



Commutation et Routage intermédiaire

Pr Cheikh Ahmadou Bamba GUEYE

<http://edmi.ucad.sn/~gueye>

Plan du cours

- Introduction
- Protocole RIPv2
- Protocole OSPF
- Protocole EIGRP
- Commutation
- VLAN

Méthodes de travail

- Préparer le **cours** en lisant attentivement la leçon en **amont** du cours
- Suivre attentivement le cours en prenant, si besoin, quelques notes
- La prise de notes n'est pas la recopie intégrale des vues projetées
- Il faut **porter** plus **d'attention** au **discours** et aux illustrations qu'à la recopie du texte des vues

Méthodes de travail

- Après le cours relire la leçon et préparer les questions
- Consulter les livres de référence
- Lors des TD et /ou TP l'enseignant est là pour répondre à vos questions et vous fournir toutes les explications supplémentaires nécessaires

Bibliographie

- **Réseaux et Télécom: cours avec 129 exercices corrigés**, Claude Servin (Auteur), Editeur : Dunod; DUNOD edition
- **Computer Networking : A Top-Down Approach Featuring the Internet**, James F. Kurose (Auteur), Keith W. Ross (Auteur), Pearson; 6th edition (March 5, 2012)
- **Réseaux d'entreprises par la pratique**, Jean Luc Montagnier (Auteur), Eyrolles
- **Cisco CCNA Exploration 4**

Introduction

- La communication numérique à base de données, de son audio et de vidéo est essentielle pour les PME
- Un réseau local correctement conçu est aujourd’hui fondamental pour mener une activité
- Un modèle de conception hiérarchique est plus idoine pour réussir votre projet

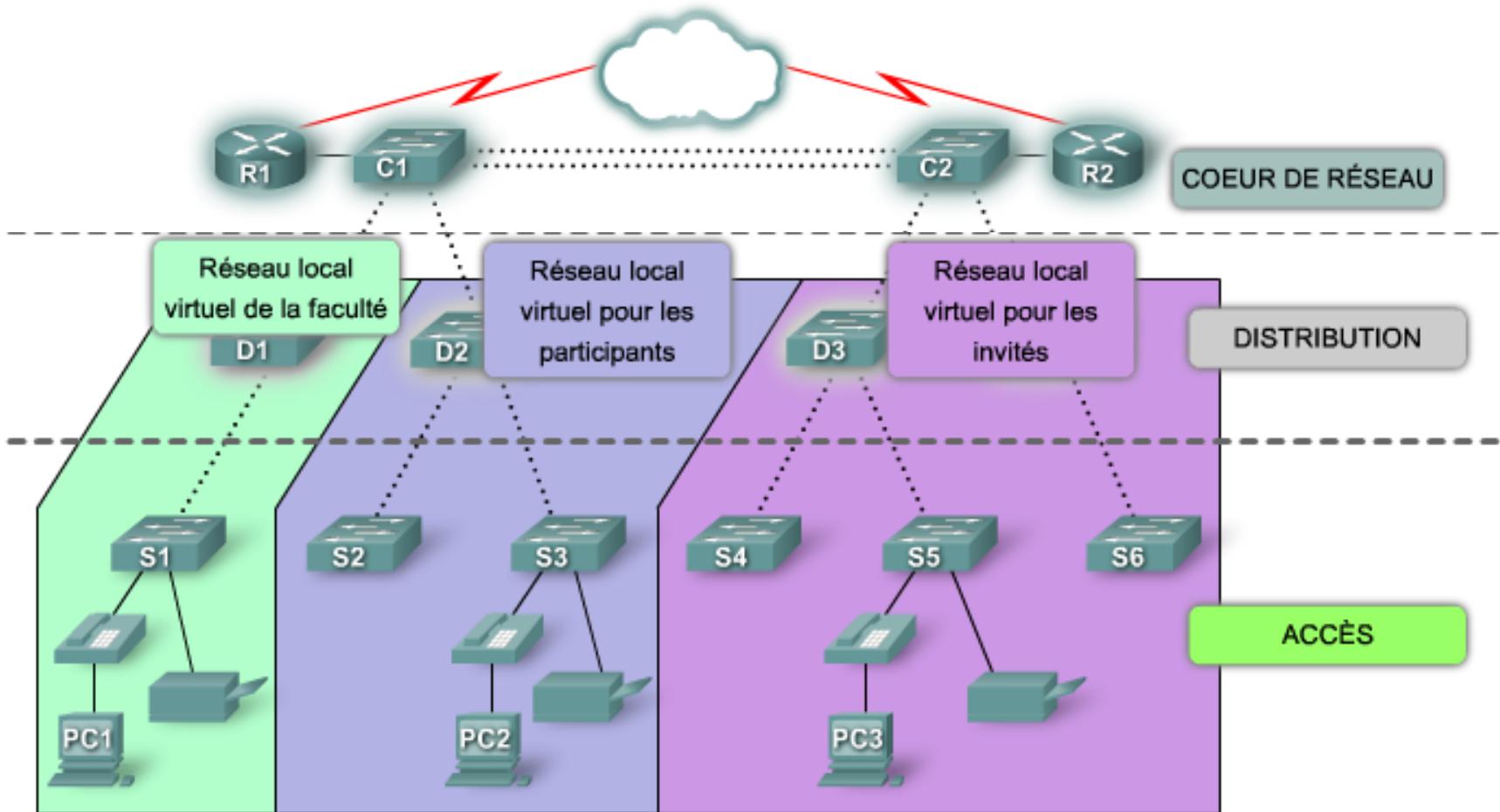
Réseau hiérarchique

- Comparé à d'autres conceptions de réseau, un réseau hiérarchique est plus simple à gérer et à développer, tandis que les problèmes sont résolus plus rapidement
- Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global
- En séparant les différentes fonctions existantes sur un réseau, la conception de réseau devient modulaire, ce qui facilite l'évolutivité et les performances
- Le modèle de conception hiérarchique classique se divise en trois couches : la couche d'accès, la couche de distribution et la couche cœur de réseau

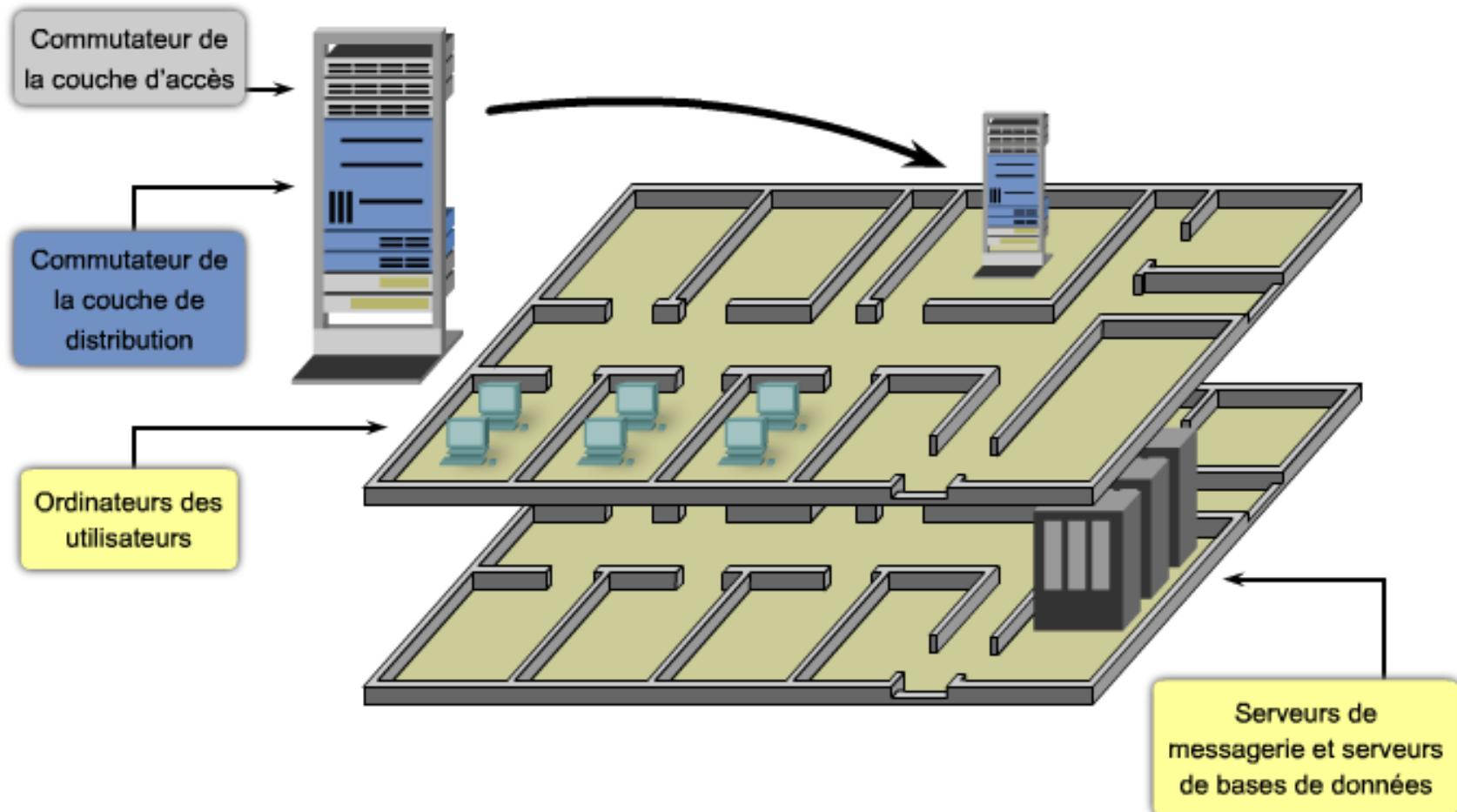
Modèle de réseau hiérarchique

- **Couche d'accès** : elle sert d'interface avec des périphériques, tels que des ordinateurs, des imprimantes et des téléphones sur IP, afin de fournir un accès au reste du réseau
 - Elle peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil
- **Couche de distribution** : elle regroupe les données reçues à partir des commutateurs de la couche d'accès, avant leur transmission vers la couche cœur de réseau, en vue du routage vers leur destination finale
 - La couche de distribution gère le flux du trafic réseau à l'aide de stratégies, et délimite les domaines de diffusion via des fonctions de routage entre des réseaux locaux virtuels (VLAN) définis au niveau de la couche d'accès
- **Couche cœur de réseau** : elle constitue le réseau fédérateur à haut débit de l'interréseau et est essentielle à l'interconnectivité entre les périphériques de la couche de distribution
 - Par conséquent, il est important qu'elle bénéficie d'une disponibilité et d'une redondance élevées
 - La zone principale peut également se connecter à des ressources Internet

Modèle de réseau hiérarchique



Réseau hiérarchique d'une entreprise moyenne



Avantage d'un réseau hiérarchique

Évolutivité

- Les réseaux hiérarchiques peuvent être aisément étendus.

Redondance

- La redondance au niveau des couches principale et de distribution garantit la disponibilité de chemins d'accès.

Performances

- L'agrégation de liaisons entre les niveaux et les commutateurs des couches principale et de distribution très performants permettent de bénéficier d'une vitesse proche de celle du câble à travers le réseau.

Sécurité

- La sécurité de port au niveau de l'accès et les stratégies au niveau de la distribution renforcent la sécurité du réseau.

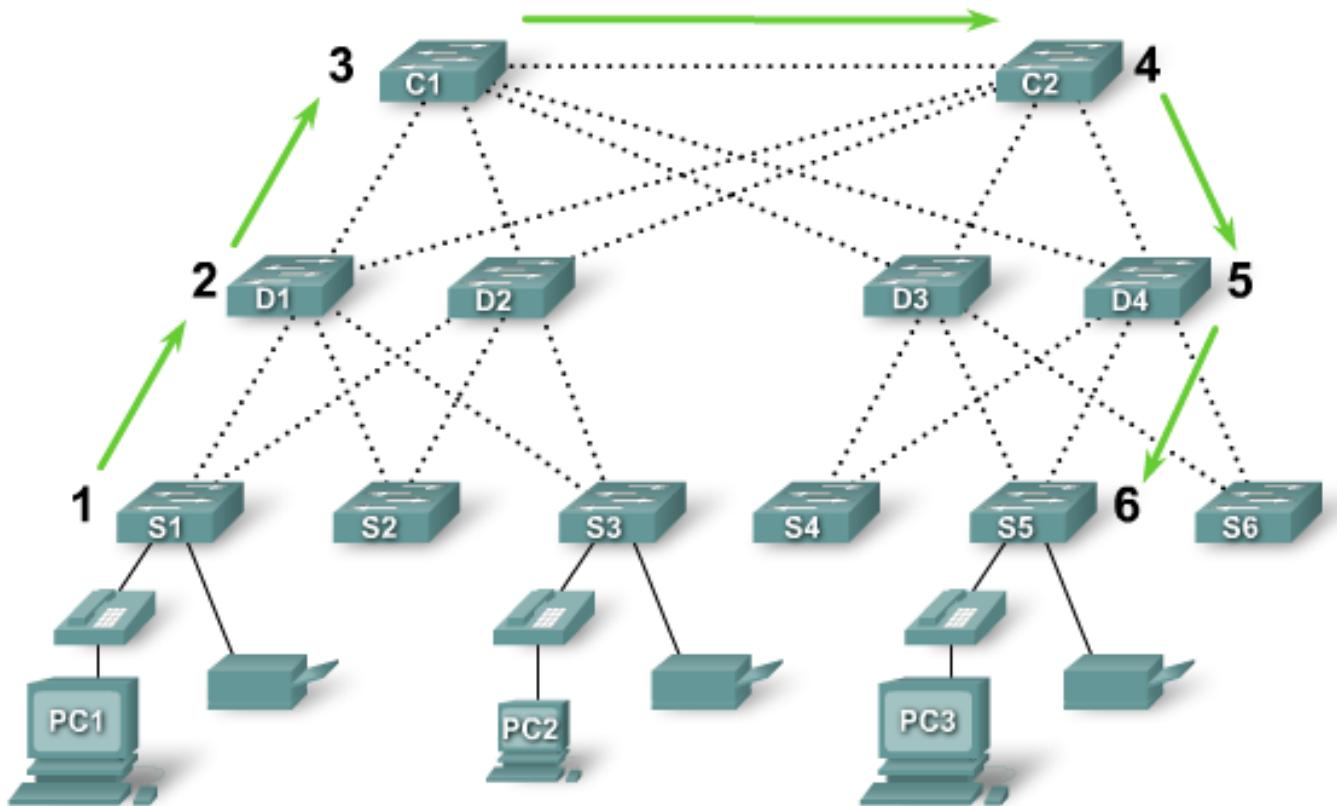
Facilité de gestion

- La cohérence entre les commutateurs à chaque niveau simplifie davantage la gestion.

Maintenance

- La modularité de la conception hiérarchique permet une mise à l'échelle du réseau sans trop de complexité.

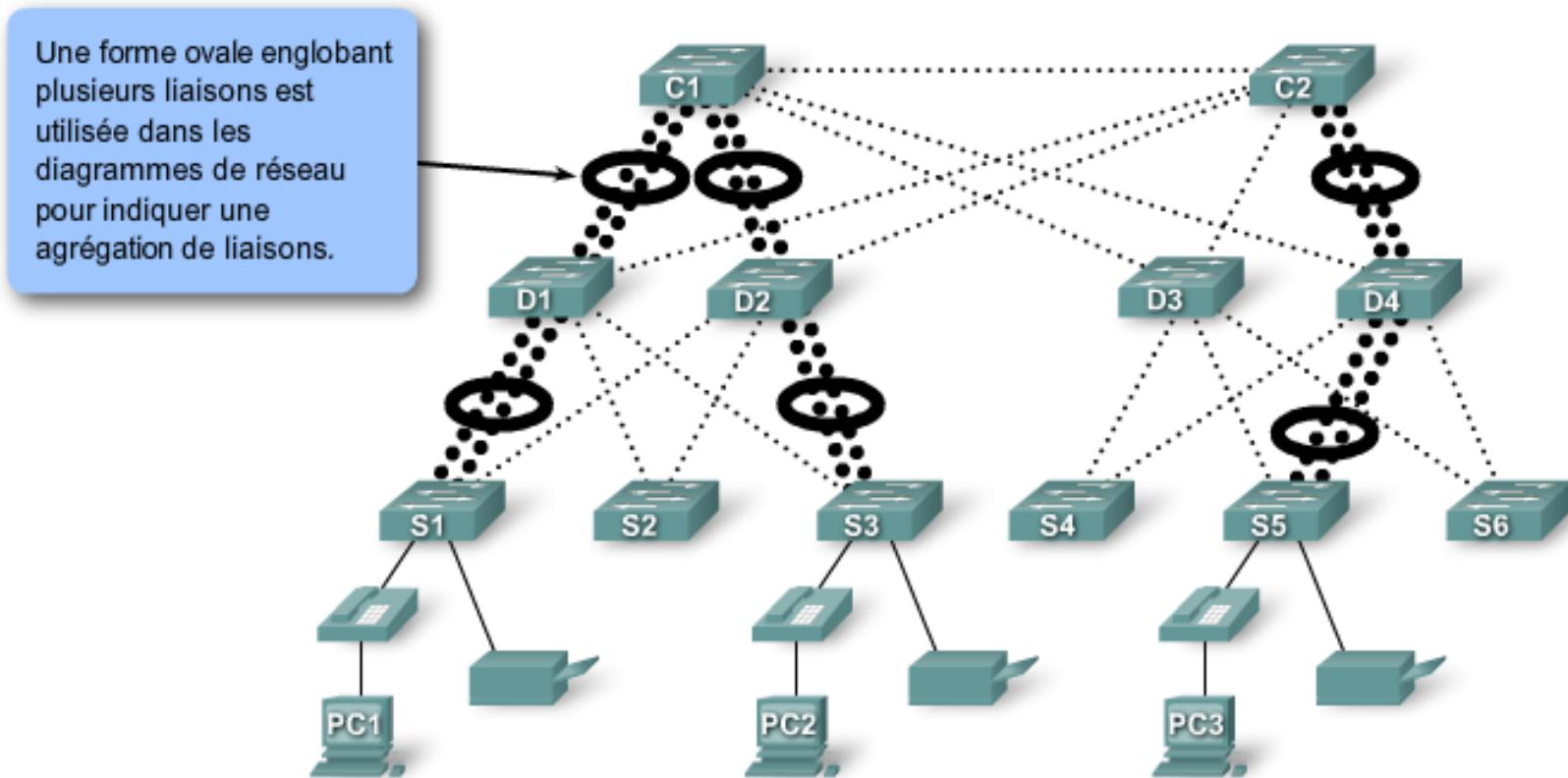
Principes du modèle de réseau hiérarchique : diamètre du réseau



- Le diamètre de réseau correspond au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination
- Lorsque vous maintenez un **faible diamètre de réseau**, cela garantit une **latence faible** et prévisible entre les périphériques

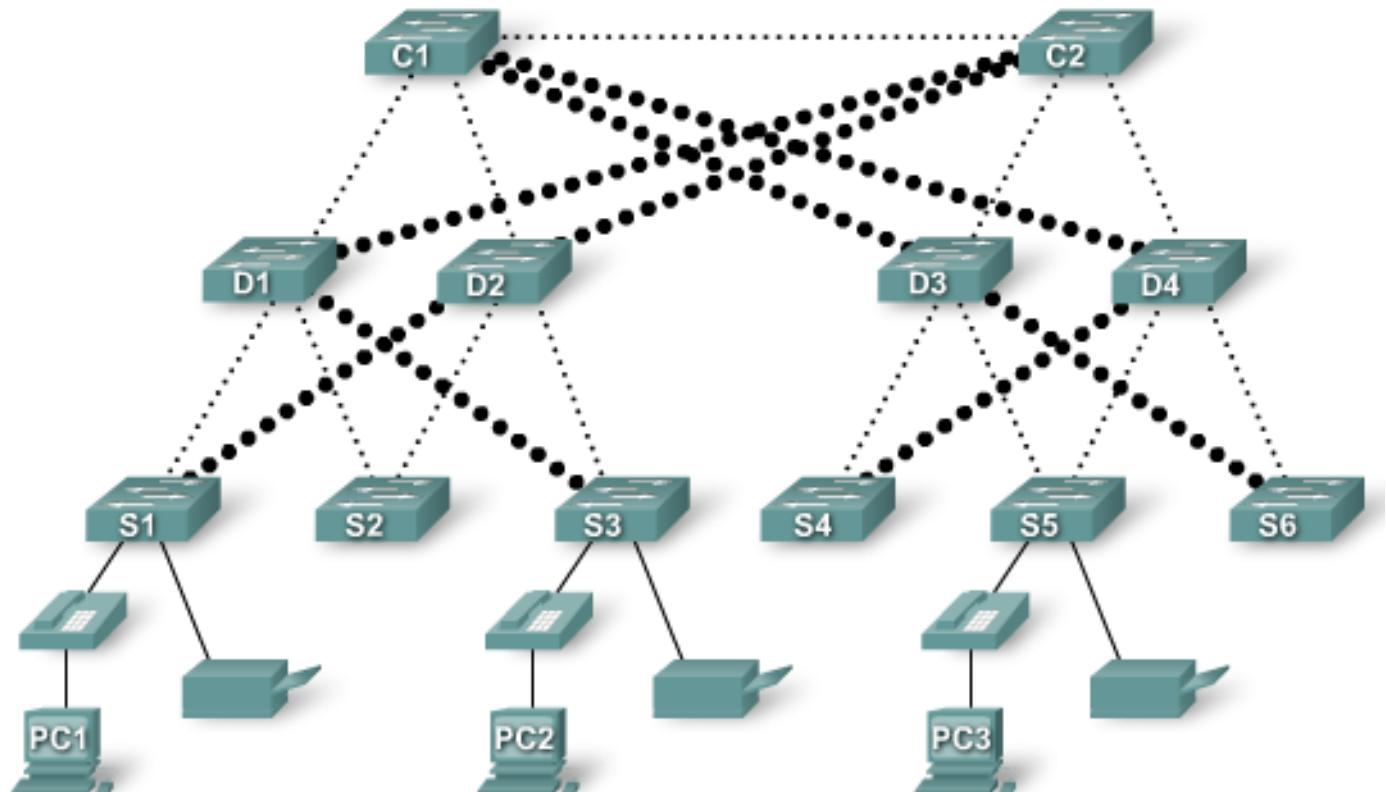
Agrégation de bande passante

L'agrégation de bande passante est normalement implémentée en combinant plusieurs liaisons parallèles entre deux commutateurs au sein d'une liaison logique.



Liaisons redondantes

Des réseaux modernes utilisent des liaisons redondantes entre des couches de réseau hiérarchique afin de garantir la disponibilité du réseau.



Réseau convergent

- Les réseaux vocaux, vidéo et de données convergents sont récemment devenus plus populaires sur le marché des petites et moyennes entreprises, en raison de progrès technologiques
- La convergence est dorénavant plus simple à implémenter et à gérer, et moins onéreuse
- L'un des avantages d'un réseau convergent est qu'il n'y a qu'un réseau à gérer
- Avec des réseaux vocaux, vidéo et de données séparés, les modifications apportées doivent être coordonnées à travers les réseaux



Moyennes à grandes entreprises



Petites à moyennes entreprises

Convergence

- Vous pouvez dorénavant associer les communications vocales et vidéo directement au sein du système informatique personnel d'un employé
- Les réseaux convergents nécessitaient aussi une vaste gestion associée à la qualité de service, car le trafic de données vocales et vidéo devait être classifié et prioritaire sur le réseau



Convergence



VLSM

VLSM

- (**V**ariable **L**ength **S**ubnet **M**ask) permet à un réseau classless d'utiliser différents masques de sous-réseaux au sein d'une organisation
- Avoir sous-réseaux plus appropriés aux besoins

Masques de longueur variable

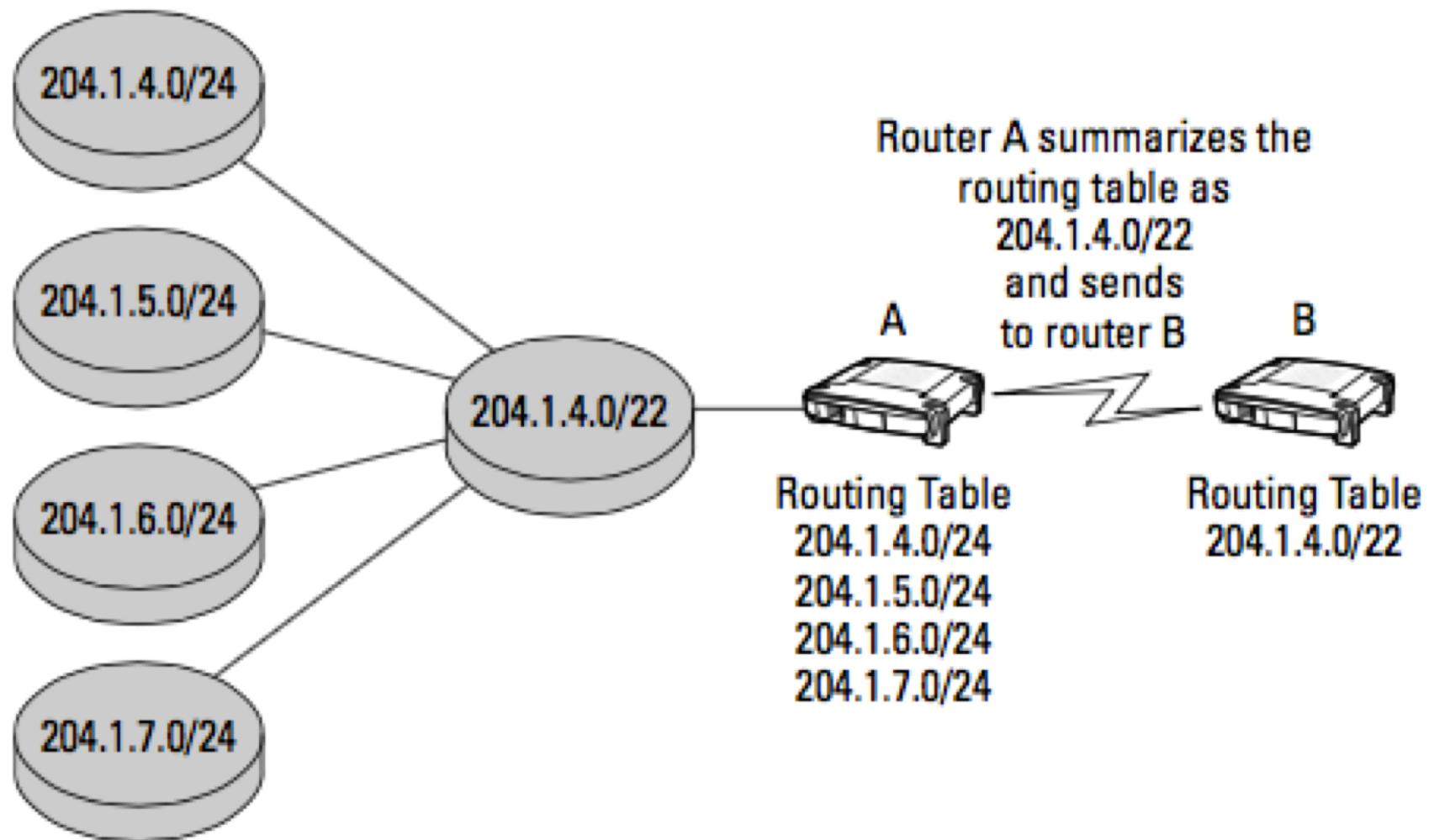
VLSM Variable Length Subnet Mask

- Besoin: créer des sous réseaux de taille différente
- Exemple : Classe B 135.8.0.0/16 découpé par le masque 255.255.254.0 ou /23 (soit $2^7 = 128$ sous-réseaux de $2^9 - 2 = 510$)
- Il se crée un nouveau sous-réseau de 15 hôtes (extension prévisible à 50)
 - Si on lui attribue une adresse de sous-réseau /23 on va perdre environ 500 adresses
 - Il serait par contre très intéressant de lui attribuer une adresse /26 d'un sous réseau de $64 - 2 = 62$ hôtes
- La solution : VLSM Variable Length Subnet Mask (RFC 1009 en 1987) : masques de taille variable

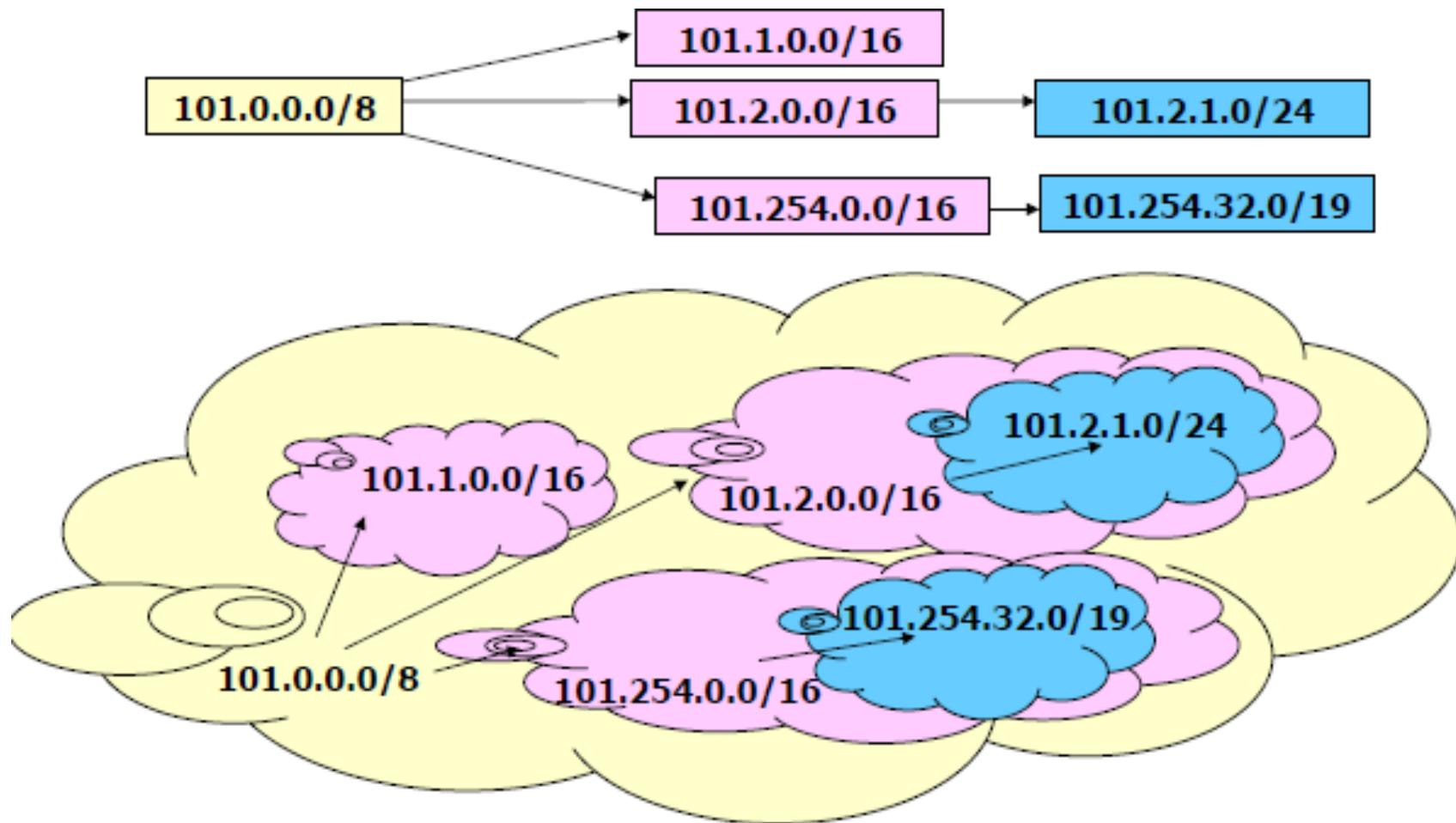
Problèmes posés par VLSM : Gestion des masques

- Chaque sous-réseau possède sa propre taille
 - Pour déterminer correctement le numéro de réseau quelque soit sa taille
 - Le protocole de routage interne doit utiliser un masque (un préfixe étendu) différent pour chaque sous réseau
 - Il doit transférer ces masques dans chaque route
- => Modifier les protocoles de routage
- RIP V2 ('Routing Information Protocol' RFC1388)
 - La version 2 permet de déployer VLSM.
 - OSPF ('Open Shortest Path First')

Résumé de route

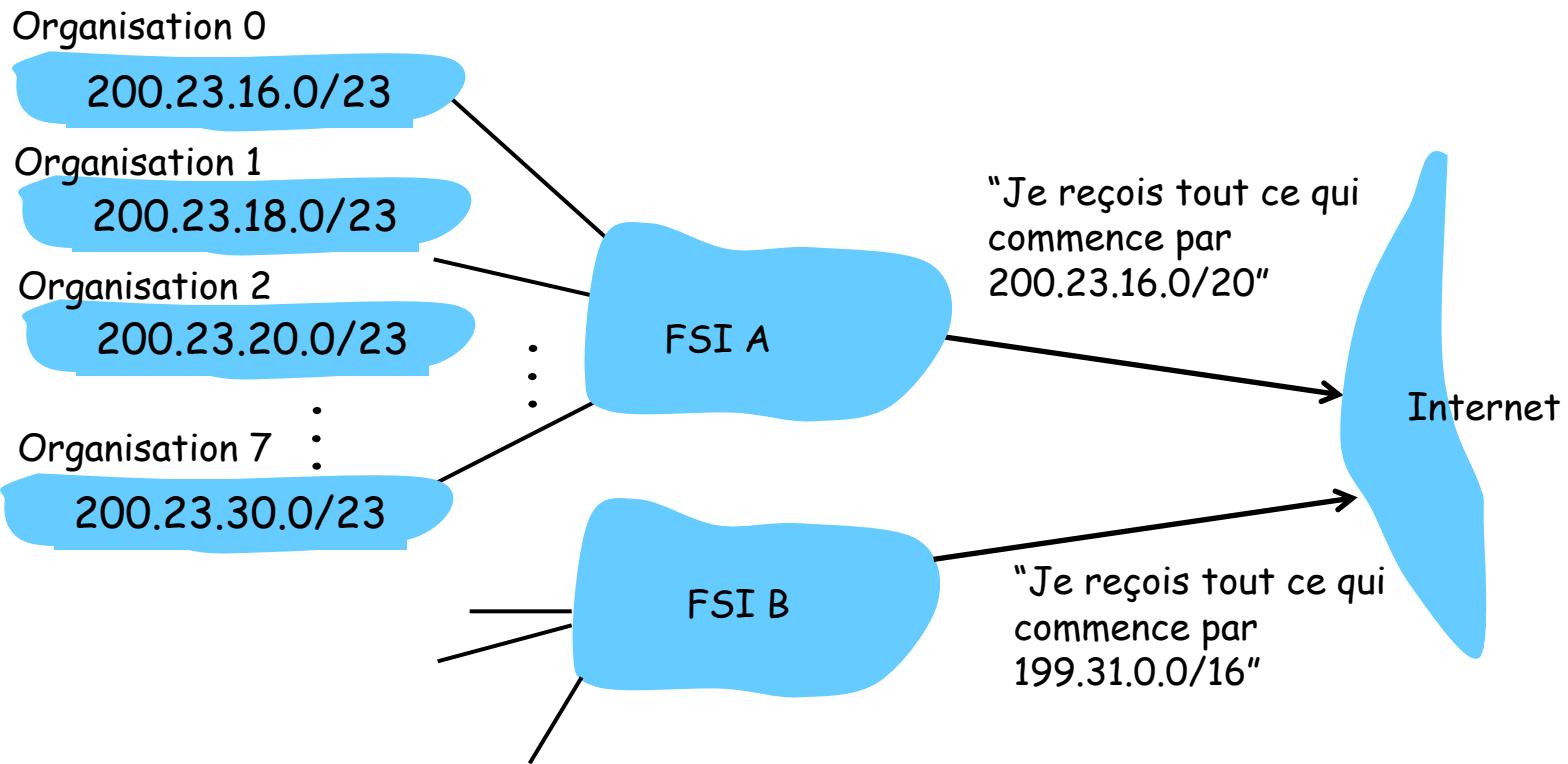


Exemple de gestion d'adresse avec agrégation 'topologique' en VLSM

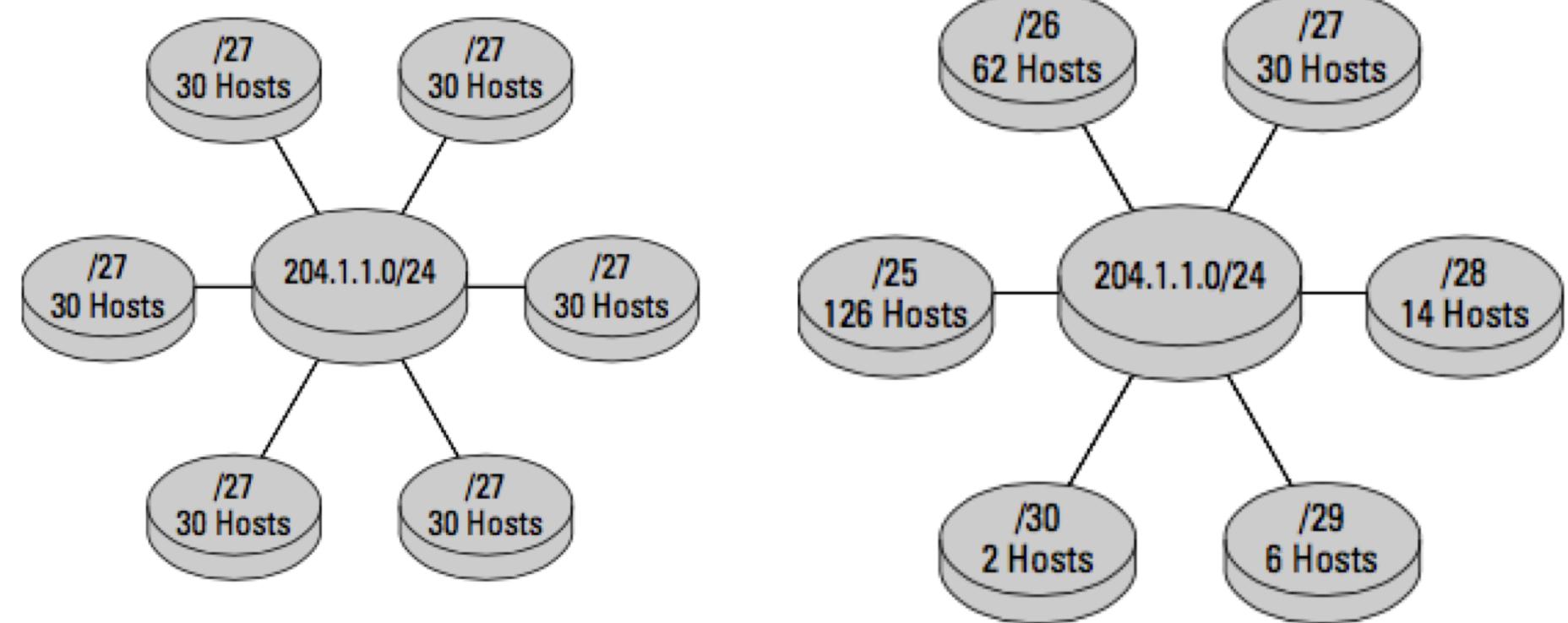


Adressage hiérarchique: agrégation de routes

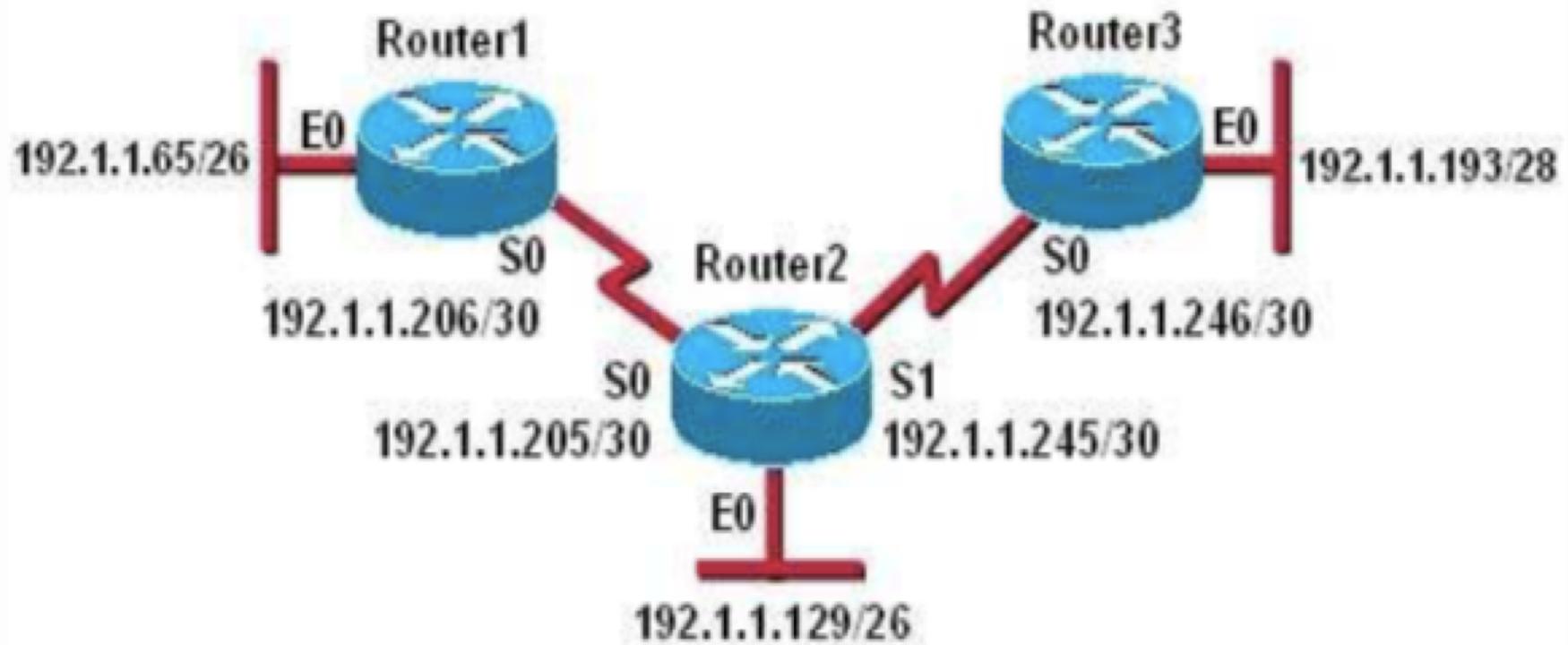
Le routage hiérarchique permet une annonce efficace des informations de routage



Etudier les pertes



Trouver l'incohérence !



ROUTAGE

TP routage Statique

#1-TP1_routage_Statique.pka

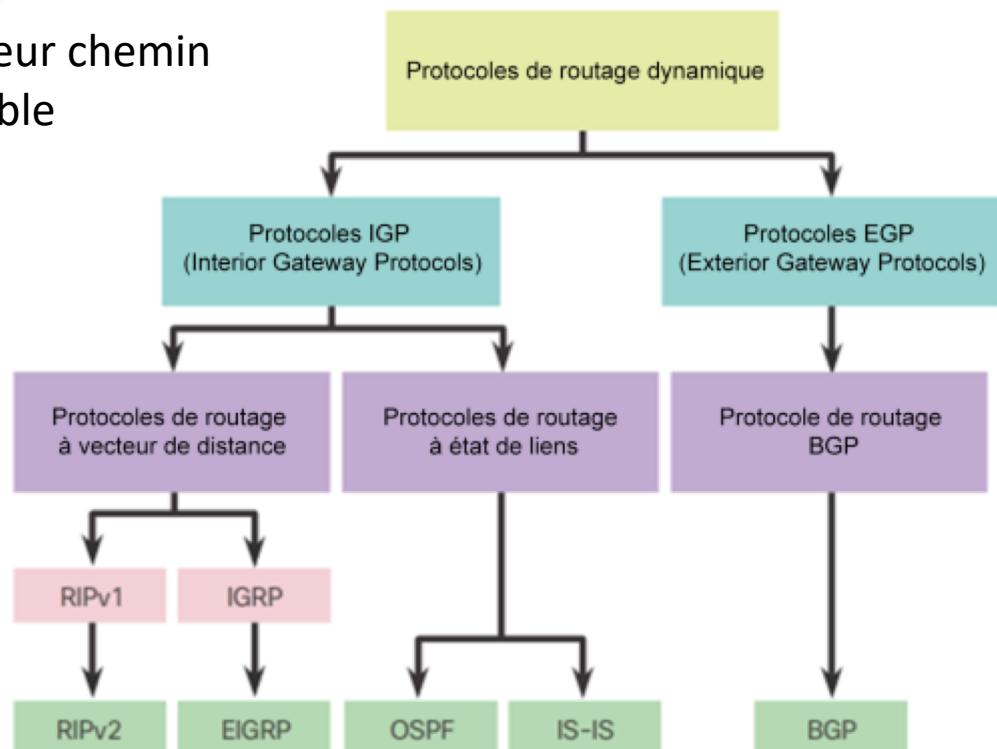
#2-TP_Bloucle_de_Routage.pka

#3-Depannage_Route_Statique.pka

#4-Routage_Statique_Projet_Final.pka (1 semaine)

Les types de protocoles de routage

- La fonction des protocoles de routage dynamique
 - Découverte des réseaux distants
 - Actualisation des informations de routage
 - Choix du meilleur chemin vers des réseaux de destination
 - Capacité à trouver un nouveau meilleur chemin si le chemin actuel n'est plus disponible
- Les types de protocoles de routage
 - État de liens
 - Vecteur de distance
 - Vecteur de chemin



Quelles autres améliorations ont été introduites dans les protocoles RIPv2 et EIGRP ?

Caractéristiques et fonctions	RIPv1	RIPv2	IGRP	EIGRP
Métrique	Les deux technologies utilisent le nombre de sauts comme simple métrique. Le nombre maximal de sauts correspond à 15.		Utilisez à la fois une métrique composée consistant en la bande passante et le délai. La fiabilité et la charge peuvent également être incluses dans le calcul de la métrique.	
Mises à jour transmises à l'adresse	255.255.255.255	224.0.0.9	255.255.255.255	224.0.0.10
Prise en charge de VLSM	✗	✓	✗	✓
Prise en charge de CIDR	✗	✓	✗	✓
Prise en charge de la récapitulation	✗	✓	✗	✓
Prise en charge de l'authentification	✗	✓	✗	✓

Le protocole RIP

- Voir répertoire TP RIP

#1-TP2_routage_Dynamique_RIPv1

#2-TP2_routage_RIP_interfacePassive.pka

#3-TP3_routage_RIP_V2.pka

#4-RoutageStatique_RIP_Projet_Final

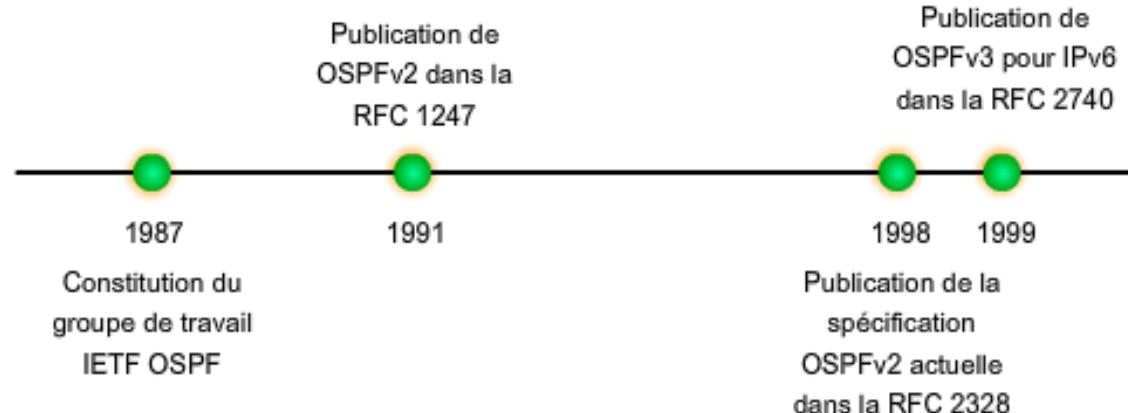
Les bénéfices des protocoles de routage à état de liens

- Avantages
 - Crée une carte topologique complète du réseau pour déterminer le chemin le plus court
 - Diffuse immédiatement le paquet LSP pour atteindre une convergence plus rapide
 - Envoie uniquement le paquet LSP avec de nouvelles informations en cas de modification de la topologie
 - Utilise le concept de zones et prend en charge la récapitulation
- Inconvénients
 - Nécessite de la mémoire supplémentaire pour assurer la maintenance de la base de données et de l'arborescence SPF
 - Requiert davantage de ressources de traitement du CPU pour calculer l'algorithme SPF et créer une carte topologique complète
 - Exige davantage de bande passante lors du démarrage initial des routeurs, ce qui peut poser problème sur les réseaux instables

OSPF

Historique de OSPF

	Protocoles de routage à vecteur de distance	Protocoles de routage à état de liens	Protocole BGP
Par classe	RIP IGRP		EGP
Sans classe	RIPv2 EIGRP	OSPFv2	IS-IS BGPv4
IPv6	RIPng EIGRP pour IPv6	OSPFv3 IS-IS pour IPv6	BGPv4 pour IPv6



OSPF (Open Shortest Path First)

- “open”: disponible gratuitement (protocole ouvert)
- Utilise un algorithme à état des liens
 - Topologie complète au niveau de chaque noeud
 - Les routes sont calculées avec l’algorithme de Dijkstra
 - La métrique utilisée est le coût des liens (administratif ou calculé à partir de la bande passante, délai)
 - Informations envoyées de manière périodique
- Algorithme relancé dès qu'il y a un changement détecté par un routeur. Il est aussi relancé systématiquement toutes les 30 secondes
- Annonces propagées au AS complet (via flooding = inondation)
 - Messages transportés directement sur IP (au lieu de TCP ou UDP)

Ce que OSPF a de plus par rapport à RIP

- **Securité:** tous les messages OSPF sont authentifiés
- **Multiple same-cost paths** sont possibles
- On peut avoir plusieurs métriques de QoS pour chaque lien
 - **TOS différents** (satellite link cost set “low” for best effort; high for real time)
- Integre uni- and **multicast** support:
 - Utilisation de Multicast OSPF (MOSPF)
- **Hierarchical** OSPF pour les domaines larges

Les 5 types de messages du protocole OSPF

Messages	Signification
Hello	Permet de découvrir qui sont les routeurs voisins
Mise à jour d'état de lien (routeur adjacent)	Informations d'état fournie à la base de données topologique
Accusé de réception de mise à jour	Acquittement d'une mise à jour d'état de lien
Demande d'état de lien	Demande d'information à la base de données topologique sur un partenaire
Description de lien	La base de données topologique donne les informations d'état de lien à qui en a besoin

Chaque message a un numéro de séquence qui permet de contrôler l'échange et la fraîcheur des informations lors de mise à jour. Seul le Master peut l'incrémenter de 1 à chaque message envoyé et le Slave recopie ce numéro dans son message d'acquittement

Messages OSPF encapsulé

En-tête de trame de liaison de données

En-tête de paquet IP

En-tête de paquet OSPF

Données spécifiques de type de paquet OSPF

Trame de liaison de données (champs Ethemet affichés ici)

Adresse MAC de destination = multidiffusion : 01-00-5E-00-00-05 ou 01-00-5E-00-00-06

Adresse MAC source = adresse de l'interface d'envoi

Paquet IP

Adresse IP source = adresse de l'interface d'envoi

Adresse IP de destination = multidiffusion : 224.0.0.5 ou 224.0.0.6

Champ de protocole = 89 pour OSPF

En-tête de paquet OSPF

Code du type de paquet OSPF

ID du routeur et ID de la zone

Types de paquet OSPF

0x01 Hello

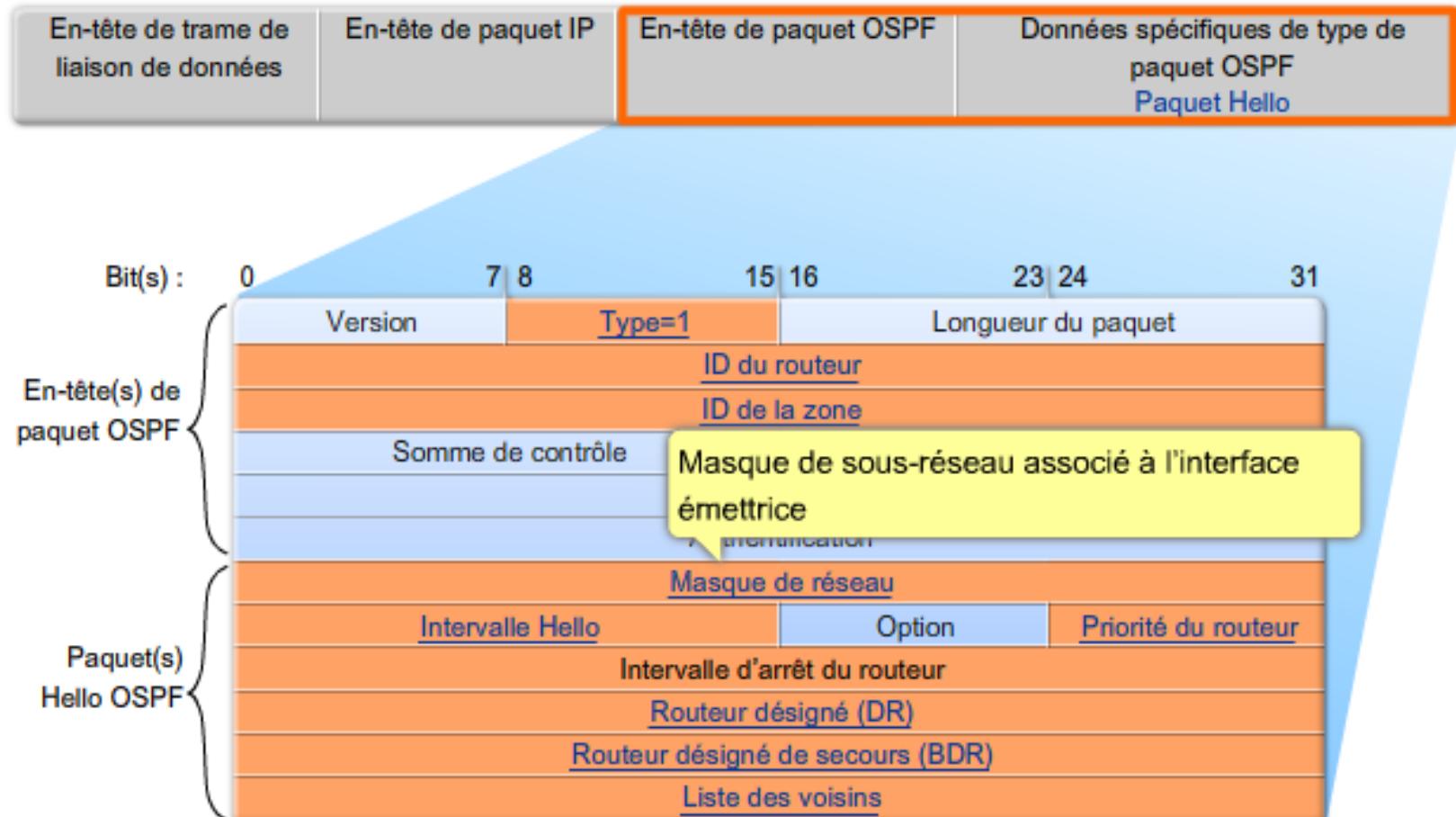
0x02 Description de base de données
(DD)

0x03 Requête d'état de liens

0x04 Mise à jour d'état de liens

0x05 Accusé de réception d'état de liens

Format de messages OSPF



Fonctionnement succinct d'OSPF

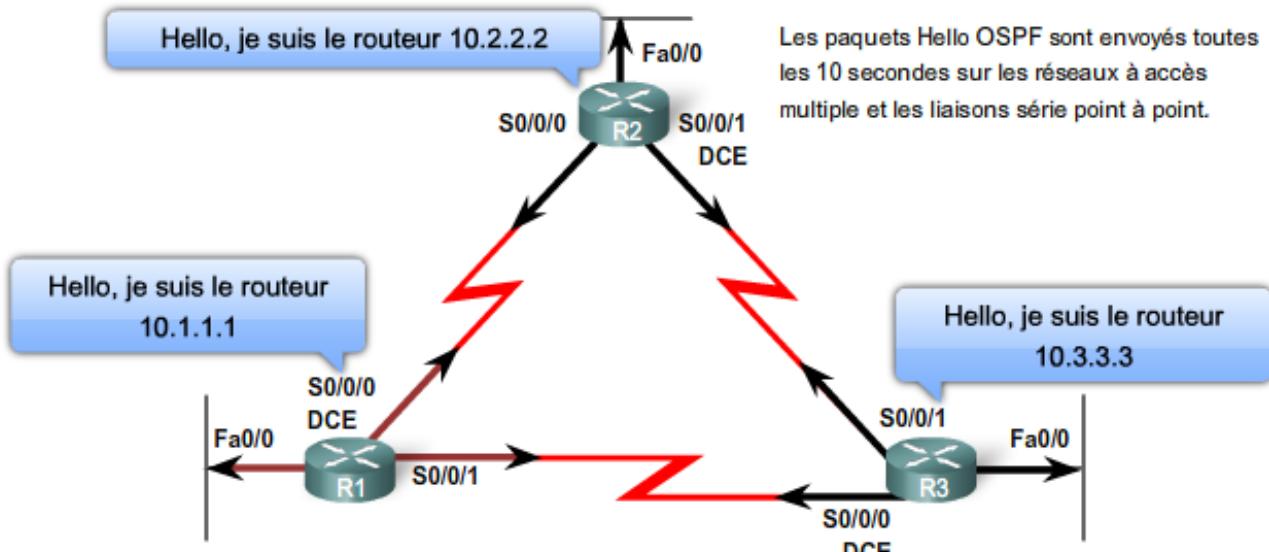
- Directement au dessus d'IP (protocole 87)
- OSPF utilise des adresses multicast **224.0.0.5** pour adresser tous les routeurs de l'aire et 224.0.0.6 pour communiquer avec le routeur désigné
 - L'adresse multicast permet au périphérique d'ignorer le paquet si son interface n'est pas activée pour accepter les paquets OSPF et par conséquent on économise du temps processeur sur les périphériques non OSPF
- Fonctionnement décomposé en quatre étapes:
 - Élection du routeur désigné
 - Synchronisation des données topologiques
 - Mise à jour des bases de données
 - Calcul du chemin le plus court

Fonctionnement succinct d'OSPF

- OSPF met en œuvre trois sous-protocoles:
 - Le protocole « Hello » est utilisé entre deux routeurs adjacents pour synchroniser leur base de connaissance
 - Permet de vérifier la connectivité entre les nœuds, d'élire le routeur désigné et le routeur de backup
 - Le protocole d'échange permet, lors de l'initialisation d'un routeur, l'acquisition des entrées de sa base de données
 - Le protocole d'inondation est utilisé par un routeur pour signaler la modification de l'état d'un lien qui lui est rattaché

Message Hello

- **Intervalle Hello** = fréquence d'envoie des paquets (10s si accès multiple et point à point; 30s pour FR, X.25, ATM)
- **Intervalle dead (arrêt)** = temps d'attente avant de déclarer le voisin « hors service » (40 s si accès multiple et point à point; 120s pour NBMA (FR, X.25, ATM))
- Types de réseaux (point à point, accès multiples avec diffusion, accès NBMA, point à multipoint, liaisons virtuelles)



Mise en correspondance des valeurs d'interface des deux routeurs afin de créer une contiguïté

$$\left. \begin{array}{l} \text{Intervalle Hello} \\ \text{Intervalle Dead} \\ \text{Type de réseau} \end{array} \right\} = \left. \begin{array}{l} \text{Intervalle Hello} \\ \text{Intervalle Dead} \\ \text{Type de réseau} \end{array} \right\}$$

Distance administrative

Source de la route	Distance administrative
Connectée	0
Statique	1
Résumé de routes EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

ID de routeur OSPF

- ID de routeur OSPF permet l'identification unique d'un routeur dans le domaine OSPF
- Les routeurs Cisco définissent leur ID de routeur en utilisant trois critères, selon la priorité ci-dessous :
 1. **Utilisation de l'adresse IP** configurée avec la commande **router-id** du protocole OSPF
 2. Si router-id n'est pas configuré, le routeur choisit l'adresse IP **la plus élevée** parmi ses interfaces de bouclage (**loopback**) IP
 3. Si aucune interface de bouclage n'est configurée, le routeur choisit l'adresse IP active **la plus élevée** parmi ses **interfaces physiques**

ID de routeur OSPF (2)

Adresse de loopback

Router(config)#interface loopback number

Router(config-if)#ip address adresse IP masque de sous-réseau

Commande router-id OSPF

Router(config)#router ospf process-id

Router(config-router)#router-id ip-address

Modification de l'ID de routeur

Router#clear ip ospf process (ou reload)

Attention: Lorsque deux routeurs portent le même ID dans un domaine OSPF, le routage risque de ne pas fonctionner correctement

En réalité ...

- Protocole complexe de routage dans sa mise en œuvre (plan d'adressage, initialisation des métriques...), complexe dans son fonctionnement (temps de calcul,...)
- OSPF remédie aux principaux inconvénients de RIP (temps de convergence, boucle,...)
- Pour une entreprise le choix du protocole est stratégique. Quelles que soient les qualités des protocoles propriétaires, ils sont et demeurent propriétaires ce qui constitue un handicap pour l'évolution du réseau ou du renouvellement des équipements

OSPF vs RIP

Characteristic	OSPF	RIPv2	RIPv1
Type of protocol	Link state	Distance vector	Distance vector
Classless support	Yes	Yes	No
VLSM support	Yes	Yes	No
Auto-summarization	No	Yes	Yes
Manual summarization	Yes	No	No
Discontiguous support	Yes	Yes	No
Route propagation	Multicast on change	Periodic multicast	Periodic broadcast
Path metric	Bandwidth	Hops	Hops
Hop count limit	None	15	15

OSPF vs RIP (2)

Characteristic	OSPF	RIPv2	RIPv1
Convergence	Fast	Slow	Slow
Peer authentication	Yes	Yes	No
Hierarchical network	Yes (using areas)	No (flat only)	No (flat only)
Updates	Event triggered	Route table updates	Route table updates
Route computation	Dijkstra	Bellman-Ford	Bellman-Ford

Exemple de configuration de OSPF

```
Lab_A(config)#router ospf ?
```

<1-65535> (processus OSPF qui peut tourner sur un même router)

```
Lab_A#config t
```

```
Lab_A(config)#router ospf 1
```

```
Lab_A(config-router)#network 10.0.0.0 0.255.255.255  
area ?
```

<0-4294967295> OSPF area ID as a decimal value

A.B.C.D OSPF area ID in IP address format

```
Lab_A(config-router)#network 10.0.0.0 0.255.255.255  
area 0
```

Debugging OSPF

Lab_A# sh ip protocols

Lab_A# sh ip ospf

Lab_A# sh ip ospf database

Lab_A# sh ip ospf interface *interface_number*

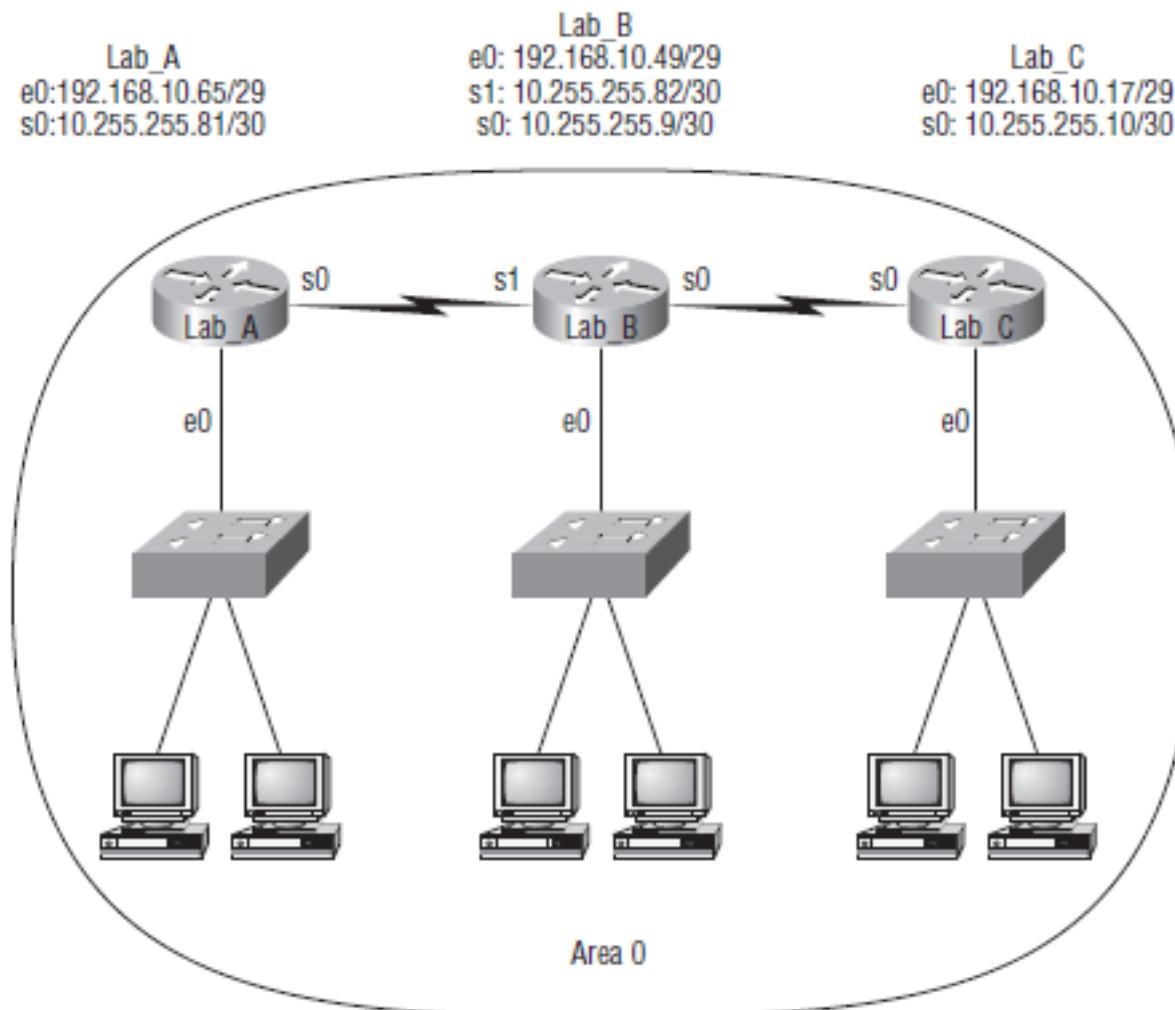
Lab_A# sh ip ospf neighbor (montre les voisins, les DR, et BDR)

Lab_A# debug ip ospf packet (montre les paquets hello)

Lab_A# debug ip ospf hello (montre les paquets hello avec plus de détails)

Lab_A# debug ip ospf adj (montre l'élection des DR et BDR)

Exemple de config OSPF



Exemple de config OSPF (2)

Lab_A#**config t**

Lab_A(config)#**router ospf 1**

Lab_A(config-router)#**network 192.168.10.64 0.0.0.7 area 0**

Lab_A(config-router)#**network 10.255.255.80 0.0.0.3 area 0**

Lab_B#**config t**

Lab_B(config)#**router ospf 1**

Lab_B(config-router)#**network 192.168.10.48 0.0.0.7 area 0**

Lab_B(config-router)#**network 10.255.255.80 0.0.0.3 area 0**

Lab_B(config-router)#**network 10.255.255.8 0.0.0.3 area 0**

Lab_C#**config t**

Lab_C(config)#**router ospf 1**

Lab_C(config-router)#**network 192.168.10.16 0.0.0.7 area 0**

Lab_C(config-router)#**network 10.255.255.8 0.0.0.3 area 0**

OSPF et les interfaces de loopback

- Configurer une interface de loopback permet d'assurer que votre interface sera toujours active pour les process OSPF
- Regardez quel est le ID des routeurs
- Configurer une interface de loopback au niveau de chaque routeur

Exemple :

```
Lab_A#sh ip ospf
```

Routing Process "ospf 132" with ID 10.1.5.1

[output cut]

Le ID du routeur est « 10.1.5.1 »

```
Lab_A(config)#int loopback 0
```

Mar 22 01:23:14.206: %LINEPROTO-5-UPDOWN: Line protocol on Interface

Loopback0, changed state to up

```
Lab_A(config-if)#ip address 10.1.1.1 255.255.255.255
```

Le prefixe /32 permet d'utiliser plus tard n'importe quelle adresse que nous souhaitons en évitant des collisions d'adresse

Réaliser TP 1

Objectifs Pédagogiques

- Vérifier la connectivité avec le périphérique du tronçon suivant
- Configurer le routage OSPF sur le routeur R1
- Configurer le routage OSPF sur le routeur R2
- Configurer le routage OSPF sur le routeur R3
- Vérifier les configurations

Métriques OSPF

- La métrique OSPF s'appelle le coût
 - Citation du document RFC 2328 : « Un coût est associé au niveau de la sortie de chaque interface de routeur. Ce coût est configurable par un administrateur système. Plus le coût est faible, plus l'interface sera utilisée pour acheminer le trafic de données. »
 - Le coût d'une route OSPF est la valeur cumulée depuis un routeur jusqu'au réseau de destination.

Type d'interface	$10^8/\text{bits/s} = \text{Coût}$
Fast Ethernet et plus rapide	$10^8/100\,000\,000 \text{ bits/s} = 1$
Ethernet	$10^8/10\,000\,000 \text{ bits/s} = 10$
E1	$10^8/2\,048\,000 \text{ bits/s} = 48$
T1	$10^8/1\,544\,000 \text{ bits/s} = 64$
128 Kbits/s	$10^8/128\,000 \text{ bits/s} = 781$
64 Kbits/s	$10^8/64\,000 \text{ bits/s} = 1562$
56 Kbits/s	$10^8/56\,000 \text{ bits/s} = 1785$

Modification coût de la liaison

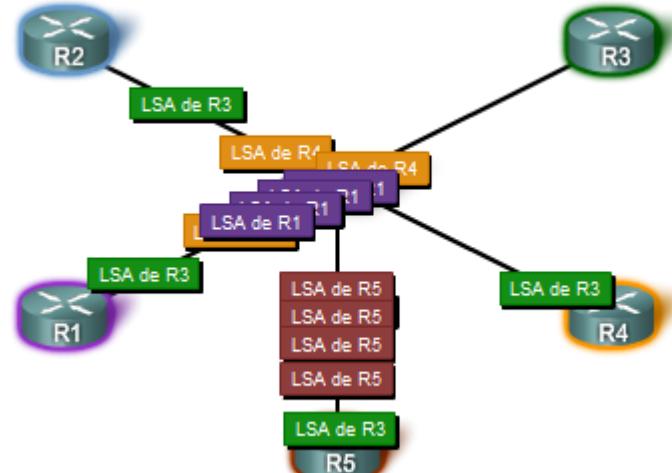
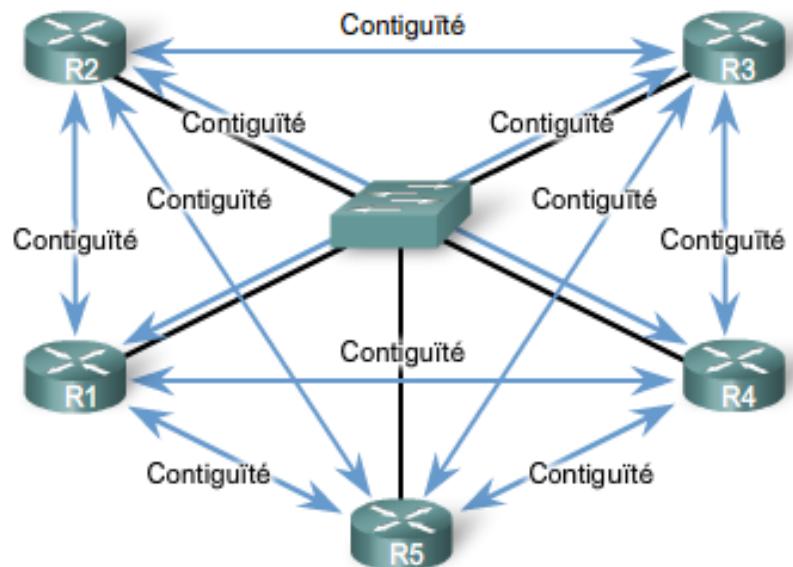
- Soit avec
 - R1(config)#interface serial 0/0/0
 - R1(config-if)#**ip ospf cost** 1562
- Ou avec
 - R1(config)#interface serial 0/0/0
 - Router(config-if)#**bandwidth bandwidth-kbps**
- Ou « auto-cost reference-bandwidth » qui permet à la bande passante de référence d'être modifiée pour s'adapter aux réseaux ayant des liaisons d'une rapidité supérieure à 100 Mbit/s

Réaliser TP 2

Objectifs pédagogiques :

- Examiner la configuration de coûts par défaut
- Modifier le coût avec la commande **ip ospf cost**
- Modifier le coût avec la commande **bandwidth**
- Vérifier les nouvelles valeurs de coût

Passage à l'échelle de OSPF



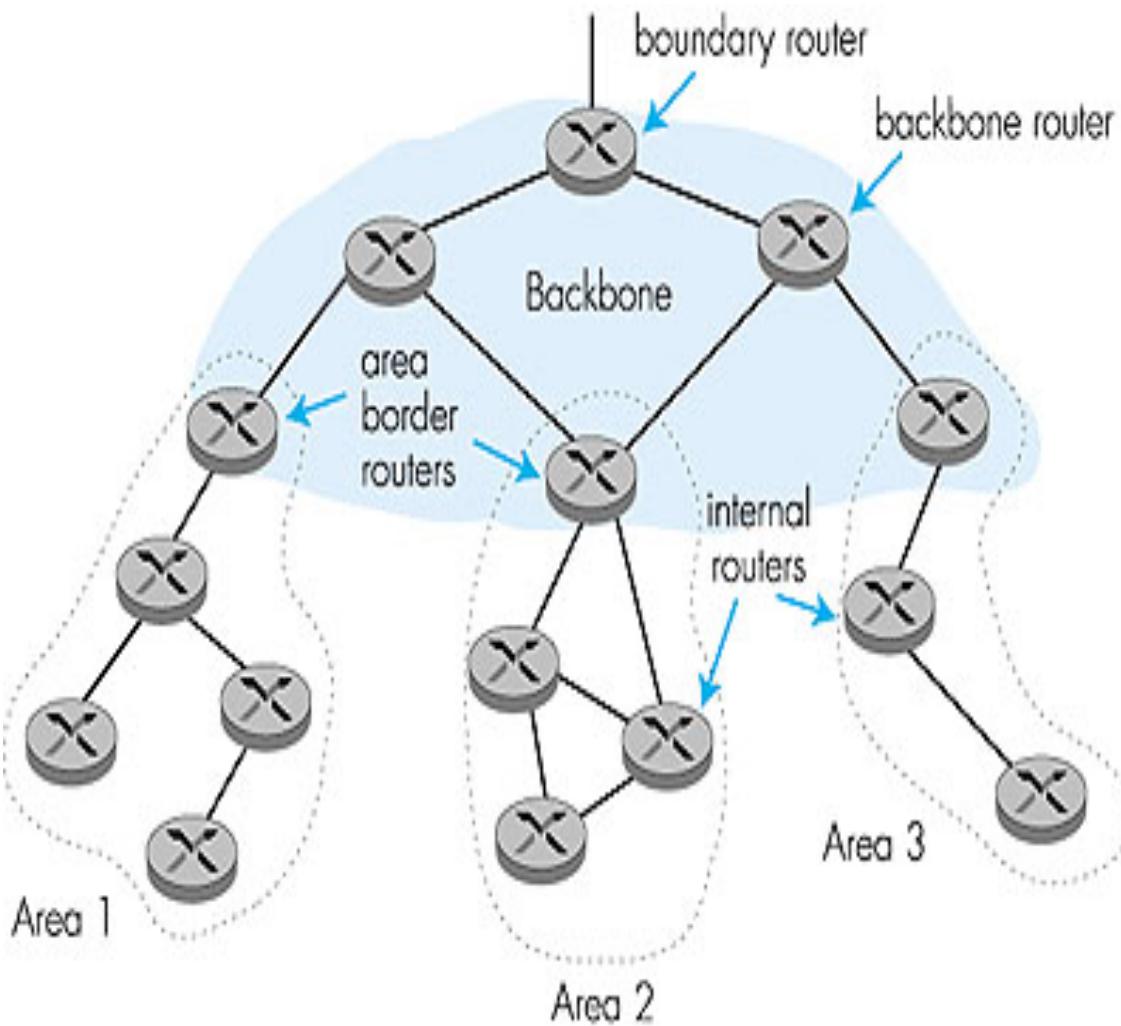
Routeurs	Contiguïtés
n	$\frac{n(n-1)}{2}$
5	10
10	45
20	190
100	4 950

$$\text{Nombre de contiguïtés} = \frac{n(n-1)}{2}$$

n = nombre de routeurs

Exemple : 5 routeurs $(5 - 1)/2 = 10$ contiguïtés

OSPF hiérarchique



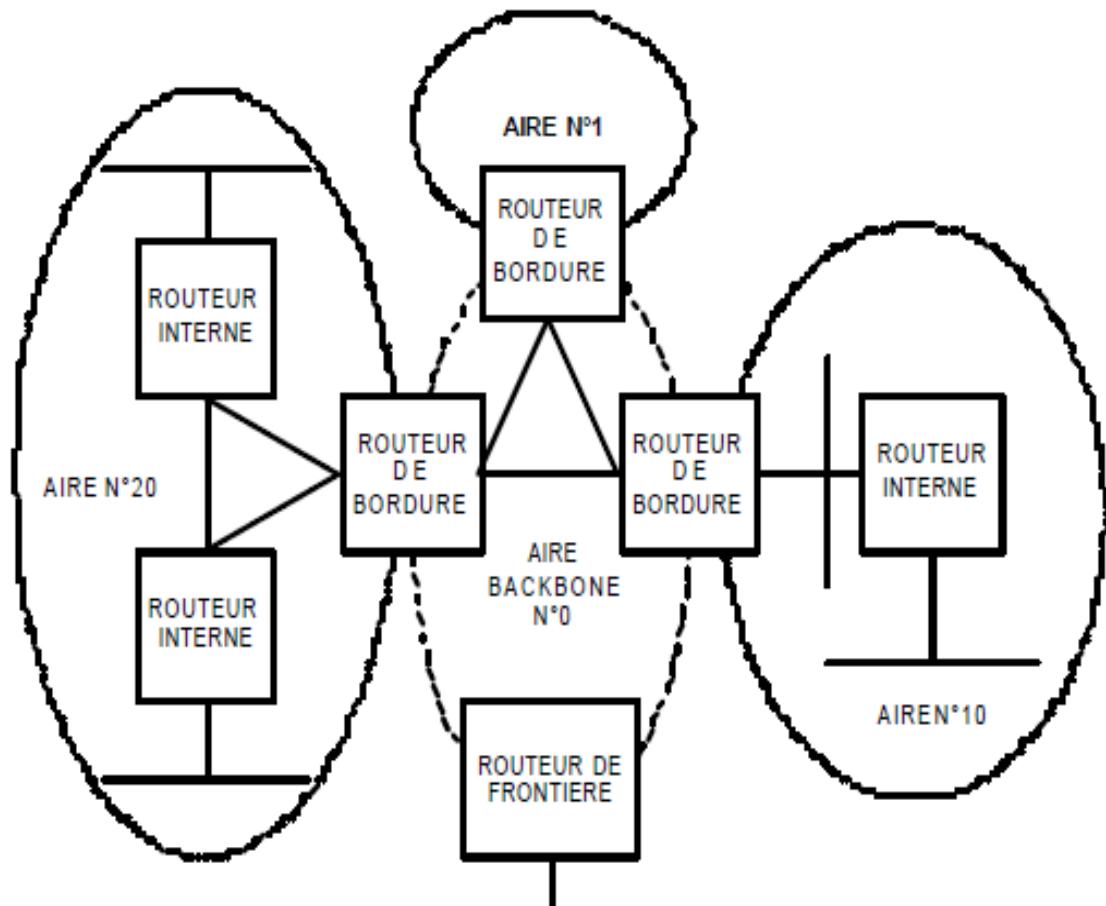
- Une aire OSPF ne possède aucune intersection avec une autre aire OSPF.
- On distingue l'aire 0, ou « backbone area » chargée d'interconnecter toutes les aires OSPF entre elles
- Les routeurs présents dans une aire, ne connaissent que la topologie de cette aire.
- Cependant, dans chaque aire, il existe au moins un routeur qui possède les bases de données permettant d'interconnecter différentes aires OSPF, soit au moins la base de données correspondant à son aire et celle correspondant à 'aire 0'

OSPF hiérarchique (2)

- **Deux niveaux hiérarchiques:** aire locale, aire zéro (area backbone)
 - Aire zéro (zone dite fédératrice) permet l’interconnexion de toutes les autres zones
 - Annonces limitées dans l’aire seulement
 - Chaque noeud détient une topologie détaillée de son aire; connaît seulement la direction (+ court chemin) vers les réseaux des autres aires
- **Area border routers (ABR):** “résume” les distances aux réseaux de son aire, annonce aux autres ABRs
- **Backbone routers:** routage OSPF limité au backbone
- **Boundary routers:** assure l’échange d’informations avec les autres AS

Hiérarchie des aires OSPF

- ❑ Les routeurs de zone ou **Internal Router (IR)** n'annoncent que les routeurs internes à leur zone (50 au routeurs au max.)
- ❑ Notion **Designated Router (DR,BackupDR)**: il diffuse les messages vers les routeurs de la zone ce qui nécessite que N messages (1 message vers le DR et N-1 messages du DR vers les hôtes)
- ❑ Nous avons les DR, BDR, et le DROther



Désignation des « routeurs désignés » (Designated Router)

- L'administrateur fixe une priorité de 0 à 255 à chaque routeur
- Le routeur de plus haute priorité est désigné dans chaque zone
- Un routeur de **priorité 0** ne pourra **jamais être élu routeur désigné**
 - **show ip ospf interface interface_number**
- Un routeur désigné de backup est aussi élu
- Si tous les routeurs ont la **même priorité** celui avec le **ID le plus grand est choisi**
 - Il est préférable de contrôler le choix des routeurs
 - **Router(config-if)#ip ospf priority {0 - 255}**
- Un routeur mis sous tension écoute le trafic et apprend ainsi quel est le routeur désigné et son backup. Il accepte même si sa priorité est grande
- C'est l'absence de trafic en provenance du routeur désigné qui permet de détecter sa panne et de déclencher le mécanisme de l'élection

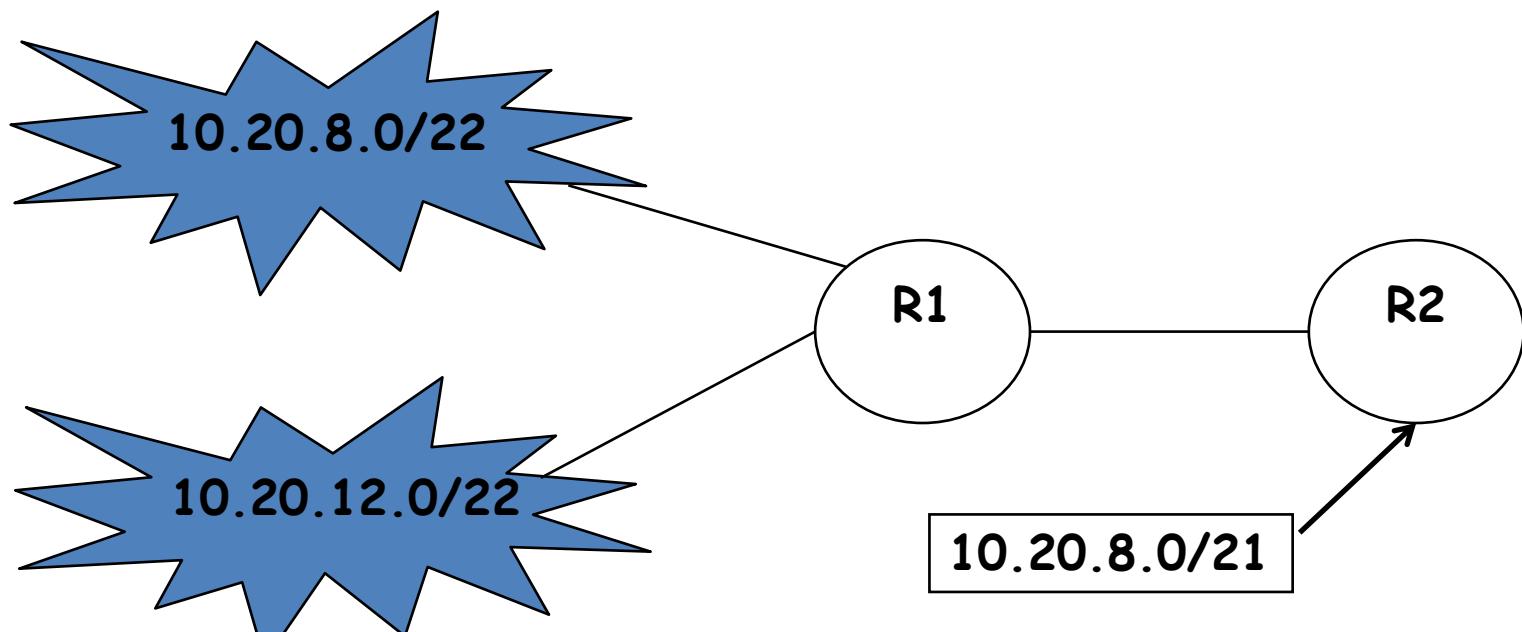
Réaliser TP 3

Objectifs pédagogiques :

- Examiner les rôles DR et BDR actuels
- Examiner les rôles DR et BDR qui changent
- Modifier la priorité de l'interface OSPF
- Forcer une nouvelle sélection
- Vérifier les nouveaux rôles DR et BDR

Agrégation des routes dans OSPF

- Si tous les réseaux d'une zone ont des adresses IP contiguës, le routeur ne signale qu'une seule route aux autres routeurs
- Permet d'une part de minimiser le trafic d'annonce et, d'autre part d'alléger les tables de routage



Redistribution du routage OSPF par défaut

- Le routeur situé entre un domaine de routage OSPF et un réseau non-OSPF est appelé **routeur ASBR** (*Autonomous System Boundary Router*)
- Comme RIP, OSPF nécessite la commande **default-information originate** pour annoncer la route statique par défaut 0.0.0.0/0 aux autres routeurs de la zone
- **R1(config-router)#default-information originate**
- Si la commande default-information originate n'est pas utilisée, la route par défaut ne sera pas diffusée aux autres routeurs de la zone OSPF

Réglage du protocole OSPF

Bandé passante de référence

- Pour obtenir des calculs de coûts plus précis, un ajustement des valeurs de bande passante de référence peut s'avérer nécessaire
- La bande passante de référence peut être modifiée pour prendre en compte ces liaisons plus rapides grâce à OSPF auto-cost reference-bandwidth

```
R1(config-if)#router ospf 1
```

```
R1(config-router)#auto-cost reference-bandwidth ?
```

```
1-4294967 The reference bandwidth in terms of  
Mbits per second
```

Réglage du protocole OSPF

Modification des intervalles

- Faites show ip ospf neighbor
- Les intervalles Dead et Hello OSPF peuvent être modifiés manuellement à l'aide des commandes d'interface suivantes :

```
Router(config-if)#ip ospf hello-interval secondes
```

```
Router(config-if)#ip ospf dead-interval secondes
```

Attention: OSPF exige que les intervalles Hello et Dead de deux routeurs correspondent pour devenir contigus

Réaliser TP 4

Objectifs pédagogiques :

- Configurer et redistribuer une route par défaut
- Vérifier que la route par défaut est redistribuée
- Vérifier les intervalles OSPF actuels
- Modifier les intervalles OSPF
- Vérifier que les contiguïtés ont été rétablies

Tester vos connaissances (1)

1. Dans la commande router ospf, l'ID de processus doit-il correspondre sur tous les routeurs ?
2. En tenant compte de la configuration suivante, quel est l'ID de routeur OSPF du routeur A?
 1. routeurA(config)# interface s0/0/0
 2. routeurA(config-f)# ip add 192.168.2.1 255.255.255.252
 3. routeurA(config-if)# interface loopback 0
 4. routeurA(config-if)# ip add 10.1.1.1 255.255.255.255
 5. routeurA(config)# router ospf 1
 6. routeurA(config-if)# network 192.168.2.0 0.0.0.3 area0
3. Quelle commande permet de vérifier ou de déterminer la valeur de la bande passante d'une interface utilisée par la métrique OSPF ?
4. Quelle commande permet de modifier le coût d'une interface sans changer la valeur de la bande passante de cette interface

Tester vos connaissances (2)

1. Quel est l'intervalle Hello par défaut sur les réseaux Ethernet et les réseaux série point à point ? Quel est l'intervalle Hello par défaut sur les réseaux NBMA?
2. Quelles valeurs doivent correspondre avant que deux routeurs ne créent une contiguïté OSPF?
3. Quels problèmes la sélection d'un DR et d'un BDR permet-elles de résoudre ?
4. Comment le DR et le BDR sont-ils sélectionnés?
5. En cas de défaillance du DR, comment est défini le nouveau DR?
6. Que se passe t-il lorsqu'un routeur avec une priorité d'interface OSPF plus élevée est ajoutée à un réseau comportant déjà un DR et BDR?
7. Que signifie la valeur 0 pour une priorité d'interface OSPF?
8. Quelle commande faut-il utiliser pour propager une route par défaut OSPF?

Projet à rendre

- LAB_Configuration OSPF Integration Competence_Projet_Final.pka (1 semaine)

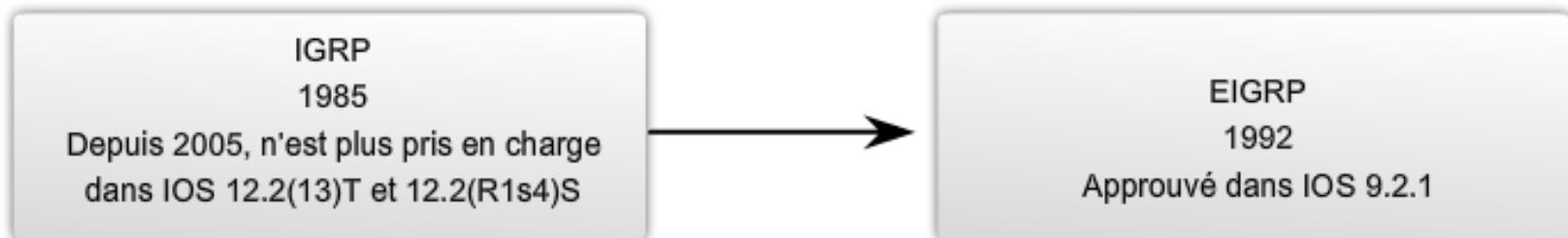
EIGRP

Objectifs

- Caractéristiques EIGRP
 - Présentation des fonctions et des caractéristiques du protocole EIGRP
- Implémentation du protocole EIGRP pour IPv4
 - Implémentation du protocole EIGRP pour IPv4 dans un réseau de PME
- Fonctionnement avancé du protocole EIGRP
 - Présentation du fonctionnement du protocole EIGRP sur un réseau de PME
- Dépannage du protocole EIGRP

IGP à EIGRP (Enhanced Interior Gateway Routing Protocol)

IGRP à EIGRP



Résumé du fonctionnement

Protocoles traditionnels de routage à vecteur de distance

- Utilisent l'algorithme de Bellman-Ford ou Ford-Fulkerson ;
- Classent les entrées de routage par ancienneté et utilisent des mises à jour périodiques ;
- N'assurent le suivi que des meilleures routes ; le meilleur chemin vers un réseau de destination ;
- Lorsqu'une route n'est plus disponible, le routeur doit attendre une nouvelle mise à jour du routage ;
- Convergence plus lente en raison des minuteurs de mise hors service.

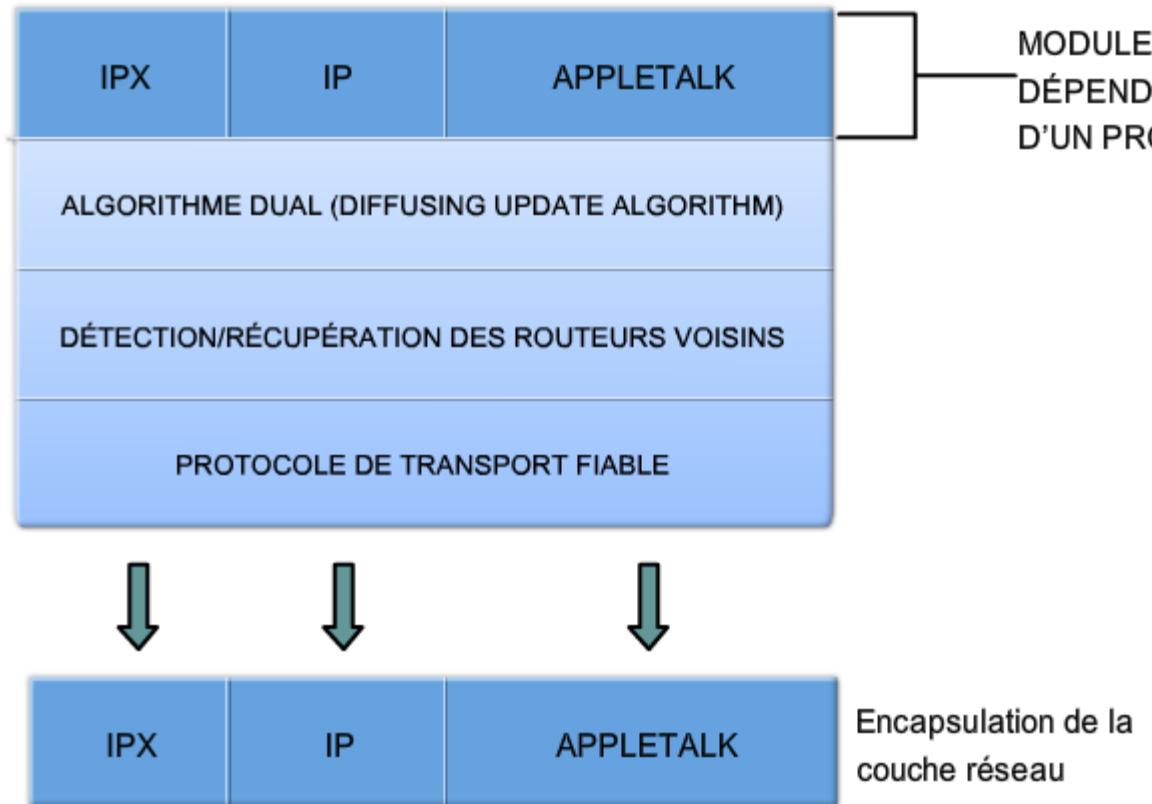
Protocole à vecteur de distance amélioré : EIGRP

- Utilise l'algorithme DUAL ;
- Ne classe pas les entrées de routage par ancienneté et n'utilise pas de mise à jour régulière ;
- Gère une table topologique séparée de la table de routage, qui comprend le meilleur chemin et les chemins de secours sans boucle ;
- Lorsqu'une route n'est plus disponible, l'algorithme DUAL utilise un chemin de secours de la table topologique ;
- Convergence plus rapide grâce à l'absence de minuteurs de mise hors service et à des calculs de routes coordonnés.

Présentation de EIGRP

- EIGRP comprend plusieurs fonctions peu répandues dans d'autres protocoles de routage par vecteur de distance tels que RIP (RIPv1 et RIPv2) et IGRP. Ces fonctions comprennent :
 - le protocole RTP (Reliable Transport Protocol) ;
 - les mises à jour limitées ;
 - l'algorithme DUAL (Diffusing Update Algorithm) ;
 - l'établissement de contiguités ;
 - les tables de voisinage et de topologie.
- EIGRP se **comporte** comme un protocole de routage à **état de liens**, mais d'après ses propriétaires (**Cisco**), il s'agit tout de même d'un **protocole de routage** à **vecteur de distance**
 - Le terme de protocole de **routage hybride** est parfois utilisé pour définir le protocole EIGRP

Présentation de EIGRP (2)



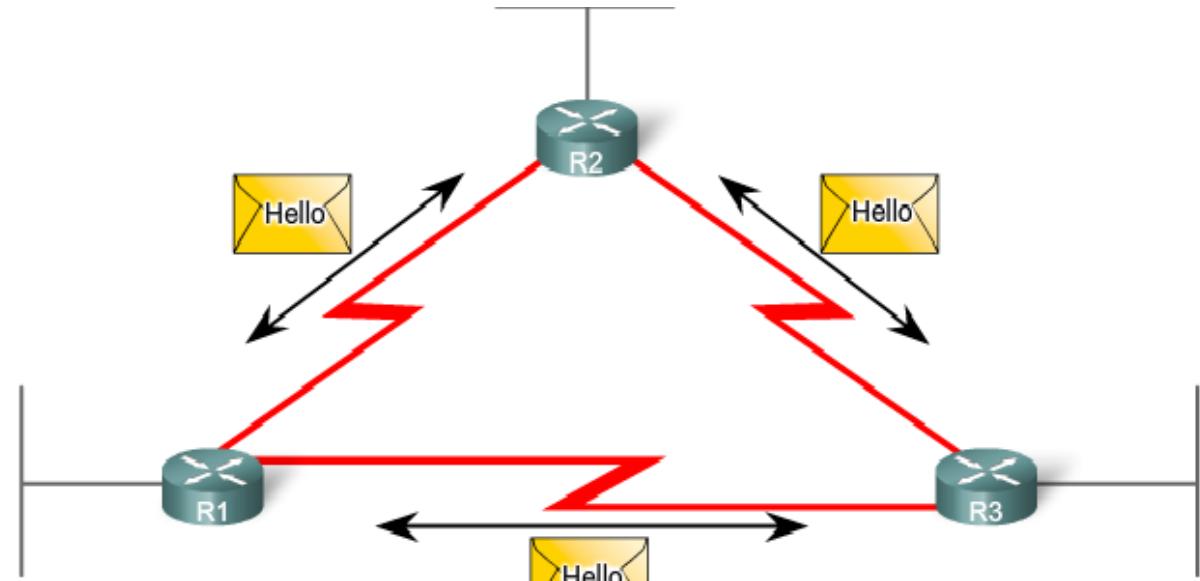
- TCP est remplacé par RTP dans EIGRP
- Utilise le protocole de transport fiable RTP (Reliable Transport Protocol) pour la livraison et la réception des paquets EIGRP
- Conçu comme un protocole de routage indépendant des couches réseau et ne peut par conséquent pas utiliser les services UDP ou TCP car IPX et Appletalk n'utilisent pas les protocoles de la suite TCP/IP

Quid de IPX et Appletalk ?

- Internetwork Packet Exchange (IPX), est l'implémentation Novell du Internet Datagram Protocol (IDP) développé par Xerox
 - IPX est un protocole datagramme sans connexion qui transmet des paquets à travers un réseau local (LAN)
- AppleTalk est un protocole de communication d'Apple en tant que protocole autonome (couches 3 à 5), le plus souvent au sein de trames Ethernet, l'ensemble étant baptisé EtherTalk

Intervalle Hello et délai de conservation

- EIGRP détecte ses voisins par des paquets « hello »
- RTP peut envoyer des paquets en monodiffusion ou en multidiffusion
- Les paquets EIGRP en multidiffusion utilisent l'adresse de multidiffusion réservée 224.0.0.10



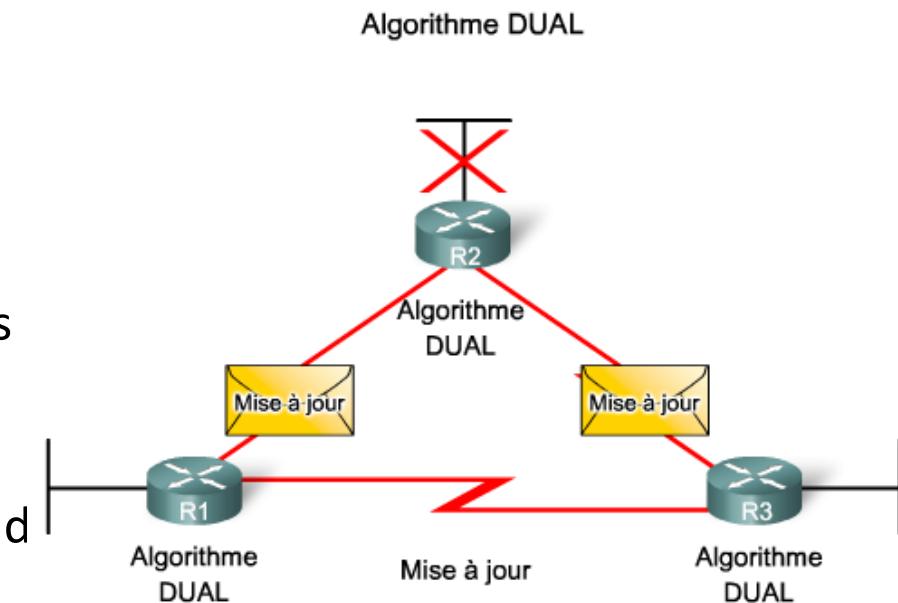
Bandé passante	Exemple de liaison	Intervalle HELLO par défaut	Temps d'attente par défaut
1,544 Mbits/s	Relais de trames multipoint	60 secondes	180 secondes
Supérieure à 1,544 Mbits/s	T1, Ethernét	5 secondes	15 secondes

Quelques notions

- **Feasible Distance** (FD) représente la métrique totale la plus faible pour joindre une destination
- **Advertised Distance** (AD) représente la métrique annoncée par le voisin, pour joindre une destination
- **Successor** représente le voisin qui a été choisi pour joindre une destination
- **Feasible Successor** (FS) représente le Successor de secours pour une destination
- Pour devenir FS, il faut avoir une AD plus faible que la FD du Successor

Présentation de l'algorithme DUAL (Diffusing Update Algorithm)

- A la place de Bellman-Ford ou Ford Fulkerson utilisé par des protocoles à vecteurs de distance, EIGRP utilise l'algo DUAL
- Les boucles de routage, même temporaires, peuvent être préjudiciables aux performances réseau
- Les protocoles de routage à vecteur de distance tels que RIP évitent les boucles de routage à l'aide de règles de découpage d'horizon et de minuteurs de mise hors service

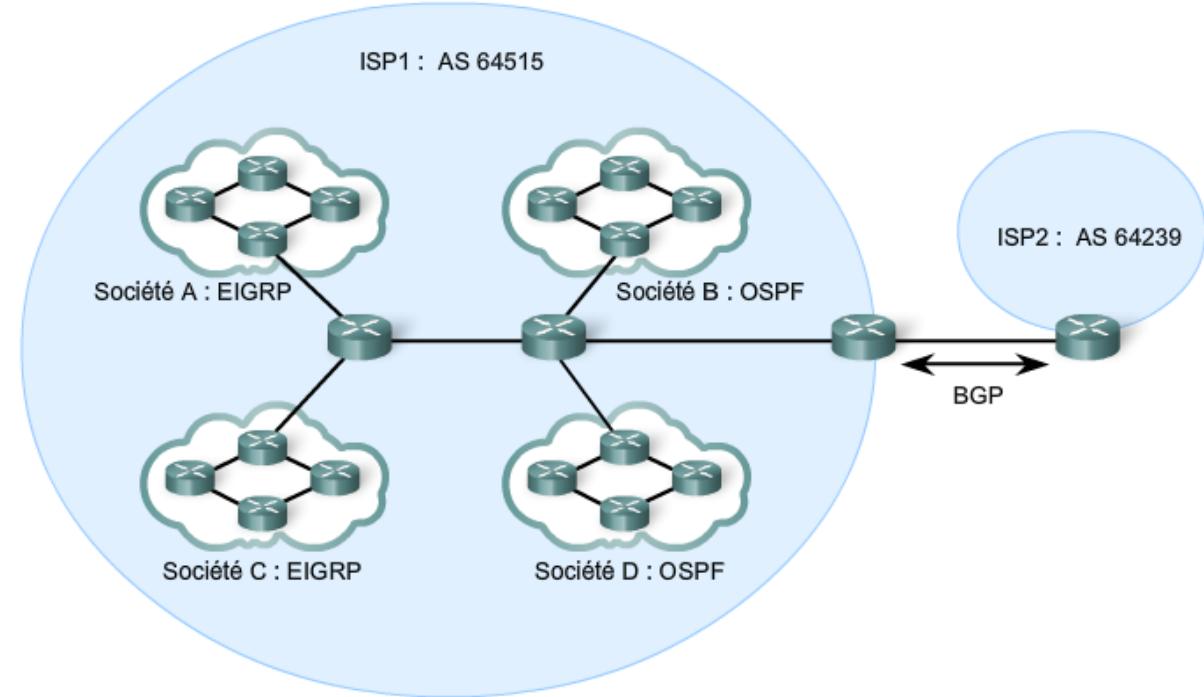


Distance administrative par défaut

- La distance administrative est la fiabilité (ou préférence) de la source de la route.
- Par rapport à d'autres protocoles IGP (Interior Gateway Protocol), le protocole EIGRP est préférable pour Cisco IOS car sa distance administrative est la plus courte

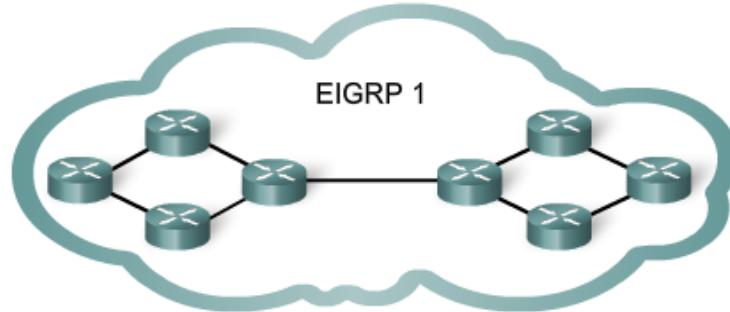
Origine de la route	Distance administrative
Connecté	0
Statique	1
Résumé de routes EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

Notion de AS



- Les principes directeurs de la création, de la sélection et de l'enregistrement d'un système autonome (AS) sont décrits dans le document RFC 193
 - Les numéros AS sont affectés par l'IANA (Internet Assigned Numbers Authority), l'autorité qui affecte les espaces d'adressage IP
 - Les registres RIR sont chargés d'affecter un numéro AS à une entité à partir du bloc de numéros AS qui lui a été affecté
 - Numéro d'AS sur 32 bits (avant 2007 16 bits)

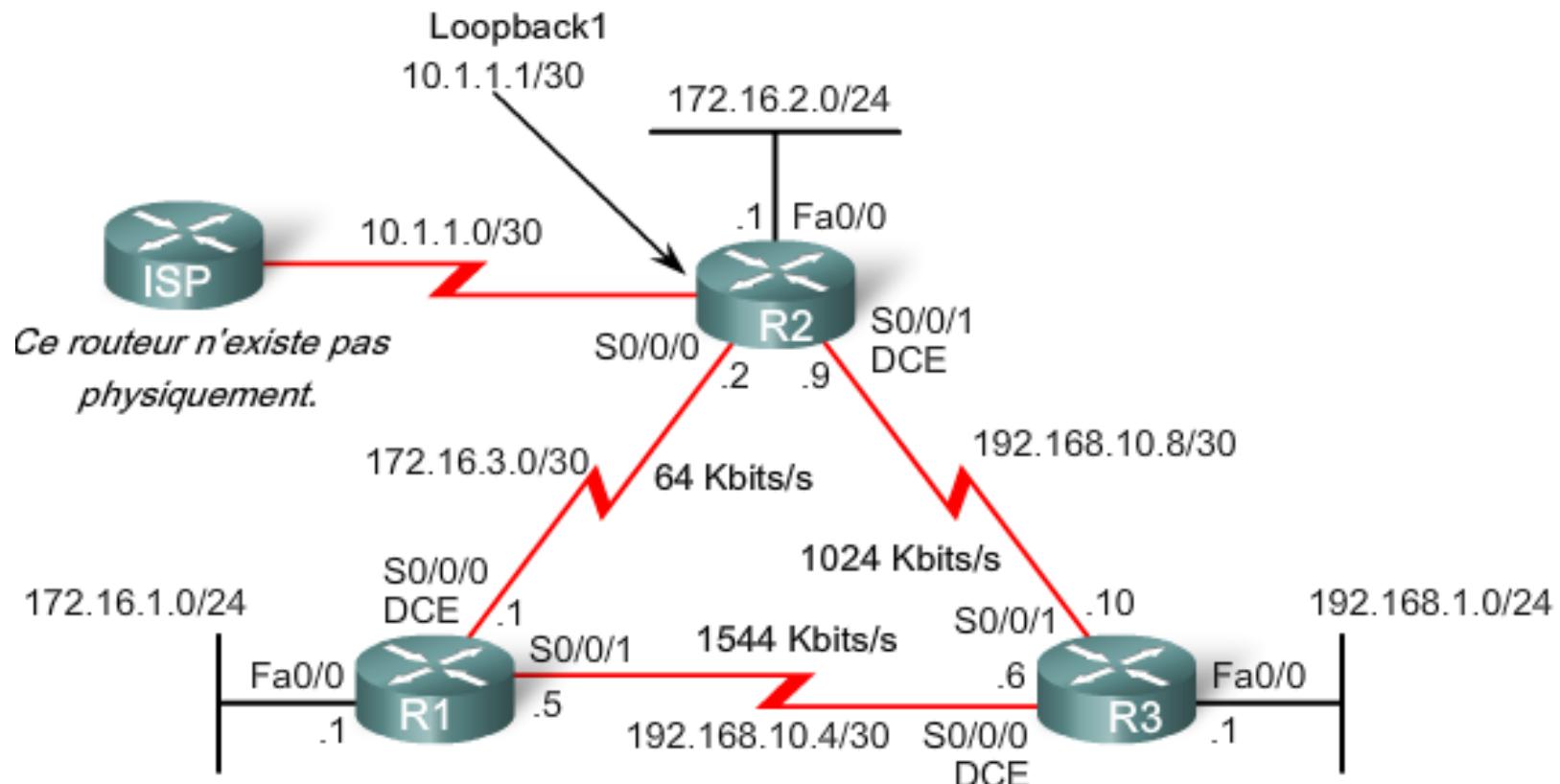
Activation du routage EIGRP



```
R1(config)#router eigrp ?  
<1-65535> Autonomous system number  
R1(config)#router eigrp 1
```

- EIGRP et OSPF utilisent tous les deux un ID de processus pour représenter une instance de leur protocole de routage respectif s'exécutant sur le routeur
- Bien qu'EIGRP appelle ce paramètre un numéro de « système autonome », celui-ci fonctionne en fait comme un ID de processus
- Pour établir des contiguïtés de voisinage, le protocole **EIGRP requiert** que **tous les routeurs du même domaine de routage soient configurés avec le même ID de processus**
 - En général, un seul ID de processus est configuré sur un routeur pour un protocole de routage donné

Activation de EIGRP



- Sur les routers R1, R2, et R3 tapez:
 - Rx(config)# **router eigrp 1**

La commande « network »

- La commande `network` du protocole EIGRP a la même fonction que dans les autres protocoles de routage IGP :
 - toute interface sur ce routeur qui correspond à l'adresse réseau figurant dans la commande `network` est activée pour envoyer et recevoir des mises à jour EIGRP ;
 - ce réseau (ou sous-réseau) sera inclus dans les mises à jour de routage EIGRP
 - Router(config-router)#**network adresse-réseau**

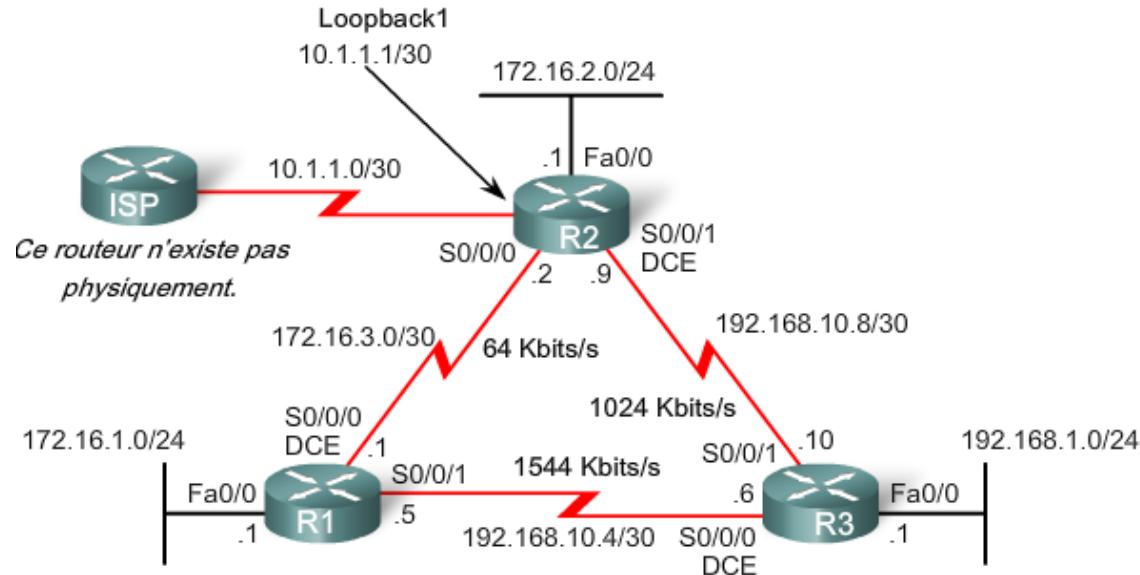
Configuration du routeur R1 et R2

- Dans la figure, une seule instruction de réseau par classe est utilisée sur R1 pour contenir les deux sous-réseaux 172.16.1.0/24 et 172.16.3.0/30 :
 - R1(config-router)#network 172.16.0.0
- Lorsqu'EIGRP est configuré sur le routeur R2, DUAL envoie un message de notification à la console indiquant qu'une relation de voisinage avec un autre routeur EIGRP a été établie
- Cette nouvelle contiguïté (utilisation d'un segment de support commun) s'établit automatiquement car R1 et R2 utilisent le même processus de **routage eigrp 1** et les deux routeurs envoient désormais des mises à jour sur le réseau 172.16.0.0
 - R2(config-router)#network 172.16.0.0
 - %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0) is up: new adjacency

Commande « network » avec masque générique

- L'administrateur réseau ne veut pas toujours inclure toutes les interfaces d'un réseau lorsqu'il active EIGRP
- Pour configurer EIGRP pour annoncer des sous-réseaux spécifiques uniquement, utilisez l'option masque-générique de la commande network :
 - Router(config-router)#**network** **adresse-réseau** **[masque-générique]**
 - R2(config-router)#**network** **192.168.10.8** **0.0.0.3**

Configuration des réseaux EIGRP



```
R1(config)#router eigrp 1
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.10.0
```

```
R2(config)#router eigrp 1
R2(config-router)#network 172.16.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
R2(config-router)#network 192.168.10.8 0.0.0.3
```

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.10.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up: new adjacency
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up: new adjacency
R3(config-router)#network 192.168.1.0
```

Vérification du protocole EIGRP

- Utilisez la commande **show ip eigrp neighbors** pour afficher la table de voisinage et vérifier que le protocole EIGRP a établi une contiguïté avec ses voisins.

R2#show ip eigrp neighbors								
IP-EIGRP neighbors for process 1								
H	Address	Interface	Hold (sec)	Uptime	SRTT	RTO	Q	Seq Type
1	192.168.10.10	Se0/0/1	10	00:01:41	20	200	0	7
0	172.16.3.1	Se0/0/0	10	00:09:49	25	200	0	28

Adresse des voisins

Interface connectée au voisin

Temps restant avant de considérer qu'un voisin est « hors service »

Délai écoulé depuis l'établissement d'une contiguïté

Vérification du protocole EIGRP

- **SRTT** (Smooth Round Trip Timer) et **RTO** (Retransmit interval) : le temps moyen nécessaire pour envoyer un message et recevoir sa réponse d'un voisin et l'intervalle de retransmission, utilisés par RTP pour la gestion des paquets EIGRP fiables. Les paramètres SRTT et RTO sont abordés en détail dans les cours CCNP.
- **Queue Count** : le nombre de paquets en attente d'envoi. Il doit toujours être égal à zéro. Si la valeur est supérieure à 0, des paquets EIGRP attendent pour être envoyés. La notion de paquets en attente d'envoi est abordée en détail dans les cours CCNP.
- **Sequence Number** : numéro d'ordre, permettant de suivre les paquets de mise à jour, de demande et de réponse. Les numéros d'ordre sont abordés en détail dans les cours CCNP.

Métrique composite EIGRP et valeurs k

- EIGRP utilise les valeurs suivantes dans sa métrique composite pour calculer le chemin préféré vers un réseau :
 - Bande passante
 - Délai
 - Fiabilité
 - Charge
- Par défaut, seuls la **bande passante** et le **délai** sont **pris en compte** pour **calculer la métrique**
 - Cisco conseille aux administrateurs de ne pas utiliser la fiabilité et la charge à moins d'en avoir explicitement besoin

Métrique composite

Formule par défaut :

$$\text{métrique} = [\text{K1} * \text{bande passante} + \text{K3} * \text{délai}]$$

Formule complète :

$$\text{métrique} = [\text{K1} * \text{bande passante} + (\text{K2} * \text{bande passante}) / (256 - \text{charge}) + \text{K3} * \text{délai}] * [\text{K5} / (\text{fiabilité} + \text{K4})]$$

(N'est pas utilisée si les valeurs « K » sont égales à 0)

Valeurs par défaut :

K1 (bande passante) = 1

K2 (charge) = 0

K3 (délai) = 1

K4 (fiabilité) = 0

K5 (fiabilité) = 0

Les valeurs « K » peuvent être modifiées à l'aide de la commande **metric weights**.

```
Router(config-router)#metric weights tos k1 k2 k3 k4 k5
```

- La formule comprend les valeurs K1 à K5, connues sous le nom de pondérations de métrique EIGRP

Vérification des valeurs de « k »

- La commande **show ip protocols** est utilisée pour vérifier les valeurs K

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for FastEthernet0/0, Serial0/0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    (this router)      90          00:03:29
    192.168.10.6      90          00:02:09
    Gateway          Distance      Last Update
    172.16.3.2        90          00:02:12
  Distance: internal 90 external 170
```

Valeurs de délai

- La métrique de délai (DLY) est une valeur statique déterminée à partir du type de liaison à laquelle l'interface est connectée et s'exprime en microsecondes
- Le délai n'est pas mesuré de façon dynamique. En d'autres termes, le routeur ne contrôle pas réellement le temps que le paquet prend pour atteindre sa destination
- La valeur de délai, comme la valeur de bande passante, est une valeur par défaut que l'administrateur peut modifier

Support	Délai
ATM 100 M	100 µs
Fast Ethernet	100 µs
FDDI	100 µs
1HSSI	20 000 µs
Token Ring 16 M	630 µs
Ethernet	1 000 µs
T1 (série par défaut)	20 000 µs
512 K	20 000 µs
DSO	20 000 µs
56 K	20 000 µs

Configurer la bande passante

```
R1(config)#inter s 0/0/0  
R1(config-if)#bandwidth 64
```

```
R2(config)#inter s 0/0/0  
R2(config-if)#bandwidth 64  
R2(config)#inter s 0/0/1  
R2(config-if)#bandwidth 1024
```

```
R3(config)#inter s 0/0/1  
R3(config-if)#bandwidth 1024
```

Remarque : la bande passante réelle de la liaison entre R1 et R3 correspond à la valeur par défaut des interfaces série (1 544 kbits/s).

- Pour vérifier la bande passante:
 - R2# show interface serial 0/0/0

Calcul de la mesure par défaut EIGRP

Mesure par défaut = [K1*bande passante + K3*délai] * 256

Comme K1 et K3 valent tous deux 1, la formule est simplifiée en : bande passante + délai

bande passante = vitesse de la liaison la plus lente de la route vers la destination
délai = somme des délais de chaque liaison de la route vers la destination

Bandé passante la plus faible : $(10\ 000\ 000/\text{bande passante en Kbits/s}) * 256$

Plus la somme des délais : $+ (\text{somme des délais}/10) * 256$

= mesure EIGRP

```
R2#show ip route
<résultat omis>
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:02:14, Serial0/0/1
```

Quelques outils

- **Désactiver le résumé automatique des routes**
 - Router(config-router)# **no auto-summary**
- Mettre en place des **résumés de route manuellement** (ou Route Summarization)
 - Le but est que les routeurs n'annoncent plus tous les réseaux mais il agrège ces réseaux en un seul réseau
 - L'ajout de routes résumées est appliqué sur les interfaces
 - R1(config-if)# **ip summary-address eigrp 1 10.1.0.0 255.255.252.0**

Passive Interfaces

- Fonctionnent différemment en EIGRP par rapport en RIP
 - Elles ne servent pas qu'à bloquer l'envoie de mise à jour de routage mais aussi à empêcher la réception de mise à jour sur les interfaces passives
 - Le réseau auquel elle appartient est toujours annoncé dans les mises à jour mais pas par cette interface
- Les interfaces passives sont donc à activer sur toutes les interfaces qui ne sont pas reliées à un voisin EIGRP

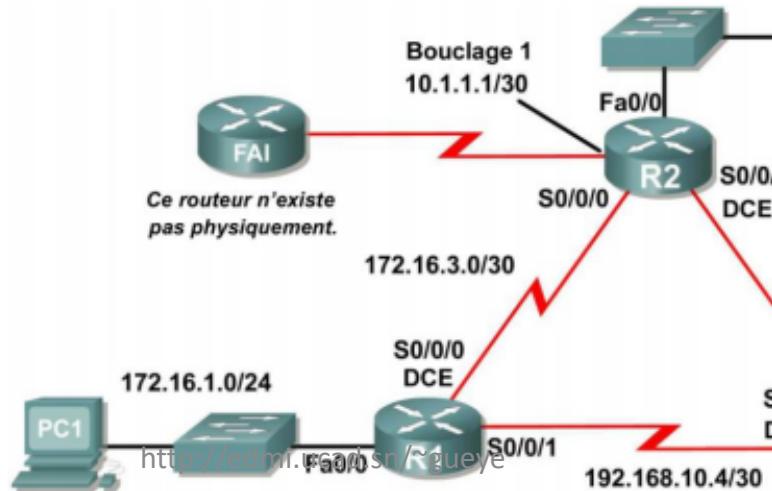
Passive Interfaces (suite)

- Pour plus de sécurité mettre **toutes les interfaces en mode passive, sauf celles choisies**

R1(config-router)#passive-interface default

R1(config-router)#no passive-interface serial 0/0/0

R1(config-router)#no passive-interface serial 0/0/1



Propagation d'une route par défaut

- Propager une route statique par défaut
 - La route statique par défaut (0.0.0.0 / 0) est habituellement configurée sur le routeur qui est connecté à un réseau en dehors du domaine de routage EIGRP, par exemple, à un fournisseur d'accès à Internet (FAI)
 - Une méthode pour propager la route statique par défaut :
 - La commande **redistribute static**
- Vérifier la route par défaut propagée

```
R1# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:25:23,
Serial0/0/1
```

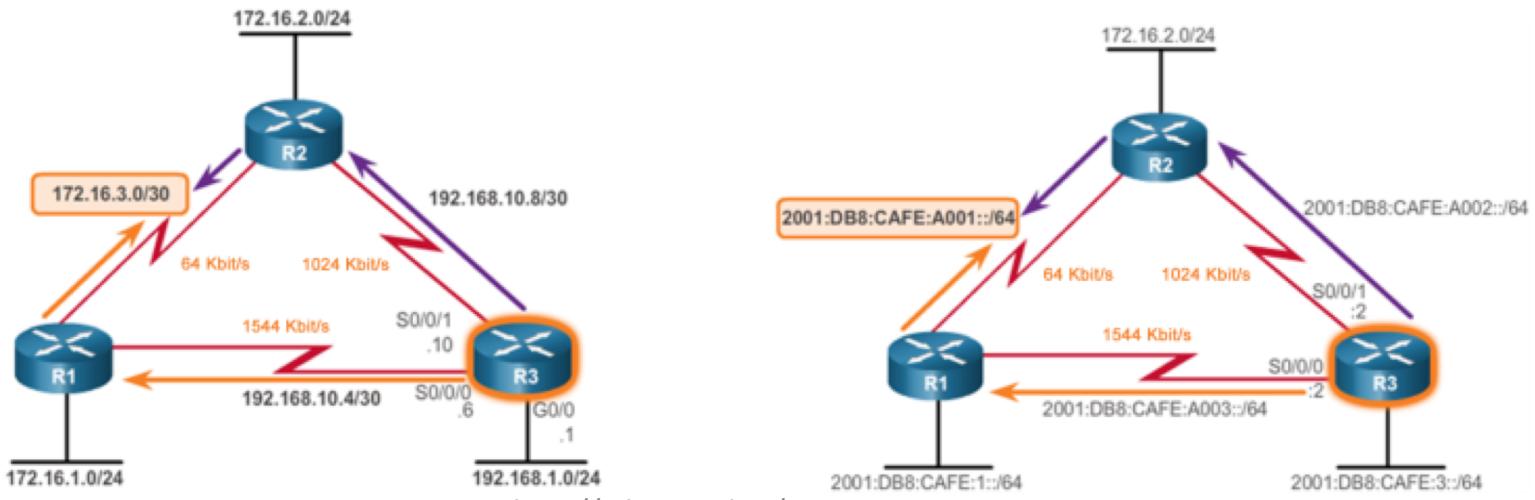
- **D** : cette route a été détectée à partir d'une mise à jour de routage EIGRP.
- ***** : la route peut convenir comme route par défaut
- **EX** : la route est une route EIGRP externe, dans le cas présent, une route statique extérieure au domaine de routage EIGRP
- **170** : il s'agit de la distance administrative d'une route EIGRP externe

Ajustement des interfaces EIGRP

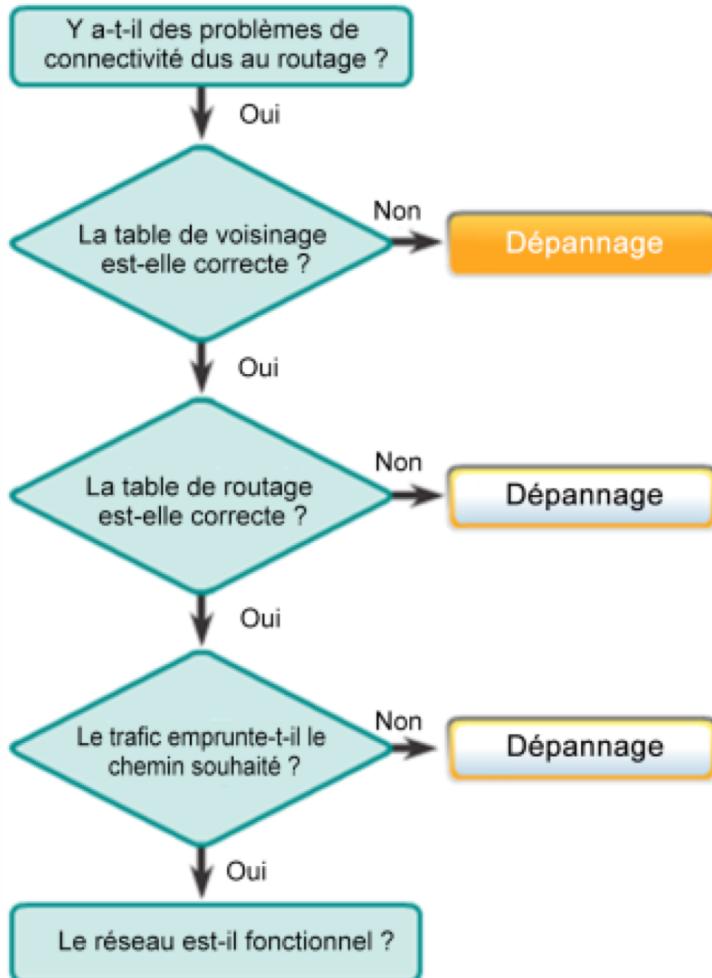
- Utilisation de la bande passante par EIGRP
 - Par défaut, le protocole EIGRP n'utilise que 50 % maximum de la bande passante d'une interface pour les informations EIGRP. Cela permet au processus EIGRP de ne pas surcharger une liaison en ne laissant pas suffisamment de bande passante pour le routage du trafic normal
 - Les commandes qui permettent de configurer le pourcentage de bande passante utilisé par le protocole EIGRP sur une interface :
 - **ip bandwidth-percent eigrp as-number percent**
- Intervalles Hello et d'attente : n'ont pas besoin d'être identiques à ceux d'autres routeurs EIGRP
 - Les paquets Hello permettent de déterminer et de surveiller l'état de la connexion des voisins.
 - Les commandes qui permettent de configurer les intervalles Hello sur chaque interface :
 - **ip hello-interval eigrp as-number seconds**
 - L'intervalle d'attente indique au routeur la durée maximale pendant laquelle il doit attendre le prochain paquet Hello avant de déclarer que ce voisin est inaccessible.
 - Les commandes qui permettent de configurer les intervalles d'attente sur chaque interface :
 - **ip hold-time eigrp as-number seconds**
- Quels sont les intervalles Hello et d'attente par défaut du protocole EIGRP ?

Ajustement des interfaces EIGRP (suite)

- Équilibrage de charge
 - Équilibrage de la charge à coût égal
 - La capacité d'un routeur à distribuer le trafic sortant à l'aide de toutes les interfaces disposant de la même métrique à partir de l'adresse de destination
 - La commande **maximum-paths value** détermine le nombre maximum de routes
 - Équilibrage de la charge à coût inégal
 - La capacité à équilibrer le trafic entre plusieurs routes qui disposent de métriques différentes
 - La commande **variance** permet d'installer plusieurs routes sans boucle avec un coût inégal dans une table de routage locale



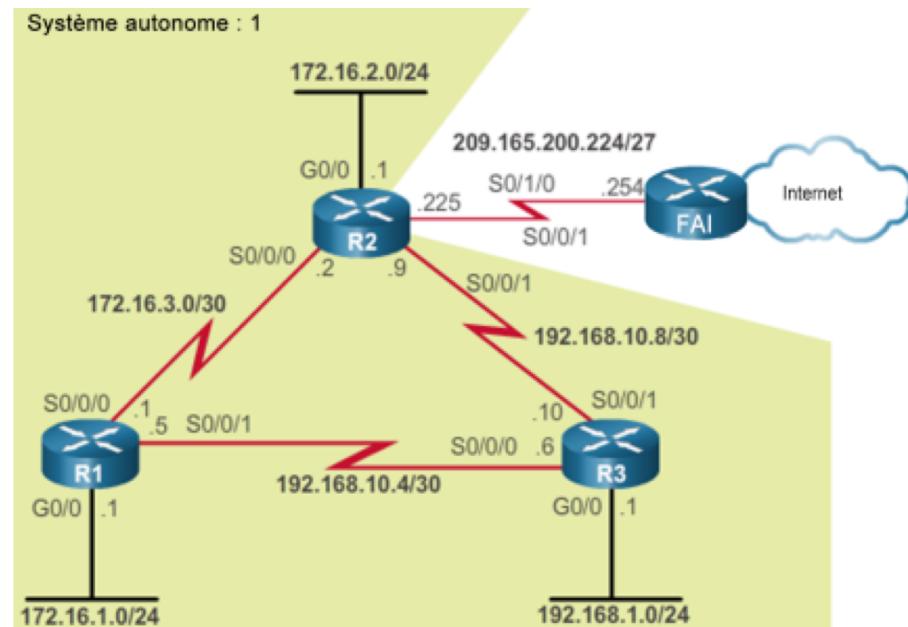
Éléments relatifs au dépannage du protocole EIGRP



- Commandes de dépannage de base EIGRP
 - Vérifier les contiguités de voisinage
 - **show ip eigrp neighbors**
 - Vérifier la route acquise vers les réseaux distants
 - **show ip route eigrp**
 - Vérifier les divers paramètres EIGRP
 - **show ip protocols**

Résolution des problèmes de voisinage EIGRP

- Connectivité de la couche 3
 - Vérifiez la connexion
 - **show ip interface brief**
 - **ping ip address**
- Paramètres EIGRP
 - Vérifiez que les routeurs se trouvent dans le même domaine EIGRP et portent le même numéro de système autonome
 - **show ip protocols**
 - Configurez le numéro de système autonome
 - **router eigrp as-number**
- Interfaces EIGRP
 - Vérifiez que les interfaces du routeur participent au réseau EIGRP
 - **show ip eigrp interfaces**
 - **show ip protocols**
 - **show running-config | section eigrp**

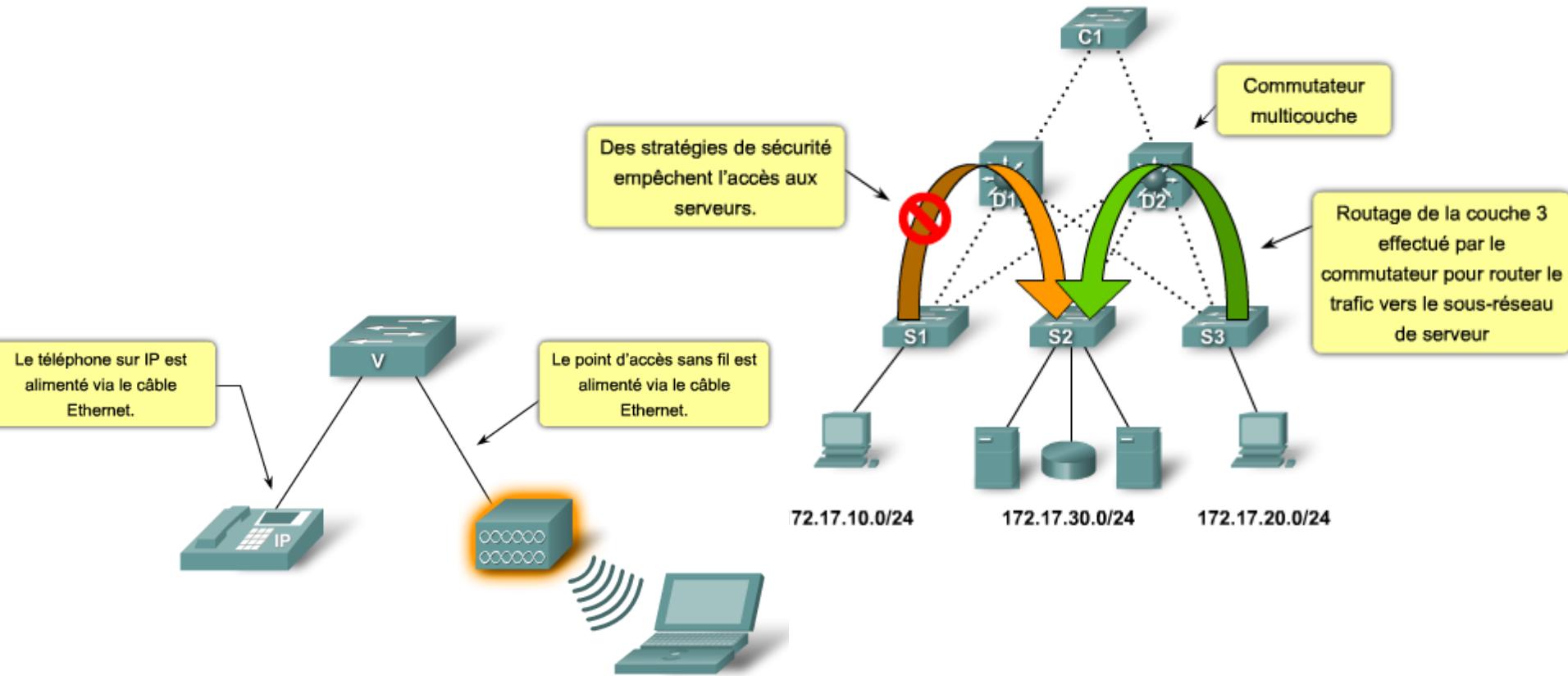


TP à faire

- #1-Routage_EIGRP.pka
- #2-Calcul_métrique_EIGRP.pka

COMMUTATION

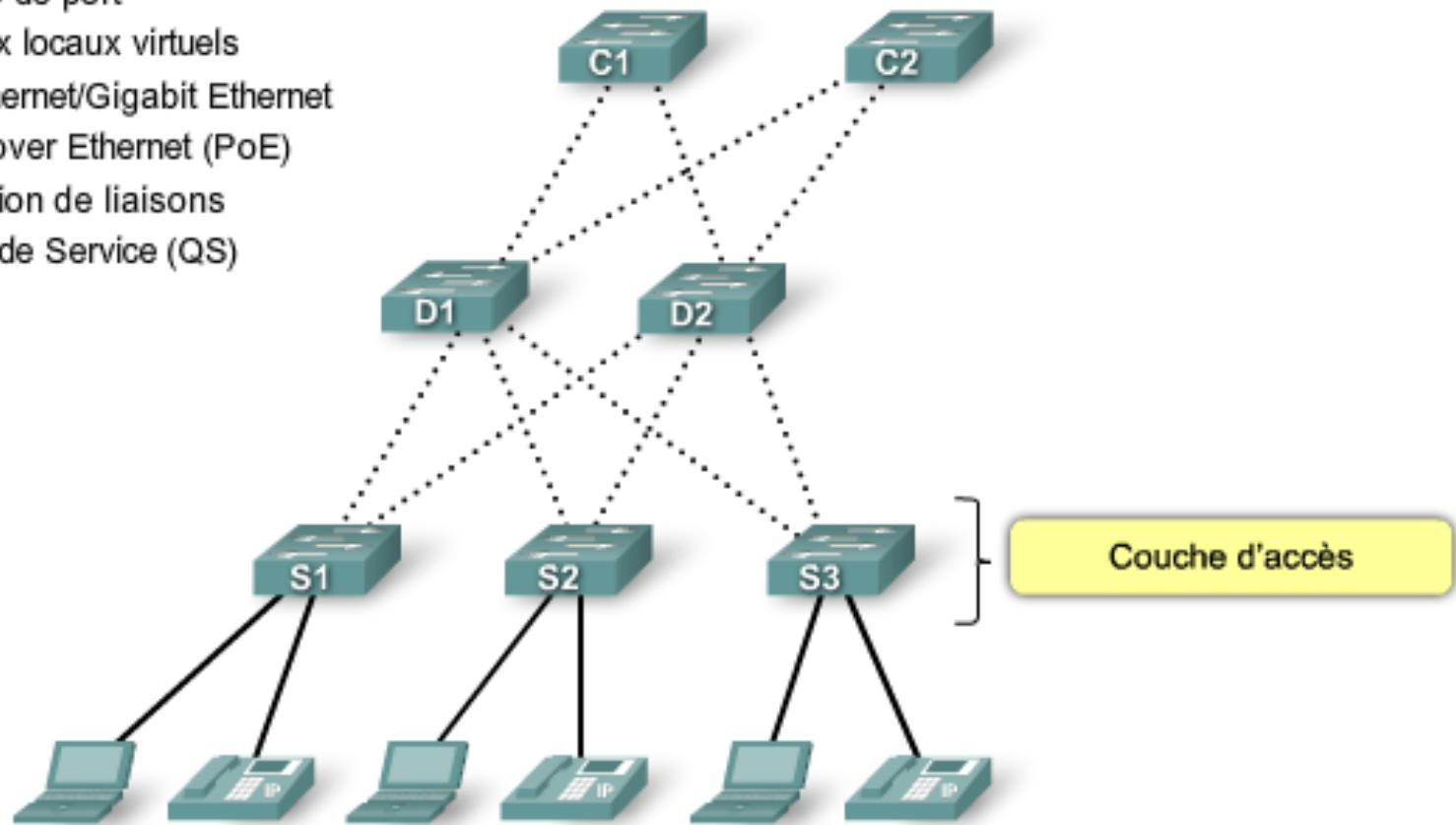
PoE et fonctionnalité de couche 3



- Les commutateurs de couche 3 proposent une fonctionnalité avancée
 - Les commutateurs de couche 3 sont également appelés commutateurs multicouche (filtre et achemine des paquets en fonction de l'adresse MAC et des adresses réseau)
 - Le Catalyst 5000 est un exemple de commutateur multicouche

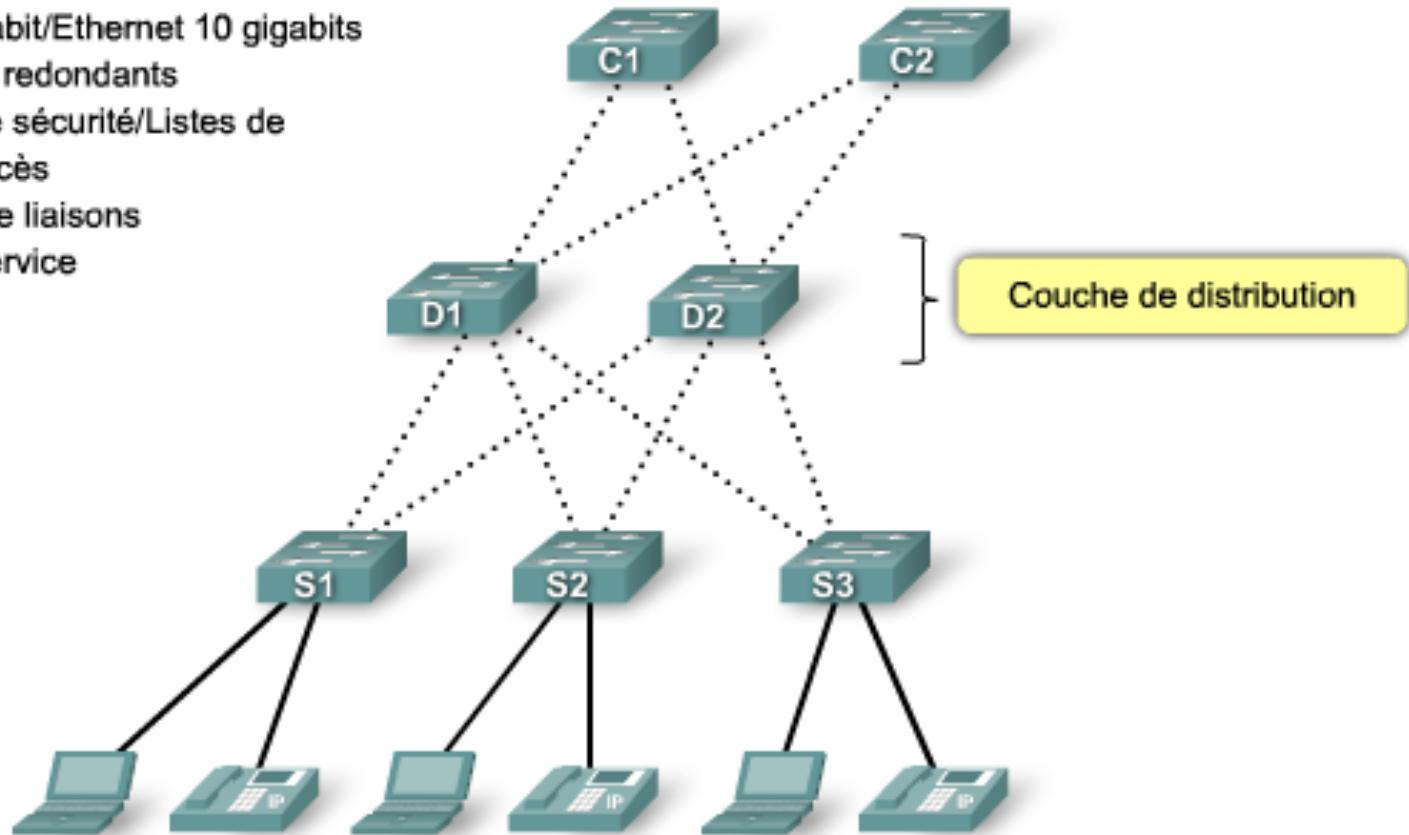
Fonctions d'un commutateur de la couche d'accès

- Sécurité de port
- Réseaux locaux virtuels
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Agrégation de liaisons
- Qualité de Service (QS)



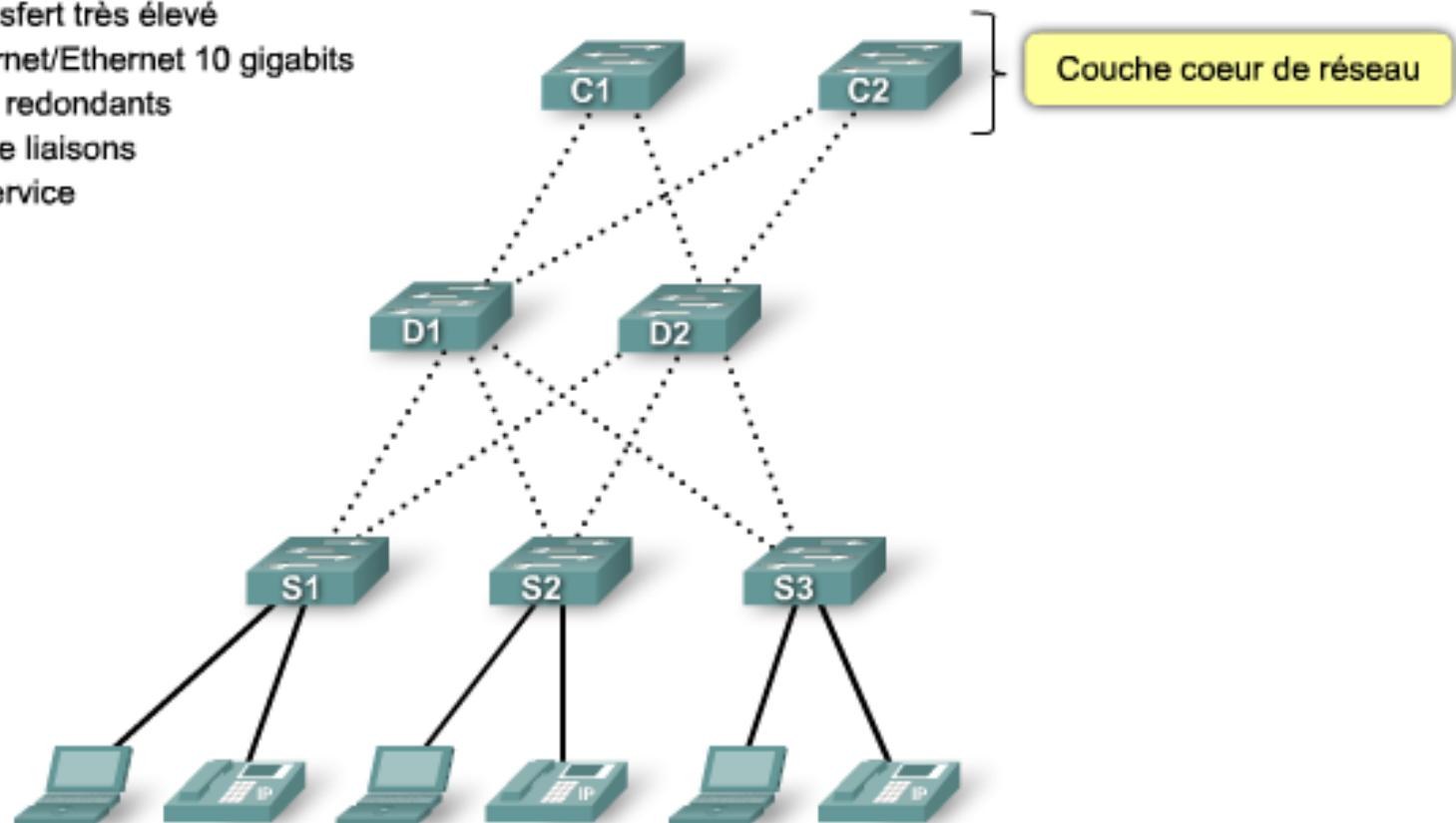
Fonctions d'un commutateur de la couche de distribution

- Prise en charge de la couche 3
- Débit de transfert élevé
- Ethernet gigabit/Ethernet 10 gigabits
- Composants redondants
- Stratégies de sécurité/Listes de contrôle d'accès
- Agrégation de liaisons
- Qualité de service

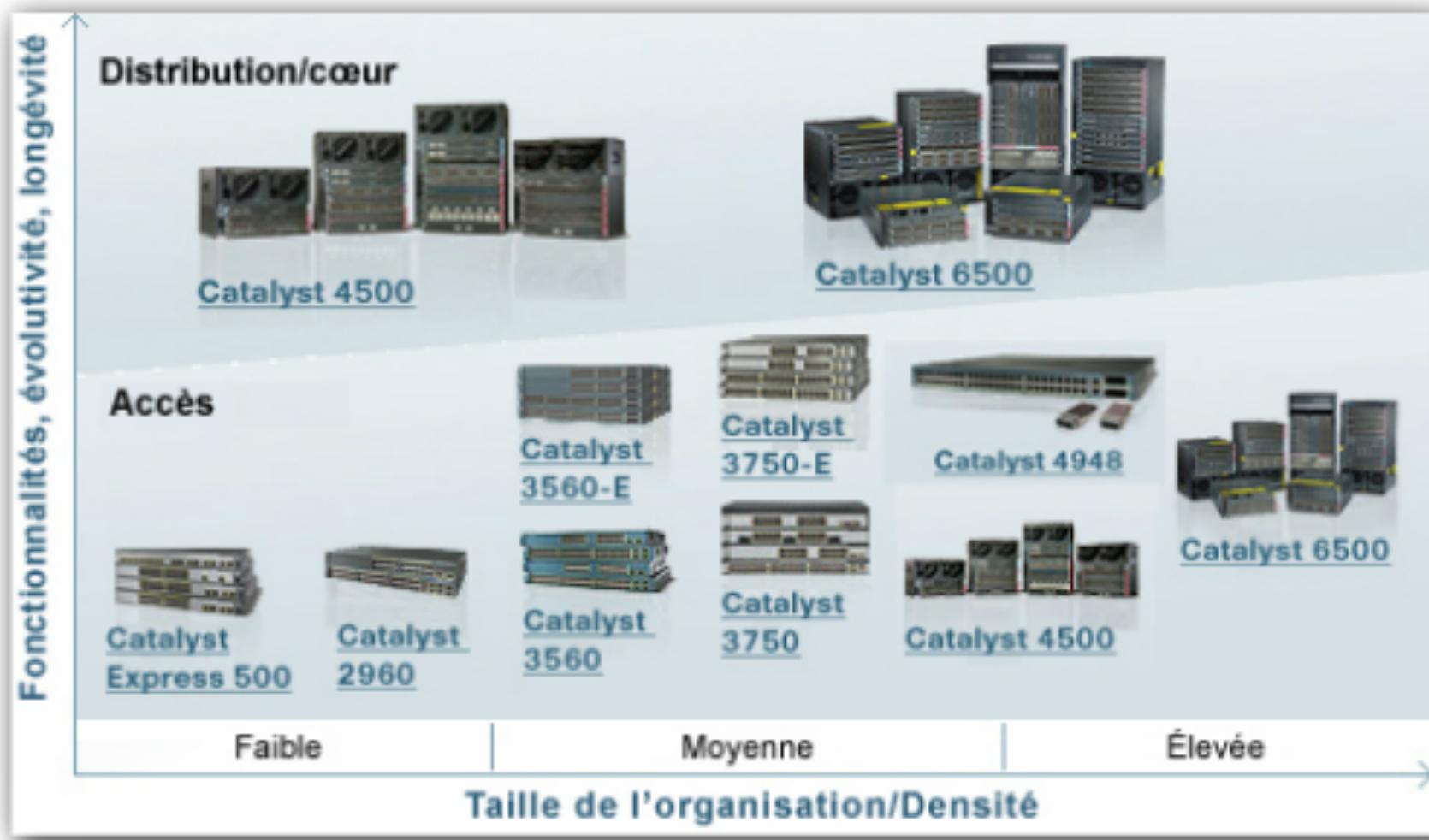


Fonctions d'un commutateur de la couche cœur de réseau

- Prise en charge de la couche 3
- Débit de transfert très élevé
- Gigabit Ethernet/Ethernet 10 gigabits
- Composants redondants
- Agrégation de liaisons
- Qualité de service



Commutateurs Cisco Catalyst pour PME



Différents types de commutateurs

Commutateurs de configuration fixe



Les fonctions et les options sont limitées à celles fournies à l'origine avec le commutateur.

Commutateurs de configuration modulaire



Commutateurs de configuration empilable



Le châssis accepte les cartes d'interface qui contiennent les ports.

Les commutateurs empilables, connectés à l'aide d'un câble spécial, fonctionnent comme un seul commutateur de grande taille.

Commutateurs pour PME

- L'outil suivant peut aider à identifier le commutateur adéquat pour une implémentation :
http://www.cisco.com/en/US/products/hw/switches/products_promotion0900aecd8050364f.html
- Le guide suivant fournit une comparaison détaillée des offres de commutateur actuelles de Cisco :
http://www.cisco.com/en/US/prod/switches/ps5718/ps708/networking_solutions_products_genericcontent0900aecd805f0955.pdf

VIRTUAL LOCAL AREA NETWORK (VLAN)

Objectifs de ce chapitre

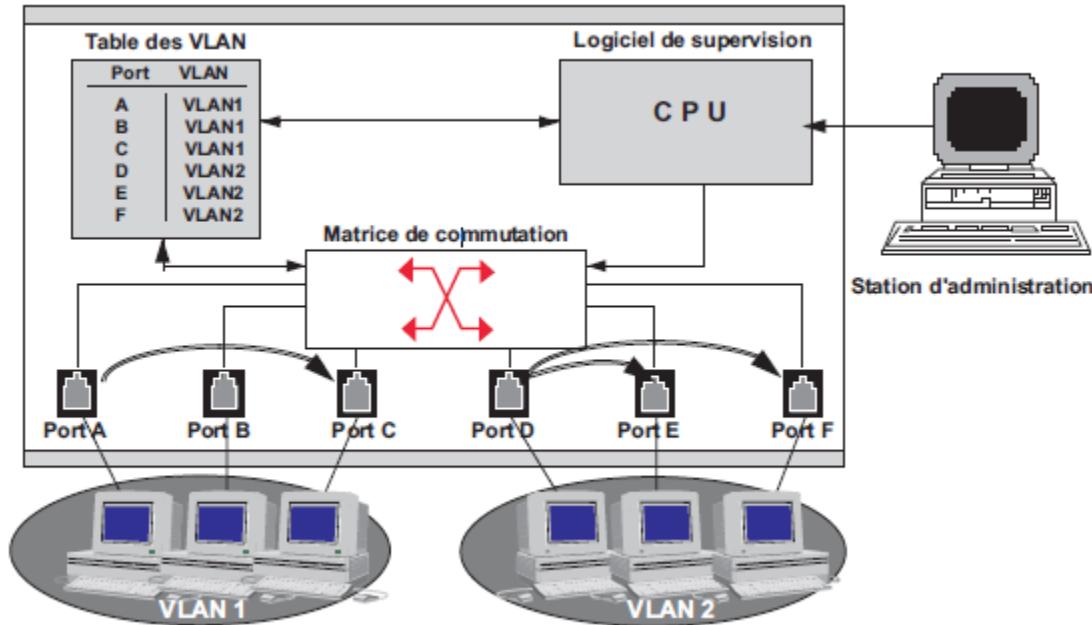
- Expliquer le rôle VLAN
- Expliquer le rôle de l'agrégation dans les VLAN
- Configurer des VLAN sur les commutateurs d'une topologie de réseau
- Résoudre les problèmes de configuration matérielle

Objectifs des VLAN

- En définissant des domaines de diffusion (domaine de broadcast) indépendamment de la situation géographique des systèmes, les VLAN (**Virtual Local Area Network**) autorisent une répartition et un partage optimal des ressources de l'entreprise
- Les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critères prédéfinis (ports, adresses MAC ou réseau...)
- Chaque VLAN défini est ainsi à la fois un domaine de collision (technologie Ethernet), un domaine de broadcast (domaine de diffusion), un domaine de multicast (liaison logique point à multipoint) et un domaine d'unicast (liaison logique point à point)
- Ainsi, un broadcast émis par une station n'est diffusé que vers les stations appartenant au même VLAN

Les réseaux locaux virtuels ou VLAN

- Application directe de la commutation statique, les VLAN autorisent, sur un même réseau physique la réalisation de plusieurs réseaux logiques totalement indépendant les uns des autres
- La communication n'est autorisée qu'entre machines d'un même VLAN et les communications inter-VLAN doivent transiter par un routeur



Niveaux de VLAN

- L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue :
 - les VLAN de niveau 1 ou VLAN par port (**Port-Based VLAN**)
 - les VLAN de niveau 2 ou VLAN MAC (**MAC Address-Based VLAN**)
 - les VLAN de niveau 3 ou VLAN d'adresses réseaux (**Network Address-Based VLAN**)

Port-Based VLAN

- Ces VLAN regroupent des stations connectées à un même port du commutateur
- La configuration est statique, le déplacement d'une station implique son changement de VLAN
- C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN
- Un port, donc les stations qui lui sont raccordées, peut appartenir à plusieurs VLAN

MAC Address-Based VLAN

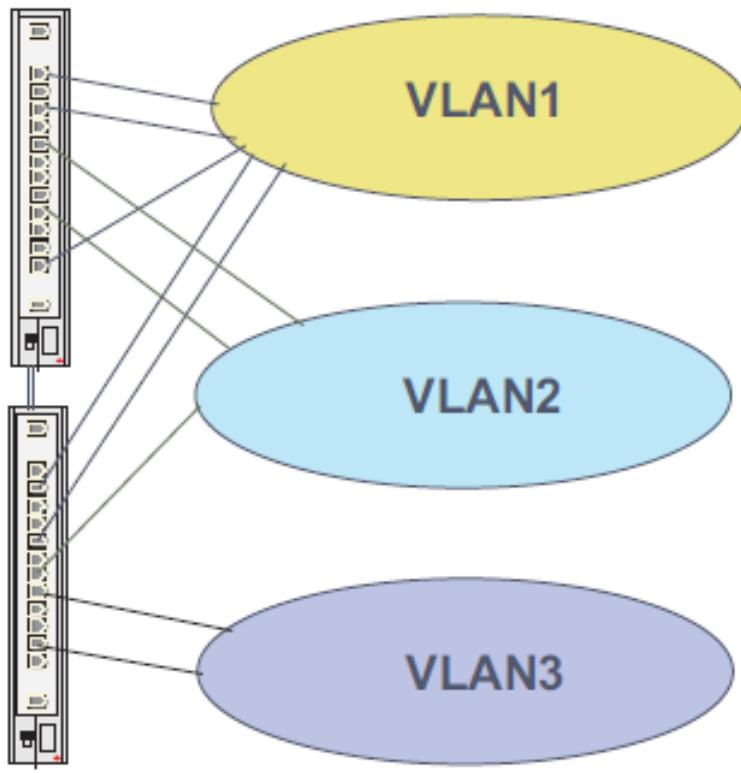
- Ces VLAN associent les stations par leur adresse MAC. De ce fait, deux stations raccordées à un même port (segment) peuvent appartenir à deux VLAN différents
- Les tables d'adresses sont introduites par l'administrateur
- Il existe des mécanismes d'apprentissage automatique d'adresses, l'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration (Drag&Drop)
- Une station peut appartenir à plusieurs VLAN. Les VLAN de niveau 2 sont indépendants des protocoles supérieurs
- La commutation, s'effectuant au niveau MAC, autorise un faible temps de latence (commutation très efficace)

Network Address-Based VLAN

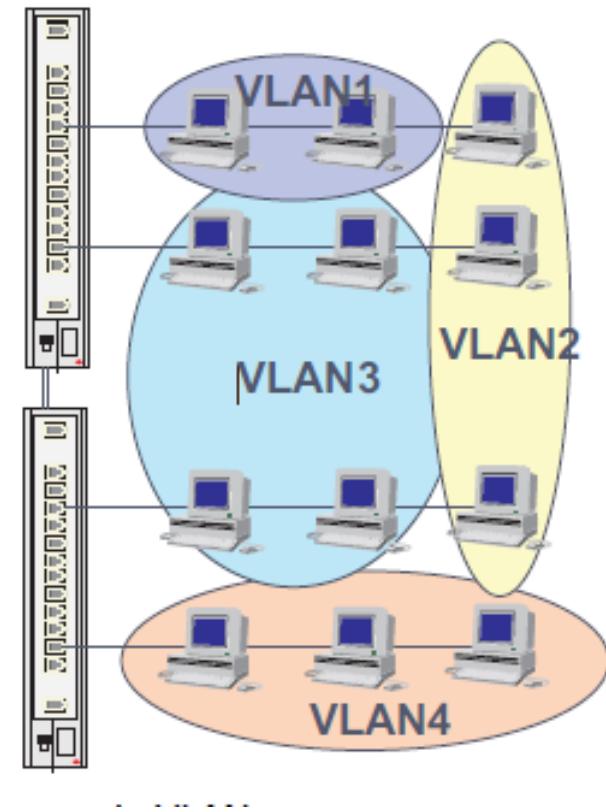
- Ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (subnet d'IP)
- Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN
- Une station peut appartenir à plusieurs VLAN par affectation statique
- Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance
- L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de **commutation et non de routage**

Les différents niveaux de VLAN

VLAN de niveau 1, par port ou segment



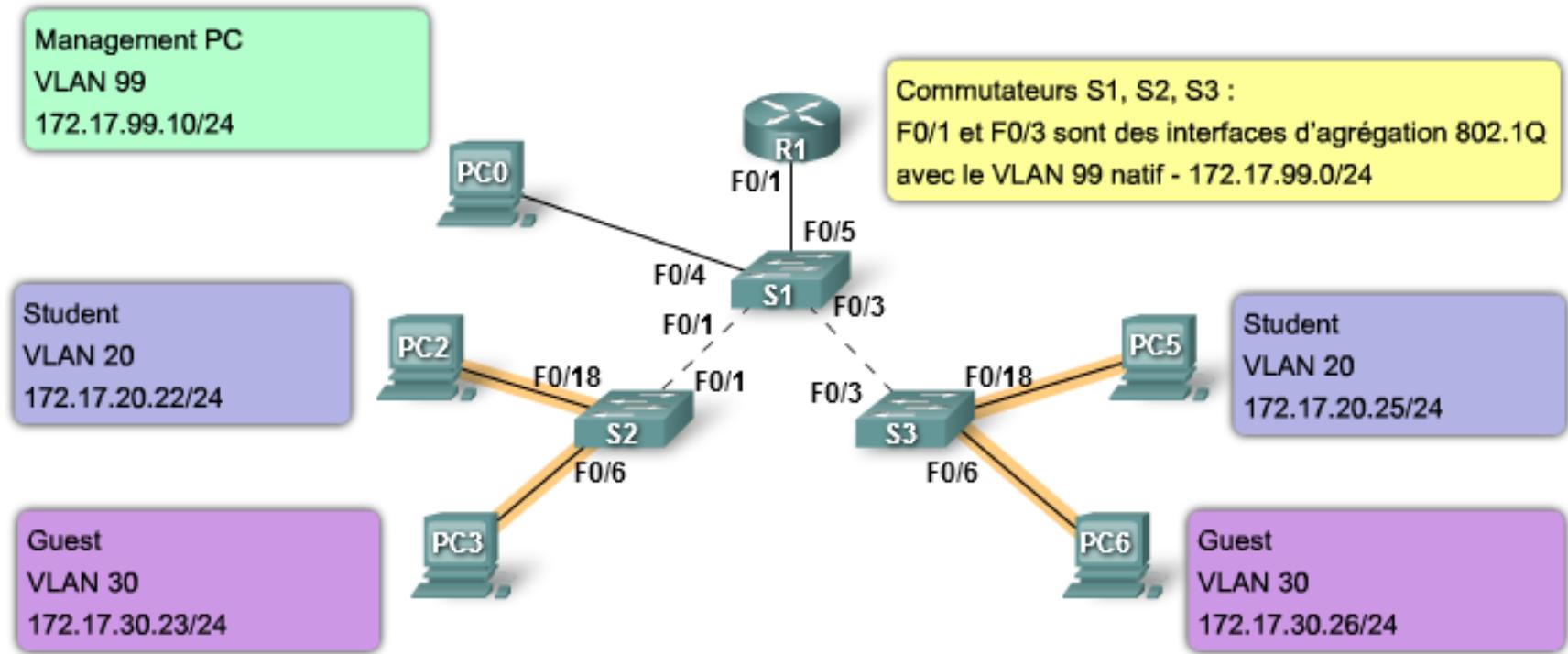
VLAN de niveau 2 (@ MAC) ou 3 (@IP)



Types de VLAN

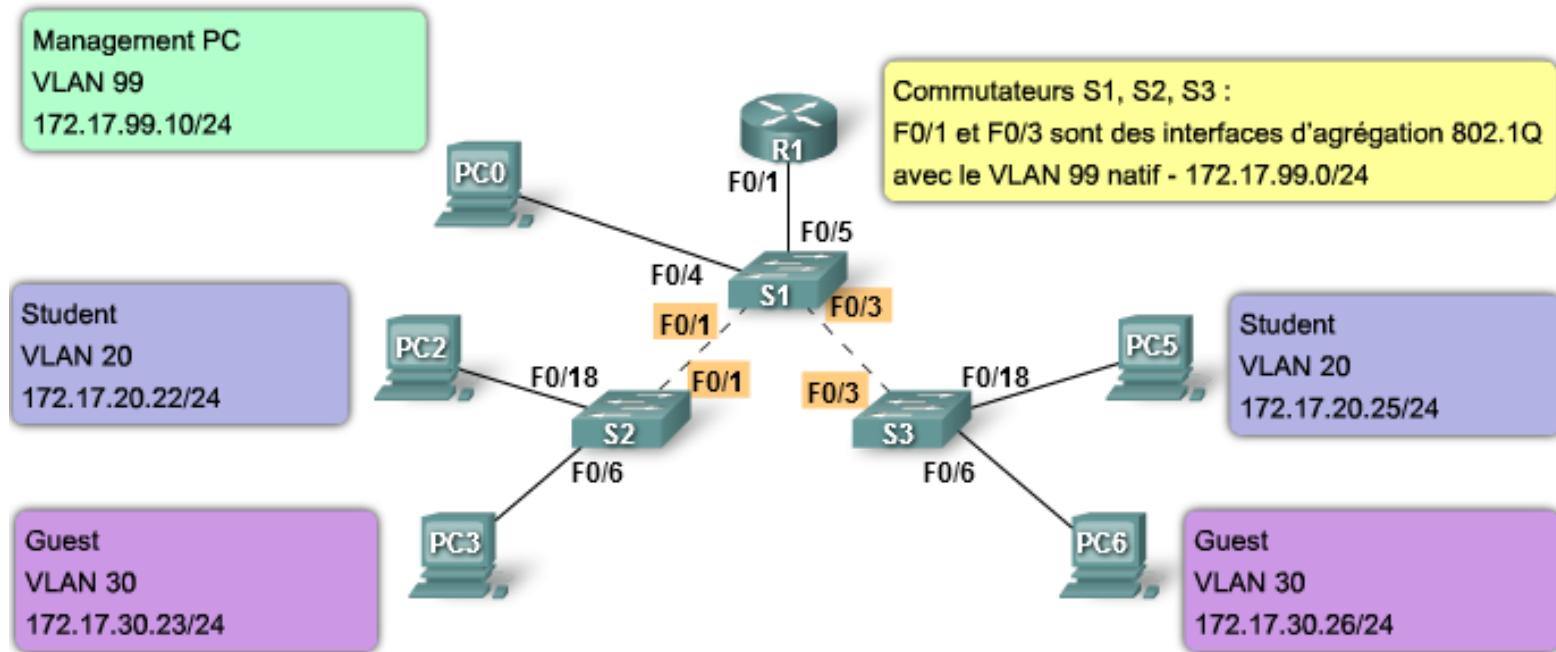
- La méthode d'implémentation des VLAN est presque toujours la même : il s'agit de VLAN basés sur le port
 - Ce type de VLAN est **associé à un port** appelé « **réseau local virtuel d'accès** »
- Il existe plusieurs termes pour désigner les VLAN dont les plus courants sont :
 - VLAN de **données** : configuré pour ne transporter que le trafic généré par l'utilisateur
 - VLAN par **défaut** : Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur
 - VLAN **natif** : est affecté à un port d'agrégation 802.1Q qui prend en charge le trafic provenant de nombreux VLAN
 - VLAN de **gestion** : configuré pour accéder aux fonctionnalités de gestion d'un commutateur

VLAN de données ou utilisateur



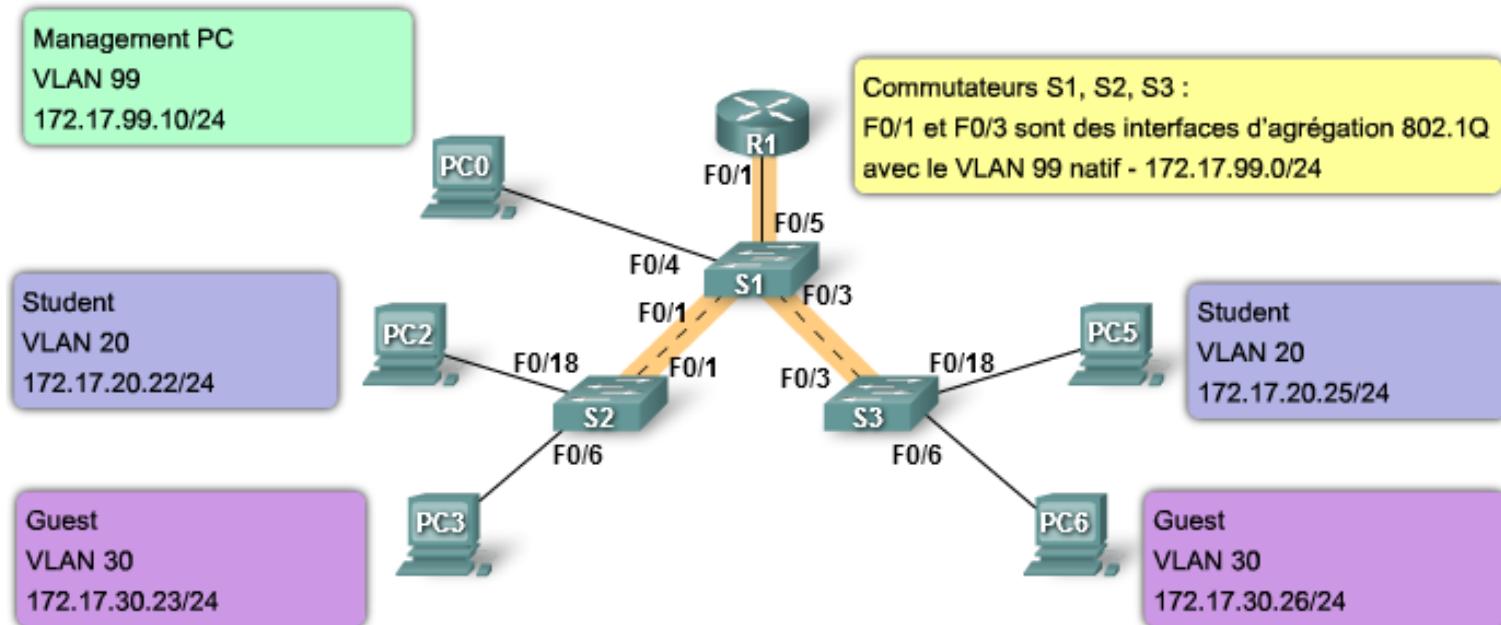
- Il est important de séparer les données utilisateur des données de contrôle de gestion des commutateurs et du trafic vocal

VLAN par défaut



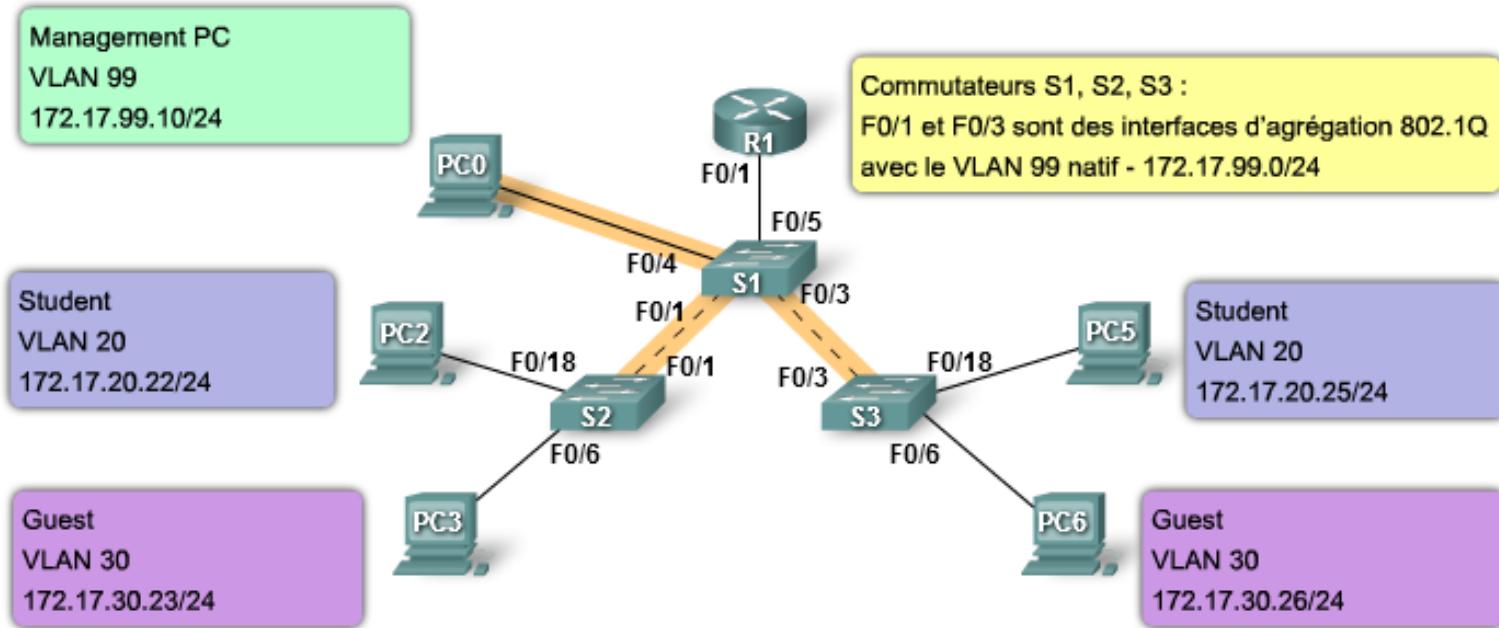
- N'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur
- Le **VLAN par défaut** des commutateurs Cisco est le **VLAN 1** et le trafic du VLAN 1 est transféré par le biais des agrégations de VLAN qui connectent les commutateurs S1, S2 et S3
- Pour des raisons de sécurité, il est conseillé de choisir un autre VLAN que le VLAN 1 en tant que VLAN par défaut. Cela suppose de configurer tous les ports du commutateur pour les associer à un autre VLAN par défaut que le VLAN 1
- Par défaut, le **trafic de contrôle de couche 2**, tel que le trafic des protocoles CDP (Cisco Discovery Protocol) et STP (Spanning Tree Protocol), est **associé au VLAN 1**

VLAN natif



- Un VLAN natif (ici VLAN 99) est affecté à un port d'agrégation 802.1Q
- Un port d'agrégation 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »)
- Le port d'agrégation 802.1Q place le trafic non étiqueté sur le VLAN natif
- Les VLAN natifs sont définis dans la spécification IEEE 802.1Q pour assurer la compatibilité descendante avec le trafic non étiqueté qui est commun aux scénarios LAN existants

VLAN de gestion

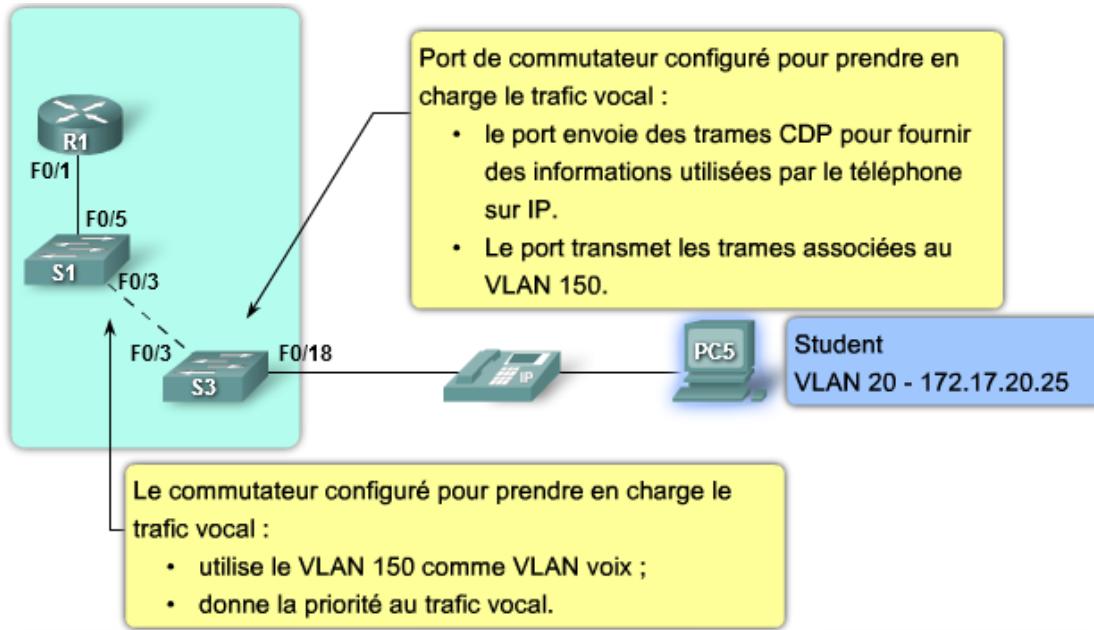


- Un VLAN de gestion est un réseau local virtuel que vous configurez pour accéder aux fonctionnalités de gestion d'un commutateur
- C'est le **VLAN 1 qui fait office de VLAN de gestion** si vous ne définissez pas explicitement un VLAN distinct pour remplir cette fonction
- Vous attribuez au VLAN de gestion une adresse IP et un masque de sous-réseau
- Étant donné que le VLAN 1 est déjà le VLAN par défaut dans la configuration initiale d'un commutateur Cisco, il est évident qu'il ne peut pas servir en plus de VLAN de gestion. Il faut en effet éviter qu'un utilisateur arbitraire qui se connecte à un commutateur ne se retrouve par défaut sur le VLAN de gestion

VLAN voix : pourquoi ?

- Imaginez que vous recevez un appel d'urgence et que soudain, la qualité de la transmission se dégrade tellement que vous ne comprenez plus ce que dit votre interlocuteur
- Le trafic de voix sur IP requiert les éléments suivants :
 - bande passante consolidée pour garantir la qualité de la voix
 - priorité de transmission par rapport aux autres types de trafic réseau
 - possibilité de routage autour des zones encombrées du réseau
 - délai inférieur à 150 millisecondes (ms) sur le réseau
- Pour plus d'info sur la config de VLAN voix consulter le lien :
 - http://www.cisco.com/en/US/docs-switches-lan/catalyst2975-software/release/12.2_46_ex/configuration-guide/swvoip.html

VLAN voix



- La liaison entre le commutateur et le téléphone IP joue le rôle d'agrégation pour acheminer aussi bien le trafic vocal étiqueté que le trafic de données non étiqueté**

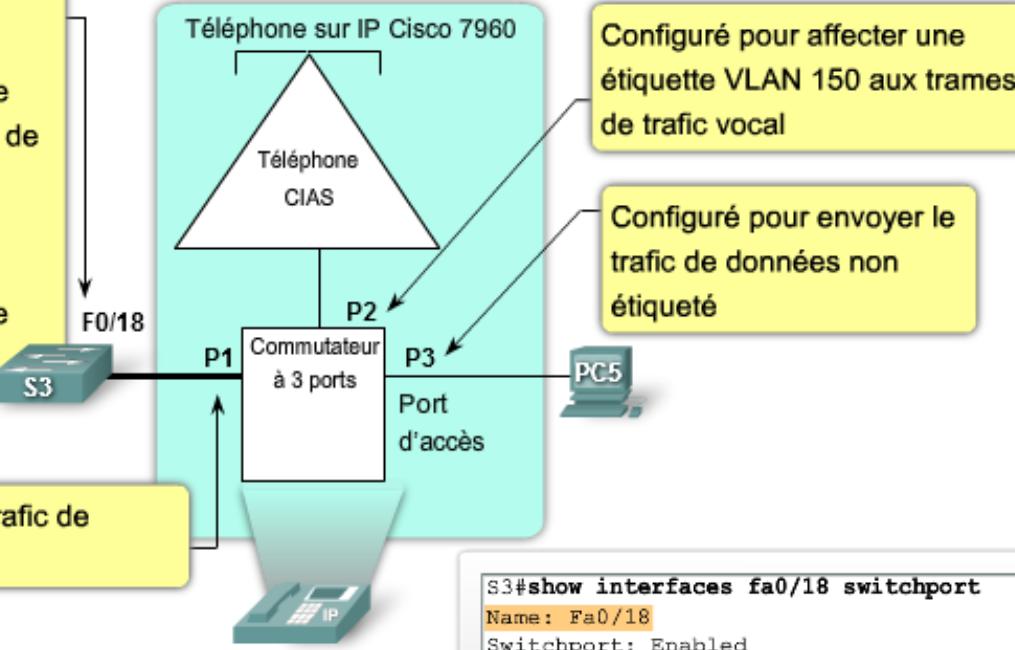
- Le port F0/18 du commutateur S3 est configuré en mode voix afin d'indiquer au téléphone d'affecter une étiquette VLAN 150 aux trames de voix
- Les trames de données qui arrivent au téléphone IP Cisco à partir de l'ordinateur PC5 ne sont pas étiquetées
- Les données destinées à PC5 qui proviennent du port F0/18 sont étiquetées VLAN 20 avant d'arriver au téléphone
- Celui-ci supprime ensuite l'étiquette VLAN avant que les données ne soient transmises à PC5
- L'étiquetage correspond à l'ajout d'octets dans un champ de la trame de données qui est utilisé par le commutateur pour identifier le VLAN auquel la trame de données doit être envoyée

Un téléphone IP Cisco est un commutateur

Le port de commutateur configuré pour prendre en charge le trafic vocal :

- indique au téléphone d'affecter une étiquette VLAN 150 aux trames de voix ;
- donne la priorité aux trames de voix ;
- transmet les trames de données au VLAN 20.

VLAN voix
Un téléphone sur IP Cisco est un commutateur



Configuré pour affecter une étiquette VLAN 150 aux trames de trafic vocal

Configuré pour envoyer le trafic de données non étiqueté

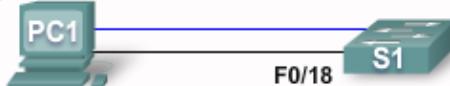
Configuré pour envoyer le trafic de données non étiqueté

```
S3#config terminal
```

```
Enter configuration commands, one per line.  
S3(config)#interface fastEthernet 0/18  
S3(config-if)#mls qos trust cos  
S3(config-if)#switchport voice vlan 150  
S3(config-if)#switchport mode access  
S3(config-if)#switchport access vlan 20
```

```
S3#show interfaces fa0/18 switchport  
Name: Fa0/18  
Switchport: Enabled  
Administrative Mode: static access  
Operational Mode: down  
Administrative Trunking Encapsulation: dot1q  
Negotiation of Trunking: Off  
Access Mode VLAN: 20 (VLAN0020)  
Trunking Native Mode VLAN: 1 (default)  
Administrative Native VLAN tagging: enabled  
Voice VLAN: 150 (VLAN0150)  
...  
Operational private-vlan: none  
Trunking VLANs Enabled: ALL  
Pruning VLANs Enabled: 2-1001  
Capture Mode Disabled
```

Configuration de base d'un commutateur



PC1 :

- Adresse IP : 172.17.99.12
- Connexion au port de console
- Connexion au port F0/18 sur le commutateur S1

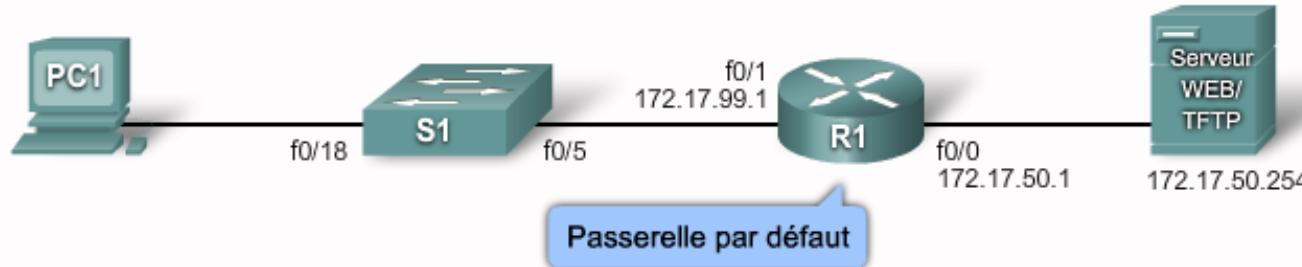
S1 :

- VLAN 99
- Réseau local virtuel de gestion
- Adresse IP : 172.17.99.11
- Port F0/18 affecté au VLAN 99

- Une adresse de couche 3 doit être affectée au commutateur pour la gestion TCP/IP.
- Le réseau local virtuel (VLAN) 1 est l'interface de gestion par défaut pour tous les commutateurs.
- L'utilisation du réseau local virtuel 1 présente des risques.
- Créez un autre réseau local virtuel (par exemple, VLAN 99 ou 150).
- Affectez ce réseau local virtuel à un port approprié (par exemple, F0/18).

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Passer en mode de configuration d'interface pour l'interface du VLAN 99.	<code>S1(config)#interface vlan 99</code>
Configurer l'adresse IP de l'interface.	<code>S1(config-if)#ip address 172.17.99.11 255.255.255.0</code>
Activer l'interface.	<code>S1(config-if)#no shutdown</code>
Repasser en mode d'exécution privilégié.	<code>S1(config-if)#end</code>
Passer en mode de configuration globale.	<code>S1#configure terminal</code>
Entrer dans l'interface pour affecter le réseau local virtuel.	<code>S1(config)#interface fastethernet 0/18</code>
Définir le mode d'appartenance du port à un réseau local virtuel.	<code>S1(config-if)#switchport mode access</code>
Affecter le port à un réseau local virtuel.	<code>S1(config-if)#switchport access vlan 99</code>
Repasser en mode d'exécution privilégié.	<code>S1(config-if)#end</code>
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	<code>S1#copy running-config startup-config</code>

Configurer la passerelle par défaut



Syntaxe de commande de l'interface de ligne de commande Cisco IOS

Configurer la passerelle par défaut sur le commutateur.

```
S1(config)#ip default-gateway 172.17.99.1
```

Repasser en mode d'exécution privilégié.

```
S1(config)#end
```

Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.

```
S1#copy running-config startup-config
```

```
S1#show running-config
...
!
interface FastEthernet0/18
  switchport access vlan 99
  switchport mode access
...
!
```

VLAN 99 configuré sur le port F0/18

```
S1#show ip interface brief
Interface          IP-Address      OK?   Method      Status
Protocol
...
Vlan99            172.17.99.11  YES   manual      up        up
...
FastEthernet0/18   unassigned     YES   unset       up        up
FastEthernet0/19   unassigned     YES   unset       down     down
```

État du VLAN 99 et du port F0/18

Configuration de l'accès console et de l'accès au terminal virtuel

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Passer du mode de configuration globale au mode de configuration de ligne pour la console 0.	<code>S1(config)#line con 0</code>
Définir cisco en tant que mot de passe pour la ligne de console 0 sur le commutateur.	<code>S1(config-line)#password cisco</code>
Définir la ligne de console pour exiger la saisie du mot de passe avant l'octroi de l'accès.	<code>S1(config-line)#login</code>
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	<code>S1(config-line)#end</code>

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Passer du mode de configuration globale au mode de configuration de ligne pour les lignes vty 0 à 4.	<code>S1(config)#line vty 0 4</code>
Définir cisco en tant que mot de passe pour les lignes vty sur le commutateur.	<code>S1(config-line)#password cisco</code>
Définir la ligne vty pour exiger la saisie du mot de passe avant l'octroi de l'accès.	<code>S1(config-line)#login</code>
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	<code>S1(config-line)#end</code>

Configuration du mot de passe

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	S1# configure terminal
Configurer la commande enable password pour le passage en mode d'exécution privilégié.	S1(config)# enable password mot_de_passe
Configurer le mot de passe enable secret pour le passage en mode d'exécution privilégié.	S1(config)# enable secret mot_de_passe
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	S1(config)# end

- La commande Cisco IOS:
 - **service password-encryption** autorise le chiffrement des mots de passe de service

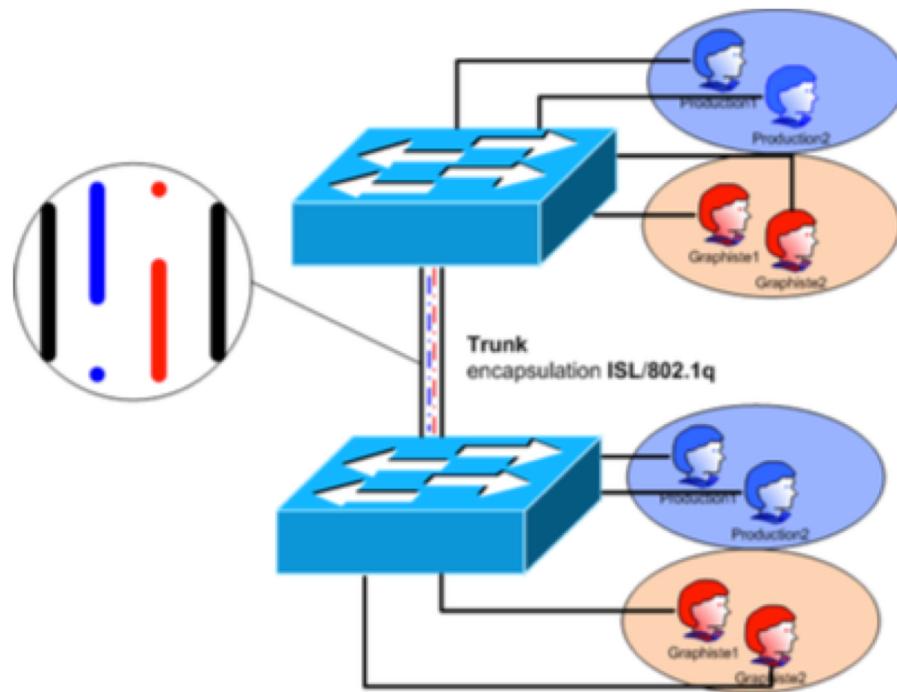
```
--  
line con 0  
password cisco  
login  
line vty 0 4  
password cisco  
no login  
line vty 5 15  
password cisco  
no login  
!  
end  
S1#config terminal  
S1(config)#service password-encryption  
S1(config)#end  
S1#Show running-config  
--  
control-plane
```

Commandes générales

- **vlan database**
 - Mode privilégié
 - Permet d'accéder au mode de configuration de VLAN
- **vlan vlan_id [name { nom du vlan }]**
 - Mode de configuration des VLAN (vlan database)
 - Permet de créer et nommer les VLANs
- **switchport mode {access | dynamic {auto | desirable} | trunk}**
 - Mode de configuration d'interface
 - Permet de configurer une interface pour le trunking ou pour un VLAN
- **switchport access vlan vlan-id**
 - Mode de configuration d'interface
 - Permet de configurer un VLAN statique sur une interface

TP0: configuration de base d'un commutateur

- **Objectifs pédagogiques**
- À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :
 - Câbler un réseau conformément au schéma de topologie
 - Supprimer une configuration existante sur un commutateur
 - Examiner et vérifier la configuration par défaut
 - Créer la configuration de base d'un commutateur, avec un nom et une adresse IP
 - Configurer des mots de passe pour sécuriser l'accès à l'interface de ligne de commande
 - Configurer les propriétés de vitesse de port et de mode bidirectionnel du commutateur pour une interface
 - Configurer la sécurité de base des ports du commutateur
 - Gérer la table d'adresses MAC
 - Affecter les adresses MAC statiques
 - Ajouter et déplacer des hôtes sur un commutateur



NOTION DE TRUNK (AGRÉGATION)

Notion de trunk (agrégation)

- Il est donc nécessaire d'élaborer une technique de partage des réseaux locaux entre équipements
 - Il faut étiqueter les trames pour identifier le trafic des différents réseaux locaux sur un même canal physique
- Ainsi, les réseaux locaux sont distribués sur les différents équipements via des liaisons logiques dédiées appelées *trunks*
- Le *trunk* est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels
- Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id)
- Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion)

Les trunks peuvent être utilisés

- **Entre deux commutateurs** : C'est le mode de distribution des réseaux locaux le plus courant
- **Entre un commutateur et un hôte** : C'est le mode de fonctionnement à surveiller étroitement
 - Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels
- **Entre un commutateur et un routeur** : C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN
- Enfin, il ne faut pas oublier que tous les VLANs véhiculés dans le même *trunk* partagent la bande passante du média utilisé
 - Le *trunk* peut donc constituer un goulot d'étranglement si sa capacité est insuffisante

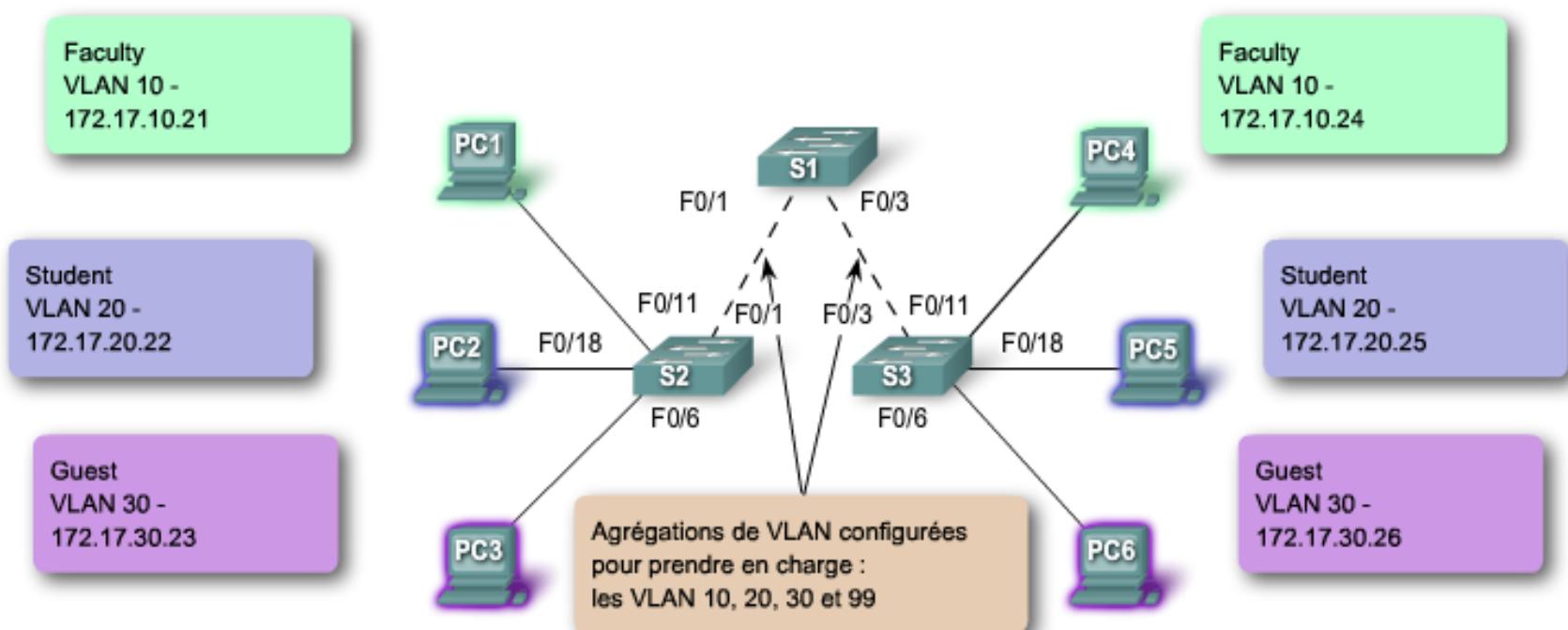
Agrégations de VLAN

- Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN
- Une agrégation de VLAN vous permet d'étendre les VLAN à l'ensemble d'un réseau
- Cisco prend en charge la norme IEEE 802.1Q pour coordonner les agrégations sur les interfaces Fast Ethernet et Gigabit Ethernet
- Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLAN entre les commutateurs et les routeurs

Agrégations de VLAN (2)

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

Ports
F0/1 à F0/5 sont des interfaces d'agrégation 802.1Q avec le VLAN 99 natif.
F0/11 à F0/17 sont dans le VLAN 10.
F0/18 à F0/24 sont dans le VLAN 20.
F0/6 à F0/10 sont dans le VLAN 30.



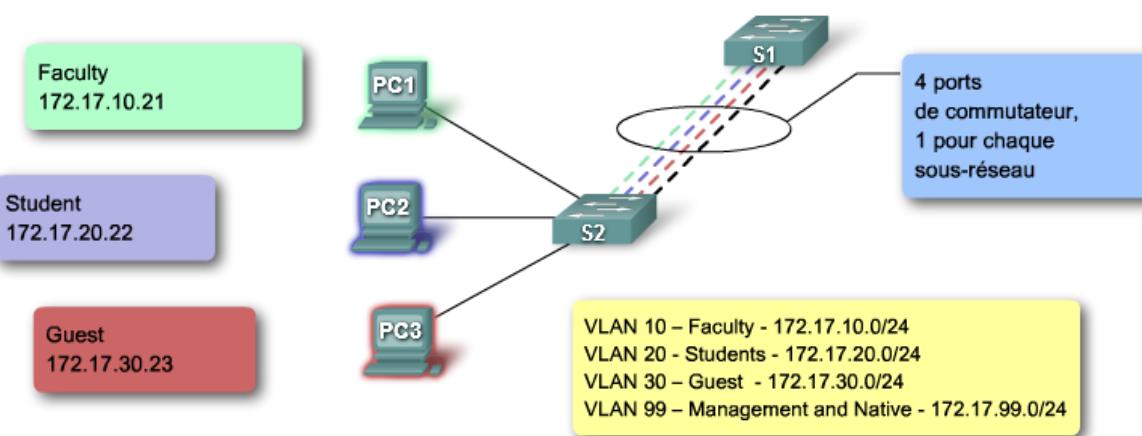
Quel problème une agrégation résout-elle ?

Faculty - 172.17.10.0/24

Students - 172.17.20.0/24

Guest - 172.17.30.0/24

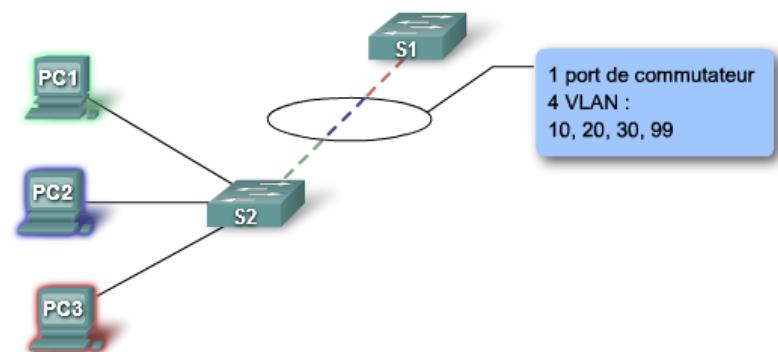
Management and Native - 172.17.99.0/24



Faculty
VLAN 10
172.17.10.21

Student
VLAN 20
172.17.20.22

Guest
VLAN 30
172.17.30.23



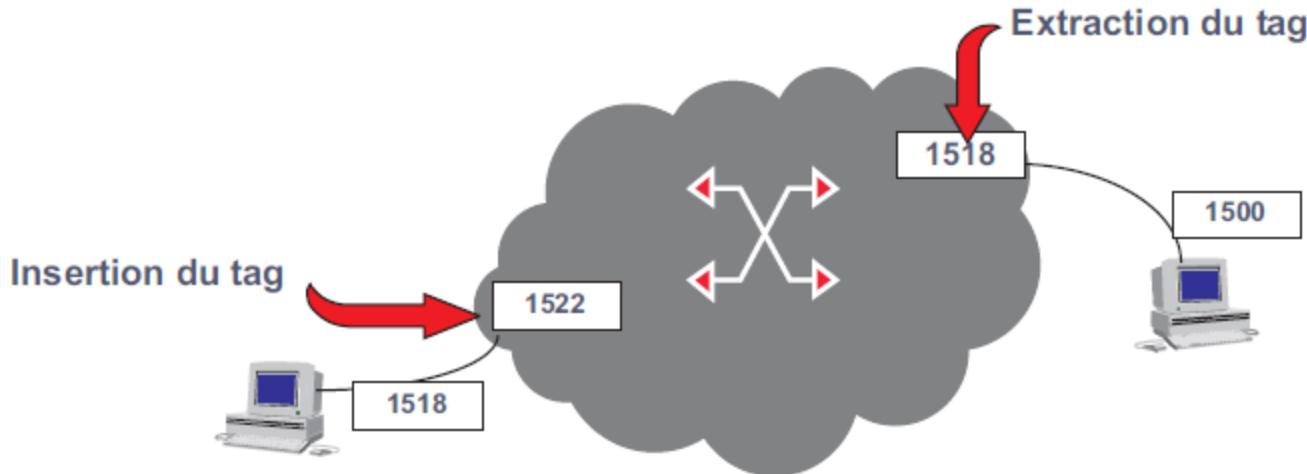
La norme 802.1 p/Q

- Un VLAN correspond à un domaine de broadcast. Cependant, lorsque plusieurs VLAN sont définis sur un même segment cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le broadcast en une rafale d'unicasts
- La solution adoptée par l'IEEE est toute différente : un seul VLAN peut être déclaré par port, les VLAN sont définis dans les normes 802.1Q (VLAN) et 802.1p (QoS) (802.1p/Q) qui introduisent quatre octets supplémentaires dans la trame MAC afin d'identifier les VLAN (VLAN tagging) et de gérer 8 niveaux de priorité (Quality of Service, QoS)

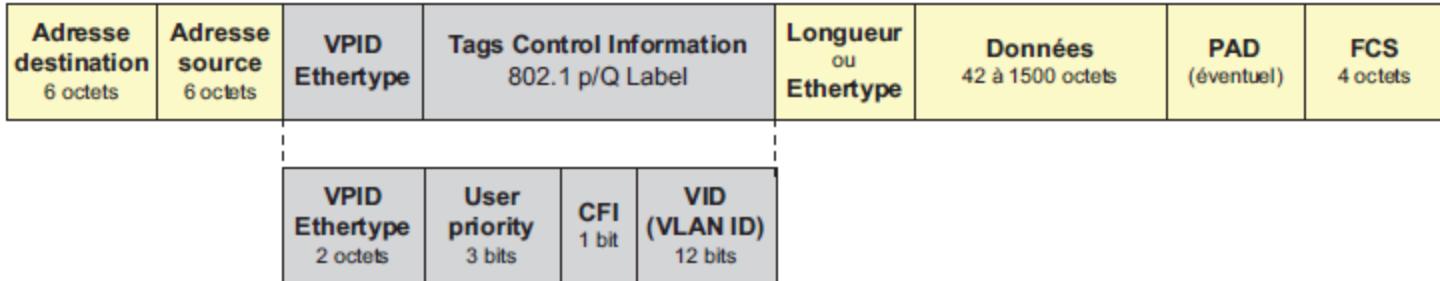
Format de la trame 802.1 p/Q

Adresse destination 6 octets	Adresse source 6 octets	VPIID EtherType	Tags Control Information 802.1 p/Q Label	Longueur ou EtherType	Données 42 à 1500 octets	PAD (éventuel)	FCS 4 octets
		VPIID EtherType 2 octets	User priority 3 bits	CFI 1 bit	VID (VLAN ID) 12 bits		

- La trame 802.1p/Q augmente la taille de la trame 802.3
 - La taille maximale passe de 1 518 à 1 522 octets. Ce format limite l'usage de la trame en interne au commutateur et au dialogue inter-commutateur

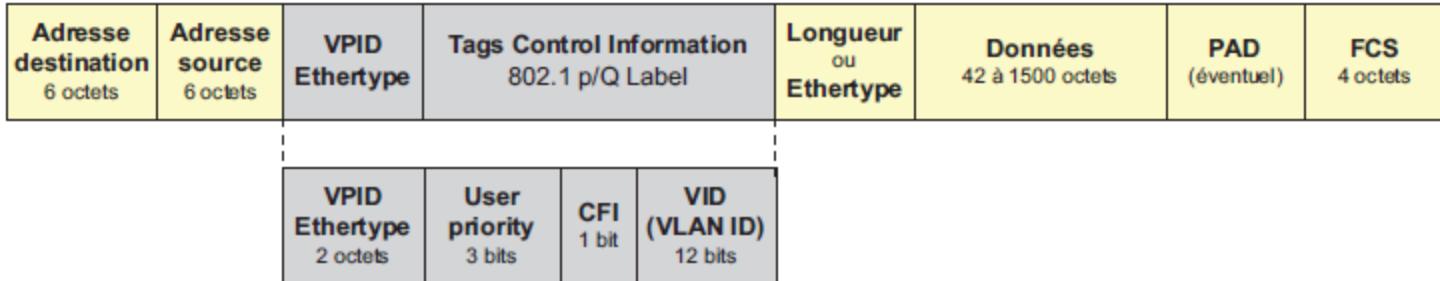


La trame 802.1 p/Q (1/2)



- Pour garantir la compatibilité avec l'existant, le marquage des trames est vu comme une encapsulation supplémentaire
- Ainsi, le champ **VPIID** (VLAN Protocol ID) est similaire au champ EtherType de la trame 802.3, il identifie le format 802.1 p/Q, sa valeur est fixée à 0x8100
- Les deux octets suivants permettent de définir huit niveaux de priorité (**User Priority**)
- Les commutateurs de dernière génération disposent de plusieurs files d'attente les trames sont affectées à telle ou telle file suivant leur niveau de priorité

La trame 802.1 p/Q (2/2)



- Le bit **CFI (Canonical Format Identifier)** est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0. Dans les réseaux Token Ring, à 1, il indique que les données du champ routage par la source sont au format non canonique
- Le champ **VID (VLAN IDentifier)** identifie sur douze bits le VLAN destination
- L'introduction de quatre octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS. On commence à trouver des cartes transporteurs capables de supporter le tagging

VLAN natifs et agrégation 802.1Q

- **Trames étiquetés sur le VLAN natif**
 - Sont abandonnées par le commutateur
 - Les périphériques ne doivent pas étiqueter le trafic de contrôle destiné au VLAN natif
- **Trames non étiquetés sur le VLAN natif**
 - Voient leur VPID remplacé par la valeur du VLAN natif (VLAN de gestion) configuré
 - Restent non étiquetés
 - Sont transférées sur le VLAN natif configuré
 - Par exemple, si le VLAN 99 est configuré en tant que VLAN natif, le VPID est égal à 99 et tout le trafic non étiqueté est transféré vers le VLAN 99. Si le VLAN natif n'a pas été reconfiguré, la valeur du VPID est définie sur le VLAN 1 (VLAN natif par défaut)

Exemple de configuration de VLAN natif

Syntaxe de commande ILC de Cisco IOS

Passer en mode de configuration globale sur le commutateur S1.	S1# configure terminal
Passer en mode de configuration d'interface.	S1(config)# interface F0/1
Définir l'interface F0/1 comme agrégation IEEE 802.1Q.	S1(config-if)# switchport mode trunk
Configurer le VLAN 99 en tant que VLAN natif.	S1(config-if)# switchport trunk native vlan 99
Revenir au mode d'exécution privilégié.	S1(config-if)# end

```
S1#show interfaces F0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
...
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
...
Trunking VLANs Enabled: ALL
```

- Vérification du VLAN natif

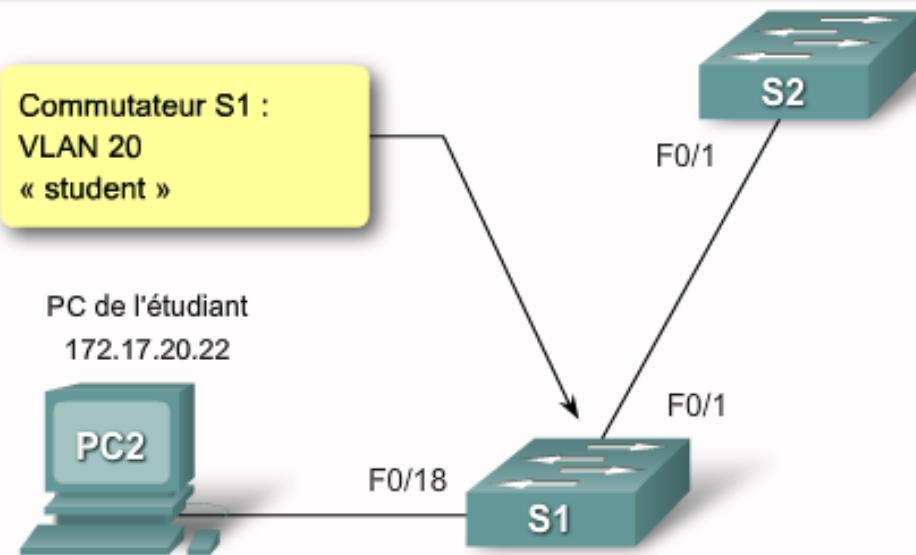
Ajout d'un VLAN

- Vous allez configurer des VLAN dont les ID se trouvent dans la **plage normale**
- Il existe deux plages d'ID de VLAN : la plage normale contient les ID compris entre 1 et 1001 tandis que la **plage étendue** contient les ID compris entre 1006 et 4094
- Le VLAN 1 et les VLAN 1002 à 1005 sont des numéros d'ID réservés aux VLAN Token Ring et aux VLAN à interface de données distribuées sur fibre (FDDI)
- Lorsque vous configurez des VLAN à plage normale, les détails de la configuration sont stockés automatiquement dans la mémoire flash du commutateur dans un fichier appelé `vlan.dat`

Ajout d'un VLAN(2)

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	S1# configure terminal
Créer un VLAN. « id de vlan » est le numéro de VLAN à créer. Passe en mode de configuration de VLAN pour l'ID de VLAN du VLAN.	S1(config)# vlan id de vlan
(Facultatif) Spécifier un nom de VLAN unique pour identifier le VLAN. Si aucun nom n'est entré, le numéro de VLAN, complété par des zéros, est ajouté au mot « VLAN », comme par exemple VLAN0020.	S1(config-vlan)# name nom_vlan
Revenir au mode d'exécution privilégié. Vous devez terminer votre session de configuration pour que la configuration soit enregistrée dans le fichier <i>vlan.dat</i> et pour qu'elle soit appliquée.	S1(config-vlan)# end

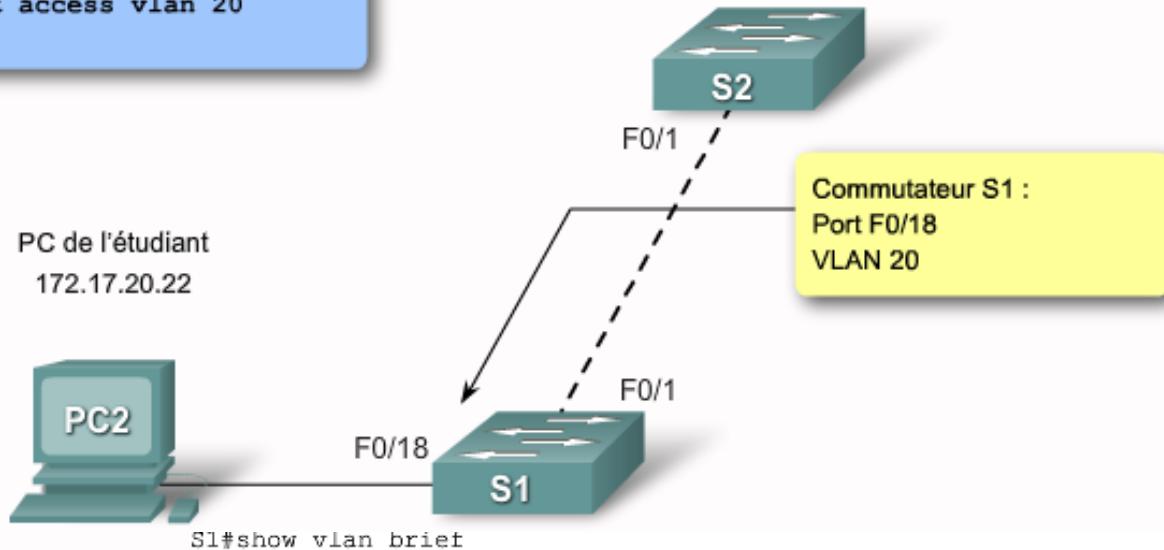
```
S1#configure terminal  
S1(config)#vlan 20  
S1(config-vlan)#name  
student  
S1(config-vlan)#end
```



S1# show vlan brief

Affectation d'un port de commutateur

```
S1#configure terminal  
S1(config)#interface F0/18  
S1(config-if)#switchport mode access  
S1(config-if)#switchport access vlan 20  
S1(config-if)#end
```



S1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
20 student	active	Fa0/18
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Vérification des VLAN et des appartenances des ports

Commande show vlan

Syntaxe de commande de l'interface de ligne de commande Cisco IOS

show vlan [brief | id *id de vlan* | name *nom_vlan* | summary]

Afficher une ligne pour chaque VLAN comportant le nom du VLAN, son état et ses ports.

brief

Afficher des informations sur un VLAN unique identifié par un numéro d'ID de VLAN.
La valeur *id de vlan* peut être comprise entre 1 et 4094.

id *id de vlan*

Afficher des informations sur un VLAN unique identifié par un nom de VLAN. Le nom de VLAN est une chaîne ASCII de 1 à 32 caractères de long.

name *nom_vlan*

Afficher un résumé sur les VLAN.

summary

Commande show interfaces

Syntaxe de commande de l'interface de ligne de commande Cisco IOS

show interfaces [*id_interface* | **vlan *id de vlan*] | switchport**

Les interfaces autorisées comprennent les ports physiques (y compris le type, le module et le numéro de port) et les canaux de port. La plage des canaux de port est comprise entre 1 et 6.

id_interface

Identification du VLAN. La plage est comprise entre 1 et 4094.

vlan *id de vlan*

Afficher l'état administratif et opérationnel d'un port de commutation, y compris les paramètres de blocage et de protection du port.

switchport

Gestion des appartenances des ports

Syntaxe de commande de l'interface de ligne de commande Cisco IOS

Passer en mode de configuration globale.

```
S1#configure terminal
```

Passer en mode de configuration d'interface pour configurer l'interface.

```
S1(config)#interface id_interface
```

Supprimer l'affectation de VLAN sur cette interface de port de commutateur et revenir à l'appartenance par défaut au VLAN 1.

```
S1(config-if)#no switchport access vlan
```

Repasser en mode d'exécution privilégié.

```
S1(config-if)#end
```

Réaffectation du VLAN

```
S1#config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
S1(config)#interface f0/11  
S1(config-if)#switchport mode access  
S1(config-if)#switchport access vlan 20  
S1(config-if)#end  
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2

Configuration du agrégation 802.1Q

Syntaxe de commande de l'interface de ligne de commande

Cisco IOS

Passer en mode de configuration globale.

```
S1#configure terminal
```

Entrer dans le mode de configuration d'interface pour l'interface définie.

```
S1(config)#interface id d'interface
```

Forcer la liaison reliant les commutateurs à devenir une liaison agrégée.

```
S1(config-if)#switchport mode trunk
```

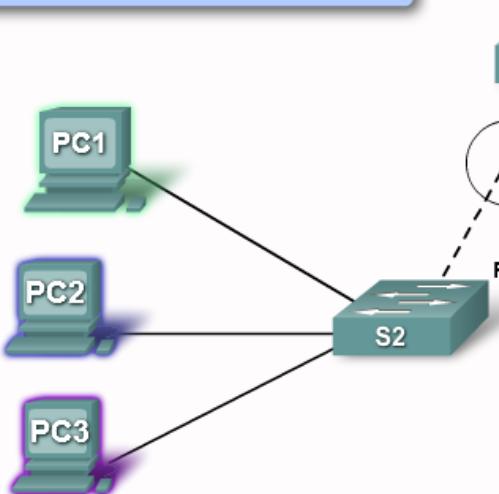
Spécifier un autre VLAN en tant que VLAN natif pour le trafic non étiqueté pour les agrégations IEEE 802.1Q.

```
S1(config-if)#switchport trunk native vlan id de vlan
```

Repasser en mode d'exécution privilégié.

```
S1(config-if)#end
```

VLAN 10 - Faculty/Staff - 172.17.10.0/24
 VLAN 20 - Students - 172.17.20.0/24
 VLAN 30 - Guest (Default) - 172.17.30.0/24
 VLAN 99 - Management and Native - 172.17.99.0/24



```
S1#config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.
 S1(config)#interface f0/1
 S1(config-if)#switchport mode trunk
 S1(config-if)#switchport trunk native vlan 99
 S1(config-if)#end

```
S1#show interfaces f0/1 switchport
```

Name: Fa0/1
 Switchport: Enabled
 Administrative Mode: trunk
 Operational Mode: down
 Administrative Trunking Encapsulation: dot1q
 Negotiation of Trunking: On
 Access Mode VLAN: 1 (default)
 Trunking Native Mode VLAN: 99 (management)
 Administrative Native VLAN tagging: enabled
 Voice VLAN: none

Gestion de la configuration d'une agrégation

Syntaxe de commande de l'interface de ligne de commande
Cisco IOS

Utilisez cette commande en mode de configuration d'interface pour réinitialiser tous les VLAN configurés sur l'interface d'agrégation.

Utilisez cette commande en mode de configuration d'interface pour réinitialiser le VLAN natif et le réaffecter au VLAN 1.

Utilisez cette commande en mode de configuration d'interface pour réinitialiser l'interface du port d'agrégation en port de mode d'accès statique.

```
S1(config-if)#no switchport trunk allowed  
vlan
```

```
S1(config-if)#no switchport trunk native  
vlan
```

```
S1(config-if)#switchport mode access
```

```
S1#config terminal  
Enter configuration commands, one per line. End  
S1(config)#interface f0/1  
S1(config-if)#no switchport trunk allowed vlan  
S1(config-if)#no switchport trunk native vlan  
S1(config-if)#end  
S1#show interfaces f0/1 switchport  
Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: trunk  
Operational Mode: down  
Administrative Trunking Encapsulation: dot1q  
Negotiation of Trunking: On  
Access Mode VLAN: 1 (default)  
Trunking Native Mode VLAN: 1 (default)  
Administrative Native VLAN tagging: enabled  
Voice VLAN: none  
...  
Trunking VLANs Enabled: ALL
```

```
S1(config)#interface f0/1  
S1(config-if)#switchport mode access  
S1(config-if)#end  
  
S1#show interfaces f0/1 switchport  
Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: static access  
Operatioss Mode VLAN: 1 (default)  
Trunking Native Mode VLAN: 1 (default)  
Administrative Native VLAN tagging: enabled  
Voice VLAN: none  
Administrative private-vlan host-association: none  
...  
Trunking VLANs Enabled: ALL  
Pruning VLANs Enabled: 2-1001  
Capture Mode Disabled  
dmiCapture VLANs Allowed: ALL
```

TP 1: Configuration de VLAN et d'agrégations

1. Créez les réseaux locaux virtuels
2. Affectez statiquement des ports de commutateur aux VLAN
3. Vérifiez la configuration des VLAN
4. Activez l'agrégation sur les connexions entre les commutateurs
5. Vérifiez la configuration des agrégations

TP2: configuration de base VLAN

- Objectifs pédagogiques
 - Exécuter des tâches de configuration de base sur un commutateur
 - Créer des réseaux locaux virtuels
 - Affecter des ports de commutateur à un réseau local virtuel
 - Ajouter, déplacer et modifier des ports
 - Vérifier la configuration des réseaux locaux virtuels
 - Activer l'agrégation sur des connexions entre commutateurs
 - Vérifier la configuration d'agrégation
 - Enregistrer la configuration des réseaux locaux virtuels

Problèmes courants avec les VLAN et les agrégations

Problème	Résultat	Exemple
Non-concordance du VLAN natif	Présente un risque pour la sécurité et génère des résultats indésirables.	Par exemple, un port est défini comme VLAN 99, l'autre comme VLAN 100.
Non-concordance du mode d'agrégation	Entraîne la perte de la connectivité réseau.	Par exemple, un port est en mode d'agrégation « désactivé » et l'autre en mode d'agrégation « actif ».
VLAN et sous-réseaux IP	Entraîne la perte de la connectivité réseau.	Par exemple, les ordinateurs des utilisateurs ont pu être configurés avec des adresses IP incorrectes.
VLAN autorisés sur les agrégations	Génère un trafic imprévu ou nul sur l'agrégation.	La liste des VLAN autorisés ne prend pas en compte les critères d'agrégation de VLAN actuels.

Leçons

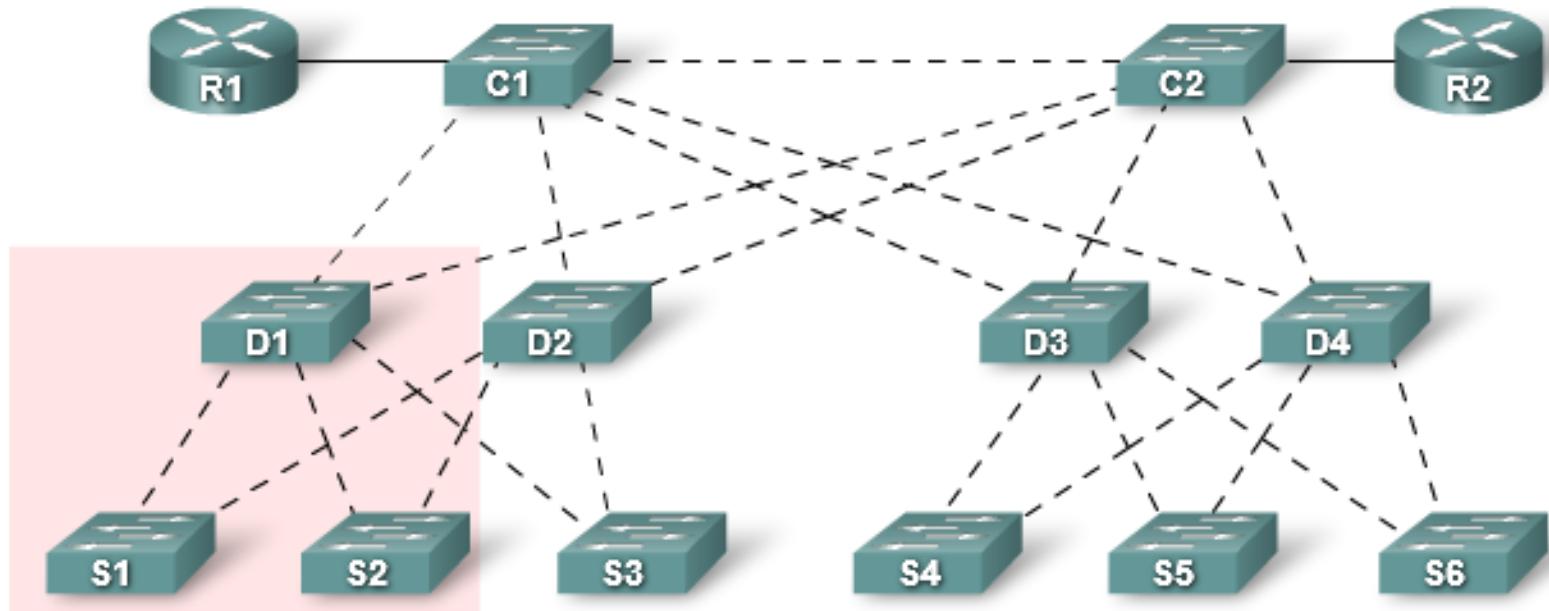
- Les VLAN séparent les domaines de diffusion sur les commutateurs et améliorent les performances, la gestion et la sécurité
- Les VLAN peuvent être utilisés pour le trafic de données, le trafic vocal, le trafic de protocole réseau et le trafic de gestion de réseau
- Ils existent trois modes d'appartenance différents : VLAN statique, VLAN dynamique et VLAN voix
- Des routeurs ou des commutateurs de couche 3 sont requis pour la communication entre les VLAN
- Les agrégations (IEEE 802.1 Q) permettent à plusieurs VLAN d'utiliser une même liaison pour simplifier la communication inter-VLAN à travers plusieurs commutateurs
- Le protocole 802.1Q qui sépare le trafic des différents VLAN, lorsqu'il traverse la liaison agrégée, n'étiquette pas le trafic du VLAN natif, ce qui peut entraîner des problèmes lorsque l'agrégation est mal configurée

Gestion des VLAN : un défi

VLAN existants : 10, 20, 99

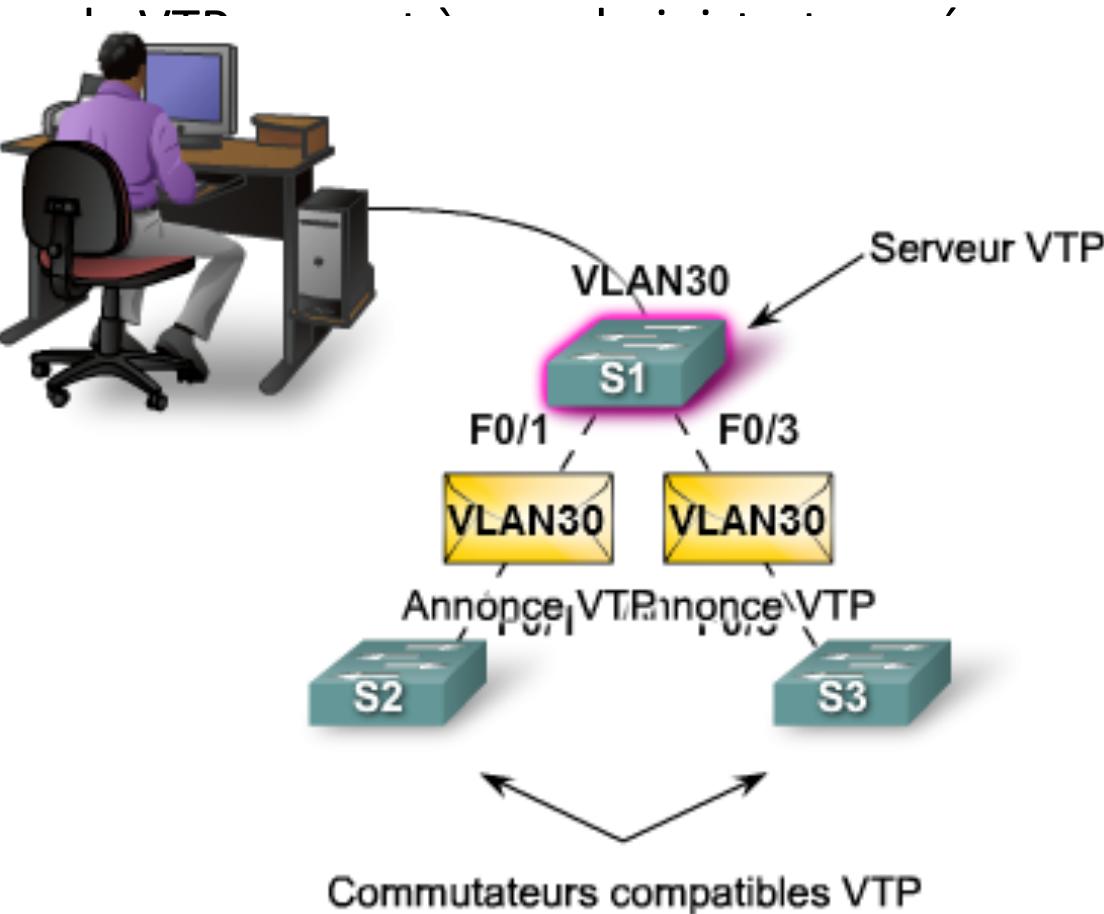
Tâche de gestion VLAN : ajout de VLAN 30

Protocole VTP (VLAN Trunking Protocol) pour ne pas configurer manuellement les VLAN et agrégations



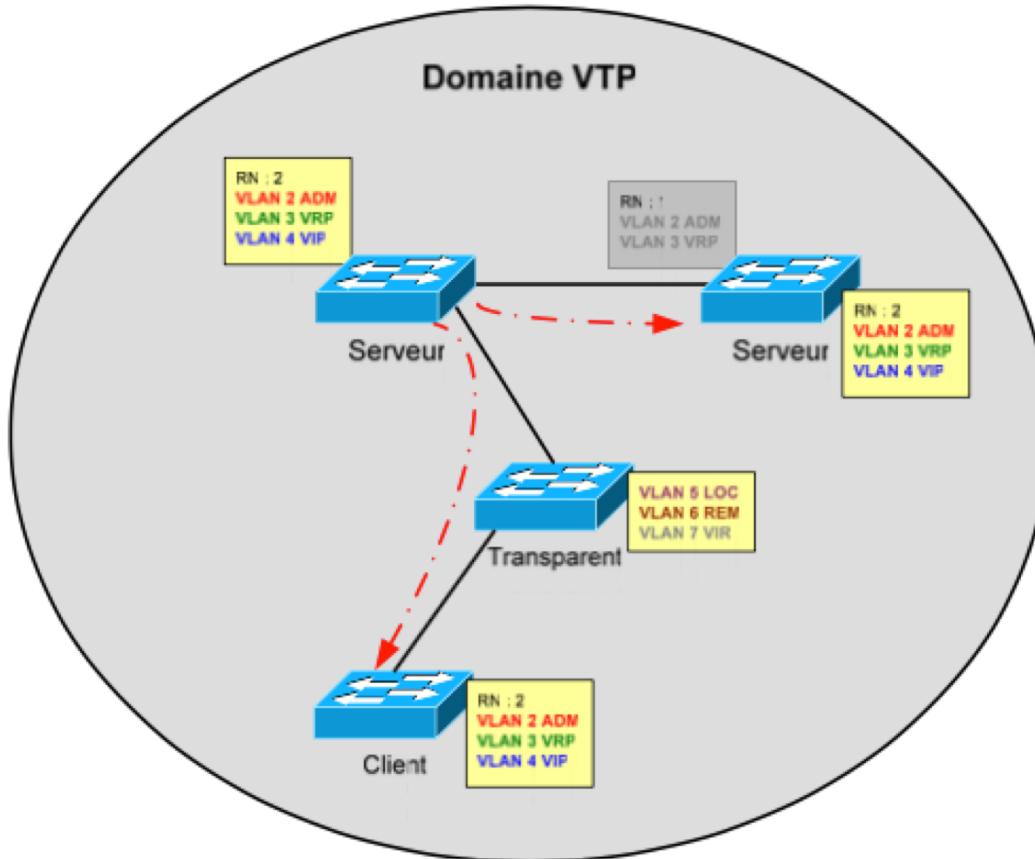
Qu'est ce que le protocole VTP?

- Le protocole VTP permet de configurer un réseau LAN à plusieurs commutateurs.
- Le fonctionnement d'un client VTP.
- Le protocole VTP utilise une plage numéro d'identification de VLAN de 1 à 1 005.
- Les réseaux VLAN sont donc centralisés.
- Le serveur VTP communique avec les autres commutateurs minimisant les erreurs ou incorrectes.
- Le protocole VTP est basé sur la donnée.



configurer un réseau LAN à plusieurs commutateurs.
Le fonctionnement d'un client VTP ou d'un serveur VTP ou d'un autre commutateur.
Les réseaux VLAN sont donc centralisés.
Le serveur VTP communique avec les autres commutateurs minimisant les erreurs ou incorrectes.
Le protocole VTP utilise une plage numéro d'identification de VLAN de 1 à 1 005) ne permet pas de créer des VLAN aux noms qui sont incorrectes.
La base de données de VLAN est mise à jour régulièrement par les serveurs VTP.

Domaine VTP



- On distingue une hiérarchie comprenant trois modes de fonctionnement :
 - VTP **serveur**
 - VTP **client**
 - VTP **transparent**

VTP serveur / VTP client

- Les commutateurs qui font office de serveur VTP peuvent créer, modifier, supprimer les VLAN et d'autres paramètres de configuration
 - Ils peuvent transmettre cette configuration aux commutateurs en mode client (ou serveur) dans leur domaine VTP
- Les commutateurs fonctionnant en mode client ne peuvent que recevoir et transmettre les mises à jour de configuration
- Les commutateurs en mode serveur et client mettent à jour leur base de données VLAN, si et seulement si, ils reçoivent une mise à jour VTP concernant leur domaine et contenant un numéro de révision supérieur à celui déjà présent dans leur base

VTP transparent

- Le mode transparent, lui, permet aux commutateurs de ne pas tenir compte des mises à jour VTP
- Ils sont autonomes dans le domaine VTP et ne peuvent configurer que leurs VLAN (connectés localement)
- Cependant, ils transmettent aux autres commutateurs les mises à jour qu'ils reçoivent

Fonctionnement VTP

Fonction	Mode Serveur	Mode Client	Mode Transparent
Envoi de messages VTP	OUI	NON	NON
Réception des messages VTP ; Synchronisation VLAN	OUI	OUI	NON
Transmission des messages VTP reçus	OUI	OUI	OUI
Sauvegarde de configuration VLAN (en NVRAM ou Flash)	OUI	NON	OUI
Édition des VLANs (création, modification, suppression)	OUI	NON	OUI

- Lorsqu'un hôte d'un VLAN envoie un broadcast, celui-ci est transmit à tous les commutateurs du domaine VTP
- Il peut arriver que dans ce domaine, des commutateurs n'ait pas le VLAN concerné sur un de leur port. Ce broadcast leur est alors destiné sans aucune utilité
- Le **VTP pruning** empêche la propagation de ces trafics de broadcast aux commutateurs qui ne sont pas concernés

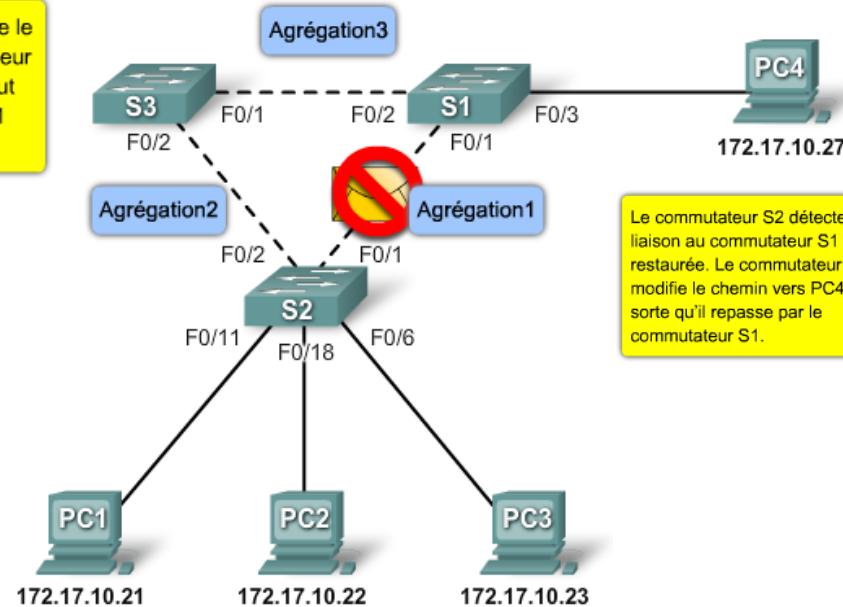
Commandes associées

- **vlan database**
 - Mode privilégié
 - Permet d'accéder au mode de configuration de VLAN
- **vlan vlan_id [name { nom du vlan }]**
 - Mode de configuration de VLAN
 - Permet de créer et nommer les VLANs
- **vtp domain nom de domaine { password mot de passe | pruning | v2-mode | {server | client | transparent}}**
 - Mode de configuration de VLAN
 - Spécifie les paramètres VTP
- **show vtp status**
 - Mode privilégié
 - Affiche la configuration VTP et le statut du processus

Bienfaits de la redondance

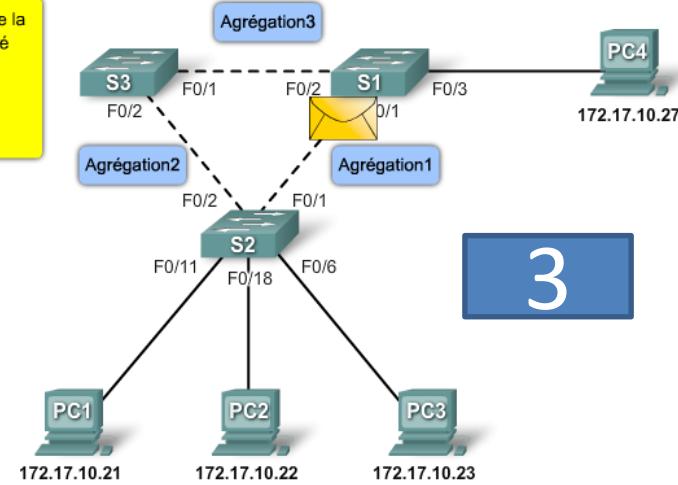
Agrégation1 est interrompu entre le commutateur S2 et le commutateur S1. La trame de données ne peut pas atteindre le commutateur S1 sur Agrégation1.

1



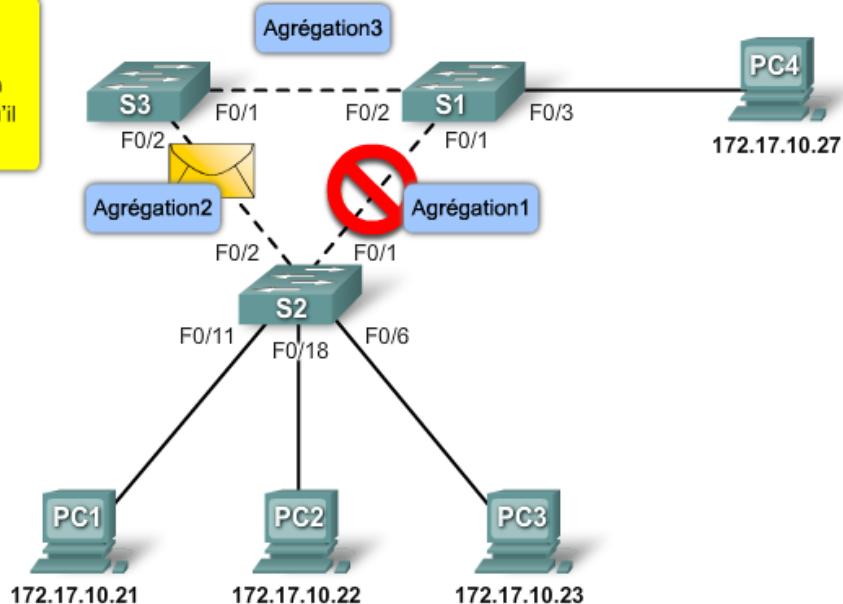
Le commutateur S2 détecte que la liaison au commutateur S1 a été restaurée. Le commutateur S2 modifie le chemin vers PC4 de sorte qu'il repasse par le commutateur S1.

3



Le commutateur S2 détecte la connexion interrompue vers le commutateur S1 et il modifie son chemin d'acheminement pour qu'il passe par le commutateur S3.

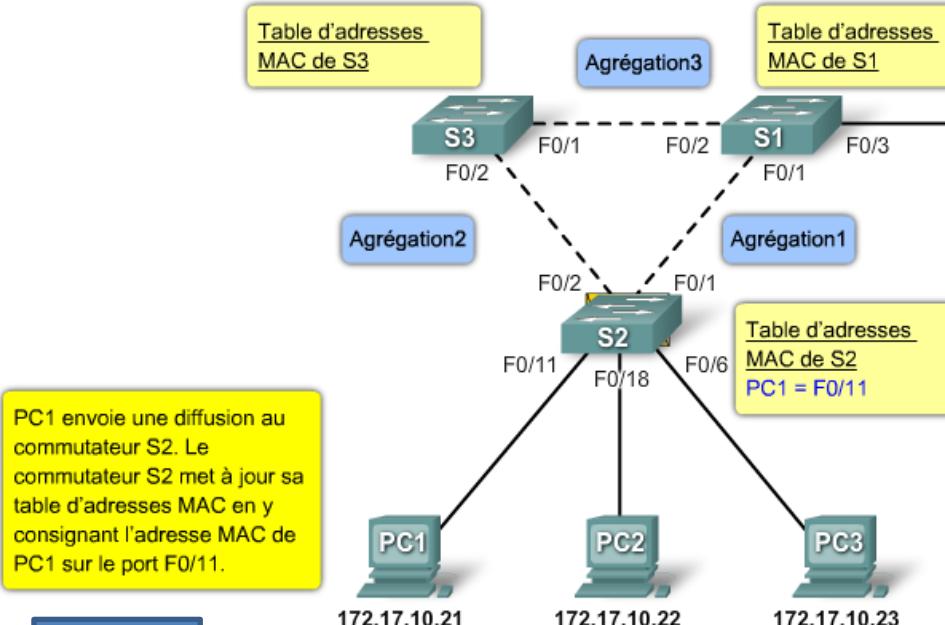
2



Problèmes liés à la redondance

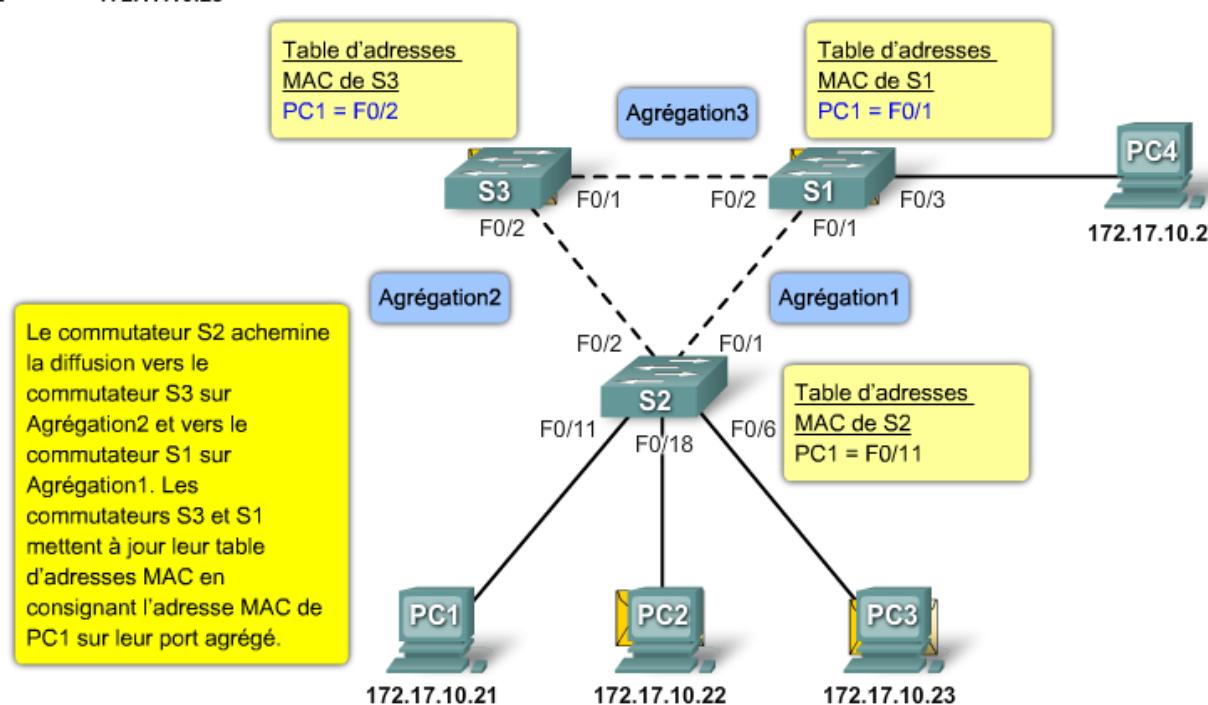
- La redondance est une composante importante de la conception hiérarchique
- Bien que la redondance soit importante pour la disponibilité du réseau, il est essentiel de prendre en compte certains facteurs avant de pouvoir envisager la mise en œuvre d'une architecture redondante dans un réseau
- Lorsqu'il existe plusieurs chemins entre deux périphériques du réseau une boucle de couche 2 peut se former
- Si le protocole STP ([Spanning Tree Protocol](#)) est activé sur ces commutateurs (paramètre par défaut), aucune boucle de couche 2 ne se forme
- STP calcule rapidement les ports devant être bloqués pour éviter la formation de boucles dans un réseau local virtuel

Boucles de couche 2

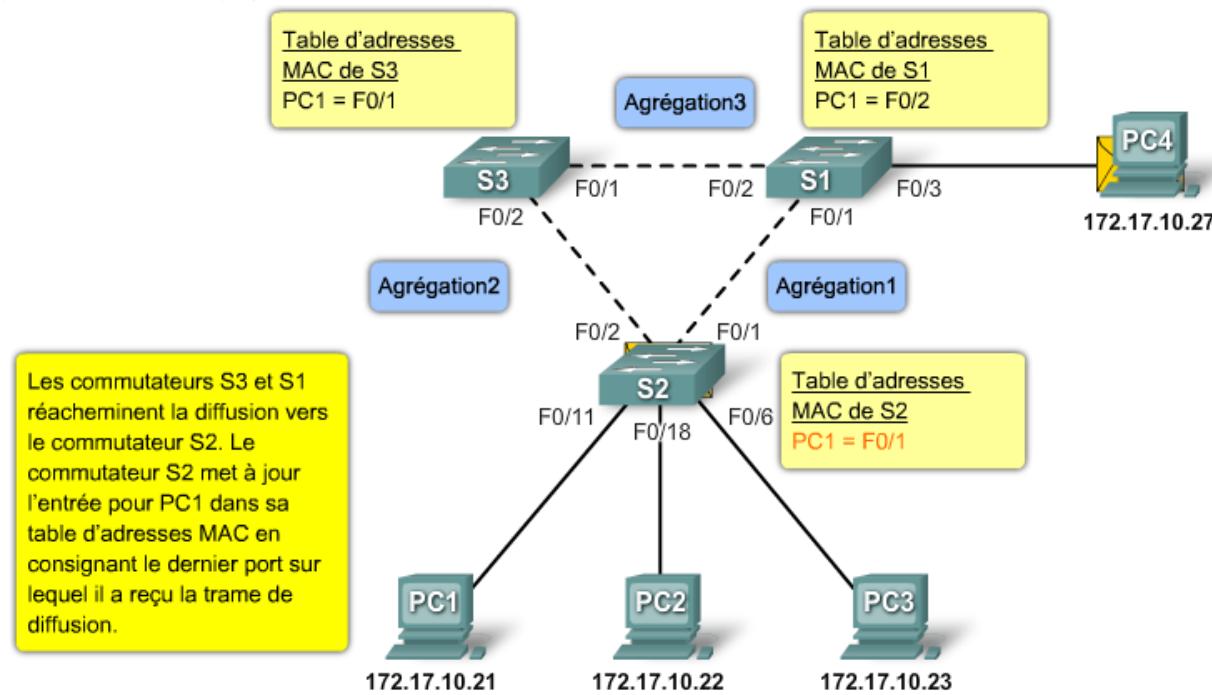
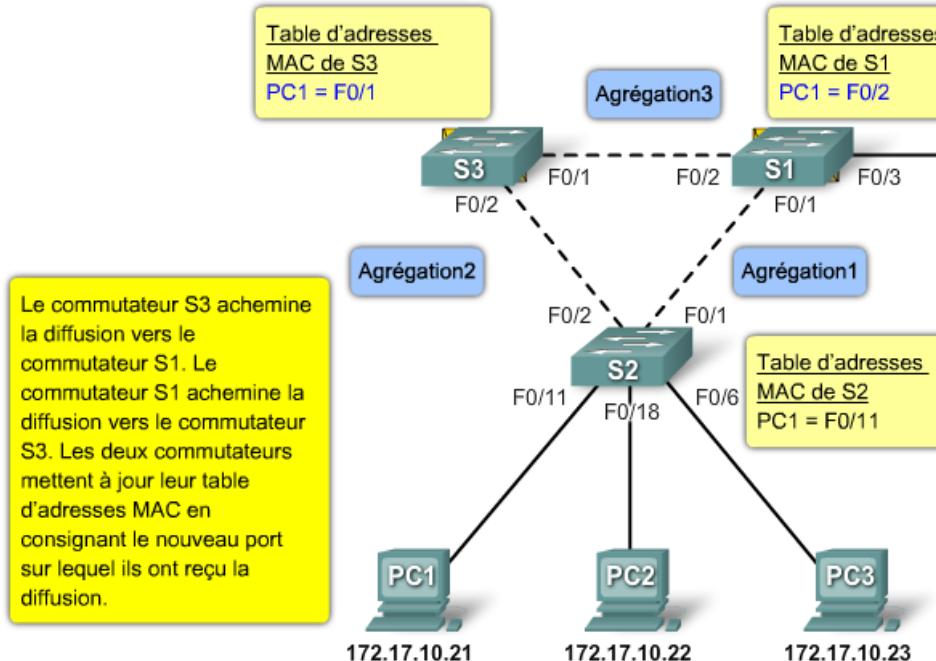


1

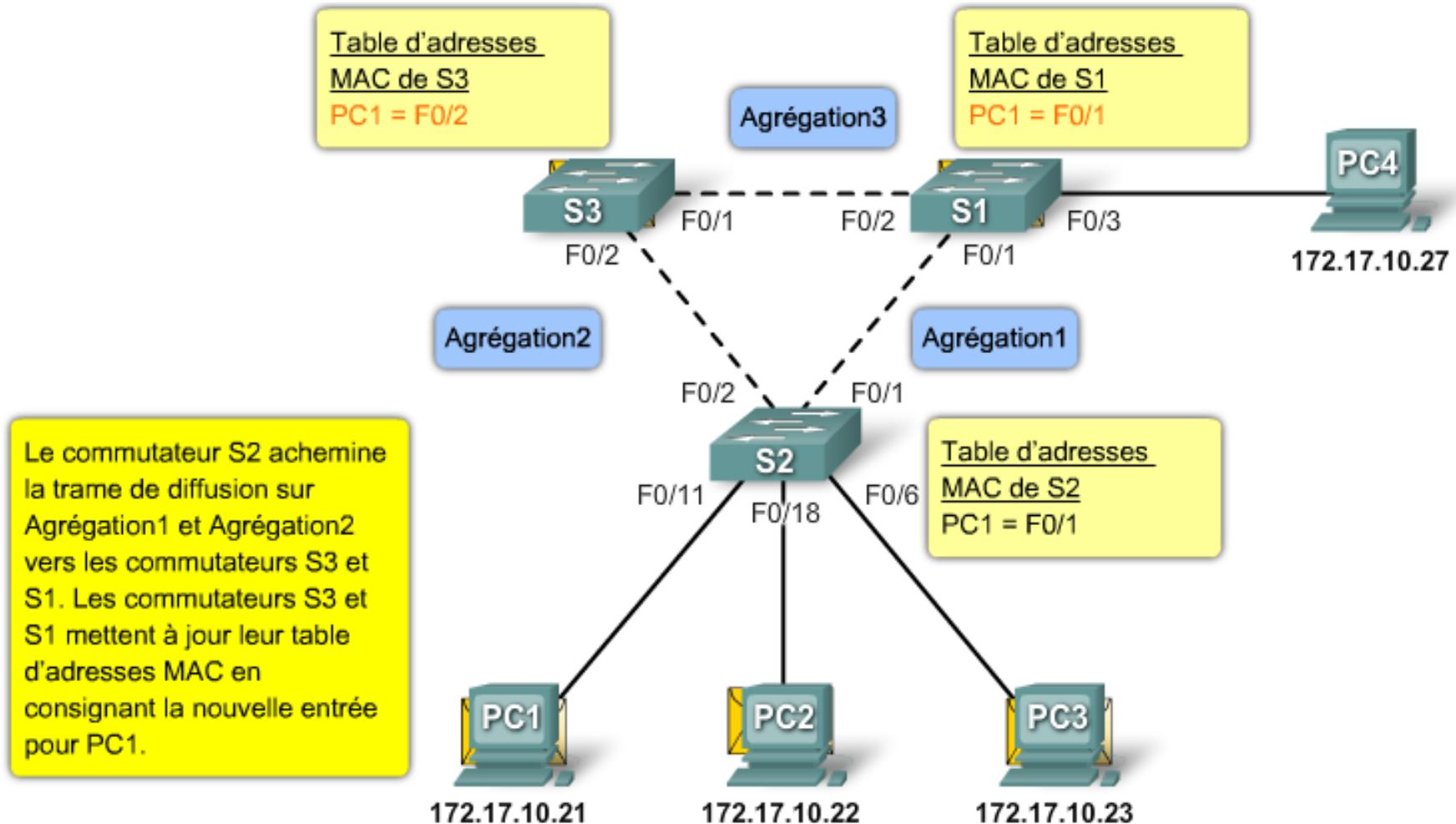
2



Boucles de couche 2



La boucle est bouclée !



Projet à rendre

- 4.4.1.2 Packet Tracer - Skills Integration Challenge - Projet Final.pka