

Scaling VLANs

VTP, DTP, STP, HSRP, EtherChannel

CCNA Routing and Switching

Scaling Networks v6.0



Gestion des VLANs → VTP et DTP

Administration des VLAN ?

- Pour ajouter un VLAN sur un réseau l'administrateur doit l'ajouter sur chaque switch !
 - Nécessite beaucoup de manipulation sur de grands réseaux
- Pour éviter cela, sur des switchs Cisco, la manipulation peut être faite sur un seul switch
 - VLAN Trunking Protocol – diffuse des informations sur les VLANs
 - DTP Dynamic Trunking Protocol – permet la négociation des Trunk

Les modes VTP

Server (default mode)

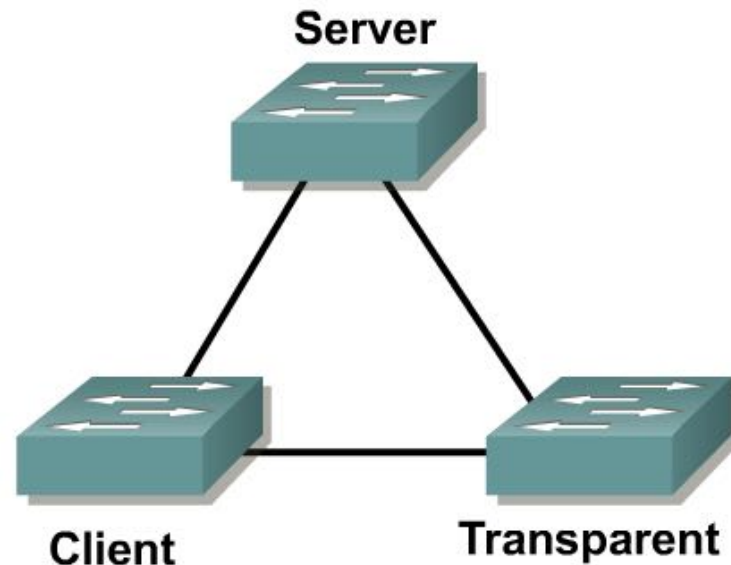
- Creates, modifies, and deletes VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations
- Saves configuration in NVRAM

Client

- Cannot create, change, or delete VLANs
- Forwards advertisements
- Synchronizes VLAN configurations
- Does not save in NVRAM

Transparent

- Creates, modifies, and deletes local VLANs
- Forwards advertisements
- Does not synchronize VLAN configurations
- Saves configuration in NVRAM



Versions

- 3 versions de VTP existent
- Les Switches dans le même domaine VTP doivent utiliser la même version VTP

VTP Version	Definition
VTP Version 1	<ul style="list-style-type: none">▪ Default VTP mode on all switches.▪ Supports normal range VLANs only.
VTP Version 2	<ul style="list-style-type: none">▪ Supports normal range VLANs only.▪ Supports legacy Token Ring networks.▪ Supports advanced features including unrecognized Type-Length-Value (TLV), version-dependent transparent mode, and consistency checks.

Attention : La dernière version 3 de VTP sera étudiée en CCNP

La configuration par défaut

- Par défaut, un switch est en **Mode server**
 - Le *VTP domain name* est "**vide**"
 - Tous les ports sont dans le VLAN 1
 - Le numéro de révision de la configuration VTP est 0
 - La version du protocole VTP est 1
- La commande `show vtp status` permet de visualiser la configuration VTP d'un switch

```
S1# show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11

Feature VLAN:
-----
VTP Operating Mode       : Transparent
Maximum VLANs supported locally : 255
Number of existing VLANs : 12
Configuration Revision    : 0
MD5 digest                : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                          : 0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

S1#
```

Les VTP revision number

- Codé sur 32 bit
- Par défaut, c'est la valeur 0
- A chaque ajout ou suppression d'un VLAN, ce nombre est incrémenté de 1 par le switch VTP server
- Au changement du nom du VTP domain, ce nombre est mis à 0
- Permet de connaître le message VTP le plus récent

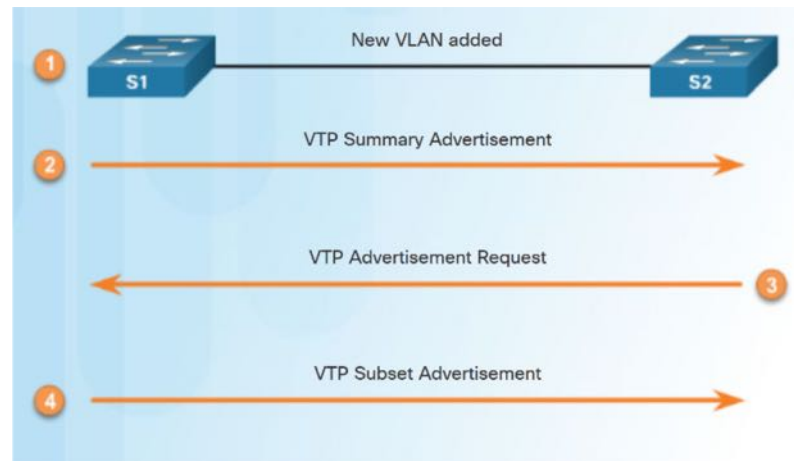
La propagation du domaine

- Les VTP Server propagent leur domaine VTP via des messages **VTP advertisement**
- Ces messages sont utilisés pour transporter
 - les informations sur les domaines VTP
 - les informations sur les modifications des VLAN
- Chaque message VTP est composé d'un VTP header et d'un VTP data field
- Chaque message VTP est inséré dans le champ de données des trames Ethernet qui sont elles-mêmes encapsulées dans une trame 802.1q trunk
- Chaque switch envoie périodiquement des VTP advertisement sur ses liens trunk, par multicast.

VTP Concepts and Operation

VTP Advertisements

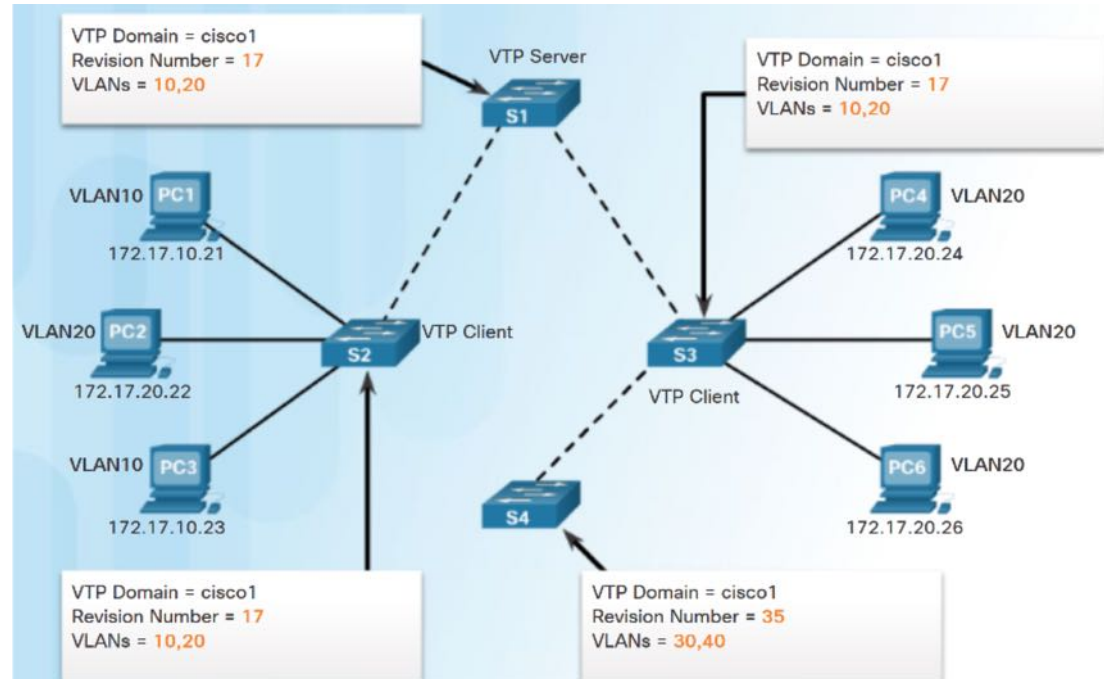
- **Summary advertisements** : échangés tous les 300 secondes (5 min) ou lors d'une mise à jour
 - Dans ce message figurent au moins le domain d'administration, la version VTP, le nom du domaine, le numéro de révision de la configuration, un timestamp et le nombre de « subset advertisements »
- **Subset advertisement** : envoyé à la suite d'un summary advertisement issu d'une modification de la base VLAN
 - Contient les changements effectués
 - Un *subset advertisement* pour chaque VID modifié
- **Advertisement request** depuis les clients : envoyé quand un switch demande des informations pour mettre à jour sa base VLAN



- Quand un switch voit un message summary avec un numéro de révision supérieur à la sienne, il demande la nouvelle configuration
- Le Serveur retourne un summary et un subset advertisements

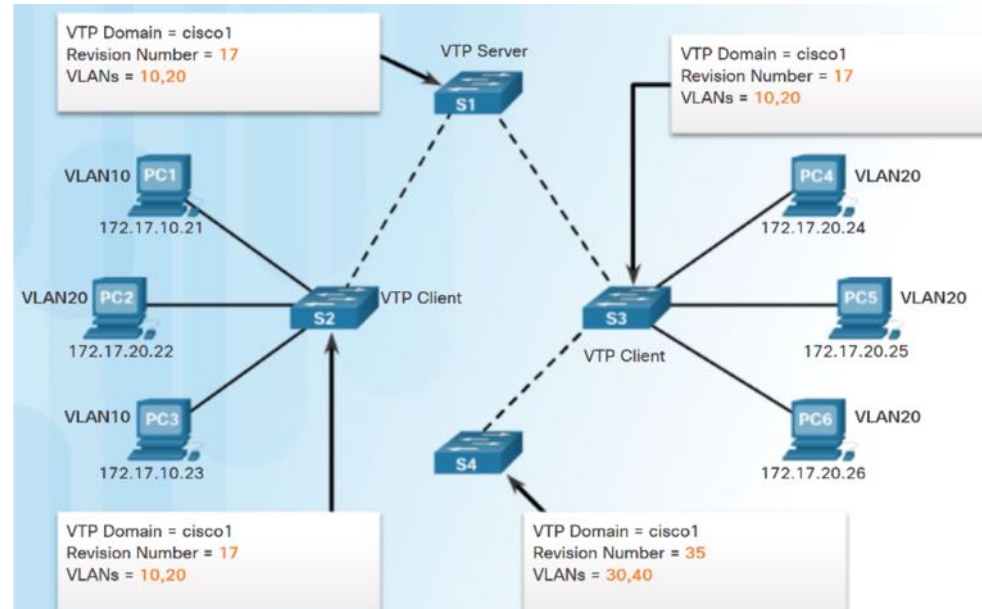
Attention au "piège"

- Le numéro de révision VTP est stocké dans la NVRAM du server.
- Pour le remettre à zéro :
 - Soit on modifie le domaine VTP pour un domaine inexistant et puis on rechange vers l'ancien
 - Soit on change le mode VTP vers transparent, et puis on revient au mode précédent



Attention au "piège"

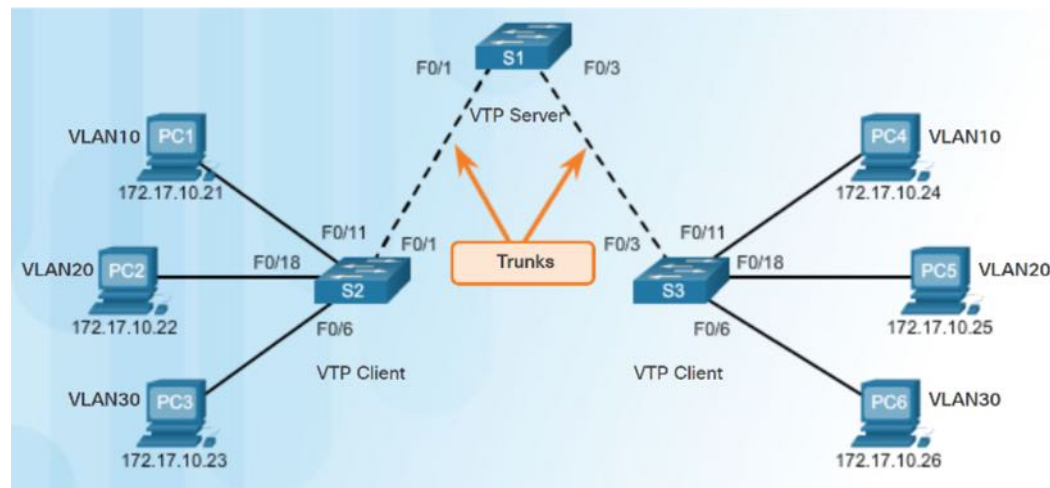
- Sans faire gaffe, on peut avoir la situation suivante :
- S4 est rajouté. Sa configuration n'a pas été effacée et le fichier VLAN.DAT de S4 n'a pas été supprimé. S4 a le même domaine VTP des autres mais son numéro de révision est 35.
- S4 a le VLAN 1 et est configuré avec les VLAN 30 et 40. Toutefois, il n'a pas les VLAN 10 et 20 dans sa base de données. Parce qu'il a le numéro de révision le plus élevé, les autres switches se synchroniseront avec S4.
- Par conséquent, les VLANs 10 et 20 disparaîtront des switches, laissant les clients sans connectivité (ces ports n'auront pas de VLAN assigné)





Configuration de VTP

Étapes de la configuration



- Étapes de la configuration VTP :
 1. Configurer le serveur VTP
 2. Configurer le domaine et le mot de passe VTP
 3. Configurer les clients VTP
 4. Configurer les VLANs dans le serveur VTP
 5. Vérifier que les clients VTP ont reçu les nouvelles informations VLAN

Étape 1 – Configurer le Serveur VTP

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# vtp mode ?
  client      Set the device to client mode.
  off         Set the device to off mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.

S1(config)# vtp mode server
Setting device to VTP Server mode for VLANs.
S1(config)# end
S1#
```

```
S1# show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
Configuration Revision   : 0
MD5 digest               : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                        : 0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

S1#
```

- Utiliser la commande **vtp mode server** pour démarrer un switch en mode serveur
 - Vérifiez que tous les switches ont des paramètres par défaut avant de faire ceci, pour éviter des problèmes liés au numéro de révision
- Utiliser **show vtp status** pour la vérification
 - On voit le numéro de révision encore à 0 et aussi 5 VLANs déjà présents.
 - Ces 5 VLANs sont le VLAN 1 (défaut) et les VLANs 1002-1005

Étape 2 – Configurer le domaine VTP et le mot de passe

- Utiliser la commande **vtp domain** *domain-name* pour configurer le nom de domaine
 - Les clients VTP devront avoir le même nom de domaine
- Configurer un mot de passe avec la commande **vtp password** *password*
 - La commande **show vtp password** permet de le vérifier

```
S1(config)# vtp domain ?
WORD The ascii name for the VTP administrative domain.

S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 02:55:42.768: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG:
VTP domain name changed to CCNA.
S1(config)#
```

```
S1(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S1(config)# end
S1# show vtp password
VTP Password: cisco12345
S1#
```

Étape 3 – Configurer les clients VTP

```
S2(config)# vtp mode client
Setting device to VTP Client mode for VLANs.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 00:12:22.484: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S2(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S2(config)#
```

- La commande **vtp mode client** permet de configurer les clients
- Utiliser le même nom de domaine et mot de passe du serveur

Étape 4 – Rajouter les VLANs au serveur VTP

- Créer les VLANs avec la commande **vlan** *vlan-number* command
- **show vlan brief** pour la vérification
- **show vtp status** pour voir leur status
 - Chaque nouveau VLAN crée augmente le numéro de révision

```
S1(config)# vlan 10
S1(config-vlan)# name SALES
S1(config-vlan)# vlan 20
S1(config-vlan)# name MARKETING
S1(config-vlan)# vlan 30
S1(config-vlan)# name ACCOUNTING
S1(config-vlan)# end
S1#
```

```
S1# show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    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, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gi0/1, Gi0/2

10   SALES                  active
20   MARKETING              active
30   ACCOUNTING             active
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
S1#
```

```
S1# show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          : CCNA
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 02:02:45
Local updater ID is 0.0.0.0 (no valid interface found)
```

```
Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 255
Number of existing VLANs  : 8
Configuration Revision    : 6
MD5 digest                : 0xFE 0x8D 0x2D 0x21 0x3A 0x30 0x99 0xC8
                           0xDB 0x29 0xBD 0xB9 0x48 0x70 0xD6 0xB6
S1#
```

Étape 5 – Vérifier que les clients ont reçu la nouvelle configuration VTP

- La commande **show vlan brief** permet de vérifier la configuration des VLANs des clients
- La commande **show vtp status** montre l'état VTP

```
S2# show vtp status
VTP Version capable      : 1 to 3
VTP Version running      : 1
VTP Domain Name          : CCNA
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : b07d.4729.2400
Configuration last modified by 0.0.0.0 at 3-1-93 02:02:45
```

Feature VLAN:

```
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs  : 8
Configuration Revision    : 6
MD5 digest               : 0xFE 0x8D 0x2D 0x21 0x3A 0x30 0x99 0xC8
                          : 0xDB 0x29 0xBD 0xE9 0x48 0x70 0xD6 0xB6
S2#
```

```
S2# show vlan brief
```

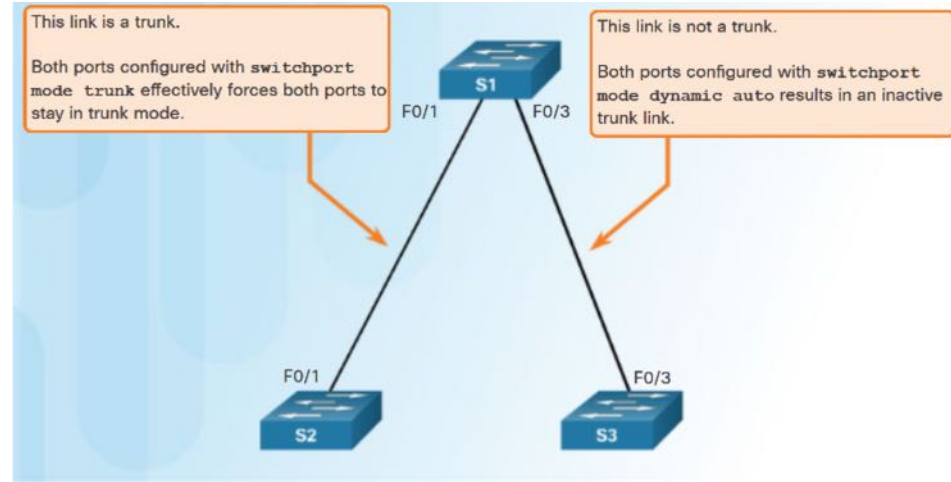
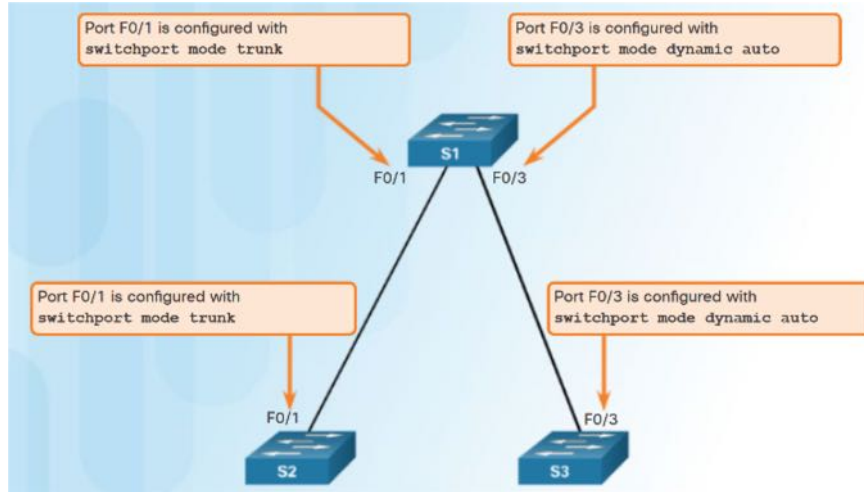
VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	SALES	active	
20	MARKETING	active	
30	ACCOUNTING	active	
1002	fddi-default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

```
S2#
```



Et les Trunk??? DTP

Introduction à DTP



- La négociation des Trunk est gérée par le Dynamic Trunking Protocol (DTP)
 - Protocole propriétaire CISCO
- Pour activer le trunking avec un routeur qui ne supporte pas DTP, il faut utiliser les commandes **switchport mode trunk** et **switchport nonegotiate**

Modes de négociation

- Les différents modes Trunking:
 - **Switchport mode access** – l'interface n'est pas en mode trunk
 - **Switchport mode dynamic auto** – l'interface devient trunk si l'interface voisine est en mode *trunk* or *desirable*
 - **Switchport mode dynamic desirable** – l'interface devient trunk si le voisin est en mode *trunk*, *desirable* ou *dynamic auto*
 - **Switchport mode trunk** – l'interface deviant trunk même si le voisin n'est pas en mode trunk
 - **Switchport nonegotiate** – empêche l'interface d'envoyer des trames DTP

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                TRUNK/ON/TRUNK
  TOT/TAT/TNT:                802.1Q/802.1Q/802.1Q
  Neighbor address 1:         0CD996D23F81
  Neighbor address 2:         000000000000
  Hello timer expiration (sec/state): 12/RUNNING
  Access timer expiration (sec/state): never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state): never/STOPPED
  FSM state:                  S6:TRUNK
  # times multi & trunk       0
  Enabled:                    sim
  In STP:                     no
```

<output omitted>

- Pour plus de sécurité, il faut privilégier la configuration statique du mode
- Utiliser **show dtp interface** pour vérifier DTP

Gérer une hiérarchie de Switches Spanning Tree

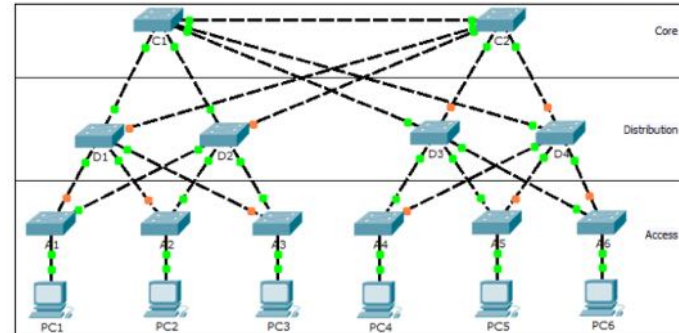
Redondance à la couche 1 et 2 OSI

La redondance a pour but d'offrir des chemins multiples entre les commutateurs :

- Une meilleure redondance physique dans un réseau commuté
- Améliore la fiabilité et la disponibilité du réseau
- Permet à des utilisateurs d'accéder à des ressources du réseau en dépit d'une rupture de chemin
- ATTENTION :

Considérations sur l'implémentation de la redondance :

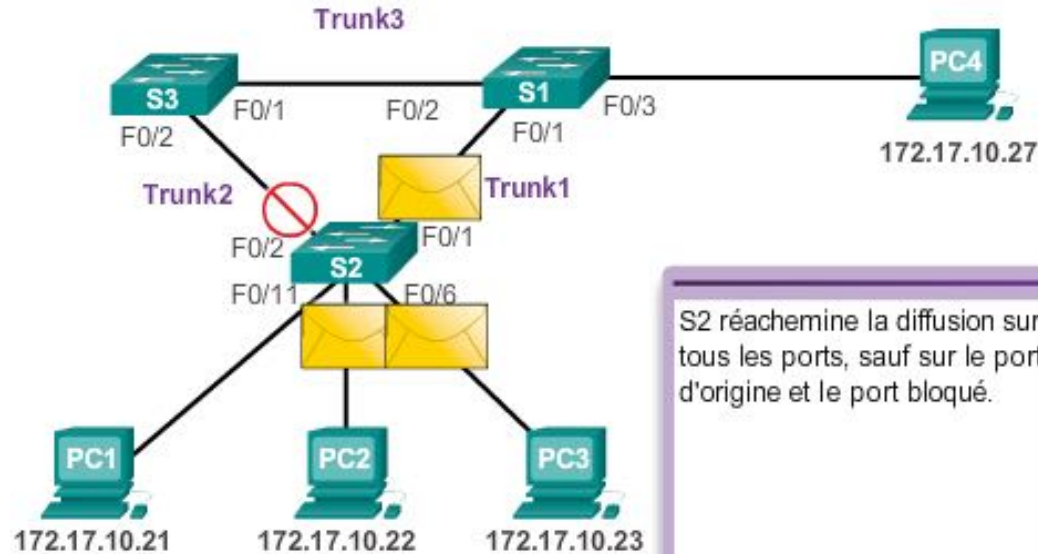
- **Instabilité de la base de données MAC** : en raison de l'instabilité du contenu de la table d'adresses MAC, des copies de la même trame sont reçues sur différents ports du commutateur. La consommation de ressources par le commutateur lorsqu'il doit faire face à l'instabilité de la table d'adresses MAC peut gêner la transmission de données.
- **Tempêtes de diffusion** : en l'absence de processus d'évitement de boucle, chaque commutateur peut inonder infiniment les ports avec les diffusions. Cette situation est connue sous le nom de tempête de diffusion.
- **Transmissions de trames multiples** : des copies multiples de trames de monodiffusion peuvent être fournies aux stations de destination. De nombreux protocoles n'attendent qu'un seul exemplaire de chaque transmission. La réception de plusieurs exemplaires de la même trame risque d'entraîner une erreur irréversible.



Algorithme Spanning Tree : Introduction

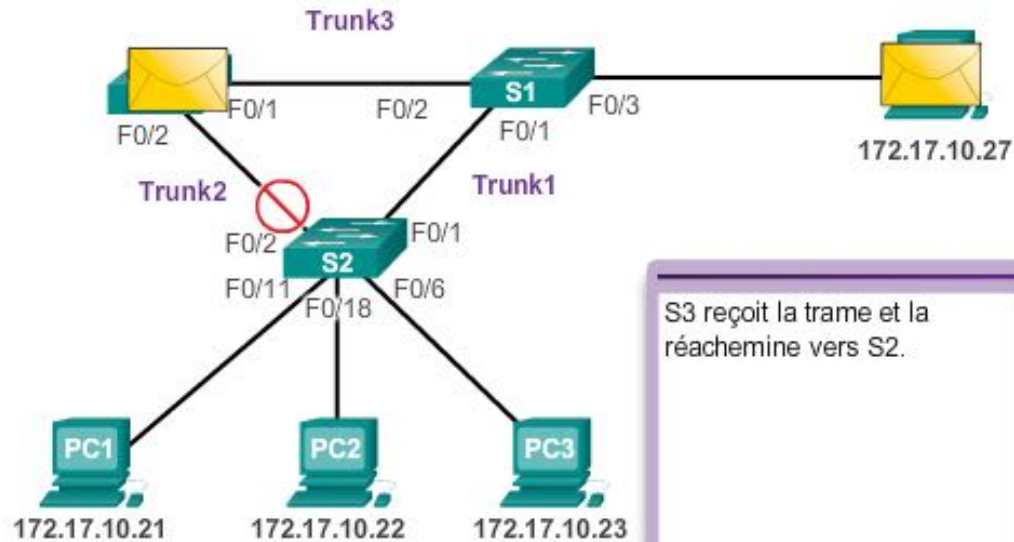
- STP s'assure qu'il y a un seul chemin logique (arbre couvrant)
 - Blocage des chemins superflus qui pourraient causer une boucle
- Un port est considéré bloqué quand des données d'utilisateur sont empêchées d'entrer ou sortir par ce port
 - Ceci n'inclut pas les trames spéciales du protocole de pont (BPDU), qui sont employées par STP pour empêcher des boucles
- Les chemins physiques existent toujours pour fournir la redondance mais ces chemins sont désactivés pour empêcher les boucles
- Si un chemin redondant devient nécessaire pour compenser un câble réseau ou un commutateur réseau en panne, STP recalcule les chemins et dégage les ports nécessaires pour permettre au chemin redondant de devenir actif

Algorithme Spanning Tree : Introduction



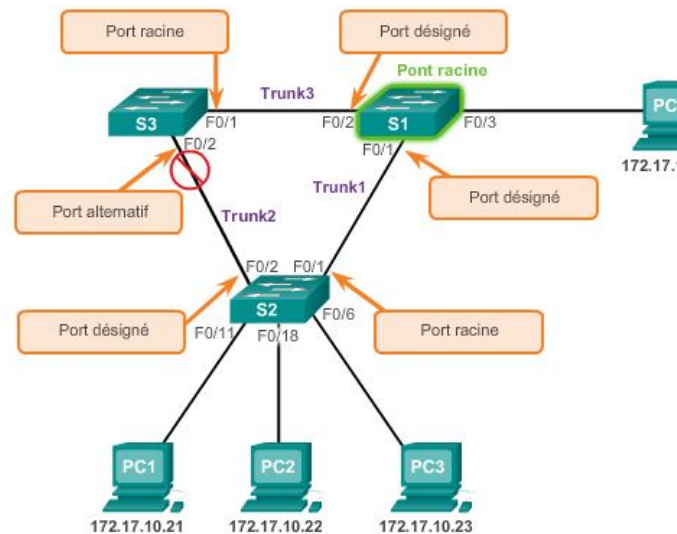
S2 réachemine la diffusion sur tous les ports, sauf sur le port d'origine et le port bloqué.

Algorithme Spanning Tree : Introduction



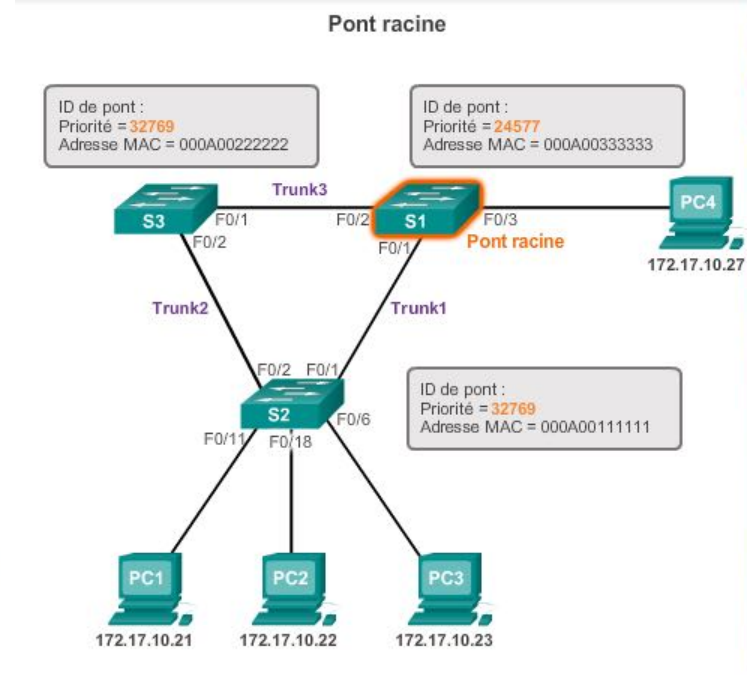
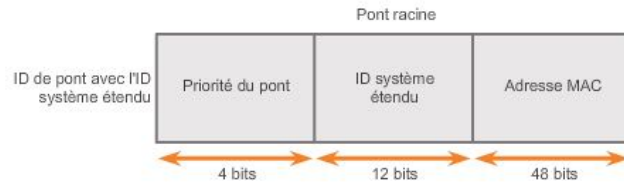
Algorithme Spanning Tree : Fonctionnement

- STP utilise un commutateur racine comme référence (le **Root Bridge**) et calcule l'arbre couvrant à partir de ce switch
- Selon le calcul, les ports peuvent avoir différents rôles
 - **Root port** : le port "le plus proche" en direction du root bridge
 - **Designate port** : tout autre port autorisé à retransmettre des trames sur le réseau ; tous les ports d'un root bridge sont des *designate port*
 - **Alternate port** : des ports en état "bloqué" mais qui peuvent être débloqués en cas de recalcul de l'arbre STP
 - **Disabled port** : un port désactivé (shutdown)
- Le calcul de l'arbre couvrant se fait grâce à l'échange de paquets BDPU

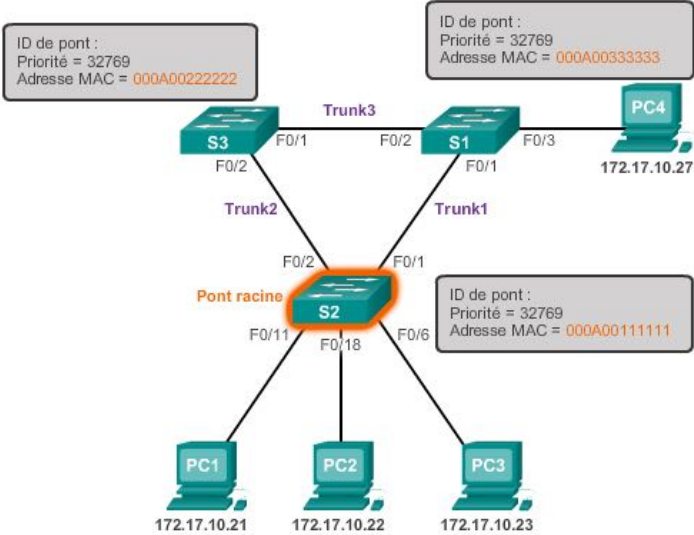
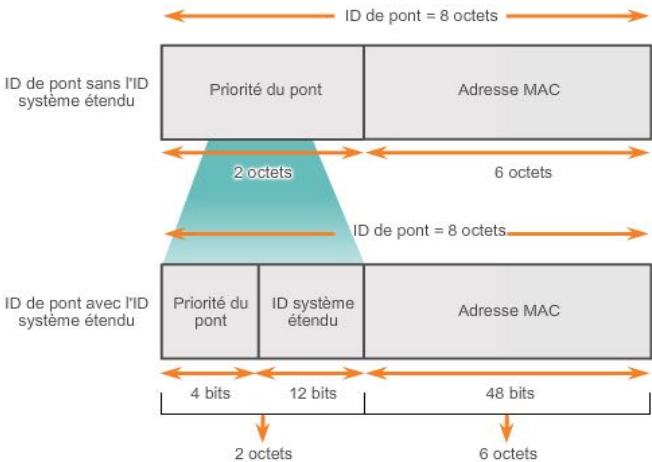


Algorithme Spanning Tree : élection du Root Bridge

- Le Root Bridge est choisi par une élection basée sur le Bridge ID
 - La plus petite valeur est considérée comme le Root Bridge



Bridge ID des systèmes étendus (avec VLANs)



Dans l'exemple, la priorité de tous les commutateurs est de 32769. La valeur est basée sur la priorité par défaut (32768) et l'identifiant du VLAN 1 liée à chaque commutateur (32768+1).

Algorithme Spanning Tree : le Path Cost

- L'algorithme essaye ensuite de déterminer le coût de chaque chemin vers une destination (port) sur le réseau en faisant la somme des coûts des liens
 - Les valeurs peuvent être reconfigurées

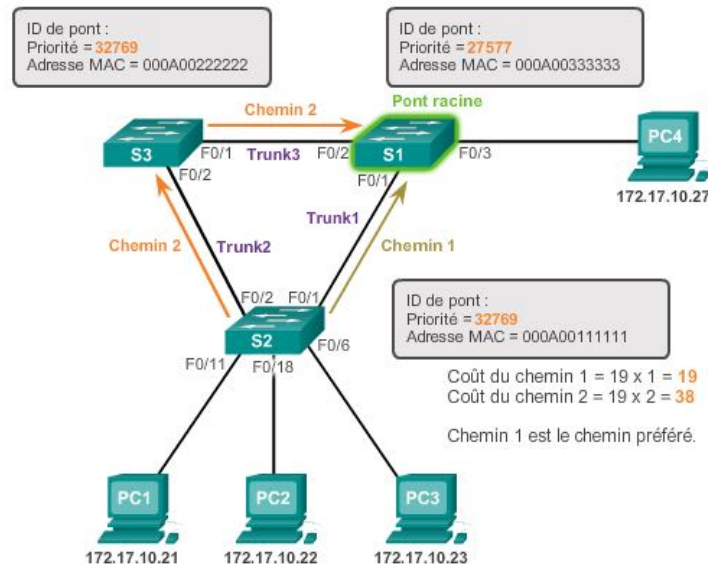
Vitesse de liaison	Coût (spécification IEEE révisée)	Coût (spécification IEEE précédente)
10Gbit/s	2	1
1Gbit/s	4	1
100Mbit/s	19	10
10 Mbit/s	100	100

S2# show spanning-tree

```
VLAN001
Spanning tree enabled protocol ieee
Root ID    Priority 27577
Address    000A.0033.3333
Cost       19
Port       1
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

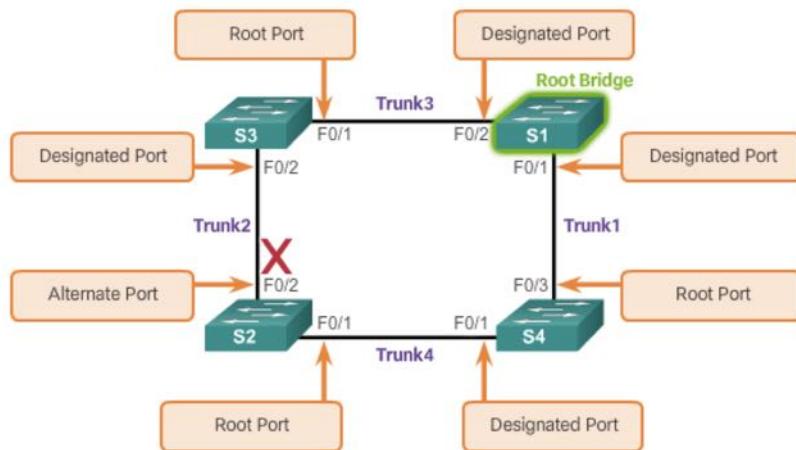
Bridge ID  Priority 32769 (priority 32768 sys-id-ext 1)
Address    000A.0011.1111
Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
F0/1	Root	FWD	19	128.1	Edge P2p
F0/2	Desg	FWD	19	128.2	Edge P2p



Algorithme Spanning Tree : attribution des rôles

- En partant du **Root Bridge**, les différents ports sont attribués selon leur distance.
 - **Root port** : les ports faisant "face" au root bridge par le chemin moins court
 - **Designated port** : les ports pouvant transmettre des trames
 - **Alternate port** : les ports bloquant les trames





Les différents protocoles Spanning Tree

Liste des Protocoles Spanning Tree

- STP or IEEE 802.1D-1998 - Version originale du protocole
 - CST (Common Spanning Tree) considère un seul arbre pour tous les VLANs
- PVST+
 - version STP améliorée par Cisco
- IEEE 802.1D-2004 – version améliorée, inclut notamment RSTP
 - Rapid Spanning Tree Protocol (RSTP) ou IEEE 802.1w
 - RSTP permet une convergence plus rapide
- Rapid PVST+
 - Amélioration de PVST+ Cisco en incorporant RSTP
- Multiple Spanning Tree Protocol (MSTP) or IEEE 802.1s
 - Permet la création d'un arbre commun à plusieurs VLANs

Caractéristiques des protocoles Spanning Tree

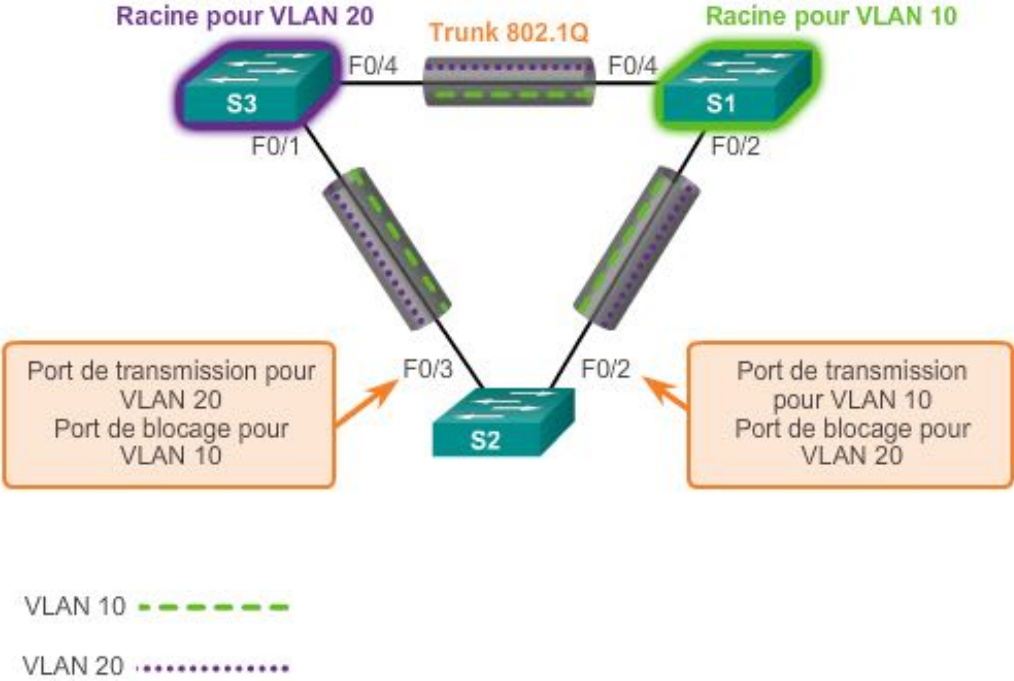
Protocole	Norme	Ressources nécessaires	Convergence	Calcul d'arborescence
STP	802.1D	Faible	Lente	Tous les VLAN
PVST+	Cisco	Élevée	Lente	Par VLAN
RSTP	802.1w	Moyenne	Rapide	Tous les VLAN
Rapid PVST+	Cisco	Très élevée	Rapide	Par VLAN
MSTP	802.1s, Cisco	Moyenne ou élevée	Rapide	Par instance

- Par défaut les commutateurs Catalyst Cisco utilisent PVST+

Aperçu du PVST+

- PVST+ se distingue de IEEE 802.1D STP par la possibilité d'exécuter des instances indépendantes de IEEE 802.1D STP pour chaque VLAN dans le réseau
 - Ceci peut être utilisé pour faire un équilibrage de charge en couche 2
- L'inconvénient est une plus grande utilisation de ressources
 - Un spanning-tree par VLAN exige plus de CPU
 - Le trafic des BPDU est aussi multiplié par le nombre de VLANs
- Ces effets sont problématiques uniquement si le nombre de VLANs est important

Aperçu de PVST+



États des ports et opération de PVST+

STP considère 5 états pour les ports :

Opération autorisée	État du port				
	Blocage	Écoute	Apprentissage	Transfert	Désactivé
Peut recevoir et traiter des trames BPDU	OUI	OUI	OUI	OUI	Non
Peut réacheminer des trames de données reçues sur l'interface	Non	Non	Non	OUI	Non
Peut réacheminer des trames de données commutées provenant d'une autre interface	Non	Non	Non	OUI	Non
Peut apprendre des adresses MAC	Non	Non	OUI	OUI	Non



Configuration du Spanning Tree

Configuration et vérification du Root Bridge

Méthode 1

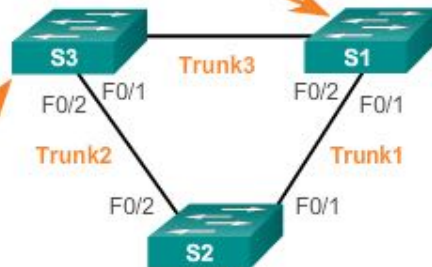
```
s1(config)# spanning-tree VLAN 1 root primary  
s1(config)# end
```

Méthode 2

```
s3(config)# spanning-tree VLAN 1 priority 24576  
s3(config)# end
```

Méthode 1

```
s2(config)# spanning-tree VLAN 1 root secondary  
s2(config)# end
```



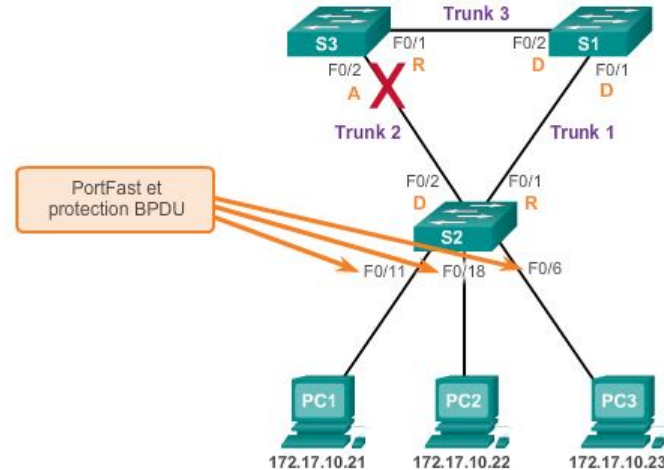
Configuration et vérification du ID de pont

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     00A.0033.3333
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID  Priority    24577 (priority 24576 sys-id-ext 1)
             Address     00A.0033.3333
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300

Interface    Role    Sts    Cost    Prio.Nbr    Type
-----
Fa0/1        Desg    FWD    4        128.1       p2p
Fa0/2        Desg    FWD    4        128.2       p2p
S3#
```


PortFast et protection BPDU

- PortFast est utilisé pour les ports attachés à des équipements terminaux
 - Passe rapidement en mode "blocage"
- La protection BPDU désactive le port si un BPDU est reçu (**boucle sur le switch**)



```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface when portfast is enabled,
can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

```
S2# show running-config interface f0/11
Building configuration...

Current configuration : 90 bytes
!
interface FastEthernet0/11
 spanning-tree portfast
 spanning-tree bpduguard enable
end

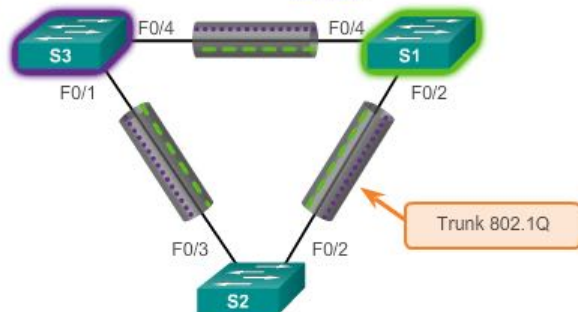
S2#
```

PVST+ Configuration

Équilibrage de charge PVST+

Pont racine principal pour VLAN 20
Pont racine secondaire pour
VLAN 10

Pont racine principal pour VLAN 10
Pont racine secondaire pour
VLAN 20



VLAN 10 - - - - -

VLAN 20

```
S1# show running-config
...
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
```

Configuration de PVST+

```
S3(config)# spanning-tree vlan 20 root primary
```

Cette commande force S3 à devenir racine principale pour VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

Cette commande force S3 à devenir racine secondaire pour VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

Cette commande force S1 à devenir racine principale pour VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

Cette commande force S1 à devenir racine secondaire pour VLAN 20.

Équilibrage de charge PVST+

- Une autre méthode pour spécifier le pont racine est de placer une priorité spanning-tree sur chaque commutateur avec la valeur la plus basse, de sorte que le commutateur soit sélectionné comme pont primaire pour son VLAN associé

```
S3(config)# spanning-tree vlan 20 priority 4096
```

Cette commande définit la priorité de S3 la plus basse possible ; il est donc très probable que S3 sera la racine principale pour VLAN 20.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

Cette commande définit la priorité de S1 la plus basse possible ; il est donc très probable que S1 sera la racine principale pour VLAN 10.

Équilibrage de charge PVST+

- Afficher et vérifier les détails de configuration spanning tree

```
S1# show spanning-tree active
<résultat omis>
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address    0019.aa9e.b000
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
             Address    0019.aa9e.b000
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300

Interface    Role    Sts    Cost    Prio.Nbr    Type
-----
Fa0/2        Desg    FWD    19       128.2       p2p
Fa0/4        Desg    FWD    19       128.4       p2p
<résultat omis>
```

Équilibrage de charge PVST+

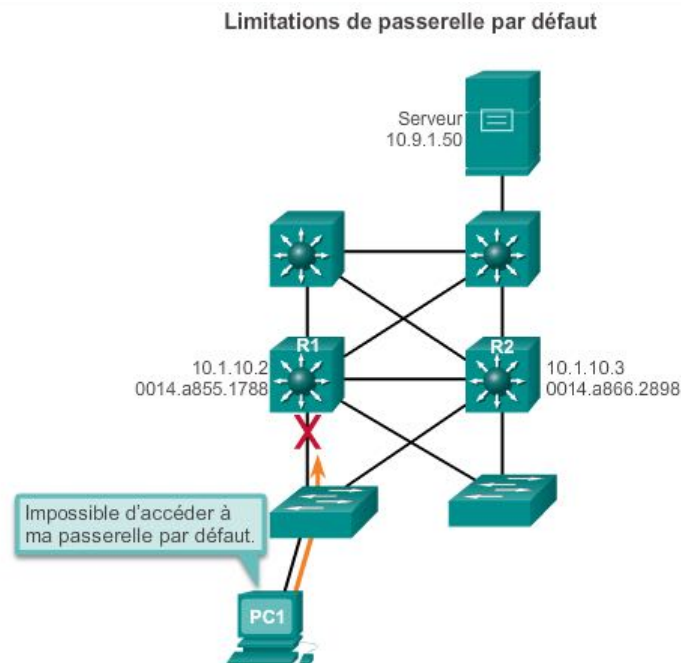
```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
<output omitted>
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
<output omitted>
```

Protocoles de redondance au premier saut

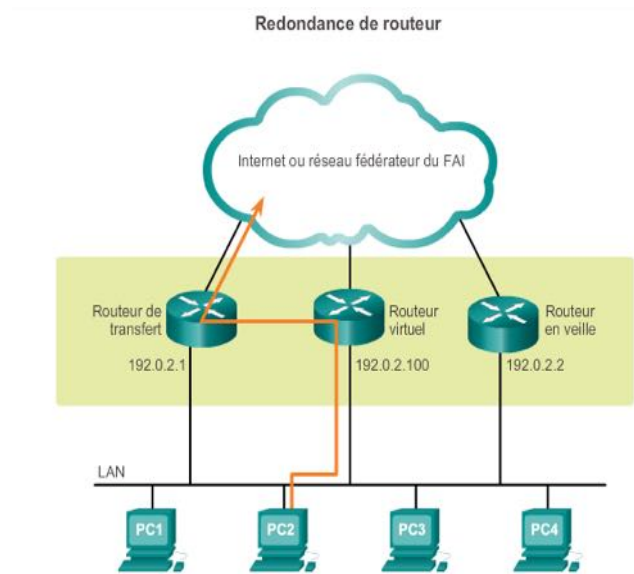
Limitations de la passerelle par défaut

- Si la passerelle par défaut ne peut pas être atteint, le dispositif local ne peut pas envoyer des paquets en dehors du segment
- Même si un routeur redondant existe et pourrait servir de passerelle par à ce segment, il n'y a aucune méthode dynamique pour mettre à jour l'adresse de la passerelle par défaut sur les dispositifs



Redondance grâce à un routeur virtuel

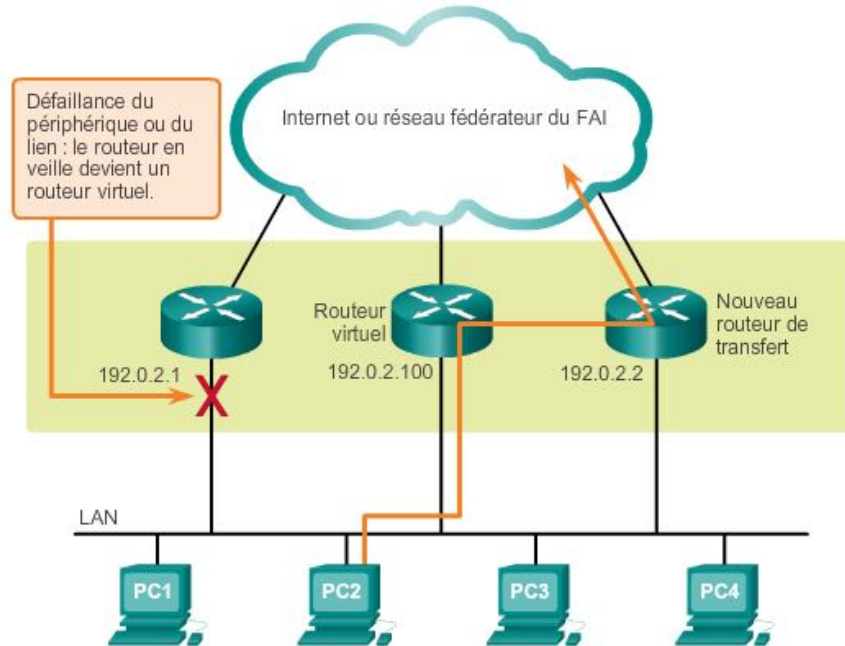
- Plusieurs routeurs peuvent être configurés pour un fonctionnement conjoint, donnant l'illusion d'un routeur unique aux hôtes du LAN
 - Ils partagent les mêmes adresses IP et MAC virtuelles
 - Un protocole spécifique sert à coordonner les routeurs
 - Le protocole ARP fait la résolution de l'adresse IP associée à la passerelle par défaut
- La capacité d'un réseau à effectuer une reprise dynamique après la défaillance d'un périphérique jouant le rôle de passerelle par défaut est appelée **redondance au premier saut**



Concept de protocoles de redondance au premier saut

Basculement du routeur par défaut

Étapes relatives au basculement du routeur



Protocoles de redondance de premier saut

- **Hot Standby Router Protocol (HSRP)**

- Protocole propriétaire Cisco, utilisé pour déterminer le routeur actif et les routeurs en attente (standby)

- HSRP pour IPv6 – mêmes fonctionnalités que HSRP

- Virtual Router Redundancy Protocol version 2 (VRRPv2)

- Protocole d'élection non propriétaire. Permet l'utilisation d'une même adresse virtuelle IPv4 dans un réseau multiaccès

- VRRPv3 – support à IPv4 et IPv6, plus scalable que la version 2

- Gateway Load Balancing Protocol (GLBP)

- Protocole propriétaire Cisco qui offre de l'équilibrage de charge en plus de la redondance de premier saut

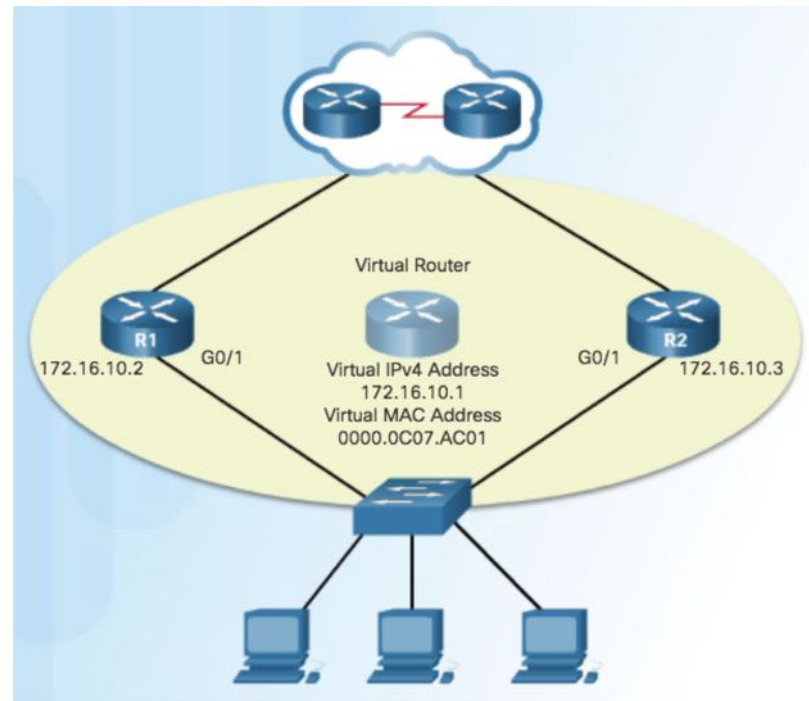
- GLBP pour IPv6

- ICMP Router Discovery Protocol (IRDP)

- Protocole ancien (legacy) défini en RFC 1256, permet la découverte de routeurs pour les réseaux distants

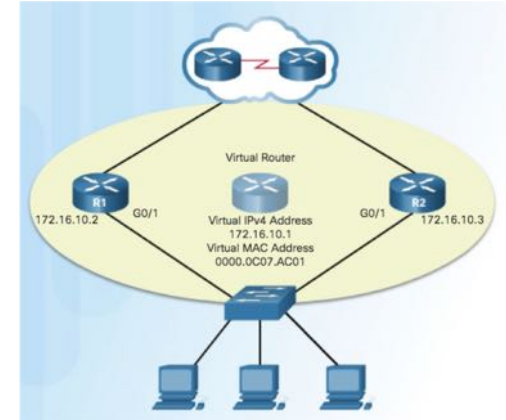
Un groupe HSRP

- L'un des routeurs est choisi pour être le routeur actif HSRP et la passerelle par défaut
- Les autres routeurs restent en attente
- Si le router actif tombe en panne, le routeur de secours assume le rôle
- Les PCs sont configurés avec une passerelle par défaut unique, avec l'IP de la passerelle virtuelle reconnue par le routeur actif et les routeurs de secours



Priorités et Prémemption

- Les rôles sont définis par une élection
- Par défaut, le routeur avec la plus grande adresse IPv4 devient le routeur actif
- Des priorités peuvent être accordées pour contrôler l'élection
- Priorité HSRP
 - La priorité par défaut HSRP est 100.
 - Plage entre 0 et 255 -> la plus grande priorité gagne
 - La commande **standby priority interface** permet de modifier la priorité
- HSRP Prémemption
 - Prémemption – possibilité de forcer une nouvelle élection
 - Pour avoir une nouvelle élection, la prémemption doit être activée avec **standby preempt interface**
 - Un routeur qui rejoint le groupe avec une priorité ou adresse plus grande devient le routeur actif

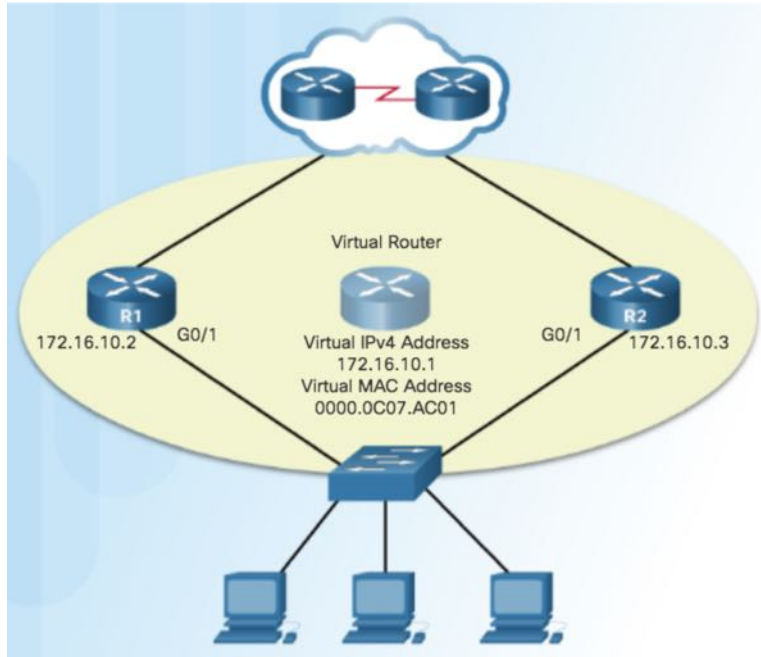


Configuration

1. Configurer HSRP version 2 sur l'interface "en face" aux PCs
2. Configurer l'adresse virtuelle du groupe (l'adresse visible par les PCs)
3. Configurer la priorité pour le routeur actif désiré (priorité supérieure à 100)
4. Configurer la préemption

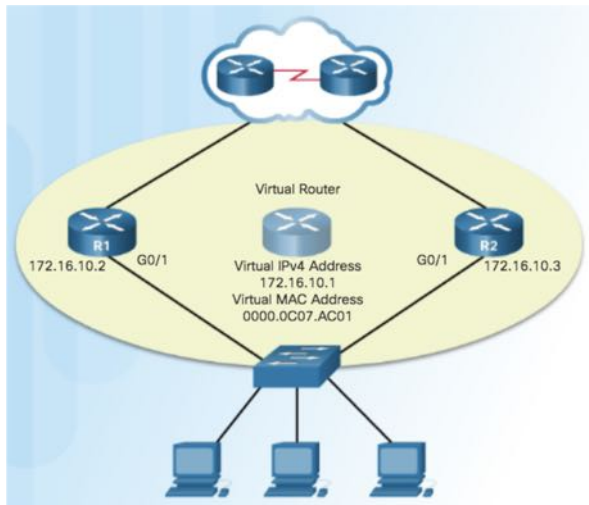
Command	Definition
Router(config-if) # standby version 2	Configures HSRP to use version 2. HSRP version 1 is the default.
Router(config-if) # standby [group-number] ip-address	Configures the HSRP virtual IP address that will be used by the specified group. If no group is configured, then the virtual IP address is assigned to group 0.
Router(config-if) # standby [group-number] priority [priority-value]	Configures the desired active router with a higher priority than default priority of 100. Range is 0 to 255. If no priority is configured or if priority is equal, then the router with the highest IP address has priority.
Router(config-if) # standby [group-number] preempt	Configures a router to preempt the currently active router.

Example de Configuration



```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

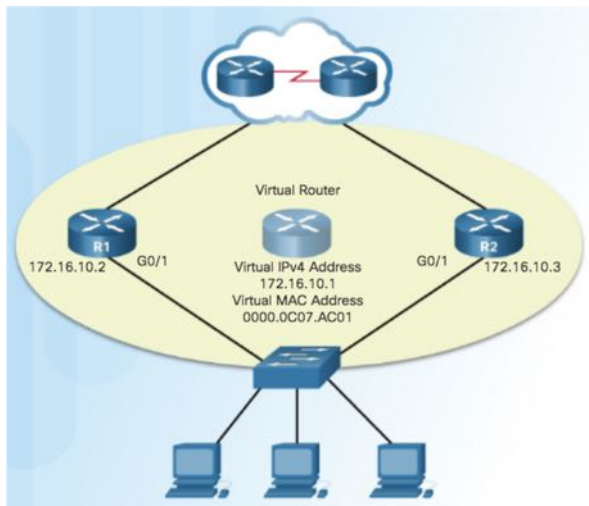
Vérification



```
R1# show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Active
    5 state changes, last state change 01:02:18
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.120 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.10.3, priority 100 (expires in 9.392 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
R1#
```

```
R2# show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Standby
    5 state changes, last state change 01:03:59
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.944 secs
  Preemption disabled
  Active router is 172.16.10.2, priority 150 (expires in 8.160 sec)
  MAC address is fc99.4775.c3e1
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi0/1-1" (default)
R2#
```

Vérification (Cont.)



```
R1# show standby brief
```

P indicates configured to preempt.

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Gi0/1	1	150	P	Active	local	172.16.10.3	172.16.10.1

```
R1#
```

```
R2# show standby brief
```

P indicates configured to preempt.

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Gi0/1	1	100		Standby	172.16.10.2	local	172.16.10.1

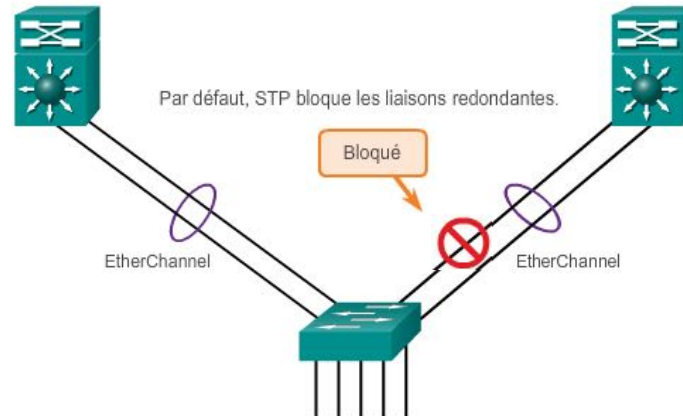
```
R2#
```


Agrégation de Liens

Introduction à l'agrégation de liaisons

- L'agrégation de liens permet la création des liens logiques composés de plusieurs liens physiques
- EtherChannel est une forme d'agrégation de liens utilisée dans les réseaux commutés

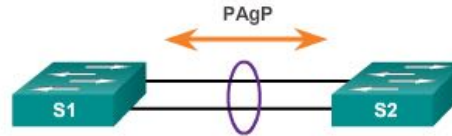
Avantages de l'EtherChannel



Protocol Aggregation Port (PAgP) CISCO

Modes PAgP :

- **Activé** : membre de canal sans négociation (pas de protocole).
- **Desirable (Souhaitable)** : demande activement si l'autre côté peut participer ou participera.
- **Auto** : attend passivement l'autre côté.



S1	S2	Établissement de canal
Activé	Activé	Oui
Auto/Desirable (Souhaitable)	Souhaitable	Oui
On (Activé)/Auto/Desirable (Souhaitable)	Non configuré	Non
Activé	Souhaitable	Non
Auto/On (Activé)	Auto	Non

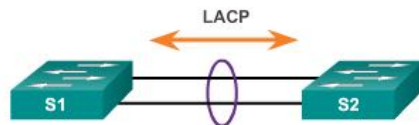
PAgP permet de créer la liaison EtherChannel en détectant la configuration de chaque côté et en assurant la compatibilité des liaisons, afin que la liaison EtherChannel puisse être activée si besoin

Protocol Liens Aggregation Port (LACP)

Protocole LACP

Modes LACP :

- **Activé** : membre de canal sans négociation (pas de protocole).
- **Active (Actif)** : demande activement si l'autre côté peut participer ou participera.
- **Passive (Passif)** : attend passivement l'autre côté.

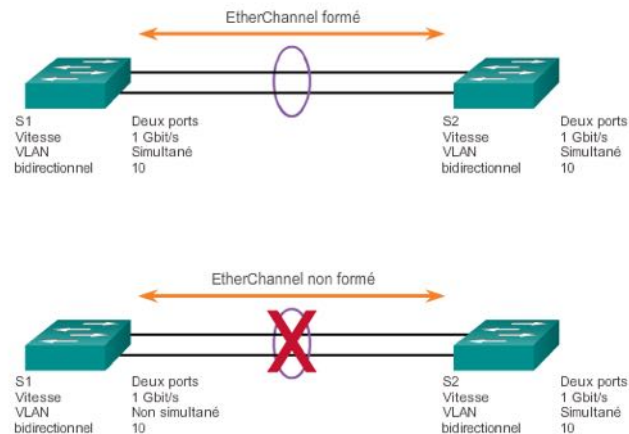


S1	S2	Établissement de canal
Activé	Activé	Oui
Active (Actif)/Passive (Passif)	Active	Oui
On (Activé)/Active (Actif)/Passive (Passif)	Non configuré	Non
Activé	Active	Non
Passive (Passif)/On (Activé)	Passif	Non

LACP offre les mêmes avantages en matière de négociation que PAgP. LACP permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin

Directives de configuration

- Prise en charge d'EtherChannel sur tous les modules/interfaces des switches
- Les paramètres de vitesse et mode duplex doivent être compatible sur tous les interfaces
- VLAN – Toutes les interfaces sont sur le même VLAN
- Plage de VLAN – Même plage sur toutes les interfaces



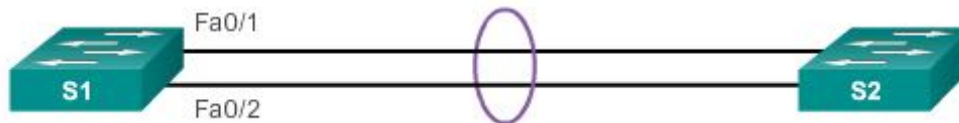
Configuration de EtherChannel

Configuration des Interfaces

Configuration d'EtherChannel avec LACP

```
S1(config)# interface range FastEthernet0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Crée EtherChannel et configure le trunk.

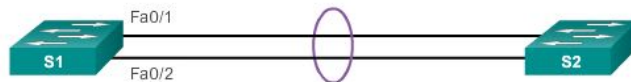


Vérification de EtherChannel

- **show interface port-channel** – affiche l'état général de l'interface port-channel
- **show etherchannel summary** – pour afficher une ligne d'informations unique par port-channel
- **show etherchannel port-channel** – pour afficher des informations concernant une interface port-channel spécifique
- **show interfaces etherchannel** – peut fournir des informations sur le rôle de l'interface dans EtherChannel

```
S1# show interface port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0cd9.96e8.8a02 (bia
0cd9.96e8.8a02)
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<résultat omis>
```

Vérifie l'état de l'interface.



Vérification et dépannage de EtherChannel

Dépannage EtherChannel

Dépannage de la fonctionnalité EtherChannel

```
S1# show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:           1
```

Group	Port-channel	Protocol	Ports
1	Po1(SD)	-	Fa0/1(D) Fa0/2(D)

```
S1# show run | begin interface port-channel
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
  channel-group 1 mode on
!
interface FastEthernet0/2
  switchport mode trunk
  channel-group 1 mode on
!
<résultat omis>
```

```
S2# show run | begin interface port-channel
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
  channel-group 1 mode desirable
!
interface FastEthernet0/2
  switchport mode trunk
  channel-group 1 mode desirable
!
```

```
S1(config)# no interface Port-channel 1
S1(config)# interface range f0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown
S1(config-if-range)# interface Port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:           1
```

- Interfaces d'un même groupe (canal) obligatoirement dans le même mode
- Interfaces entre deux commutateurs dans des modes compatibles

