grâce a la construction d'une base de données topologique.
  - La base de données topologique représente la topologie du réseau.
  - Exemple : protocole OSPF

# Introduction au routage

- ▶ Les protocoles Advanced vecteur distance
  - Les protocoles de routages de type « distance vector » (vecteur de distance avancé)
  - Le fonctionnement global ressemble très fort à un protocole de type « distance vector »
  - Il dispose d'une série de caractéristiques que l'on retrouve dans les protocoles état de liens
  - Exemple : protocole EIGRP

- ▶ Routage inter-Vlan  
Solution Routeur on-a-stick



# Routage Inter-Vlan

## ► Cote Switch

```
Switch(config)#vlan 10
Switch(config-vlan)#name SUBNET-A
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name SUBNET-B
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/2 - 12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/13 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#int fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#^Z
Switch#
```

# Routage Inter-Vlan

## ► Cote routeur

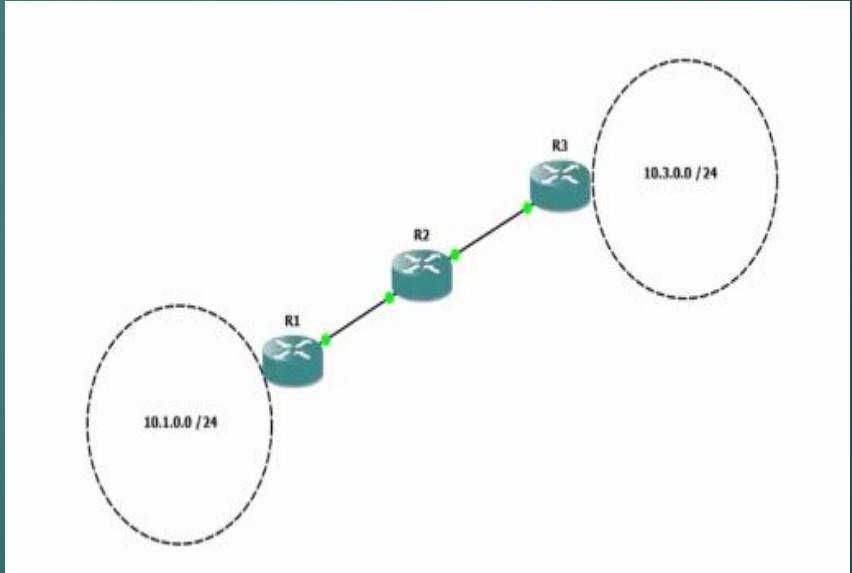
```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#^Z
Router#
```

# Introduction au protocole EIGRP

57

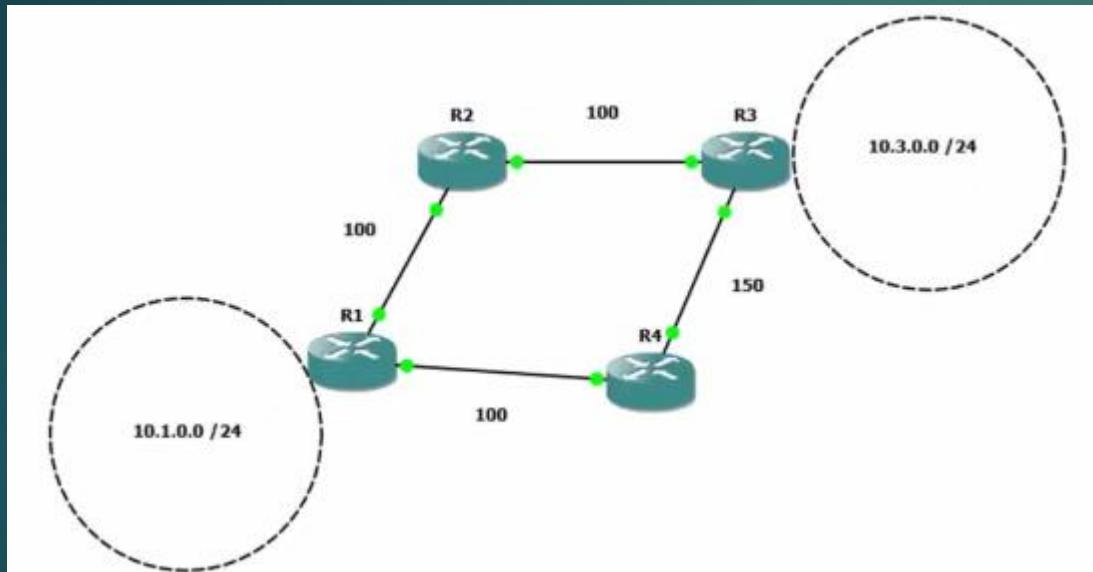
Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Introduction
  - Propriétaire Cisco
  - IGP (routage interne à un AS)
  - Distance administrative : 90 (170 pour les routes externes)
  - Utilise le protocole RTP pour communiquer
  - Supporte le VLSM
  - Utilise 224.0.0.10 pour communiquer
  - Routage multi protocole (IP, IPX, Apple Talk)
- ▶ EIGRP est un protocole à vecteur distance



# Introduction au protocole EIGRP

## ► Unequal Cost Load Ballancing



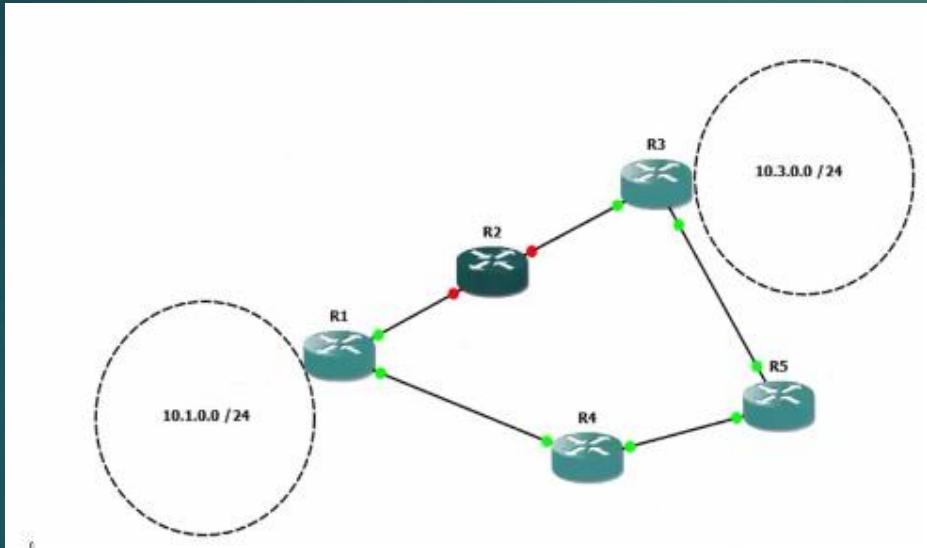
## ► Les messages EIGRP

- Hello : Créer et entretenir les relations de voisinage. Toutes les 5 secondes. 3 Hello sans réponse = voisin Down. Envoyé sur 224.0.0.10
- Update : MAJ de routage. Envoyée en cas de changement. Seul le changement est inclus
- Query : demande de route pour une destination. Si un routeur ne peut pas répondre, il transmet la Query pour les voisins
- Reply : Ce Reply va indiquer que la destination recherchée peut être jointe en passant par ce routeur
- Ack : Accuse de réception des Updates, Query et Reply

# Introduction au protocole EIGRP

59

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



## ▶ La métrique EIGRP

- K1 : Bande passante (utilisé par défaut)
- K3 : délai (utilisé par défaut)
- K2 et K4 : fiabilité
- K5 : charge

Le MTU est annoncée, mais n'est pas utilisée dans le calcul de la métrique

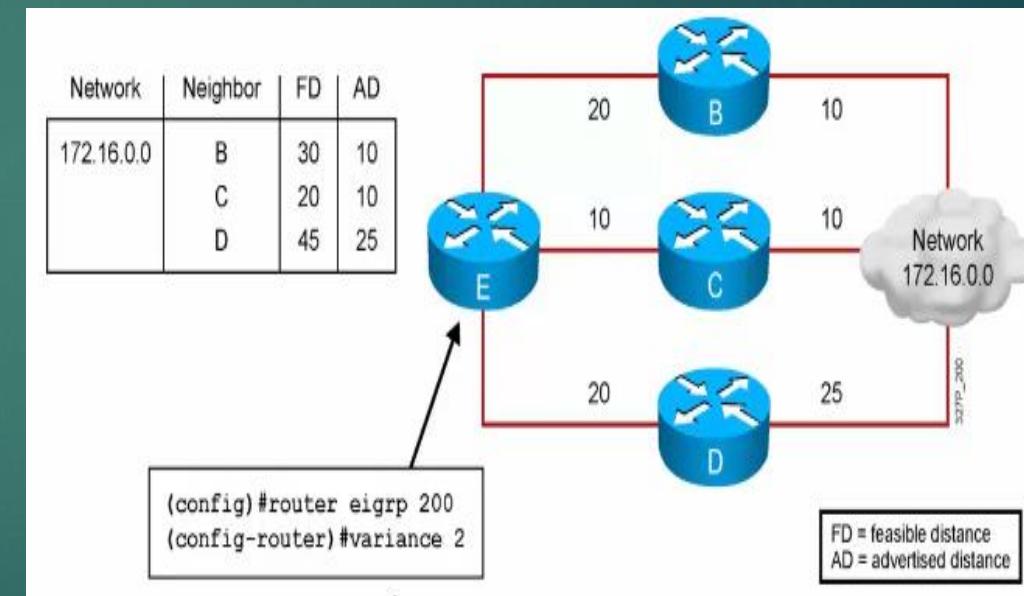
# Fonctionnement du protocole EIGRP

- ▶ Calcul de la métrique du protocole EIGRP
- Métrique composite

Formule composite par défaut :  
 métrique = [K1\*bande passante + K3\*délai]

Formule composite complète :  
 métrique = [K1\*bande passante + (K2\*bande passante)/(256 - charge) + K3\*délai] \* [K5/(fiabilité + K4)]

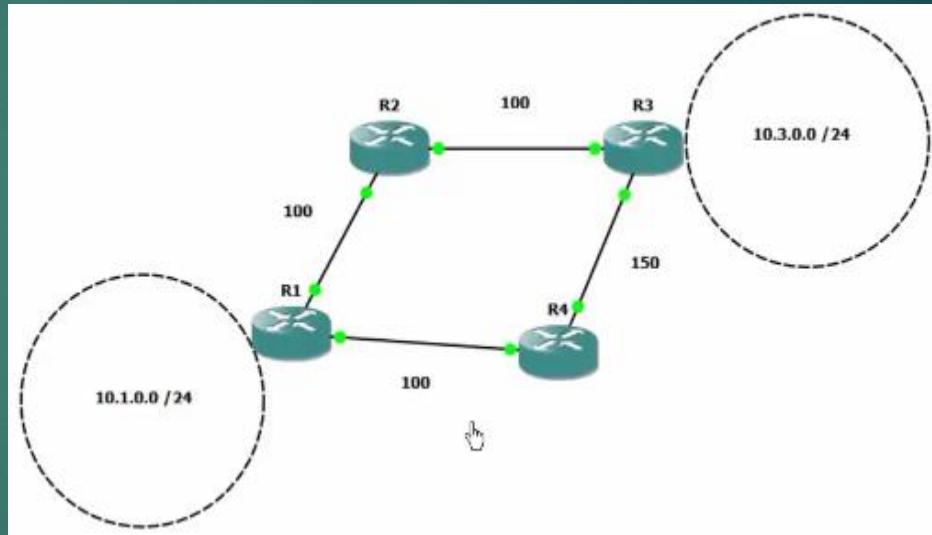
(Non utilisée si les valeurs « K » sont nulles)



# Terminologie du protocole EIGRP

- ▶ Feasible Distance – FD : métrique totale la plus faible, pour joindre la destination.
- ▶ Avertised Distance – AD : métrique annoncée par le voisin, pour joindre une destination.

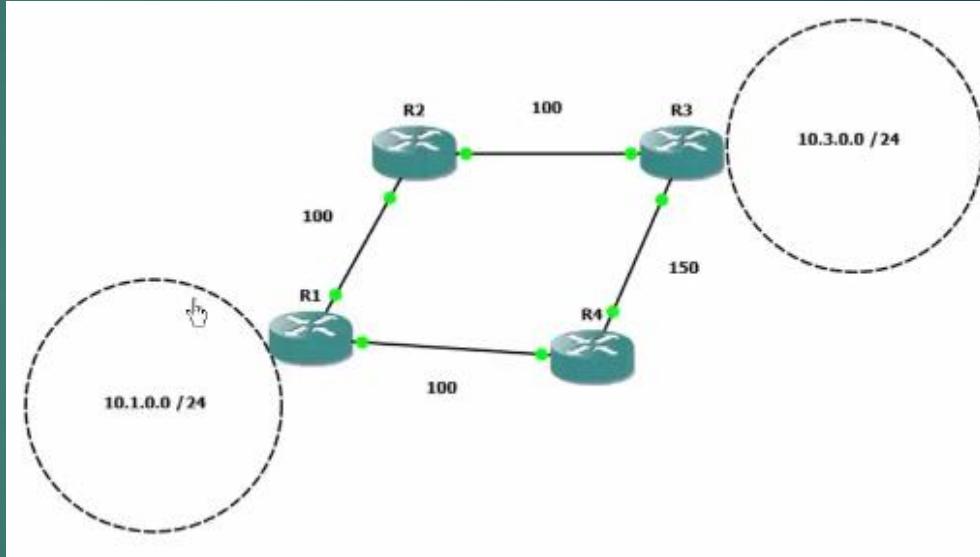
## ▶ La Feasible distance



# Terminologie du protocole EIGRP

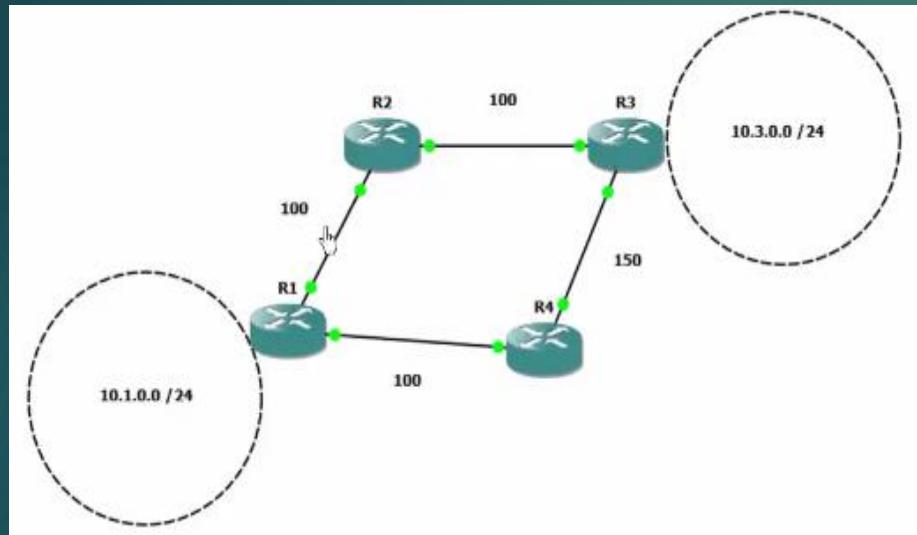
- ▶ Successor : le voisin que l'on utilise pour joindre une destination.
- ▶ Feasible Successor - FS : successor de secours pour une destination. Pour devenir FS, il faut avoir une AD plus faible que la FD du successor.

## ▶ Le Successor



# Terminologie du protocole EIGRP

## ► La Feasible Successor



- Pour devenir FS, il faut avoir une AD (Advertised Distance) plus faible que la FD (Feasible Distance) du Successor.

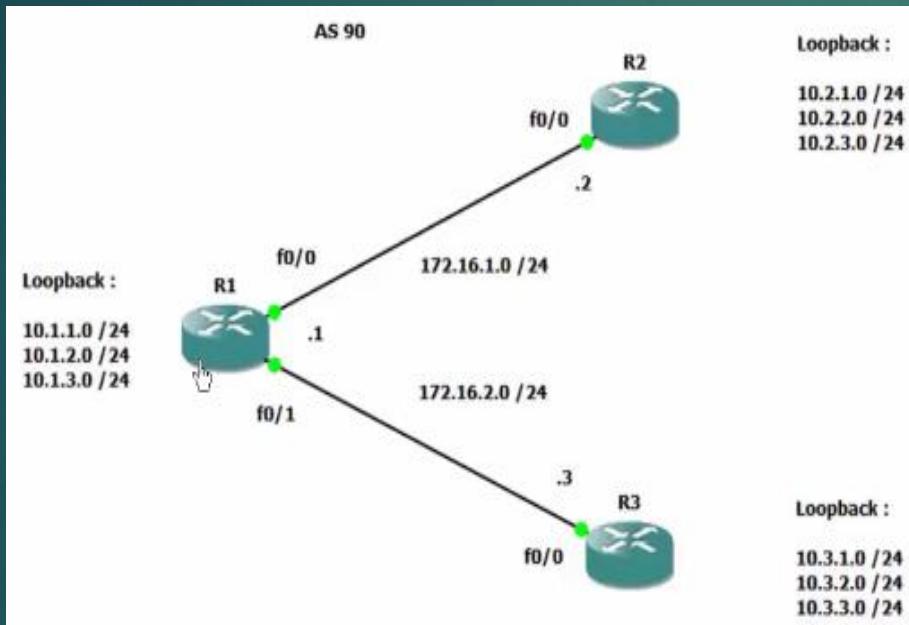
## ► Les tables du protocole EIGRP

Il existe trois tables en EIGRP :

- ✓ La Neighbor Table
- ✓ La Topology Table
- ✓ La Routing Table

# Les Tables du protocole EIGRP

## ► La Neighbor Table

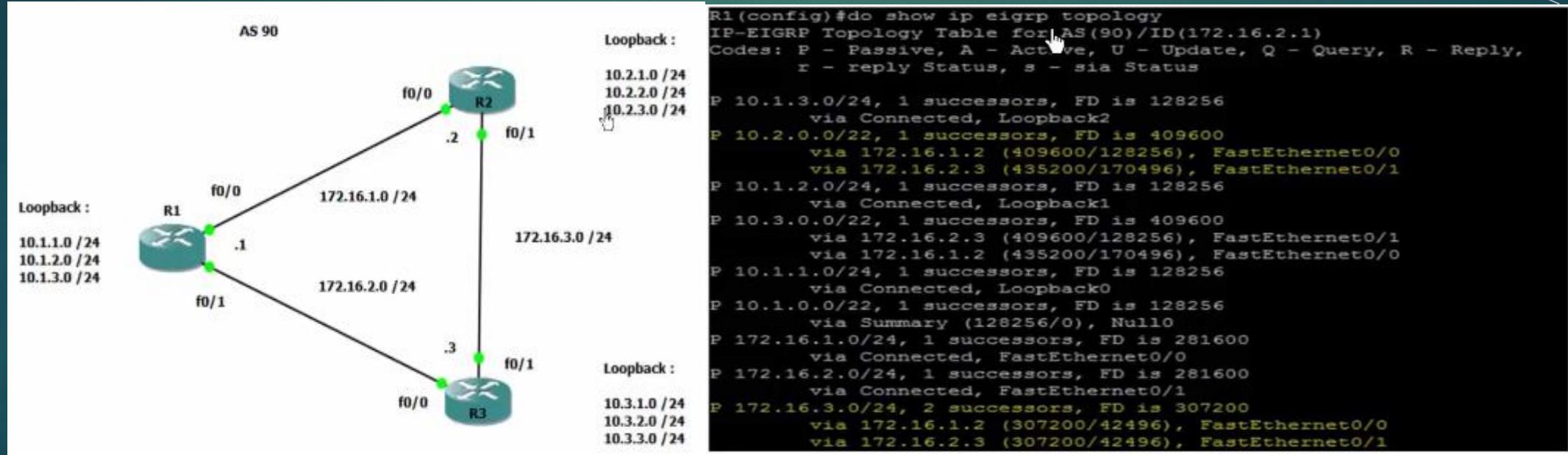


## ► La Neighbor Table

R1#show ip eigrp neighbors							
IP-EIGRP neighbors for process 90							
	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO Q	Seq Cnt	Num
1	172.16.2.3	Fa0/1	14 00:10:10	66	396	0	7
0	172.16.1.2	Fa0/0	13 00:10:40	88	528	0	6

# Les Tables du protocole EIGRP

## ► La Topology Table



# Les tables du protocole EIGRP

## ► La Table de routage

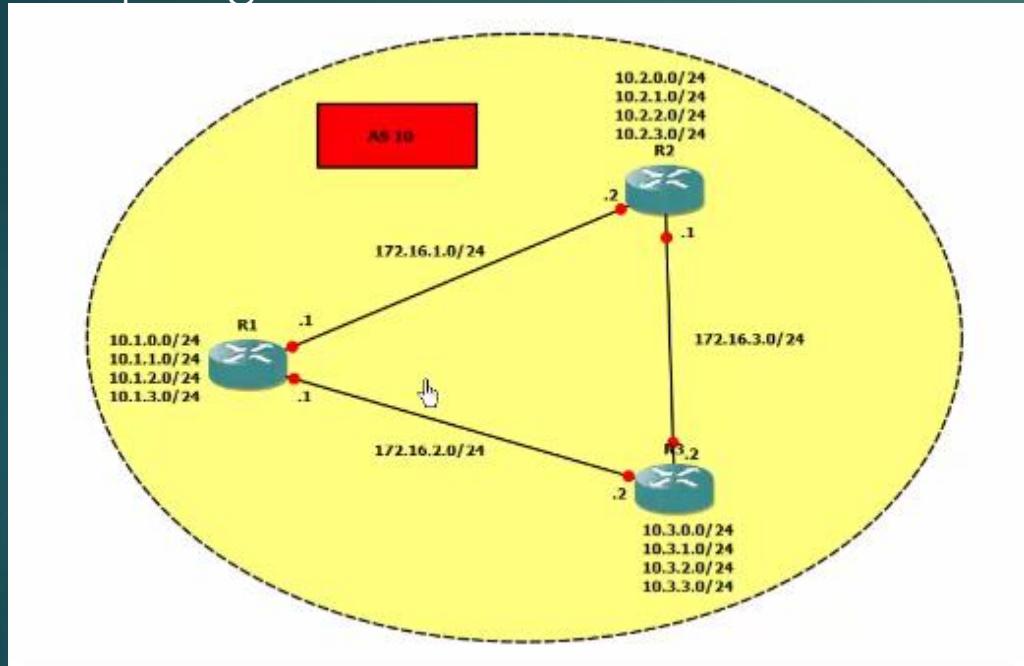
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  172.16.0.0/24 is subnetted, 3 subnets
    C 172.16.1.0 is directly connected, FastEthernet0/0
    C 172.16.2.0 is directly connected, FastEthernet0/1
    D 172.16.3.0 [90/307200] via 172.16.2.3, 04:45:56, FastEthernet0/1
       [90/307200] via 172.16.1.2, 04:45:56, FastEthernet0/0
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
    D 10.2.0.0/22 [90/409600] via 172.16.1.2, 04:43:14, FastEthernet0/0
    C 10.1.3.0/24 is directly connected, Loopback2
    D 10.3.0.0/22 [90/409600] via 172.16.2.3, 04:42:41, FastEthernet0/1
    C 10.1.2.0/24 is directly connected, Loopback1
    C 10.1.1.0/24 is directly connected, Loopback0
    D 10.1.0.0/22 is a summary, 04:51:22, Null0
```

# Configuration du protocole EIGRP

## ► Topologie à utiliser



## ► Résumé des routes automatique

- Désactiver le résumé automatique de routes
- Le résumé de route est une bonne chose, mais il est préférable de la faire soi-même.

```
R1(config-router)#no auto-summary
```

# Résumé des routes

- ▶ Résumé des routes manuel
- Le but est que les routeurs n'annoncent plus tous les réseaux 10.0.0.0/8

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip summary-address eigrp 90 10.1.0.0 255.255.252.0
```

- ▶ Configuration de base

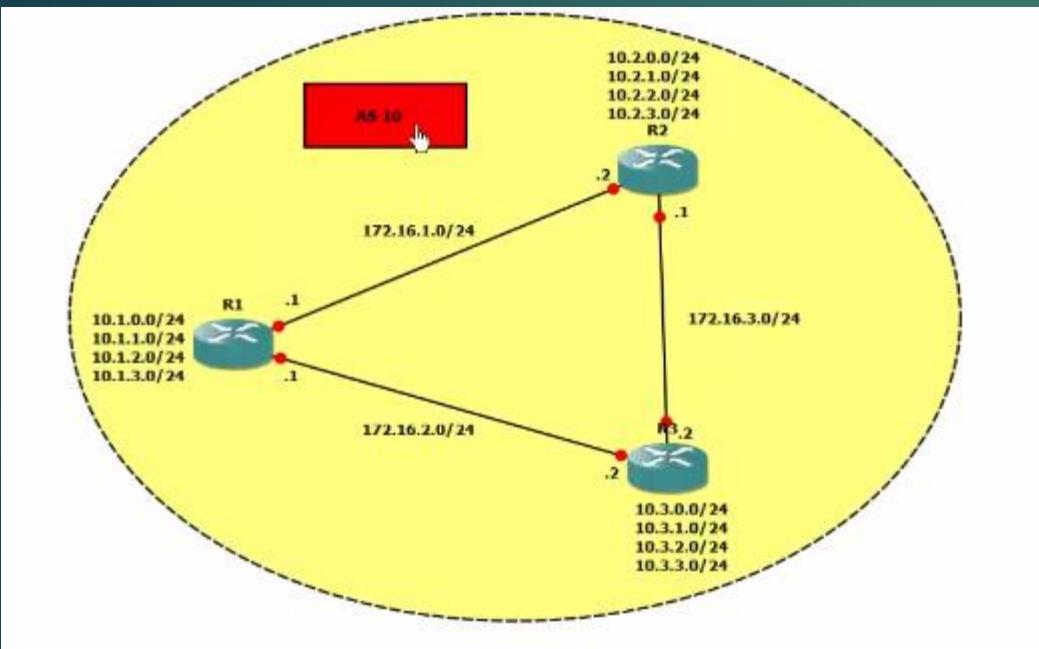
```
R2(config)#router eigrp 90
R2(config-router)#no auto-summary
R2(config-router)#network 172.16.1.2 0.0.0.0
R2(config-router)#network 172.16.3.2 0.0.0.0
```

```
R1(config)#router eigrp 90
R1(config-router)#network 192.168.150.0
```

255	255	255	255
-	255	255	255
0	0	0	255

# Optimisation du protocole EIGRP

## ► Topologie à utiliser



## ► Passive Interface

Le détail des fonctionnalités d'une Passive Interface

- N'envoie pas des MAJ de routage
- N'envoie pas de Hello, donc pas de relation de voisinage
- Ignore les MAJ et Hello entrant
- Si l'interface est inclue dans une commande « Network », le réseau auquel elle appartient est toujours annoncé dans les MAJ (mais pas par cette interface).

# Optimisation du protocole EIGRP

71

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Configuration du passive interface
- ▶ Pour plus de sécurité, et pour une configuration plus simple, le mieux est de mettre toutes les interfaces en mode Passive, sauf celles choisies.

```
R1(config)#router eigrp 90
R1(config-router)#passive-interface loopback 0
```



```
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface fastEthernet 0/0
R1(config-router)#no passive-interface fastEthernet 0/1
```

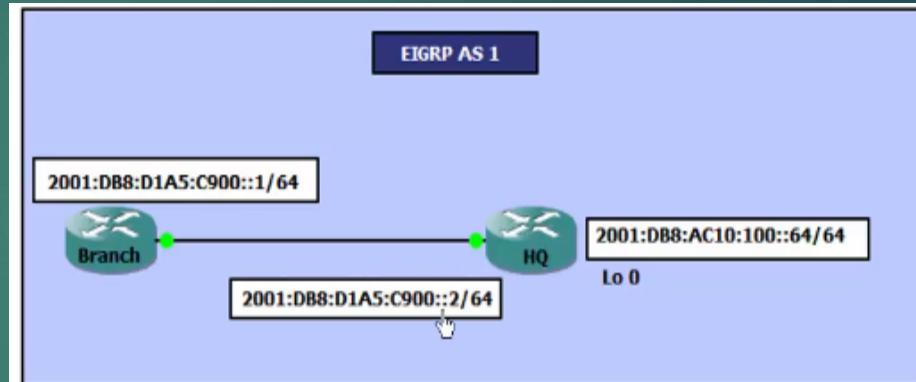
- ▶ Load Ballancing
- EIGRP permet de faire du Load Balancing en utilisant des liens de métrique égales (par défaut)
- EIGRP propose de faire de l'Unequal Load Balancing

```
R1(config)#router eigrp 90
R1(config-router)#variance 2
```

# Configuration du protocole EIGRP en IPv6

- ▶ Caractéristiques du protocole EIGRP en IPv6
  - Facile à configurer
  - Protocole Advanced distance vector
  - Mise à jour incrémentée
  - Utilise le Multicast
  - Métrique composé
  - Load Balancing
  - Table des voisins
  - Table topologique
  - Table de routage

- ▶ Topologie à utiliser



# Configuration du protocole EIGRP en IPv6

- ▶ Activation du protocole EIGRP avec de l'IPv6

```
Router(config)#ipv6 unicast-routing  
  
Router(config)#ipv6 router eigrp 1  
  
Router(config-if)#ipv6 eigrp 1  
Router(config-if)#no shutdown
```

- ▶ Exemple de configuration

```
Branch(config)#ipv6 router eigrp 1  
Branch(config-router)#exit  
Branch(config)#interface GigabitEthernet0/1  
Branch(config-if)#ipv6 eigrp 1  
  
HQ(config)#ipv6 router eigrp 1  
HQ(config)#exit  
HQ(config)#interface GigabitEthernet0/0  
HQ(config-if)#ipv6 eigrp 1  
HQ(config-if)#exit  
HQ(config)#interface GigabitEthernet0/1  
HQ(config-if)#ipv6 eigrp 1
```

# Configuration du protocole EIGRP en IPv6

## ► Vérification de la configuration

```
Branch#show ipv6 eigrp interfaces
```

EIGRP-IPv6 Interfaces for AS(1)

Interface	Xmit Peers	Queue Un/Reliable	PeerQ Un/Reliable	Mean Un/Reliable	Pacing SRTT	Multicast Un/Reliable	Pending Flow Timer Routes
Gi0/1	1	0/0	0/0	9	0/0	50	0

```
Branch#show ipv6 eigrp neighbors
```

EIGRP-IPv6 Neighbors for AS(1)

H	Address	Interface	Hold (sec)	Uptime (ms)	SRTT (ms)	RTO	Q Cnt	Seq Num
O	Link-local address: FE80::FE99:47FF:FE00:1	Gi0/1	12	00:20:48	9	100	0	2

## ► Vérification de la configuration

```
Branch#show ipv6 eigrp topology
```

EIGRP-IPv6 Topology Table for AS(1)/ID(209.165.201.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
 r - reply Status, s - sia Status

P 2001:DB8:D1A5:C900::/64, 1 successors, FD is 28160  
 via Connected, GigabitEthernet0/1

P 2001:DB8:AC10:100::/64, 1 successors, FD is 156160  
 via FE80::FE99:47FF:FE00:1 (156160/128256), GigabitEthernet0/1

```
Branch#show ipv6 route eigrp
```

IPv6 Routing Table - default - 4 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP

external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D 2001:DB8:AC10:100::/64 [90/156160]

via FE80::FE99:47FF:FE00:1, GigabitEthernet0/1

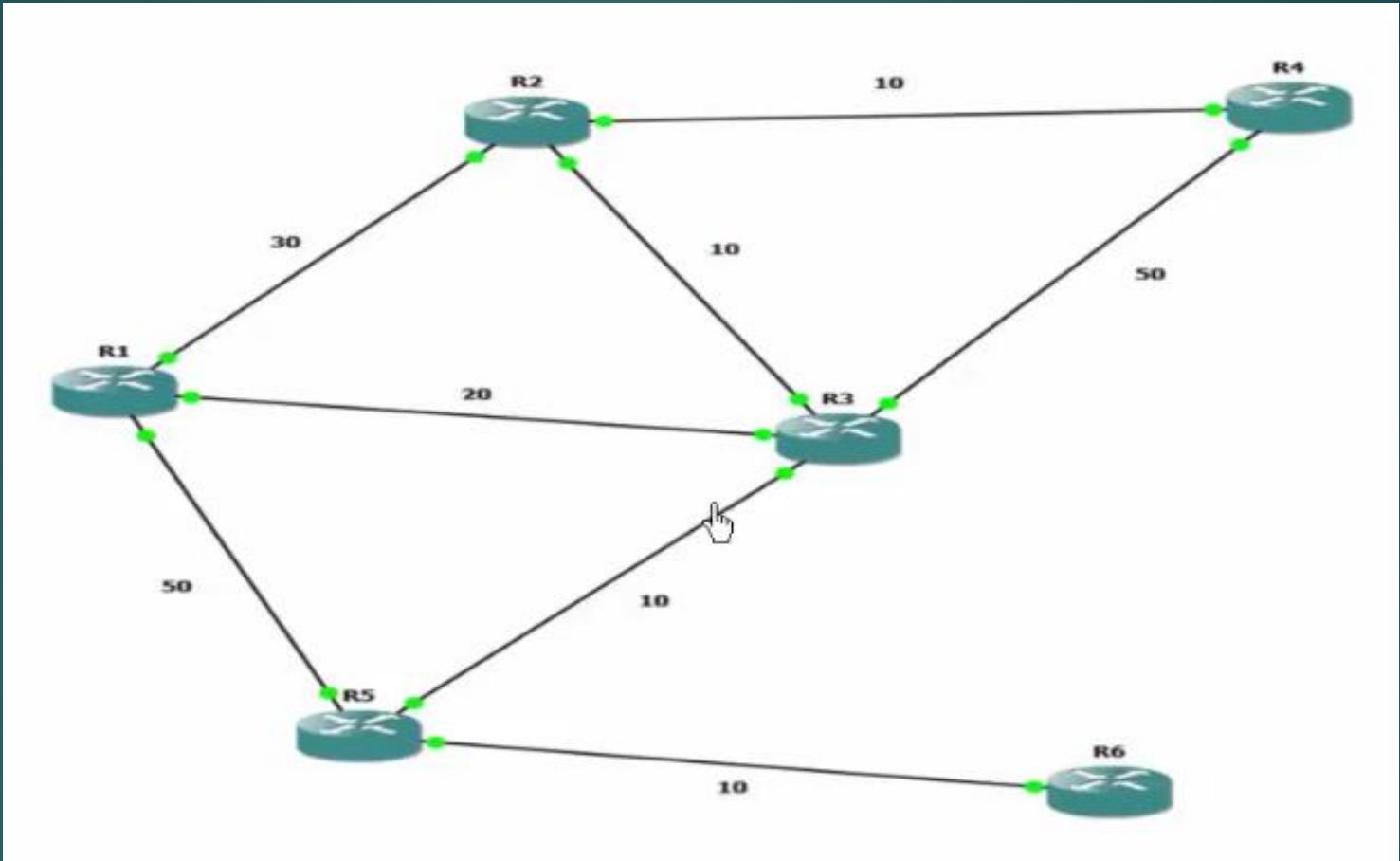
# Introduction au protocole OSPF

75

- ▶ Introduction
  - OSPF est protocole Standard (interopérable)
  - Convergence très rapide
  - Adapte aux grands réseaux (pas de limite de saut, etc...)
  - Faible utilisation de la bande passante
  - Distance administrative : 110
  - Supporte le VLSM
- ▶ OSPF est un protocole à état de lien.
  - L'Algorithm de Dijkstra est utilisé par OSPF pour trouver le plus court chemin
  - Tous les routeurs connaissent la topologie complète du réseau

# Introduction au protocole OSPF

76



# Introduction au protocole OSPF

77

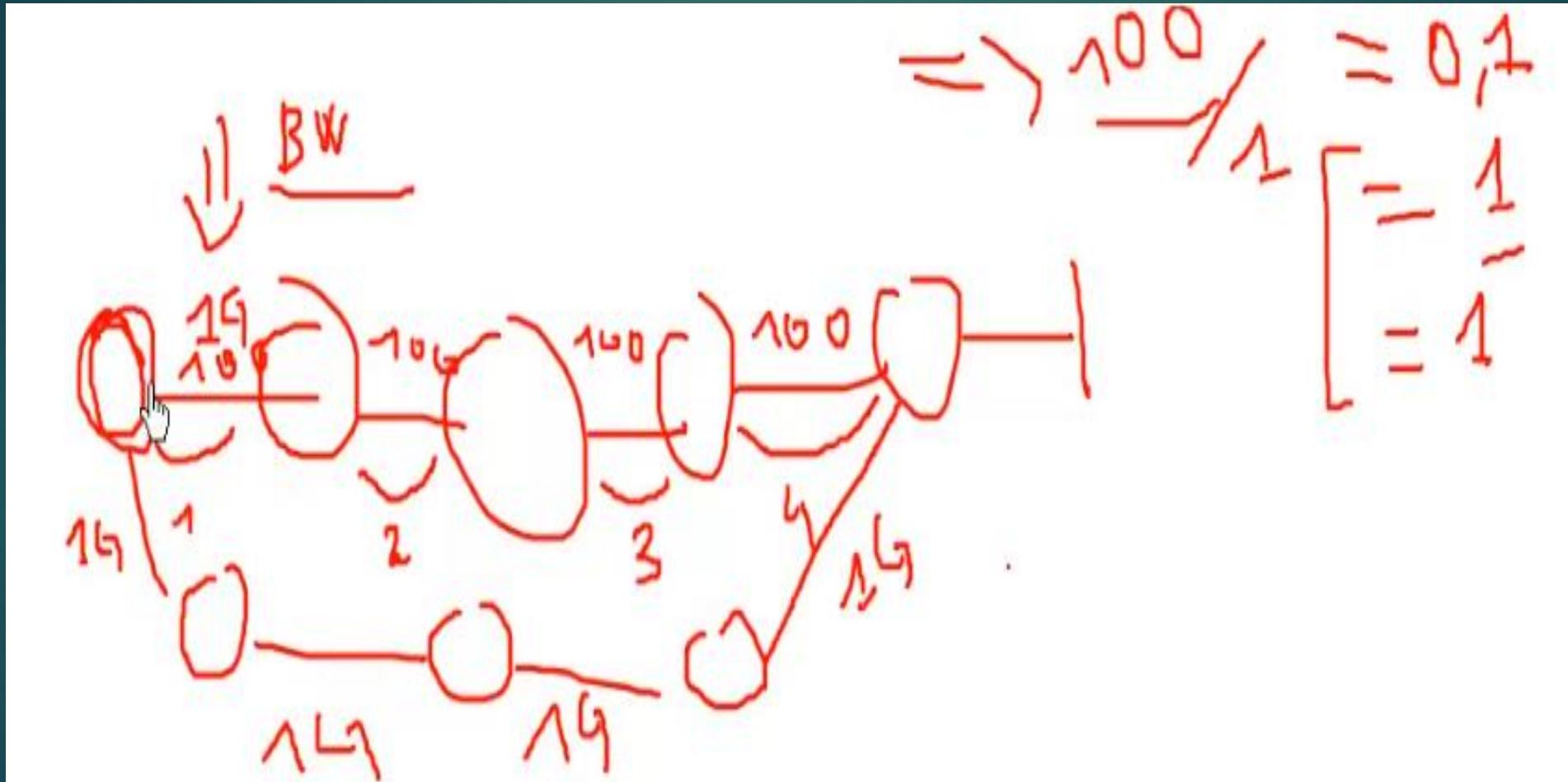
Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Le calcul du cout (la métrique) : 100 000 Kbps/bande passante du lien (en Kbps)
- ▶ La valeur la plus faible est 1
- ▶ Il est possible de modifier le calcul de la formule en cas de lien ayant une bande passante supérieure à 100 Mbps
- ▶ Les messages OSPF
  - Hello : Créer et entretenir les relations de voisinage. Toutes les 10 secondes. Toutes les 30 secondes sur un réseau NBMA
  - Le DBD – Data Base Description
  - Le LSR – Link State Request
  - Le LSA – Link State Advertisement
  - Le LSU – Link State Update

# Introduction au protocole OSPF

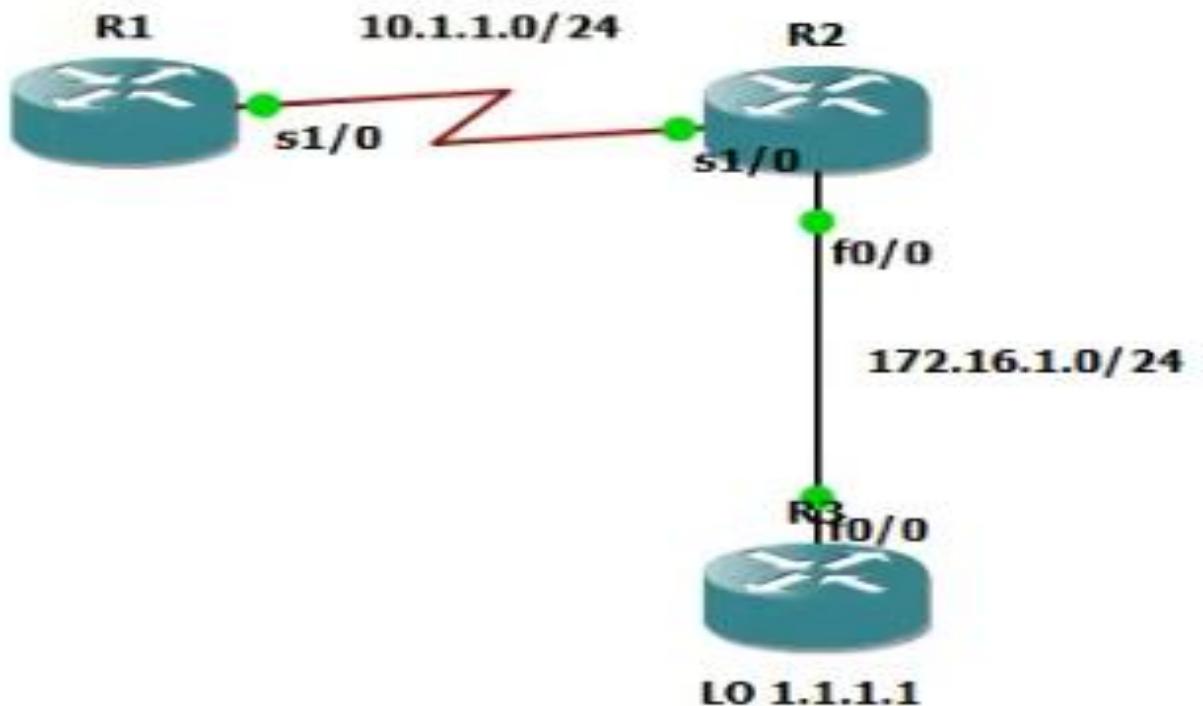
78

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



# Introduction au protocole OSPF:

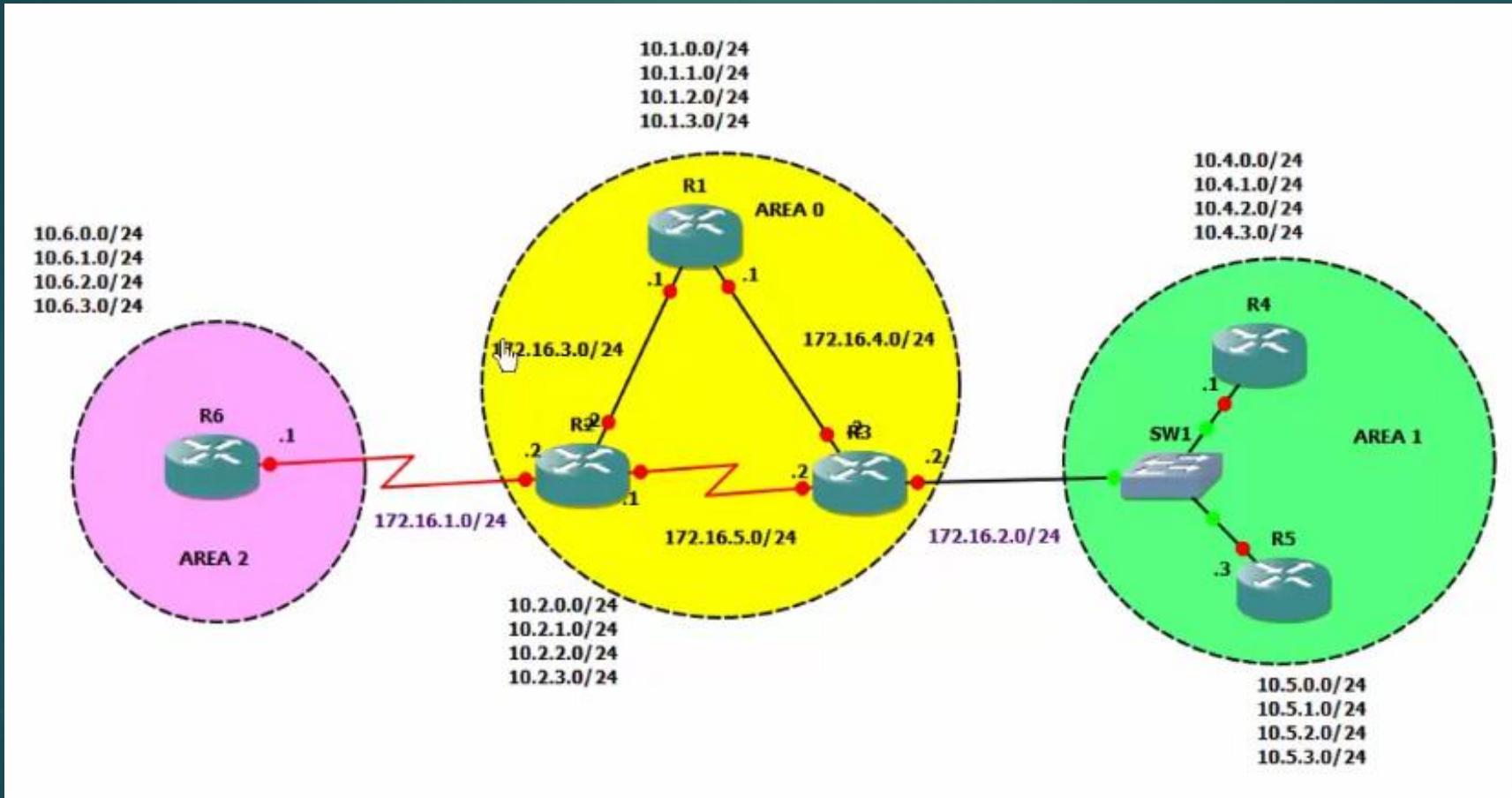
## Le calcul du cout (la métrique)



# Les zones OSPF

- ▶ Les messages Hello
  - L'ID du routeur
  - Le Netmask (masque de sous réseau)\*
  - L'ID de l'area\*
  - La liste de voisin
  - La priorité du routeur (élection maître esclave, élection DR / BDR)
  - L'IP du DR et du BDR
  - La password (si configuré)\*
- ▶ Les zones OSPF
  - OSPF introduit la notion d'area
  - Alléger le processus OSPF
  - Dans chacune des zones, tous les routeurs se connaissent
  - Le routeur ne connaît que la topologie de sa propre zone
  - Il est important que l'adressage soit hiérarchique
  - Il faut aussi que toutes les zones soient connectées à la zone 0

# Les zones OSPF



# Les zones OSPF

- ▶ Types de routeurs dans le protocole OSPF
  - **Internal** : les routeurs interne
  - **ABR** : Area Border Router
  - **ASBR** : Autonomous System Border Router.
- ▶ Types de packets LSA

Il existe plusieurs types de LSA :

  - **Type 1** : Décrit les interfaces d'un routeur
  - **Type 2** : décrit les routeurs connectés au segment. Envoyé par le DR sur les liens Broadcast
  - Type 3 : route de résumé envoyée dans une autre Area par l'ABR – Area Border Router
  - Type 4 : décrit l'ASBR – Autonomous System Border Router. Généré par l'ASBR et envoyé dans les autres zones. Permet de faire connaître le routeur ID dans d'autres zones.
  - Type 5 : Routes redistribuées par l'ASBR (route externes, type RIP, EIGRP, etc...)
  - Type 7 : comme le type 5, mais qui peut circuler dans une NSSA. Il est transformé en type 5 à la sortie de la NSSA.

# A retenir

- ▶ Utilise des zones : localiser les MAJ à la zone, réduire la taille de la topologie à connaître
  - ▶ Toutes les zones doivent être connectées à la zone 0
  - ▶ L'adressage doit être hiérarchique (pour le résumé entre les zones)
  - ▶ Internal Router
  - ▶ ABR : fait le lien entre plusieurs zones
  - ▶ ASBR : injecte des routes venant d'autres protocoles de routage
  - ▶ Plusieurs types de LSA
- 
- ▶ Fonctionnement du protocole OSPF
    - Les relations de voisinage en OSPF
    - ✓ Etape 1 : Déterminer son Routeur ID
    - ✓ Etape 2: ajout des interfaces au processus OSPF
    - ✓ Etape 3 : Envoie de message HELLO
    - ✓ Etape 4 : Réception d'un HELLO
    - ✓ Etape 5 : Envoie d'un REPLY HELLO
    - ✓ Etape 6 : Détermination du maître et de l'esclave
    - ✓ Etape 7 : Demande de détails sur la topologie
    - ✓ Etape 8 : Les voisins sont synchronisés

# Fonctionnement du protocole OSPF : les états d'une relation de voisinage

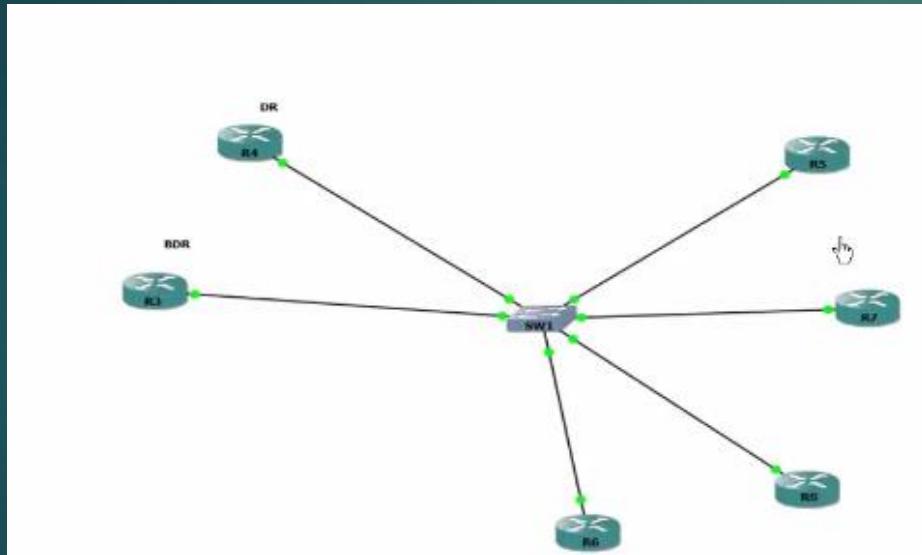
- ▶ Down : nous n'avons pas encore reçu de HELLO du voisin, mais nous essayons de le joindre
- ▶ Init : on reçoit un Hello du voisin, mais notre routeur n'est pas listé dans le champ Neighbors
- ▶ 2-Way : la relation est créée (notre routeur est liste dans le champ Neighbors). Election DR / BDR si nécessaire
- ▶ Exchange : Echange de DBD – Data Base Description
- ▶ Loading : Echange de LSU - Link State Update
- ▶ Full : Base de données synchronisées.

## ▶ OSPF dans un Réseau Multi Access

- Chaque relation va faire objet de multiple échanges (DBD, LSR, LSU, etc...).
- A chaque changement, beaucoup de message vont transiter
- Sur un réseau Multi-Access, le protocole OSPF peut engendrer un engorgement du réseau.
- Imaginer la même topologie avec 10 ou 20 routeurs.

La quantité de message transitant va probablement vite devenir problématique

# Fonctionnement du protocole OSPF : les états d'une relation de voisinage



Solution :

- OSPF propose donc d'élire un routeur comme DR – Designated Router
- Un autre comme BDR – Backup Designated Router.
- Celui qui gagne l' élection est celui qui a la priorité la plus élevée:
- En cas d'égalité c'est celui qui a l'ID du routeur de plus haut

# Fonctionnement du protocole OSPF : les états d'une relation de voisinage

- ▶ Forcer un routeur à devenir DR :

```
R4(config)#interface fastEthernet 0/0
R4(config-if)#ip ospf priority 200
```

- ▶ Par défaut la priorité est à 1
- ▶ Une priorité de 0 signifie que le routeur ne peut pas devenir le DR/BDR

```
R5(config)#interface fastEthernet 0/0
R5(config-if)#ip ospf priority 0
```

```
R3#clear ip ospf process
```

# Fonctionnement du protocole OSPF : les états d'une relation de voisinage

SOLUTION SYSTEM

- Les autres routeurs c'est les DROTHERS
- Quand un routeur souhaite envoyer une MAJ de routage, il l'envoie au DR et au BDR sur l'IP 224.0.0.6
- DR va renvoyer le message aux autres routeurs sur l'IP 224.0.0.5

## ► Les tables du protocole OSPF

Il existe trois tables en **OSPF** :

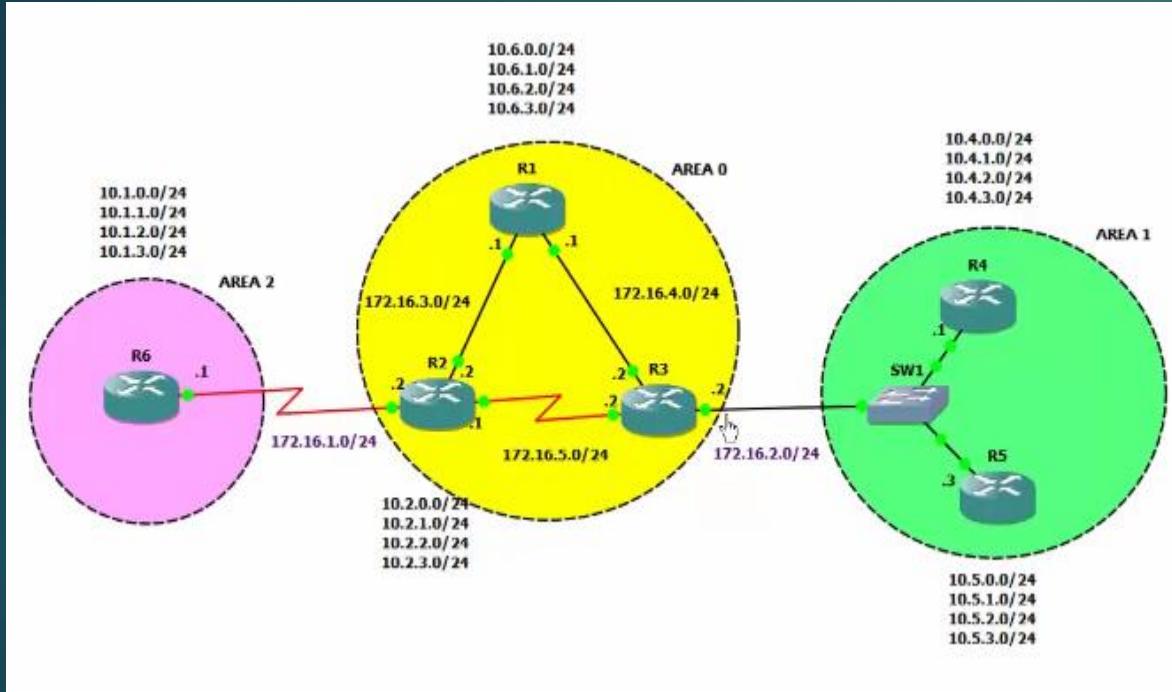
- ✓ La Neighbor **Table**
- ✓ La Topology **Table (LSDB)**
- ✓ La Routing **Table**

# Fonctionnement du protocole OSPF : les états d'une relation de voisinage

- En réseau Multi Access, élection DR/BDR
- DR/BDR : plus haute priorité, sinon plus haut Routeur ID
- MAJ envoyé par le DR sur 224.0.0.6
- MAJ redistribue par le DR sur 224.0.0.5
- Relation avec le DR / BDR : FULL
- Relation avec les DROTHERS : 2-Way.

# Configuration du protocole OSPF

## ► Topologie à utiliser



## ► Activation du protocole

- Single Area

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.16.1.1 0.0.0.0 area 0
R1(config-router)#network 172.16.2.1 0.0.0.0 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 172.16.1.2 0.0.0.0 area 0
R2(config-router)#network 172.16.3.2 0.0.0.0 area 0
R2(config-router)#network 10.0.0.0 0.0.3.255 area 0
```

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.3.3 0.0.0.0 area 0
R3(config-router)#network 172.16.2.3 0.0.0.0 area 0
```

# Configuration du protocole OSPF

- Multi Area

```
R2(config)#router ospf 1  
R2(config-router)#network 172.16.20.2 0.0.0.0 area 20
```

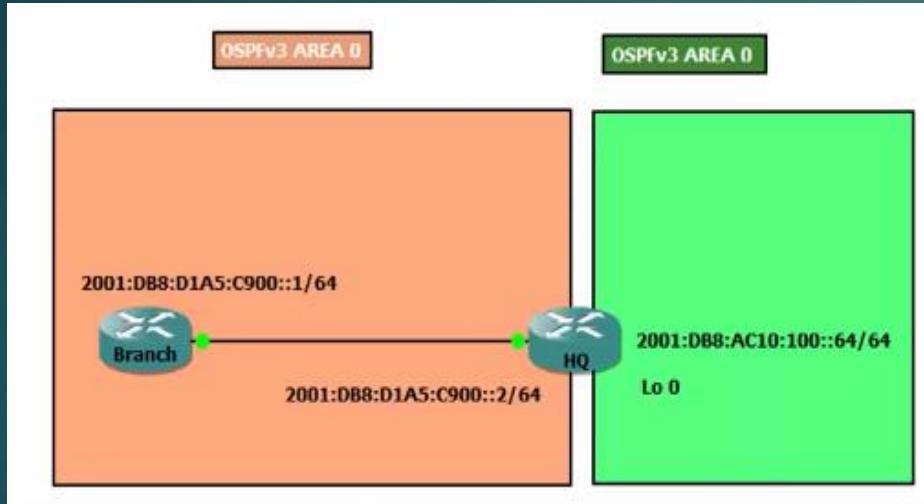
- ▶ Configuration du protocole OSPF en IPV6

## Caractéristiques du protocole **OSPFv3**

- OSPFv3 est une version de OSPF pour le IPv6
- OSPFv2 (Pour l'IPv4) et OSPFv3 (Pour l'IPv6) fonctionnent indépendamment
- OSPFv3 a les mêmes caractéristiques que l'OSPFv2
- Le routeur ID est sur 32 bit
- OSPFv3 est active par lien, et non pas par réseau
- OSPFv3 communique en utilisant des adresses multicast

# Configuration du protocole OSPF en IPv6

- Topologie à utiliser



- Configuration du protocole OSPF avec de l'IPv6

```
Branch(config)#ipv6 router ospf 99
Branch(config-rtr)#router-id 1.1.1.1
Branch(config-rtr)#exit
Branch(config)#interface GigabitEthernet0/1
Branch(config-if)#ipv6 address 2001:DB8:D1A5:C900::1/64
Branch(config-if)#ipv6 ospf 99 area 0

HQ(config)#ipv6 router ospf 99
HQ(config-rtr)#router-id 2.2.2.2
HQ(config-rtr)#exit
HQ(config)#interface Loopback0
HQ(config-if)#ipv6 address 2001:DB8:AC10:100::64/64
HQ(config-if)#ipv6 ospf 99 area 0.0.0.1
HQ(config-if)#exit
HQ(config)#interface GigabitEthernet0/1
HQ(config-if)#ipv6 address 2001:DB8:D1A5:C900::2/64
HQ(config-if)#ipv6 ospf 99 area 0.0.0.0
```

# Configuration du protocole OSPF en IPv6

► Vérification

```
Branch#show ipv6 ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Link Local Address FE80::21E:7AFF:FEA3:5E71, Interface ID 5
  Area 0.0.0.0, Process ID 99, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::21E:7AFF:FEA3:5E71
  Backup Designated router (ID) 2.2.2.2, local address
  FE80::21E:7AFF:FEA3:5F31
  <output omitted>
    Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  <output omitted>
```

```
Branch#show ipv6 ospf
  Routing Process "ospfv3 99" with ID 1.1.1.1
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  <output omitted>
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Reference bandwidth unit is 100 mbps
  Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
  <output omitted>
```

# Configuration du protocole OSPF en IPv6

```
Branch#show ipv6 ospf neighbor
```

OSPFv3 Router with ID (1.1.1.1) (Process ID 99)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	0	FULL/ -	00:00:37	6	Gi0/1

```
Branch#show ipv6 route ospf
```

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

OI 2001:DB8:AC10:100::64/64 [110/64]

via FE80::21E:7AFF:FEA3:5F31, GigabitEthernet0/1

# WAN

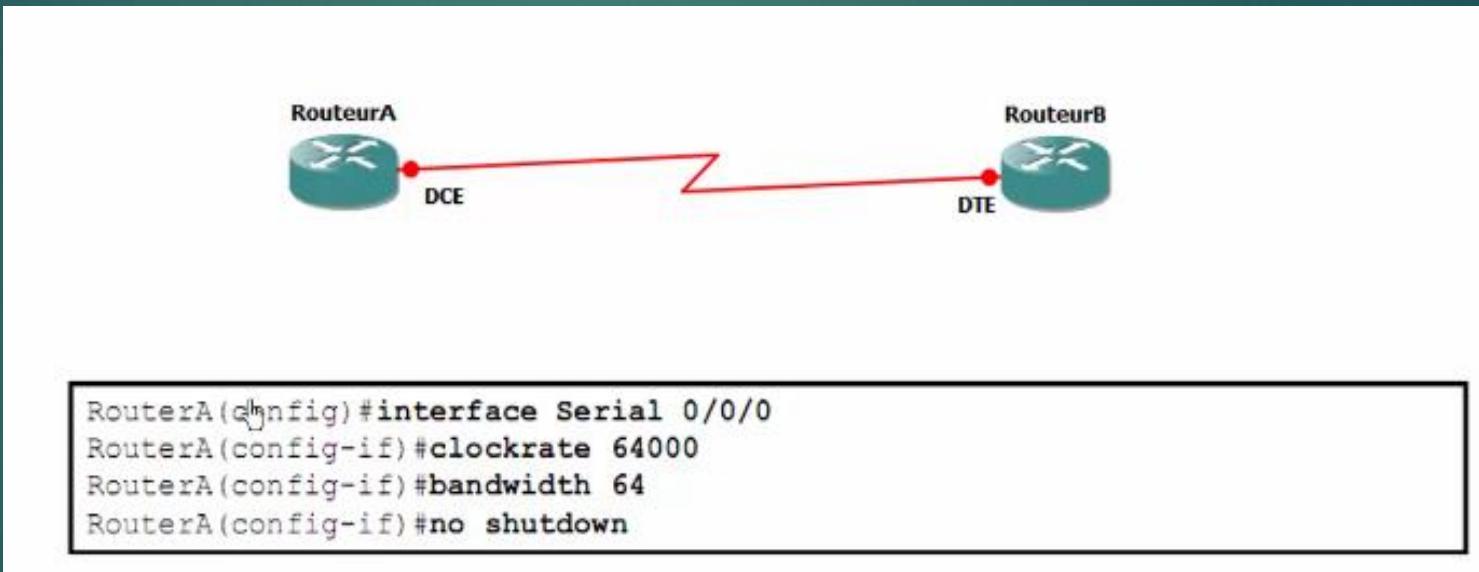
## LES PROTOCOLES HDLC ET PPP

# Configuration des interfaces serial

95

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ DCE Data Controller Equipment
- ▶ DTE Data Terminal Equipment



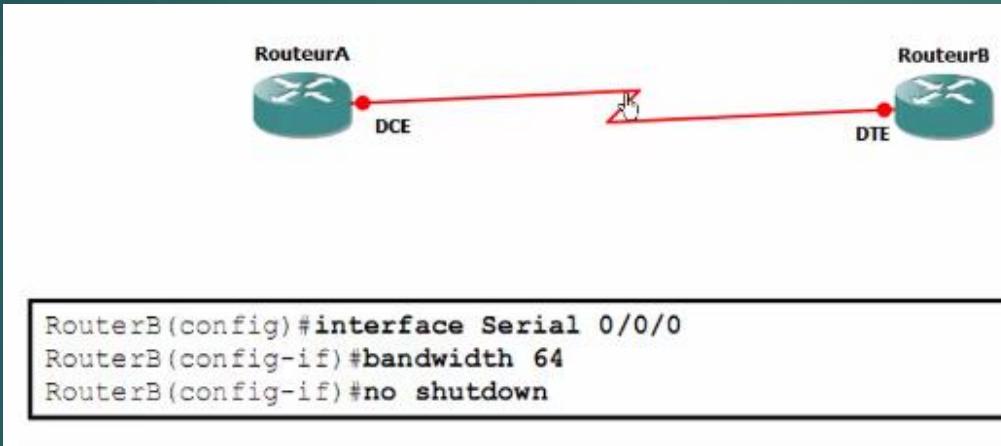
# Configuration des interfaces serial

96

Cours de CCNP : Network Fundamentals  
Katakpe Kossi Kuma  
28 February 2024

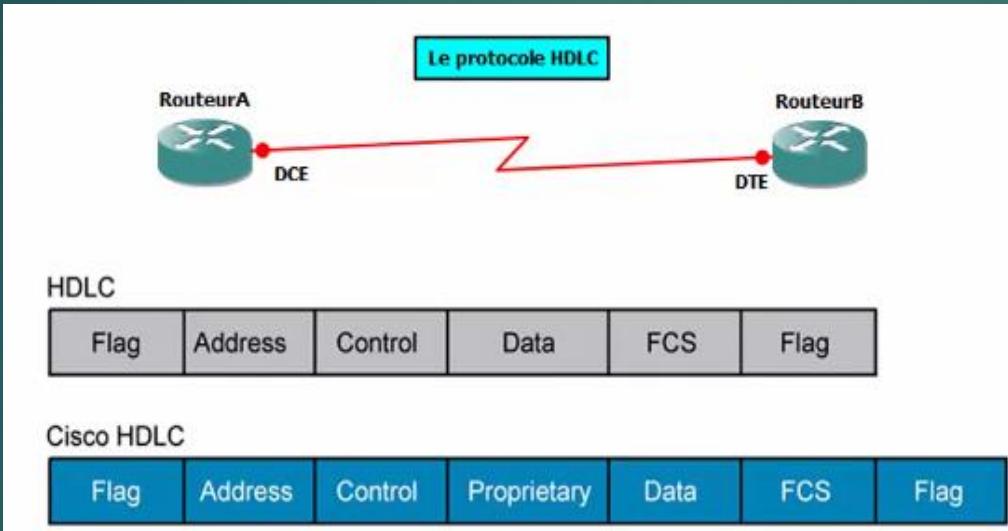
senté par

- ▶ Comment vérifier si l'interface est DTE ou DCE?



# Le protocole HDLC

- ▶ Utiliser comme protocole de la couche Liaison de données



- ▶ Par défaut c'est le protocole HDLC qui est active

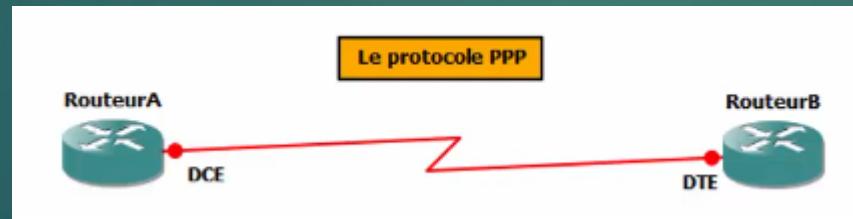
```

RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Description: Link to HQ
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
CRC checking enabled
Last input 00:00:02, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
<output omitted>

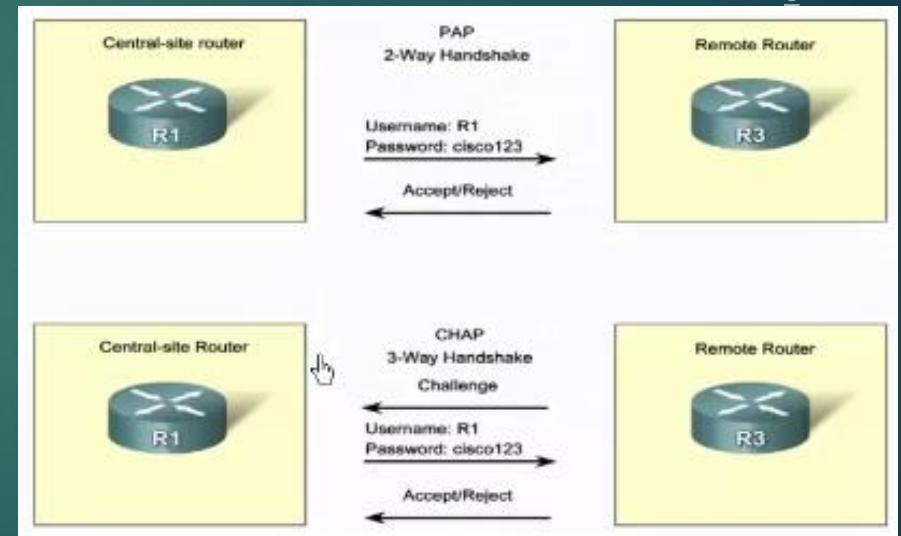
```

# Le protocole PPP

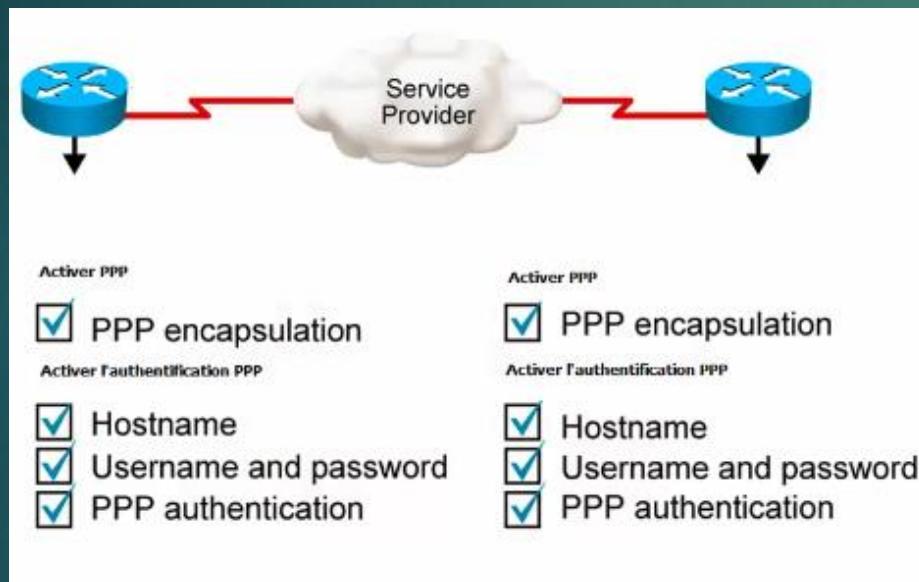
- ▶ PPP est un protocole standard
- ▶ PPP supporte l'authentification
- ▶ NCP (Network Control Protocol) qui sert d'interface pour les protocoles de niveau 3
- ▶ LCP (Link Control Protocol) qui sert à établir (ou rompre) la liaison



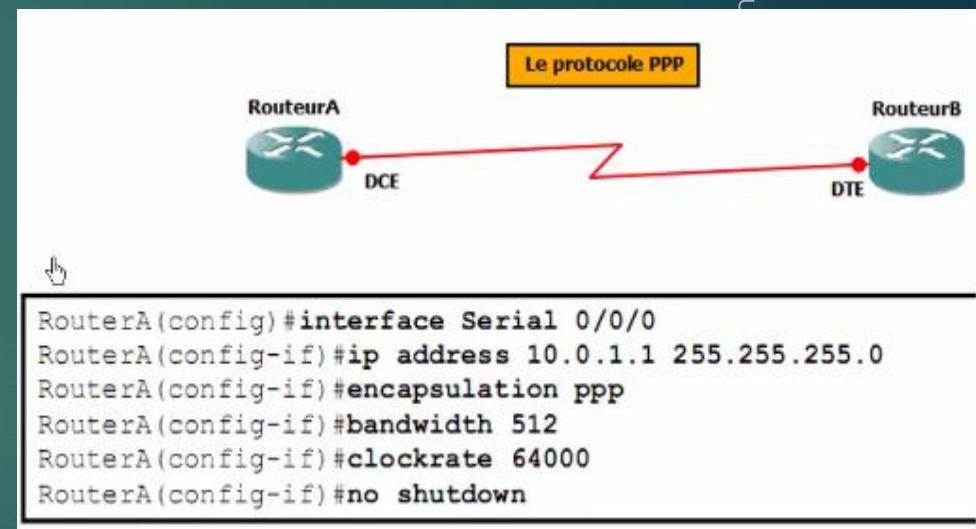
- ▶ PAP – Password Authentication Protocol
- ▶ CHAP – Challenge Authentication Protocol



# Le protocole PPP



- ▶ Configuration du protocole PPP sur le routeur A



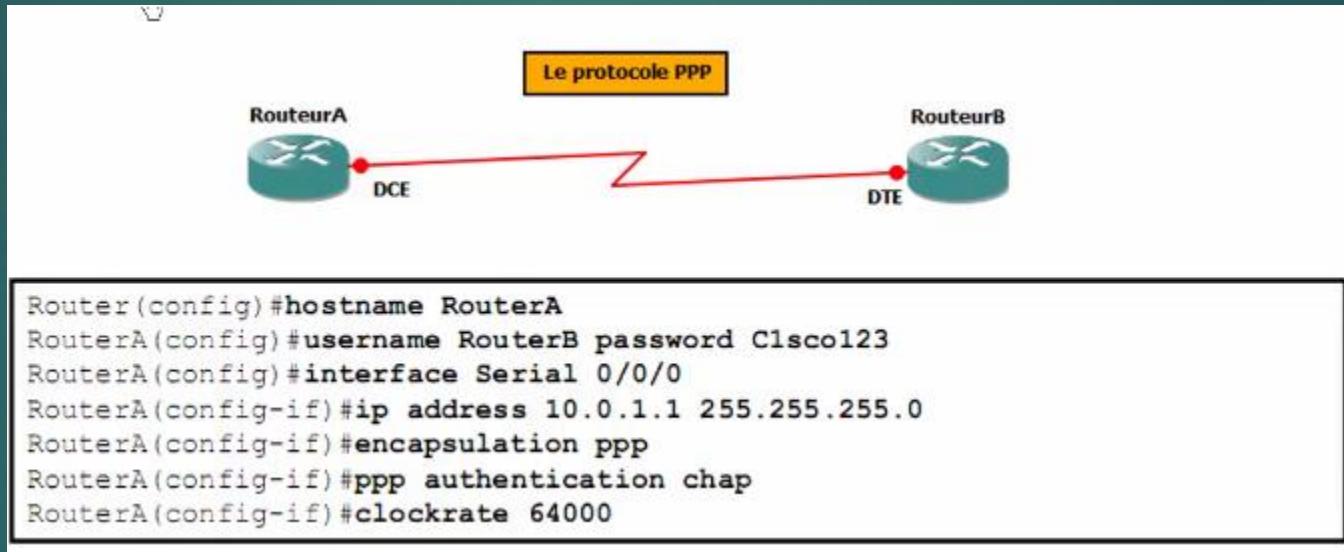
# Le protocole PPP

## ► Vérification de la configuration

```
RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
    Description: Link to RouterB
    Internet address is 10.0.1.1/24
    MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation PPP, LCP Open
    Open: IPCP, CDPCP, loopback not set
    Keepalive set (10 sec)
    CRC checking enabled
    Last input 00:00:36, output 00:00:01, output hang never
    Last clearing of "show interface" counters 00:01:09
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: weighted fair
    Output queue: 0/1000/64/0 (size/max total/threshold/drops)
      Conversations 0/1/256 (active/max active/max total)
      Reserved Conversations 0/0 (allocated/max allocated)
      Available Bandwidth 384 kilobits/sec
<output omitted>
```

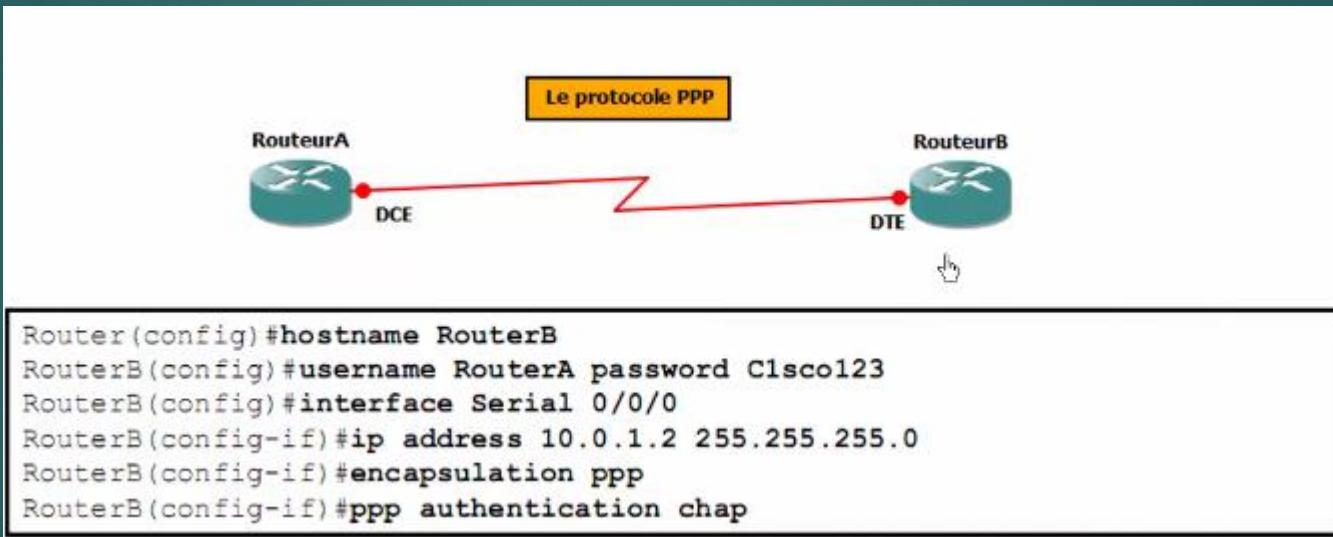
# Le protocole PPP

## ► CHAP



# Le protocole PPP

## ► CHAP



# Le protocole PPP

- ▶ Vérifier la configuration PPP sur l'interface serial 0/0/0

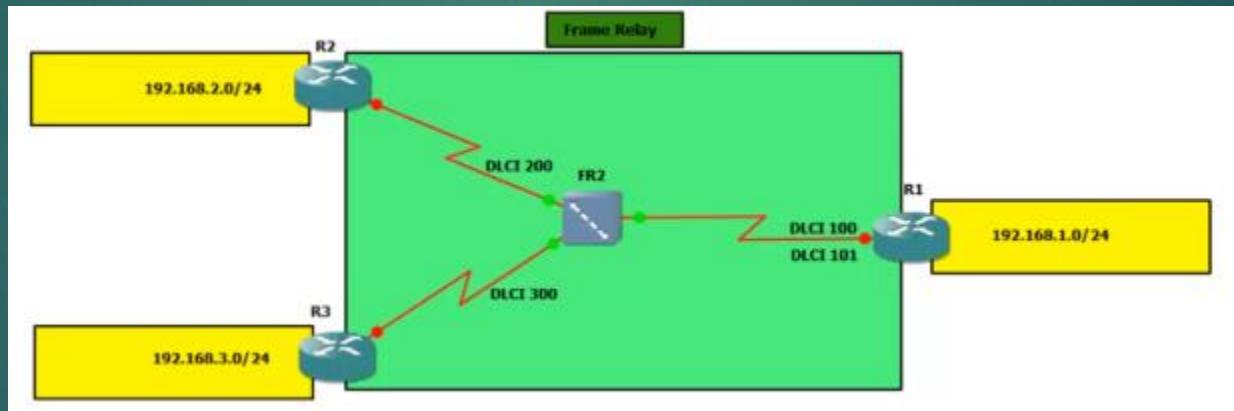
```
RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLV 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDP/CP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:21, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:00:47
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
<output omitted>
```

# Authentification pour le protocole PPP

```
RouterA#debug ppp authentication
Oct 23 11:08:10.642: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state
to up
Oct 23 11:08:10.642: Se0/0/0 PPP: Authorization required
Oct 23 11:08:10.674: Se0/0/0 CHAP: O CHALLENGE id 4 len 28 from "RouterX"
Oct 23 11:08:10.718: Se0/0/0 CHAP: I CHALLENGE id 1 len 28 from "RouterY"
Oct 23 11:08:10.718: Se0/0/0 CHAP: Using hostname from unknown source
Oct 23 11:08:10.718: Se0/0/0 CHAP: Using password from AAA
Oct 23 11:08:10.718: Se0/0/0 CHAP: O RESPONSE id 1 len 28 from "RouterX"
Oct 23 11:08:10.722: Se0/0/0 CHAP: I RESPONSE id 4 len 28 from "RouterY"
Oct 23 11:08:10.722: Se0/0/0 PPP: Sent CHAP LOGIN Request
Oct 23 11:08:10.726: Se0/0/0 PPP: Received LOGIN Response PASS
Oct 23 11:08:10.726: Se0/0/0 PPP: Sent LCP AUTHOR Request
Oct 23 11:08:10.726: Se0/0/0 PPP: Sent IPCP AUTHOR Request
Oct 23 11:08:10.726: Se0/0/0 LCP: Received AAA AUTHOR Response PASS
Oct 23 11:08:10.726: Se0/0/0 IPCP: Received AAA AUTHOR Response PASS
Oct 23 11:08:10.726: Se0/0/0 CHAP: O SUCCESS id 4 len 4
Oct 23 11:08:10.742: Se0/0/0 CHAP: I SUCCESS id 1 len 4
Oct 23 11:08:11.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```

# Le protocole Frame Relay

- ▶ C'est un protocole de la couche 2 du modèle OSI
- ▶ C'est un protocole standard de communication à commutation de paquets



# Le protocole Frame Relay

- ▶ Des réseaux à accès multiples comme les protocoles des LAN
- ▶ Plusieurs périphériques peuvent être connectés au réseau
- ▶ Non-Broadcast Multi-Access networks (NBMA) : il est impossible d'envoyer une trame à plusieurs périphériques en une seule fois

# Le protocole Frame Relay : Les avantages

- ▶ Les réseaux à commutation de paquets fournissent un multiplexage de nombreuses données à travers un seul lien de communication
- ▶ Les fournisseurs de service peuvent concevoir des réseaux plus rentables qu'avec des lignes louées.
- ▶ Les réseaux à commutation de paquets utilisent dans ce cas des circuits virtuels pour acheminer les données entre les utilisateurs, à travers une infrastructure partagée.
- ▶ Si 2 sites distants veulent communiquer via Frame Relay, ils ont donc juste à continuer un circuit entre ces sites, à travers le réseau Frame Relay

# Les circuits virtuels

- ▶ Un circuit virtuel définit un chemin logique entre 2 extrémités (2 Frame Relay DTE)
- ▶ Permet de créer une connexion point a point entre deux équipement à travers un WAN sans qu'il y ait réellement de circuit physique qui les relie
- ▶ Les routeurs utilisent les Data Link connections identifier (DLCI) comme adresse Frame Relay
- ▶ Les DLCI permettent de designer les circuits virtuels (VC) qui seront utilisés pour transmettre les données vers la destination
- ▶ Il existe deux types de circuits virtuels : permanent (PVC) et commutes (SVC) :
  - ✓ Les PVC sont reconfigures par l'opérateur lors de l'abonnement
  - ✓ Les SVC sont établis dynamiquement à l'initiative de l'Usager

- ▶ A chaque circuit virtuel est associé un identifiant de connexion
- ▶ Une table est utilisée par le provider pour faire le routage vers les bonnes sorties car désigner uniquement l'interface n'est pas suffisant.
- ▶ **Les DLCI**
  - Les DLCI ont une portée locale puisque l'identifiant renvoie au point situé entre le routeur local et le commutateur auquel il est connecté. Les équipements placés à la fin de la connexion peuvent identifier un même circuit virtuel par un DLCI différent

# Local Management Interface (LMI)

110

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

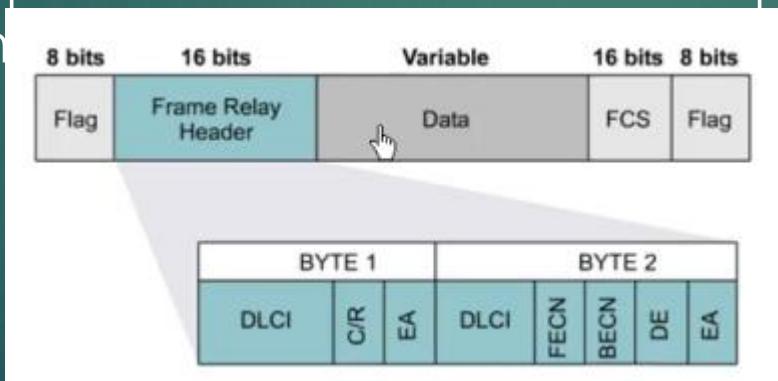
- ▶ LMI est un standard pour la signalisation entre la DTE et les commutateurs Frame Relay
- ▶ Il est responsable de l'administration des connexion et du maintien du statuts entre les périphériques
- ▶ Un maintien en vie de la connexion (fonction keepalive). En cas de panne du lien d'accès, l'absence de messages keepalive indiquera l'indisponibilité de la ligne
- ▶ Des informations sur le status des PVC : existence de nouveaux PVC et suppression des existants

# Local Management Interface (LMI)

111

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Les LMI ont été développé indépendamment de Frame Relay et mis en place avant. Ainsi il existe 3 LMI (Cisco, ITU, ANSI) incompatibles entre eux
- ▶ En raison des types différents de LMI, il est préconisé de laisser le type par défaut sur l'équipement (DTE et DCE)
- ▶ Chaque paquet de la couche 3 est encapsule dans la couche 2 entre une en

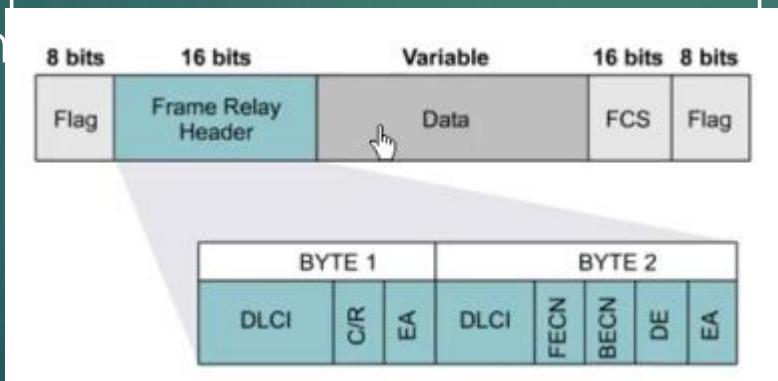


# Local Management Interface (LMI)

112

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Les LMI ont été développé indépendamment de Frame Relay et mis en place avant. Ainsi il existe 3 LMI (Cisco, ITU, ANSI) incompatibles entre eux
- ▶ En raison des types différents de LMI, il est préconisé de laisser le type par défaut sur l'équipement (DTE et DCE)
- ▶ Chaque paquet de la couche 3 est encapsule dans la couche 2 entre une en



# Association entre les DLCI et les adresses de couche 3

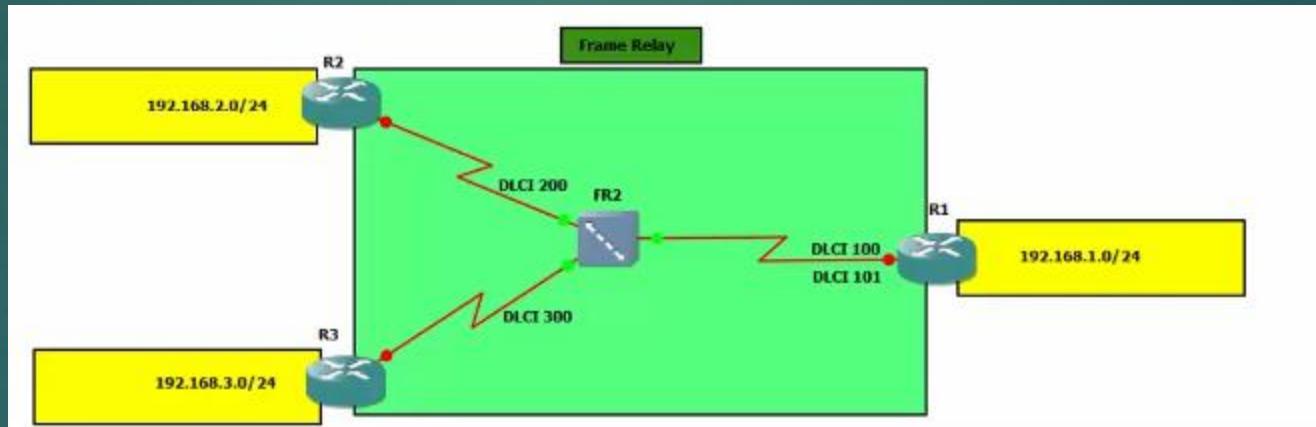
- ▶ Comment établir une correspondance entre l'adresse de niveau 3 d'un routeur Frame Relay et le DLCI qu'il faut utiliser pour l'atteindre?
  - ✓ L'association établie entre une adresse de niveau 3 de prochain saut et l'adresse de niveau 2 (DLCI) qu'il faut employer pour l'atteindre.
  - ✓ Exemple du protocole ARP pour les LAN
- ▶ Deux méthodes :
  - ✓ Manuelle via la commande **frame relay map** (configuration statique)
  - ✓ Dynamique via Inverse ARP

# Inverse ARP

- ▶ Inverse ARP a été développé pour fournir un mécanisme à l'association de DLCI dynamique à des adresses de couche 3
  - ✓ Fonctionne de la même manière que ARP sur un LAN
  - ✓ Sur IP, avec ARP, le matériel connaît l'adresse IP et souhaite connaître l'adresse MAC.
  - ✓ Avec Inverse ARP, le routeur connaît l'adresse de la couche 2 qui est le DLCI et souhaite connaître l'adresse de couche 3.

# Configuration du protocole Frame Relay

- ▶ Le protocole Frame Relay point à point
- ▶ Le protocole Frame Relay Multipoint



# Configuration du protocole Frame Relay

116

Cours de CONP :  
Katakpe Kofi Kum  
28 February 2024

## ▶ Activation du Frame Relay

```
R1> enable
R1# configure terminal
R1(config)# interface serial 0/0
R1(config-if)# encapsulation frame-relay
R1(config-if)# no frame-relay inverse-arp
R1(config-if)# ip address 172.16.0.1 255.255.255.0
R1(config-if)# no shutdown
```

## ▶ Mappage des adresses IP et DLCI

```
R1(config-if)# frame-relay map ip 172.16.0.2 200 broadcast
R1(config-if)# frame-relay map ip 172.16.0.3 300 broadcast
R1(config-if)# exit ↵
```

## ▶ Vérification de la configuration Frame Relay

```
Branch#show interfaces Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.1.1/24
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI eng sent 630, LMI stat recv 616, LMI upd recv 0, DTE LMI up
  LMI eng recv 15, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 9/0, interface broadcasts 0
  Last input 00:00:04, output 00:00:04, output hang never
  Last clearing of "show interface" counters 01:45:04
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair

<output omitted>
```

# Configuration du protocole Frame

## Verification

```
Branch#show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0           Invalid Prot Disc 0
  Invalid dummy Call Ref 0         Invalid Msg Type 0
  Invalid Status Message 0        Invalid Lock Shift 0
  Invalid Information ID 0       Invalid Report IE Len 0
  Invalid Report Request 0      Invalid Keep IE Len 0
  Num Status Enq. Sent 834        Num Status msgs Rcvd 820
  Num Update Status Rcvd 0       Num Status Timeouts 14
  Last Full Status Req 00:00:21    Last Full Status Rcvd 00:00:21

Branch#show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
          Active     Inactive     Deleted     Static
Local          1            0            0            0
Switched       0            0            0            0
Unused         0            0            0            0

DLCI = 120, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/0
      input pkts 18          output pkts 18          in bytes 962
      out bytes 962          dropped pkts 0          in pkts dropped 0
      out pkts dropped 0      out bytes dropped 0
      in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
      out BECN pkts 0          in DE pkts 0          out DE pkts 0
      out bcast pkts 13        out bcast bytes 442
      5 minute input rate 0 bits/sec, 0 packets/sec
      5 minute output rate 0 bits/sec, 0 packets/sec
      pvc create time 02:32:29, last time pvc status changed 02:32:29
```

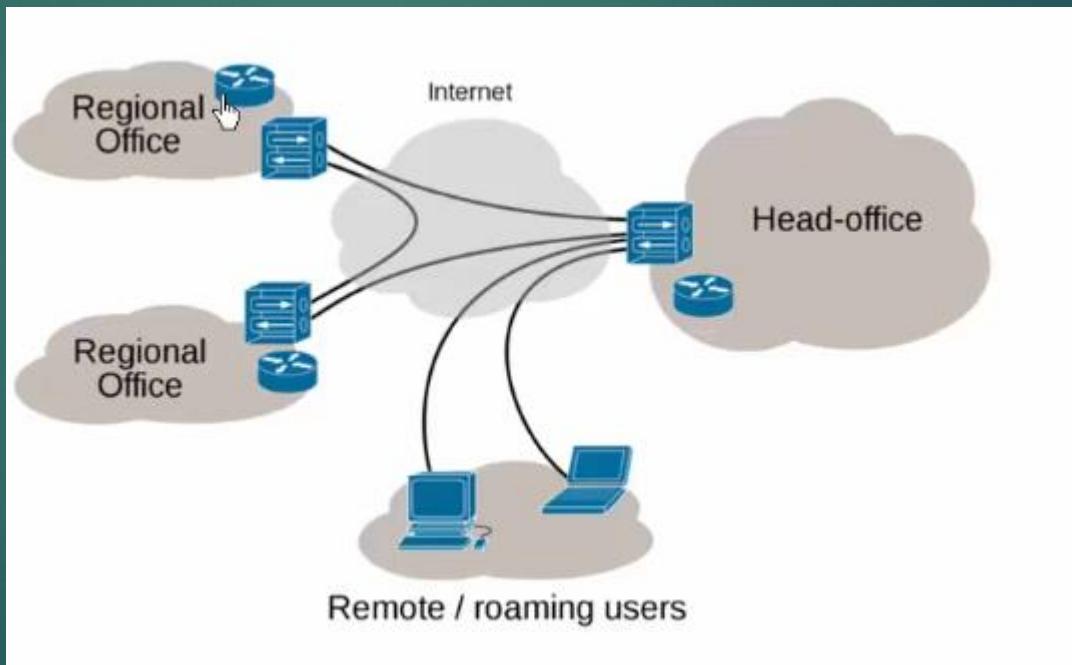
# Configuration du protocole Frame Relay

## Verification

```
Branch#show frame-relay map  
Serial0/0/0 (up): ip 192.168.1.2 dlci 120(0x78,0x1C80), dynamic,  
broadcast,  
CISCO, status defined, active
```

# Introduction aux solutions VPN

- ▶ Un VPN est un réseau privé qui utilise le réseau public comme Backbone



- ▶ Seuls les utilisateurs ou les groupes qui sont enregisitres dans ce VPN peuvent y accéder.
- ▶ Les données transitent dans un tunnel après avoir été chiffrées
- ▶ Tout se passe comme si la connexion se faisait en dehors d'infrastructure d'accès partage comme Internet
- ▶ Les avantages des VPN
  - Accès aux différentes ressources interne de l'entreprise
  - Le cout faible
  - Evolutivité
  - Compatibilité
  - La sécurité

# • Les VPN

- ▶ Les différentes solutions des VPN
  - VPN site a site (site to site)
  - Accès distant (Remote Access)
    - ✓ Easy VPN
    - ✓ Cisco AnyConnect SSL VPN
    - ✓ Clientless Cisco SSL VPN
- ▶ Le protocole IPSEC
  - IPsec est un protocole destiné à fournir différents services de sécurité
  - Un Framework standard

- Les services IPsec fournissent quatre fonctions:
  - ✓ Confidentialité
  - ✓ Intégrité
  - ✓ Authentification
  - ✓ Protection Anti-reply

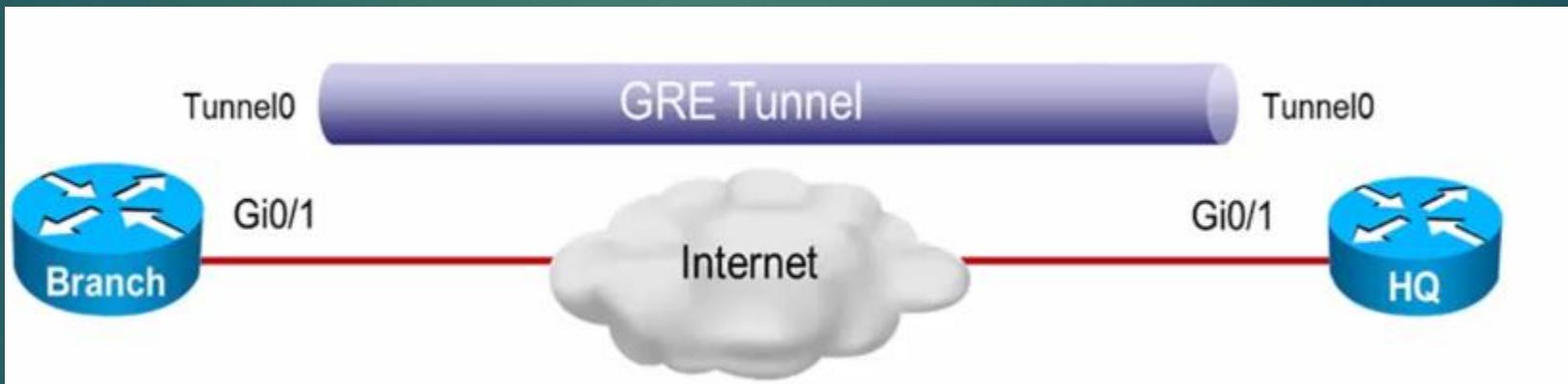
# Le protocole GRE

- ▶ Generic Routing Encapsulation
- ▶ GRE a été développé par Cisco
- ▶ Un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau dans n'importe quel paquet de la couche réseau.
- ▶ Utiliser pour échanger les informations des protocoles de routage en



# Configuration du protocole GRE

- ▶ Créer les interfaces virtuel
- ▶ Spécifier l'adresse IP source et destination du tunnel
- ▶ Configurer les adresses ip pour le tunnel



# Configuration du protocole GRE

124

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Configuration du tunnel GRE entre les deux routeurs Branch et HQ

```
Branch(config)#interface Tunnel0
Branch(config-if)#tunnel mode gre ip
Branch(config-if)#ip address 192.168.2.1 255.255.255.0
Branch(config-if)#tunnel source 209.165.201.1
Branch(config-if)#tunnel destination 209.165.202.130
```



```
HQ(config)#interface Tunnel0
HQ(config-if)#tunnel mode gre ip
HQ(config-if)#ip address 192.168.2.2 255.255.255.0
HQ(config-if)#tunnel source 209.165.202.130
HQ(config-if)#tunnel destination 209.165.201.1
```

# Configuration du protocole GRE

- ▶ Vérifier si les interfaces sont up

```
Branch#show ip interface brief | include Tunnel
      ↗
Tunnel0          192.168.2.1    YES manual up           up
```

Voir les détails des interfaces tunnel

```
Branch#show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.202.130
  Tunnel protocol/transport GRE/IP

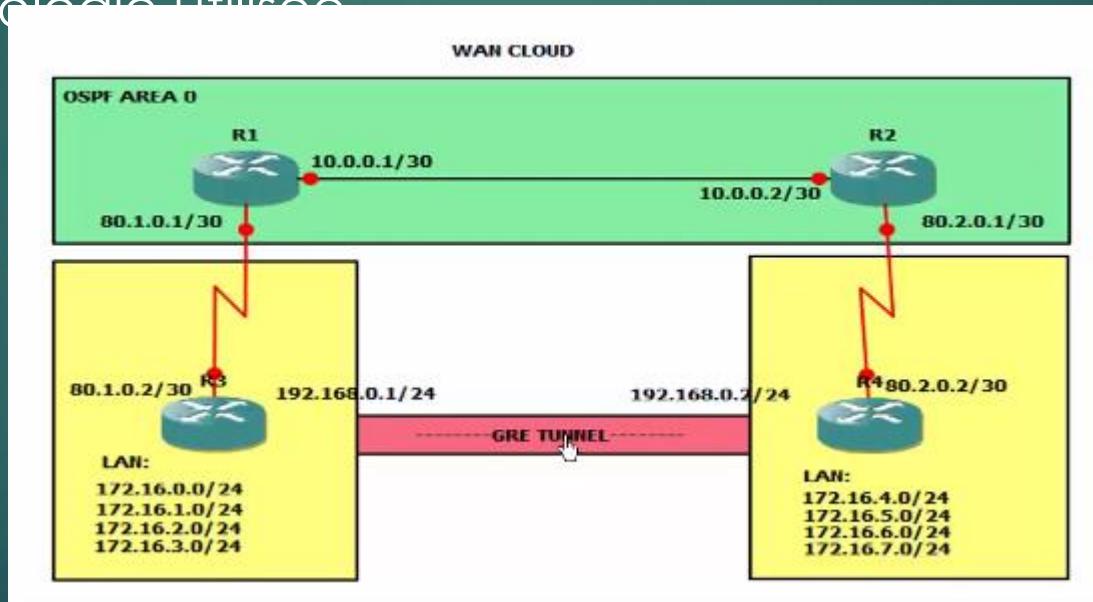
<output omitted>
```

# Configuration du protocole GRE

- Vérifier les routes échangées entre les routeurs

```
Branch#show ip route
<output omitted>
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, Tunnel0
L      192.168.2.1/32 is directly connected, Tunnel0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.0/27 is directly connected, GigabitEthernet0/1
L      209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

- Topologie utilisée



# Le protocole SNMP

127

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Simple Network Management Protocol
- ▶ Réduire les perdes d'indisponibilité
- ▶ Fournir à tout moment l'état du réseau et de ses composants
- ▶ Inventorier les équipements
- ▶ Quantifier et optimiser les trafics
- ▶ Faciliter la planification des interventions sur le réseau
- ▶ Permettre une autorisation des procédures de correction des problèmes

# Le protocole SNMP

128

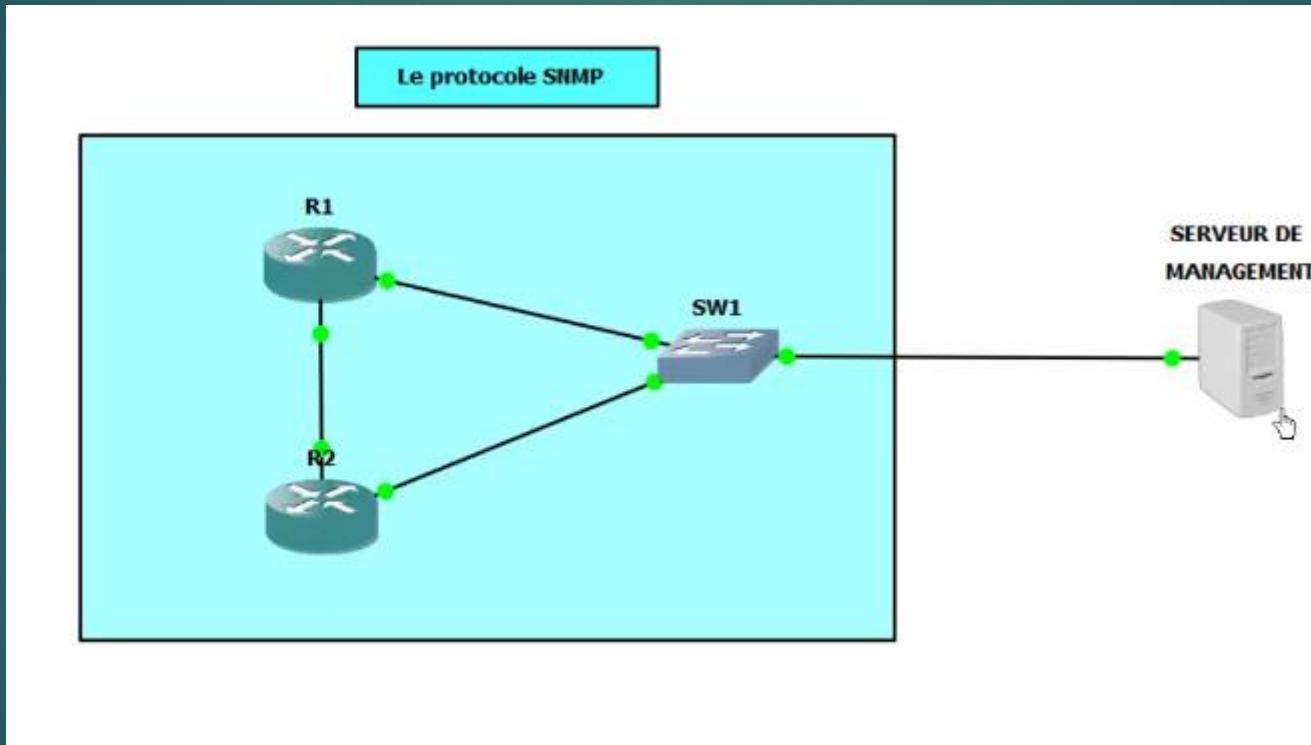
Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Le SNMP est un protocole standard permettant la supervision de machines informatiques
- ▶ Il permet entre autre de récupérer une foule d'informations sur l'état de l'équipement
- ▶ SNMP permet aussi d'agir sur l'équipement (modification de la configuration, etc...)
- ▶ Un serveur de supervision peut envoyer des requêtes aux clients
- ▶ SNMP utilise UDP sur le port 161
- ▶ Il est aussi possible que le client prenne l'initiative d'envoyer des informations au serveur. Le message s'appelle alors une trap
- ▶ Les traps sont envoyées en UDP sur le port 162.

# Le protocole SNMP

129

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



# Le protocole SNMP

130

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Une architecture SNMP est divisée en 3 parties :
  - Les Managed Devices : les clients managés
  - Les Agents : applications sur les clients, chargées d'envoyer les informations
  - Les Network Managed Systems : interfaces à travers lesquelles les administrateurs peuvent réaliser des tâches d'administration

# Les communies du protocole SNMP

131

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

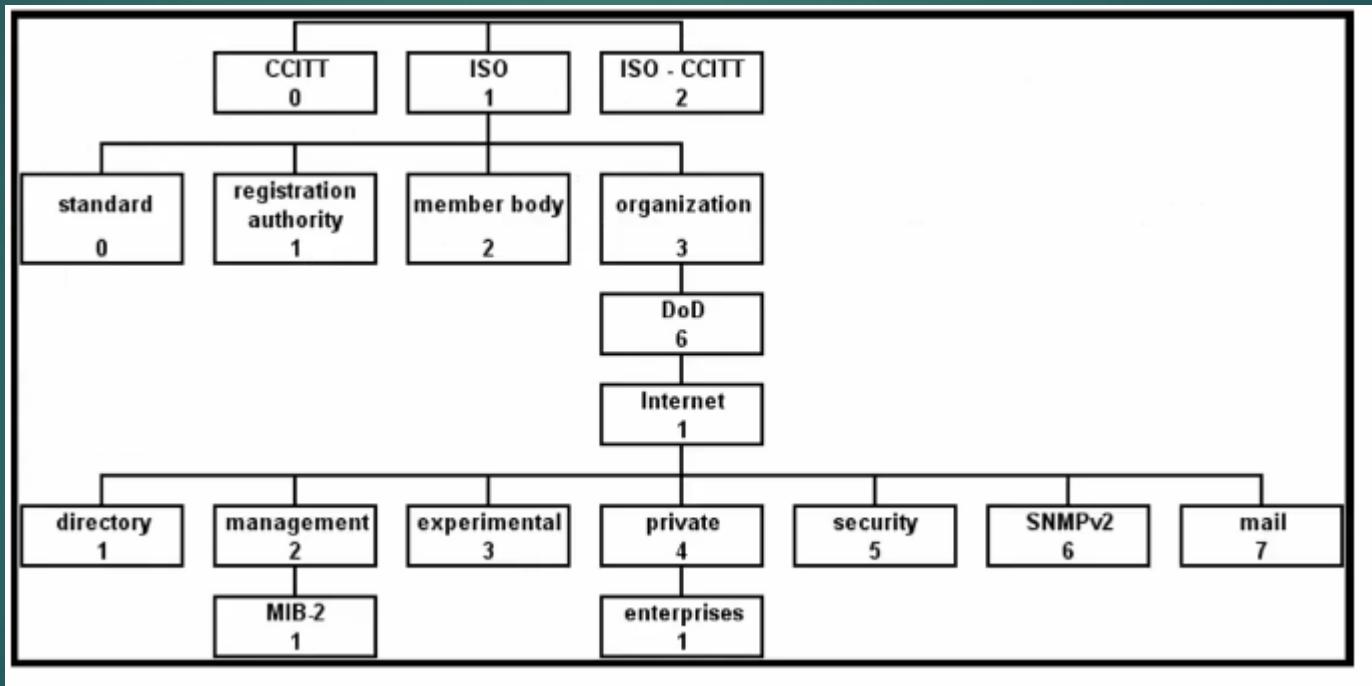
- ▶ Il existe 3 versions de SNMP : V1, V2 et V3:
  - ✓ En version 1 et 2, le mécanisme de sécurité repose sur des communautés
  - ✓ Dans le V3, la sécurité est plus poussée. Elle propose le chiffrement et l'authentification
    - RO – Read Only
    - RW – Read White

# Protocole SNMP

132

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

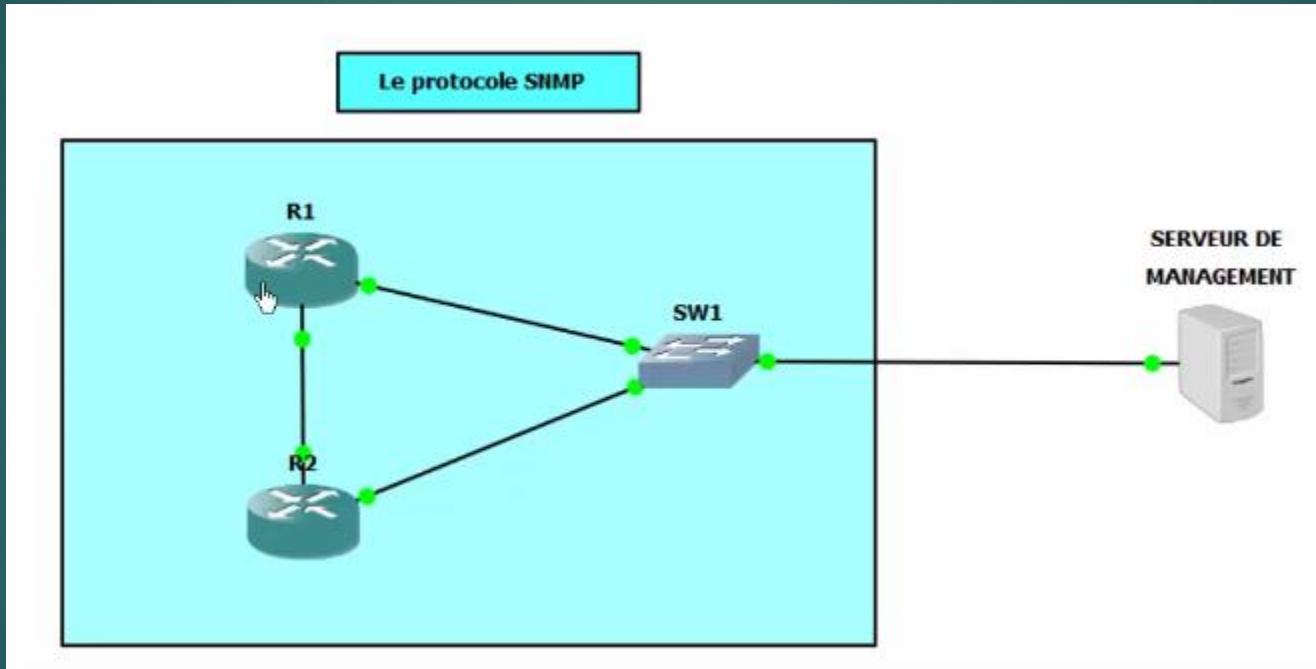
## ► Les MIB



# Configuration du protocole SNMP

133

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024



# Configuration du protocole SNMP

134

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

- Choisir les IP autorisées à interroger l'équipement

```
R1(config)# ip access-list standard SNMPSrv
R1(config std-nacl)# permit 10.0.1.1 0.0.0.0
```

- Configuration des communautés

```
R1(config)#snmp-server community ALPHORM ro SNMPSrv
R1(config)#snmp-server community ALPHORM rw SNMPSrv
```

# Configuration du protocole SNMP

- Activer les traps voulus

```
R1(config)#snmp-server enable traps <type>
```



- Il est aussi possible de choisir toutes les traps

```
R1(config)#snmp-server enable traps
```

- Spécifier l'adresse de destination des traps

```
R1(config)#snmp-server host 10.0.1.1 ALPHORM
```

# Configuration du protocole SNMP

- ▶ Il peut être bon d'utiliser les options suivantes

```
R1(config)#snmp-server contact support@networklab.fr
R1(config)#snmp-server location Bat1Baie2
R1(config)#snmp-server chassis-id 65GT126E
R1(config)#snmp-server ifindex persist
```

## ▶ Introduction

- Les logs peuvent s'afficher directement dans la console
- Être stockés dans un buffer sur l'équipement
- Être envoyés sur un serveur Syslog

## ▶ Le protocole SYSLOG

- Un protocole standard permettant la collecte de log à travers le réseau
- Syslog UDP 514
- Le serveur Syslog stocke les logs dans les journaux

```
R1(config)#exit
R1#
Sep 23 23:27:42.915: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

# Le protocole Syslog

- ▶ Il existe différents niveaux de log
- ▶ Un log se constitue comme ceci :

		Facility (ici SYS)
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition
3	Error	Error condition
4	Warning	Warning condition
5	Notice	Normal but significant condition
6	Informational	Informational message only
7	Debug	Appears during debugging only

Facility (ici SYS)

Severity (ici 5)

Facility (ici CONFIG\_I)

Message

# Configuration du protocole SYSLOG

- ▶ Pour que les log soient stockés dans un buffer, la configuration est la suivante
- ▶ Le chiffre à la fin de la commande correspond au niveau de Log à stocker
- ▶ Tous les niveaux inférieurs seront aussi pris en compte (donc ici de 5 à 0)

```
R1(config)#logging buffered 5
```

- ▶ Pour choisir le niveau de log affiché dans la console, la commande est la suivante

```
R1(config)#logging console 5
```

- ▶ Pour que les log soient stockés dans un buffer

```
R1(config)#logging buffered 5
```

- ▶ Pour choisir le niveau de log affiché dans la console

```
R1(config)#logging console 5
```

# Configuration du protocole SYSLOG

- ▶ Pour que les logs soient affichés en live dans la console, entrer la commande suivante

```
R1#terminal monitor
```

- ▶ Pour ajouter la date aux logs, il faut ajouter la commande suivante

```
R1(config)#service timestamps log datetime msec
```

- ▶ Il est aussi possible de remplacer la date par la uptime de l'équipement

```
R1(config)#service timestamps log uptime
```

# Configuration du protocole SYSLOG

- ▶ Afin de ne pas perturber l'utilisation de la console' mieux vaut activer la synchronisation

```
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config)#line vty 0 15
R1(config-line)#logging synchronous
```

- ▶ Pour enregistrer les logs dans le buffer de l'équipement, la configuration est la suivant

```
R1(config)#logging buffered 4096 5
```

# Configuration du protocole SYSLOG

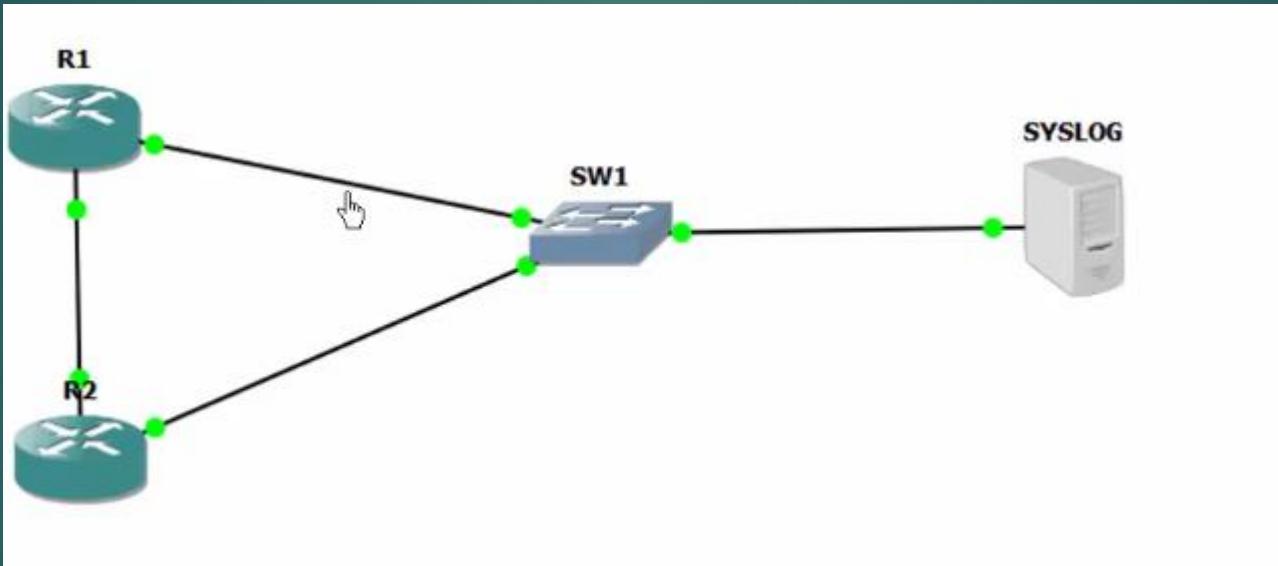
- ▶ Enfin, pour envoyer les logs sur un serveur Syslog, la configuration est la suivante

```
R1(config)#logging 10.0.1.1
R1(config)#logging trap 3
```

- ▶ Il est aussi possible de choisir l' interface à utiliser pour envoyer les logs

```
R1(config)#logging source-interface fastEthernet 0/0
```

# Configuration du protocole SYSLOG



# Introduction au protocole Netflow

144

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Netflow est un protocole Cisco permettant de collecter des informations sur les flux IP
- ▶ Un équipement va envoyer des informations sur ses interfaces à un collecteur
- ▶ Netflow utilise le port **UDP 2055**
  - Qu'est ce qu'un flux:
    - ✓ IFindex In
    - ✓ IP SRC
    - ✓ IP DST
    - ✓ TOS
    - ✓ Protocol
    - ✓ TCP/UDP SRC
    - ✓ TCP/UDP DST

# Introduction au protocole Netflow

145

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Les informations envoyées pour un collecteur peuvent porter sur:
  - Adresse source et destination du trafic
  - Interfaces sources et destination
  - Ports applicatifs utilisés
  - Nombre de paquets par seconde
  - Type de service
  - Etc...

# Configuration du protocole Netflow

146

Cours de CCNP : Net  
Katakpe Kossi Kuma  
28 February  
2024

g & security Présenté par

- ▶ Premièrement, il faut choisir l'interface, et le sens du trafic
- ▶ Ensuite, nous pouvons choisir la destination

```
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip flow ingress
R3(config-if)#ip flow egress
```

```
R3(config)#ip flow-export source fastEthernet 0/0
```

- ▶ Ensuite, nous pouvons choisir la destination

```
R3(config)#ip flow-export destination 10.0.1.1 2055
```

- ▶ Il faut aussi choisir la version de Netflow à utiliser

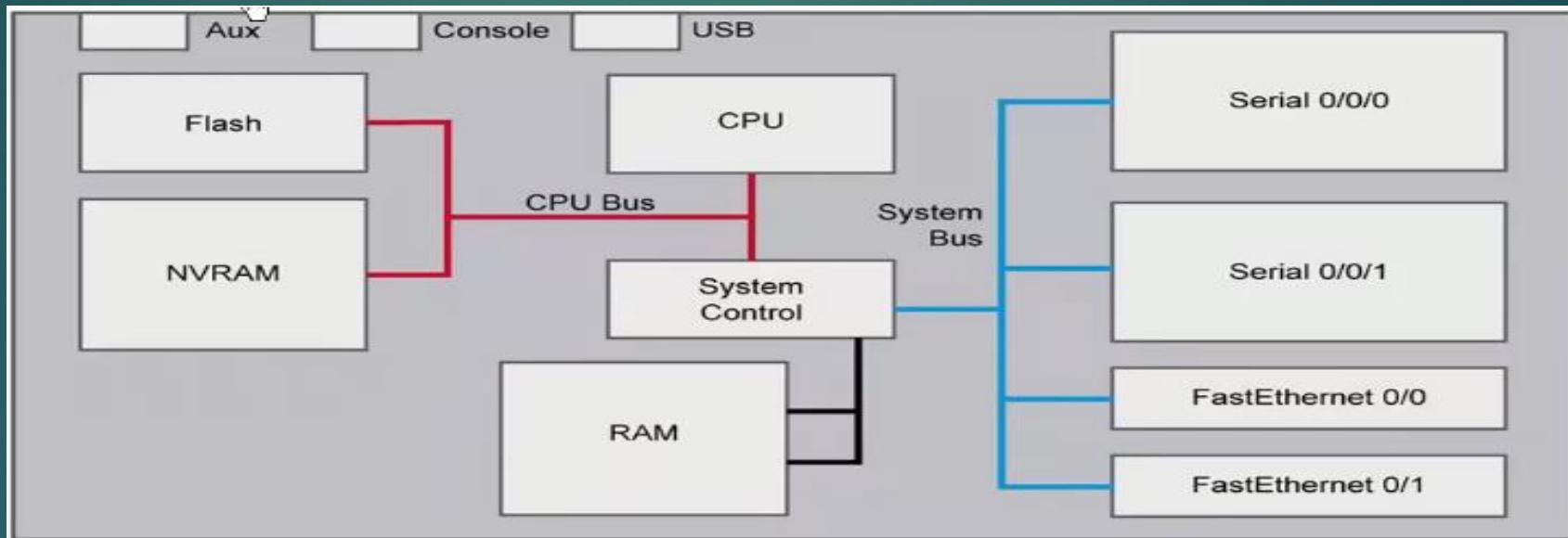
```
R3(config)#ip flow-export version ?
1
5
9
```

# Gestion des configurations et des IOS

147

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

- ▶ Les composants internes d'un routeur



# Les fichiers de configuration

```
Branch#show running-config
Building configuration...
Current configuration : 1318 bytes
!
! Last configuration change at 13:11:38 UTC Tue Nov 20 2012
! NVRAM config last updated at 13:11:38 UTC Tue Nov 20 2012
! NVRAM config last updated at 13:11:38 UTC Tue Nov 20 2012
version 15.2
<output omitted>
```

- ▶ Afficher le fichier de configuration actuel

# Gestion des configurations et des IOS

149

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

```
Branch#show startup-config
Using 1318 out of 262136 bytes
!
! Last configuration change at 13:11:38 UTC Tue Nov 20 2012
! NVRAM config last updated at 13:11:38 UTC Tue Nov 20 2012
! NVRAM config last updated at 13:11:38 UTC Tue Nov 20 2012
version 15.2
<output omitted> ➔
```

- ▶ Afficher le fichier de configuration initial

# Gestion des configurations et des IOS

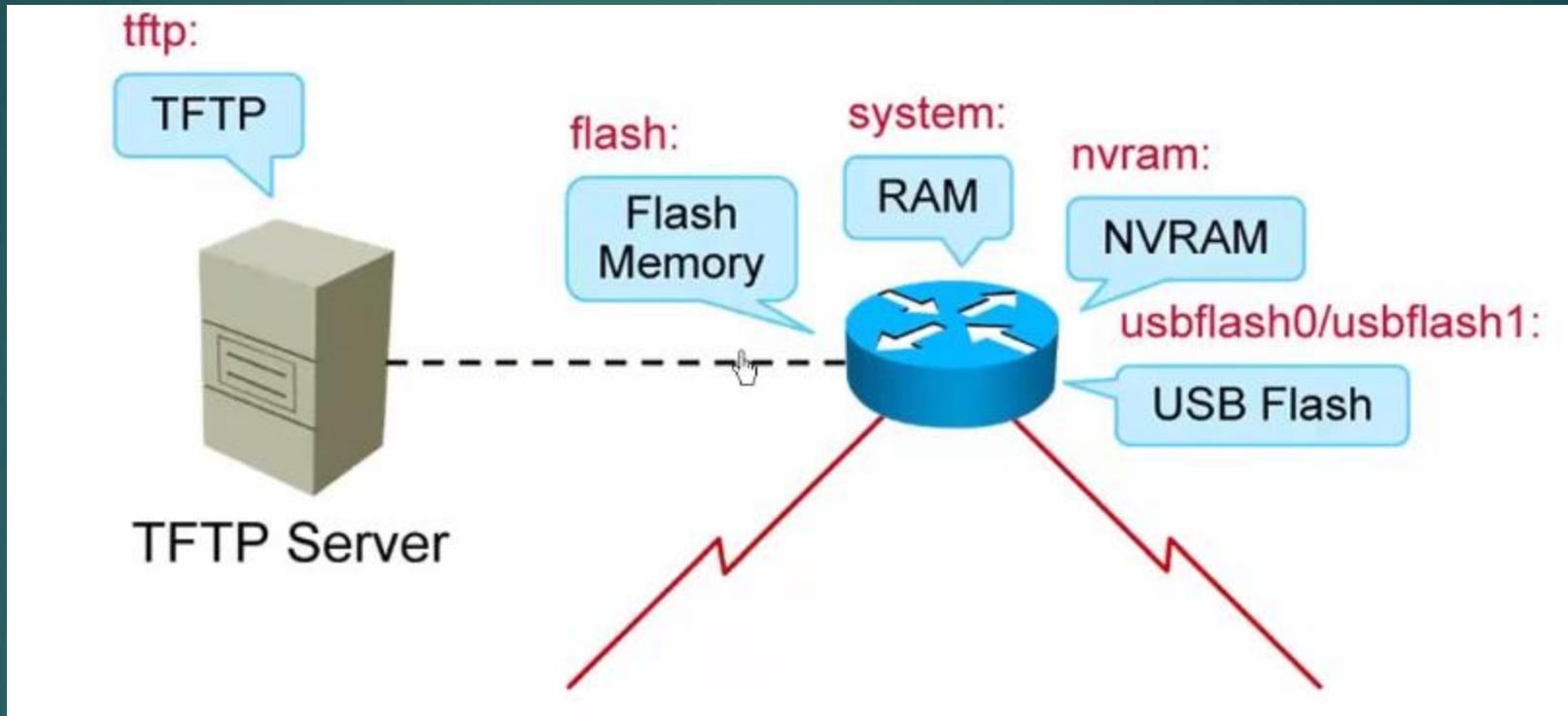
150

Cours de CCNP : Networking & security  
Katakpe Kossi Kuma  
28 February  
2024

```
Branch#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Branch uptime is 39 minutes
System returned to ROM by reload at 11:39:24 UTC Tue Nov 20 2012
System image file is "flash0:c2900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command
<output omitted>
```

- ▶ Chargement de l'IOS Cisco

# Gestion des configurations et des IOS



- ▶ Les différents mémoire au niveau d'un routeur

# Gestion des configurations et des IOS

- ▶ Vérifier la connectivité avec le serveur
- ▶ Vérifier qu'on a suffisamment d'espace disque
- ▶ Télécharger une nouvelle version IOS
- ▶ Copier le fichier IOS vers le serveur TFTP
- ▶ Configurer le boot avec la nouvelle version IOS
- ▶ Redémarrer le routeur



# Mise à jour IOS

```
Branch#ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

- Vérifier la connectivité vers le serveur

```
Branch#show flash0:
-- --length-- -----date/time----- path
1      97794040 Nov 30 1983 00:00:00 +00:00 c2900-universalk9-mz.SPA.152-
4.M1.bin
<output omitted>
```

- Vérifier la taille de l'image IOS

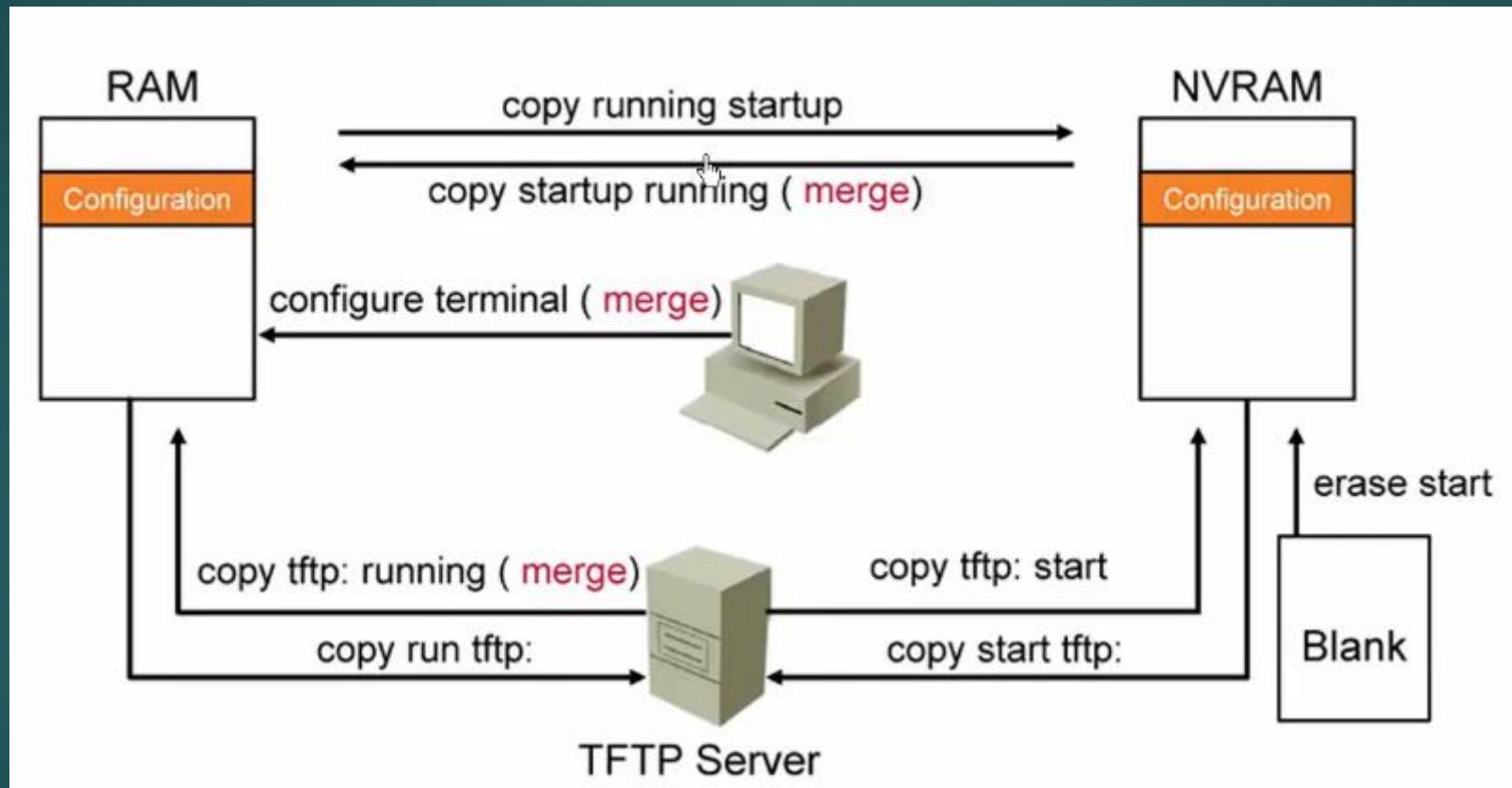
# Mise à jour IOS

## ► Copier le fichier IOS vers le serveur TFTP

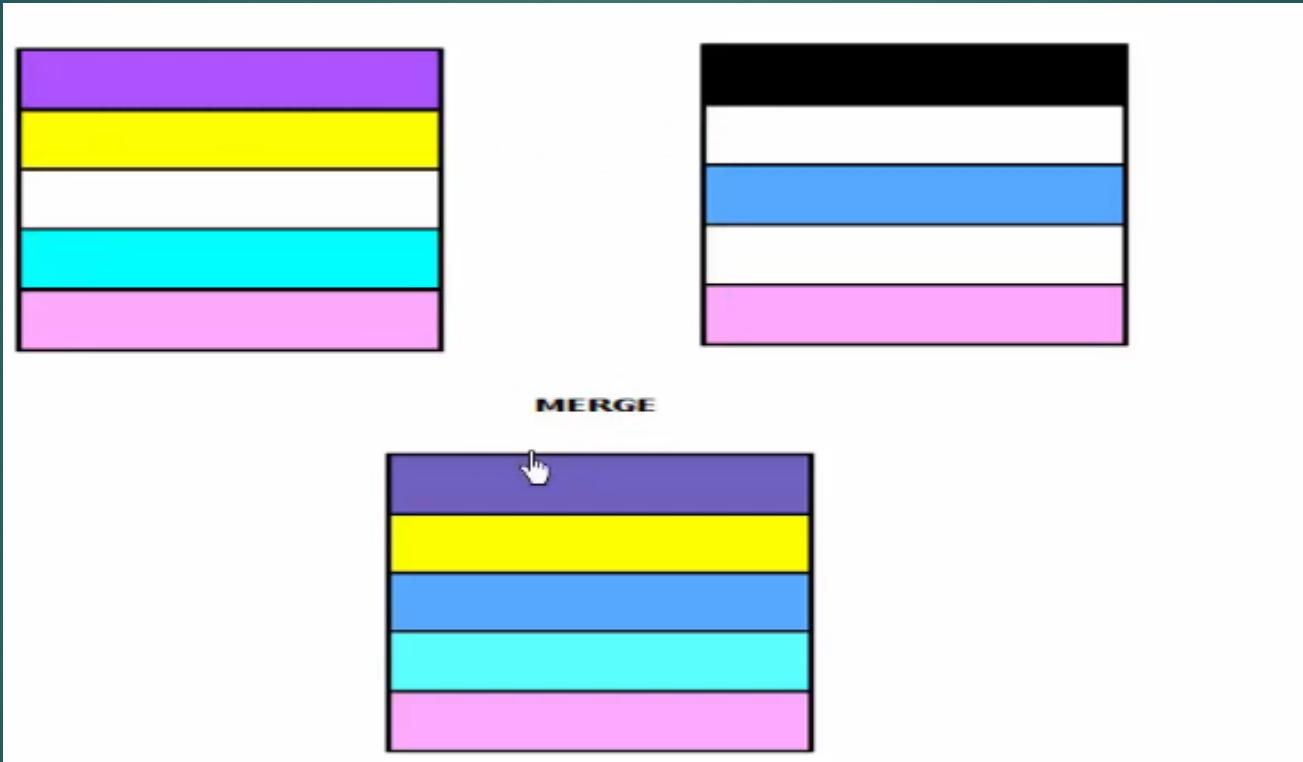
```
Branch#copy tftp: flash0:  
Address or name of remote host []? 2001:DB8:AC10:100::64  
Source filename []? c2900-universalk9-mz.SPA.152-4.M1.bin  
Destination filename []? c2900-universalk9-mz.SPA.152-4.M1.bin  
Accessing tftp://2001:DB8:AC10:100::64/c2900-universalk9-mz.SPA.152-  
4.M1.bin...  
  
Loading c2900-universalk9-mz.SPA.152-4.M1.bin from 2001:DB8:AC10:100::64  
(via GigabitEthernet0/0): !!!!!!!  
<output omitted>  
[OK - 97794040 bytes]  
97794040 bytes copied in 368.128 secs (265652 bytes/sec)
```

```
Branch#configure terminal  
Branch(config)#boot system flash0://c2900-universalk9-mz.SPA.152-4.M1.bin  
Branch#copy running-config startup-config  
Branch#reload
```

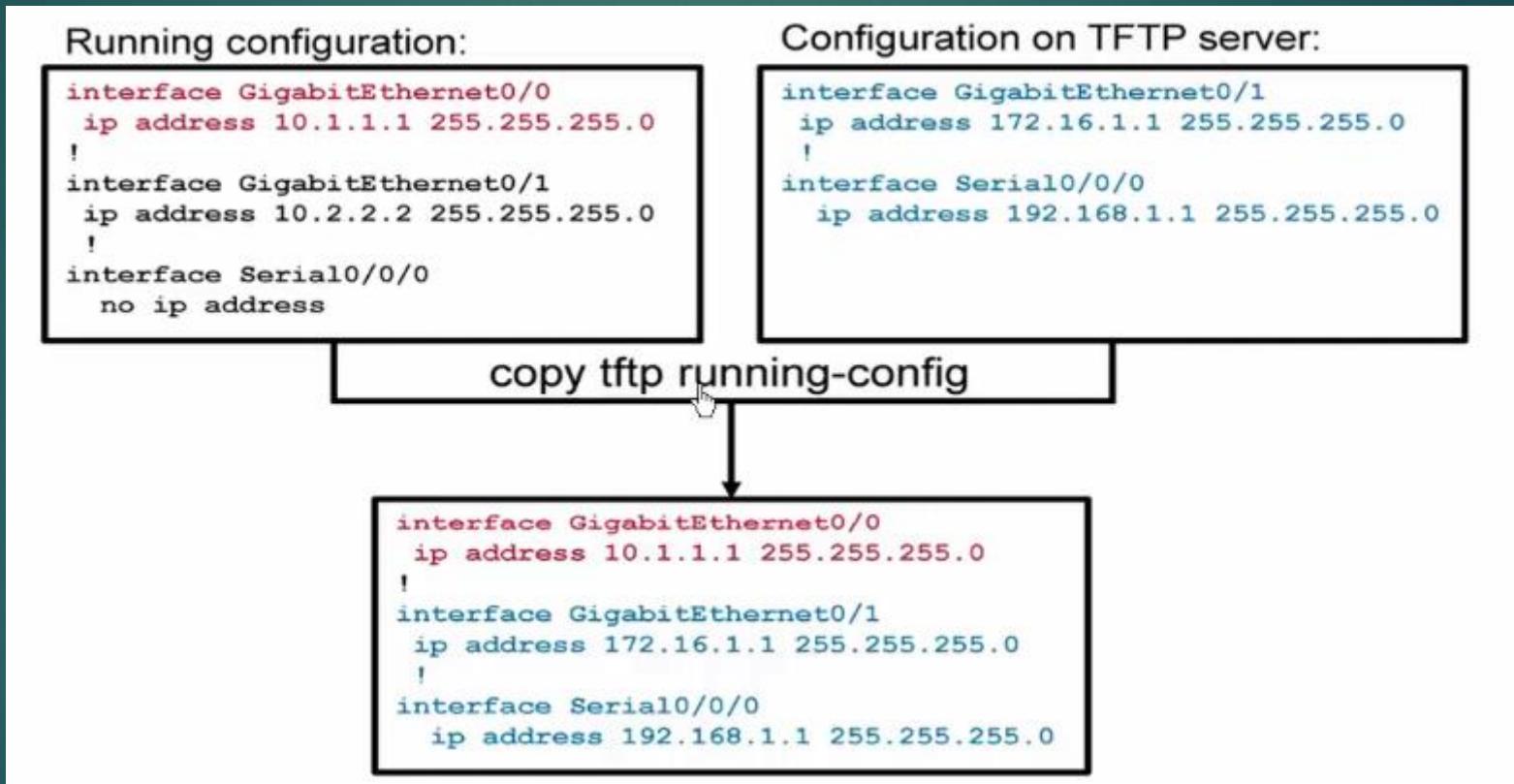
# Gestion des fichiers de configuration



# Gestion des fichiers de configuration



# Gestion des fichiers de configuration



# Gestion des fichiers de configuration

## ► Chargement des fichiers de configuration vers le serveur TFTP

```
Branch#copy running-config tftp
Address ↵ name of remote host []? 172.16.1.100
Destination filename [running-config]? config.cfg
.!!
1684 bytes copied in 13.300 secs (129 bytes/sec)
```

```
Branch#copy tftp running-config
Address or name of remote host []? 2001:DB8:AC10:100::64
Source filename []? config.cfg
Destination filename [running-config]?
Accessing tftp://2001:DB8:AC10:100::64/config.cfg...
Loading config.cfg from 2001:DB8:AC10:100::64 (via GigabitEthernet0/0): !
[OK - 1684/3072 bytes]

1684 bytes copied in 17.692 secs (99 bytes/sec)
```

# Configuration

159

Cours de CCNP : Networking & security  
Présenté par  
Katakpe Kossi Kuma  
28 February  
2024

## ► Topologie à utiliser

