Réseaux de Campus R301

Cours 1:

- Fonctionnement des commutateurs
- Rappels sur les VLAN
- Configurations avancées de STP

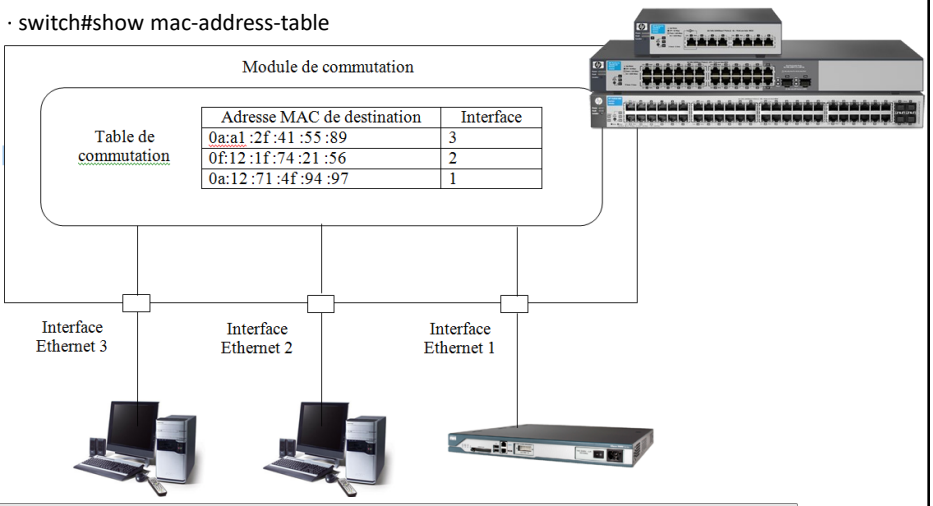
2022/2023

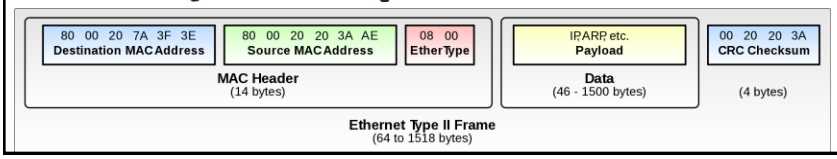
1

1

Fonctionnement d'un commutateur (switch)

- switch#show mac-address-table





2

2

Notes:

1) - A la mise sous tension du commutateur, ce dernier ne connait pas l'adresse MAC des ordinateurs reliés à ses ports,
2) Lorsque le switch reçoit une trame, il en déduit quel est l'ordinateur relié à ce port en lisant l'adresse MAC source et complète sa table de commutation
3) A ce stade il ne sait pas à quel port est relié l'hôte destinataire de la trame et émet cette trame sur tous ses ports (flooding)
4) Au fil du temps, il sera capable de diriger les trames uniquement sur le port auquel sont reliés les destinataires de la trame

3

3

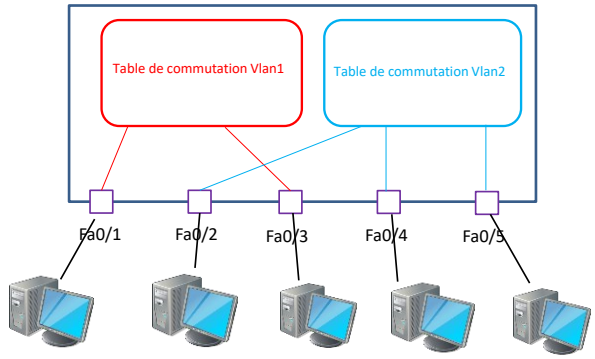
Les VLAN

- Le principal intérêt des VLAN est de séparer les flux. L'objectif est de créer plusieurs réseaux séparés sur un même LAN sans avoir besoin d'ajouter des commutateurs.
- Au niveau du commutateur, on crée autant de tables de commutation qu'il y a de VLAN

```
switch(config)#vlan 2
```

- On doit définir quelle table de commutation sera utilisée par quels ports

```
switch(config)#int fa0/4
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

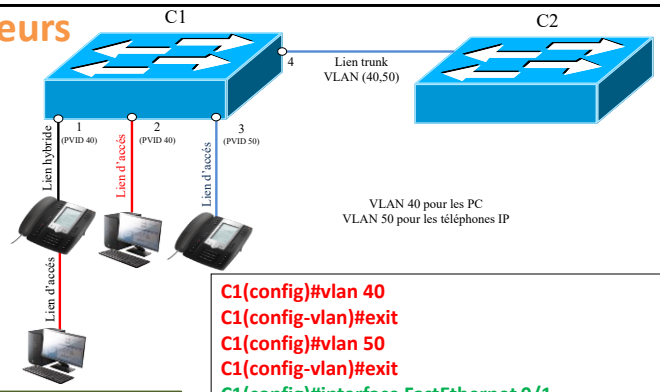


4

4

VLAN sur plusieurs switchs

los Cisco



Principe de sauvegarde d'un fichier de configuration lors des TP

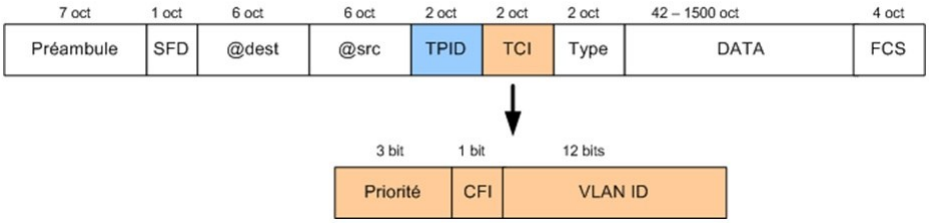
Initialiser un switch Cisco en ligne de commande:
switch#erase startup-config
switch#show flash
switch#delete flash:/vlan.dat

```
C1(config)#vlan 40
C1(config-vlan)#exit
C1(config)#vlan 50
C1(config-vlan)#exit
C1(config)#interface FastEthernet 0/1
C1(config-if)#switchport mode access
C1(config-if)#switchport access vlan 40
C1(config-if)#switchport voice vlan 50
C1(config)#interface FastEthernet 0/2
C1(config-if)#switchport mode access
C1(config-if)#switchport access vlan 40
C1(config)#interface FastEthernet 0/3
C1(config-if)#switchport mode access
C1(config-if)#switchport access vlan 50
C1(config)#interface FastEthernet 0/4
C1(config-if)#switchport mode trunk
C1(config-if)#switchport trunk allowed vlan 40,50
```

5

5

Trame 802.1Q



Le champ TPID détermine le type du tag, 0x8100 pour 802.1Q, ce champ est utilisé pour prévoir des évolutions futures afin de pouvoir utiliser le principe du tagging pour différentes fonctionnalités.Le champ TCI se décline en plusieurs éléments :

- Priorité: niveaux de priorité définis par l'IEEE 802.1P. Ce champ permet de réaliser une priorisation des flux. Le champ étant sur trois bits il est possible de déterminer 7 niveaux de priorité.

- CFI: Ce bit permet de déterminer si le tag s'applique à une trame de type Ethernet ou Token-Ring.

- VID: VLAN identifier. C'est l'identifiant du VLAN. L'appartenance d'une trame à un VLAN se fait grâce à cet identifiant. Le champ étant sur 12 bits, il est donc possible de déclarer jusqu'à 4096 VLANs.

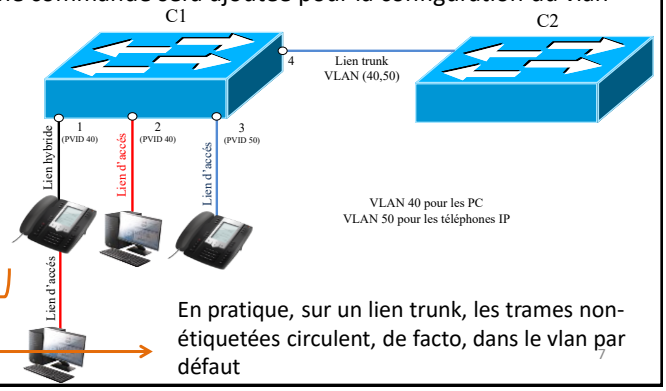
6

6

Rappel sur les VLAN - TD

3. Extrait de "http://www.omnisecu.com/"

- **Access link:** An access link is a link that is part of only one VLAN, and normally access links are for end devices. An access-link connection can understand only standard Ethernet frames.
- **Trunk link:** A Trunk link can carry multiple VLAN traffic and normally a trunk link is used to connect switches to other switches or to routers.
- **Hybrid port**: Cas particulier de la connexion d'un téléphone IP suivi d'un PC sur un port. Dans le cas de l'utilisation d'un ordinateur connecté à un téléphone IP (ce dernier étant connecté à un port du switch), le port aura deux vlans (un vlan dédié au réseau donnée et un vlan dédié au réseau voix). Le port sera configuré en général en mode *access*, une commande sera ajoutée pour la configuration du vlan voix (*voice vlan*).
- **PVID**: toutes les trames reçues sur un port sans identification de VLAN ("untagged" ou "priority tagged") sont classifiées par un commutateur comme appartenant au PVID "Port VLAN ID" aussi appelé "Local default VLAN" LAN local par défaut.



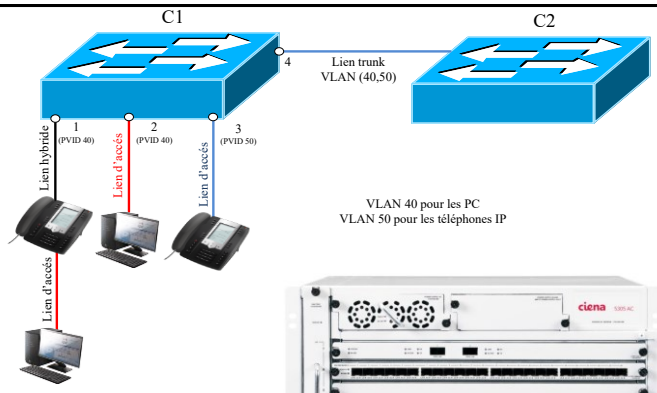
En pratique, sur un lien trunk, les trames non-étiquetées circulent, de facto, dans le vlan par défaut

7

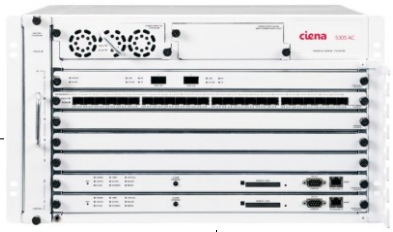
7

Rappel sur les VLAN - TD

3. Extrait



los Cenia



C1>vlan create vlan 40,50

C1>vlan add vlan 40 port 1,2,4

C1>vlan add vlan 50 port 1,3,4

C1> port set port 1 acceptable-frame-type all

C1> port set port 2,3 acceptable-frame-type untagged-only

C1> port set port 4 acceptable-frame-type tagged-only

C1> port set port 1,2 pvid 40

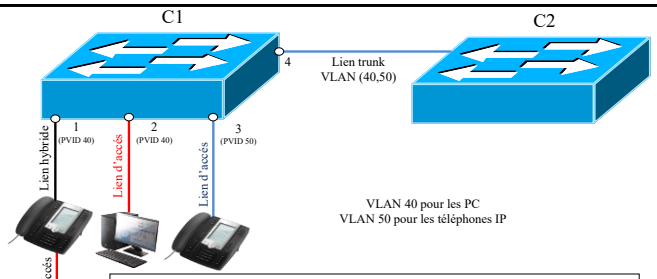
C1> port set port 3 pvid 50

8

8

Rappel sur les VLAN - TD

3. Extrait



los HP

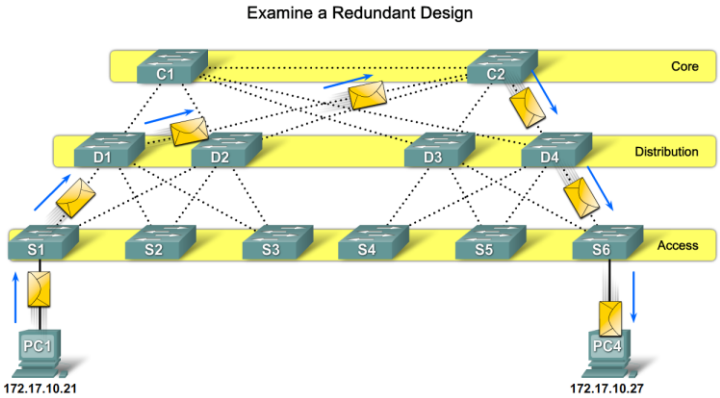
```
C1#config
C1(config)#vlan 40
C1(vlan-40)#untagged 1-2
C1(vlan-40)#tagged 4
C1(config)#vlan50
C1(vlan-50)#tagged  1 4
C1(vlan-50)#untagged 3
C1(vlan-50)#exit
C1(config)#int 1-4 enable
C1(config)#int 5-24 disable
C1(config)#write memory
```

9

9

STP: Spanning Tree Protocol (802.11D)

1. Infrastructure assurant la haute disponibilité sur un réseau Ethernet



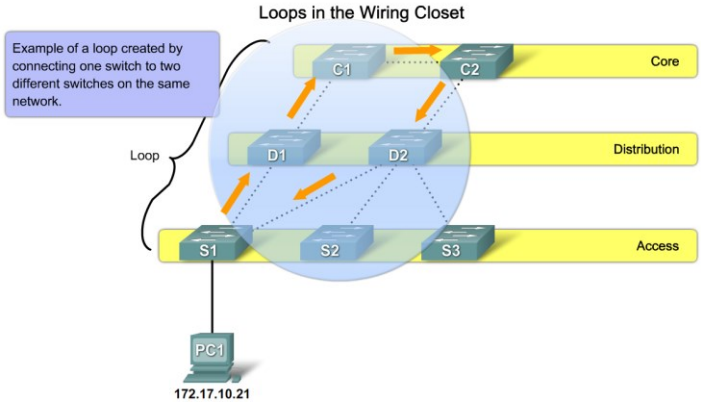
Le processus gérant, sur un commutateur, l'algorithme STP est appelé instance STP.

10

10

STP: Spanning Tree Protocol

1. Problématique de boucle dans les réseaux Ethernet



- Les trames Ethernet n'ont pas de durée de vie (TTL)
- Avec la multiplication progressive des trames qui circulent en boucle sur le réseau, des dysfonctionnements peuvent se produire.

11

11

STP: Spanning Tree Protocol

1. Les trames de diffusion sont envoyées à tous les ports de commutation, excepté au port d'entrée initial. Ceci garantit que tous les périphériques d'un domaine de diffusion reçoivent bien les trames. **S'il existe plusieurs chemins possibles pour le réacheminement des trames, une boucle sans fin risque de se former**. Dans un tel cas, la table d'adresses MAC d'un commutateur peut réagir en changeant constamment pour s'adapter à la mise à jour des trames de diffusion, entraînant une instabilité de la base de données MAC.

CCNA Scaling Networks
Chapitre 2: Redondance LAN 2.1.1.2 Problèmes liés à la *redondance de la couche 1* : ***instabilité de la base de données MAC***

12

12

STP: Spanning Tree Protocol

1. Une tempête de diffusion est inévitable sur un réseau comportant des boucles. En raison du nombre croissant des périphériques qui envoient des diffusions sur le réseau (ex: requêtes ARP), une quantité croissante de trafic est prise dans la boucle, ce qui consomme des ressources. Cela finit par créer une tempête de diffusion, provoquant ainsi la défaillance du réseau.

Chapitre 2: Redondance LAN 2.1.1.3 Problèmes liés à la redondance de la couche 1 : ***tempêtes de diffusion***

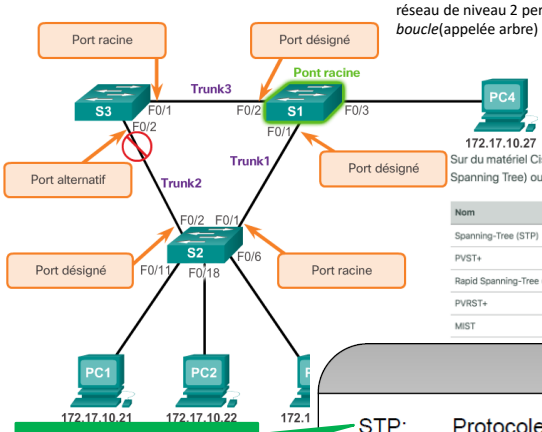
Chapitre 2: Redondance LAN 2.1.1.4 Problèmes liés à la redondance de la couche 1 : ***trames de monodiffusion en double***

13

13

Algorithme STP

Objectifs du protocole STP (définition Wikipedia):
Le ***Spanning Tree Protocol*** (algorithme de l'arbre recouvrant) est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau *sans boucle*(appelée arbre) dans les LAN avec ponts.



Sur du matériel Cisco, Spanning-Tree fonctionne en mode propriétaire avec PVST+ (Per-VLAN Spanning Tree) ou avec PVRST+ (Per-VLAN Rapid Spanning Tree).

Nom	Standard
Spanning-Tree (STP)	IEEE 802.1D
PVST+	STP Cisco
Rapid Spanning-Tree (RSTP)	IEEE 802.1w
PVRST+	RSTP Cisco
MIST	IEEE 802.1s

Durée de convergence lente (environ 50 sec.)

Implémenté sur les commutateurs Cisco: plusieurs instances STP c.a.d. une par Vlan

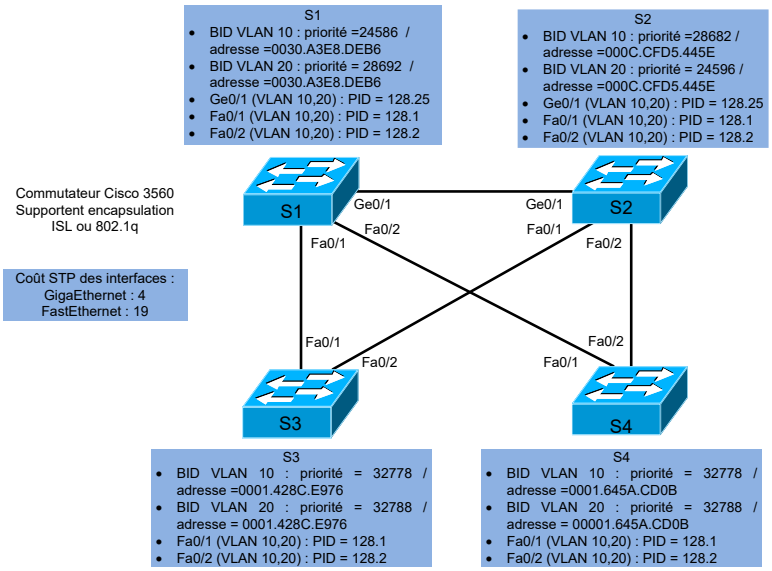
Versions

STP: Protocole de base.
PVST: Per VLAN STP, une instance de STP par VLAN. Uniquement avec ISL.
PVST+: Per VLAN STP fonctionnant avec dot1q.
RSTP+: STP Amélioré pour réduire la durée du passage d'un port en « blocking » à « forwarding ». (IEEE 802.1w)
MSTP: Multiple Spanning Tree Protocol. Une instance de RSTP par groupe de VLANs.

4

14

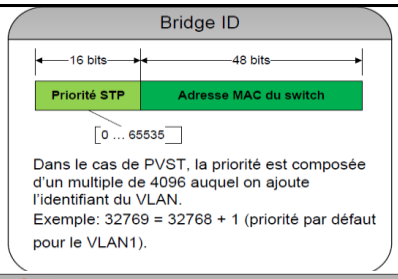
Soit l'architecture réseau donnée ci-dessous avec 4 commutateurs Ethernet. Ces commutateurs sont configurés pour utiliser les VLAN 10 et 20 (ainsi que le vlan par défaut = VLAN 1). Les commutateurs sont interconnectés via des liens trunk pour les VLAN 10 et 20.



15

15

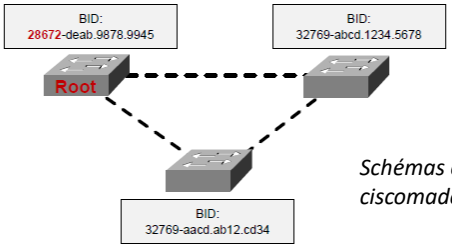
L'identité de pont:



Etape1: algorithme STP 1 - Election du Root Bridge

Le switch dont le BridgeID est le plus petit remporte l'élection du Root Bridge.

- Chaque Switch s'annonce comme le root.
- Quand un switch découvre un meilleur BID que le RootBridge qu'il connait actuellement (lui-même au début du processus), il remplace ce RootID par celui qu'il vient de découvrir.



Schémas extrait de ciscomadesimple.be

Une fois l'élection terminée, seul le Root Bridge envoi des BPDUs.

16

16

Pour supprimer les boucles dans le réseau, les commutateurs utilisent l'algorithme STP et s'envoient des trames Ethernet 802.3 spécifiques appelées BPDU « Bridge Protocol Data Unit ».

Structure d'un BPDU (Bridge Protocol Data Unit)

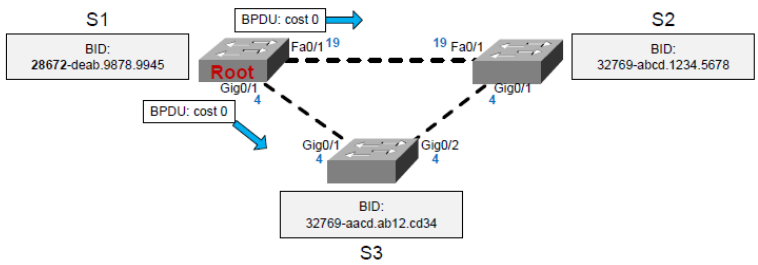
Protocole ID	Version	Message Type	Flags	Root ID	Root Path Cost	Bridge ID	Port ID	Message Age	Maximum Age	Hello Time	Forward Delay

Root Path Cost: Représente le coût du trajet depuis le root vers le switch en fonction du chemin utilisé.

Après l'élection du root bridge, l'algorithme STP comporte 3 étapes (donc 4 étapes avec l'élection du root bridge).

Etape2: algorithme STP

Le Root-Bridge envoi un BPDU dans chaque direction.

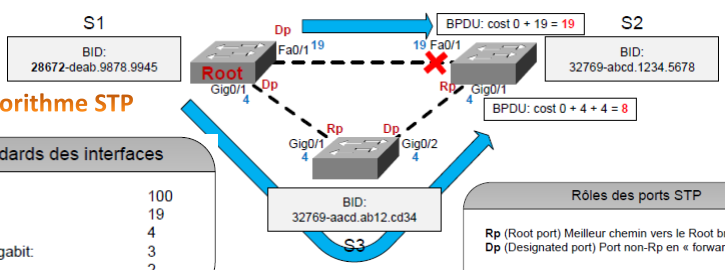


17

17

A chaque entrée sur une interface, le coût de l'interface est additionné au « Root Path Cost » du BPDU.

Etape3: algorithme STP



Coûts standards des interfaces

Ethernet:	100
Fast-Ethernet:	19
Gigabit:	4
Etherchannel Gigabit:	3
Ten-Gigabit:	2

Rôles des ports STP

Rp (Root port) Meilleur chemin vers le Root bridge.
Dp (Designated port) Port non-Rp en « forwarding ».

Un port qui n'est ni **Rp** ni **Dp** est un port bloqué.

S2 reçoit deux BPDUs, l'un venant directement de S1, l'autre par le côté de S3. Celui provenant de S3 a un « Root Path Cost » de 8, inférieur à celui venant de S1 (19), le chemin passant par S3 est donc le meilleur chemin vers le Root Bridge, l'interface Gig0/1 de S2 sera donc un Rp.

Un port faisant face à un Rp ne peut être qu'un Designated Port (Dp). Gig0/2 sur S3 sera donc un Dp.

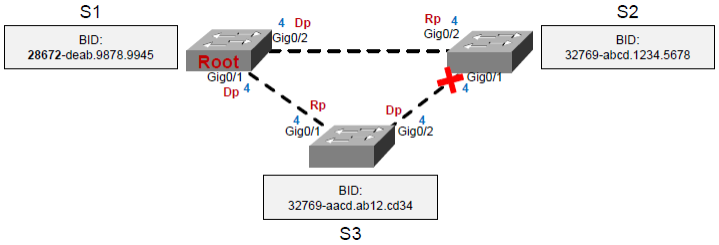
Les ports d'un Root Bridge sont toujours des Designated Ports. Fa0/1 et Gig0/1 de S1 seront donc des Dp.

Pour ouvrir la boucle il suffit de bloquer un seul port. Dans ce cas, la seule possibilité est Fa0/1 sur S2.

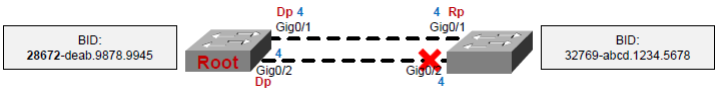
18

18

Si le coût de l'interface est égal des deux côtés du lien, le Bridge ID est utilisé pour définir le côté du lien où le port sera bloqué. Ici, S2 a un BID plus grand que S3 (donc moins bon), le lien entre S3 et S2 sera alors bloqué du côté de S2.



Si ni le coût de l'interface, ni le BID ne permettent de faire un choix, c'est alors le nom de l'interface qui est utilisé. Le « plus petit » nom d'interface sera le meilleur. (A est plus petit que Z, 1 est plus petit que 2)



Dans ce cas, S1 est Root Bridge, tous ses ports sont donc Dp. C'est alors du côté de S2 qu'il y aura un port bloqué. Les coûts sont égaux, le BID aussi. C'est donc le nom de l'interface qui va permettre de choisir. Gig0/1 est plus petit que Gig0/2, donc meilleur. Gig0/2 sera donc le port bloqué.

19

19

Configurer la priorité STP

```
MLS1>enable
MLS1#configure terminal
MLS1(config)#spanning-tree vlan 1 root primary
```

```
MLS1>enable
MLS1#configure terminal
MLS1(config)#spanning-tree vlan 1 priority 24576
```

Priorité STP par défaut

32768

L'effet de ces deux commandes est identique. L'option « root primary » est un raccourci pour définir une priorité de 24576 (soit 32768 – 2x 4096).

La commande « spanning-tree vlan 1 root secondary » revient à définir une priorité de 28672 (soit 32768 – 1x 4096).

Si la priorité est définie explicitement via la commande « spanning-tree vlan 1 priority XXXXX », la valeur donnée doit être un multiple de 4096.

Avec PVST+ , il faut soustraire le numéro de VLAN pour calculer la priorité d'un switch. Exemple: S1(config)#spanning-tree vlan 30 root primary; BID priority = 32768 -2x4096 + 30 = 24546

20

20

Etats des ports STP

Initialisation		Activation du port
Blocking	20 sec (*)	Le port jette les trames entrantes. Le port accepte les BPDUs mais ne les retransmets pas. Le port ne complète pas sa table d'adresses MAC.
Listening	15 sec	Le port jette les trames entrantes. Le port accepte les BPDUs et les retransmets. Le port ne complète pas sa table d'adresses MAC.
Learning	15 sec	Le port accepte les trames entrantes mais ne les retransmet pas. Le port accepte les BPDUs et les retransmets. Le port incorpore les nouvelle adresse MAC dans sa table.
Forwarding		Le port accepte et retransmets les trames entrantes. Le port accepte les BPDUs et les retransmets. Le port incorpore les nouvelle adresse MAC dans sa table.

(*) Lors d'un changement d'état un port restera en « Blocking » pendant 20 secondes afin d'éviter un recalcul de la topologie STP si ce n'est pas nécessaire (Un câble débranché et directement rebranché par exemple).

21

21

Afficher les informations STP

```
SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0013.c3ff.2580
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

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

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
SW1#
```

Nom du VLAN concerné

Protocol STP utilisé

Priorité configurée

Adresse MAC

Root Path Cost

Interface à laquelle le switch actuel est connecté

Informations concernant le Root Bridge

Le switch où l'on se trouve

Root Port (Rp)

Port en « Blocking »

« Cost » de l'interface

22

22

```
S1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0030.A3E8.DEB6
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0030.A3E8.DEB6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p

S1#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    28692
             Address     0030.A3E8.DEB6
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     0030.A3E8.DEB6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p
```

```
S2#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0030.A3E8.DEB6
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000C.CFD5.445E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 4         128.25   P2p

S2#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    28692
             Address     0030.A3E8.DEB6
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     000C.CFD5.445E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 4         128.25   P2p
```

23

23

```
S3#sh spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0030.A3E8.DEB6
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.428C.E976
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

S3#sh spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    28692
             Address     0030.A3E8.DEB6
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0001.428C.E976
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

```
S4#sh spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0030.A3E8.DEB6
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.645A.CD0B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

S4#sh spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    28692
             Address     0030.A3E8.DEB6
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0001.645A.CD0B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

24

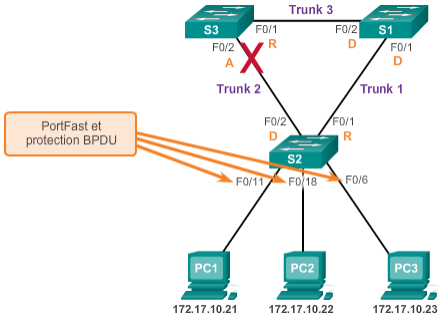
24

Portfast

PortFast est une fonction Cisco destinée aux environnements PVST+

Cette fonctionnalité doit être appliquée aux ports d'accès afin qu'ils passent de l'état de blocage à l'état de réacheminement immédiatement. (le port est opérationnel plus vite, par exemple, une requête cliente DHCP sera réacheminée instantanément).

Il est recommandé aussi d'activer la fonction BPDUGuard qui permet au port de passer à l'état shutdown s'il reçoit des trames BPDU (nb: un port d'accès ne reçoit théoriquement jamais de trames BPDU sauf si un personne mal intentionnée essaye de perturber le processus STP).




```
S1# show running-config | begin spanning-tree
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1 priority 0
spanning-tree vlan 10 priority 24576
spanning-tree vlan 20 priority 28672
<résultat omis>
```

25

25

Travaux Pratiques:
- 2.3.2.3 Lab - Configuring Rapid PVST, PortFast, and BPDU Guard

Topologie

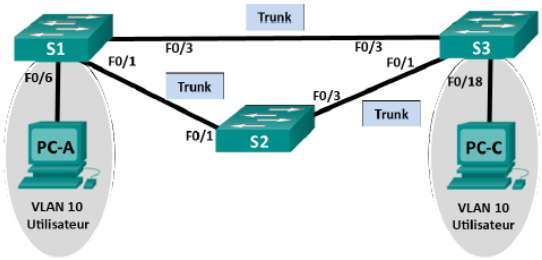


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Affectations de VLAN

VLAN	Nom
10	Utilisateur
99	Administration

Objectifs

Partie 1 : création du réseau et configuration des paramètres de base du périphérique
Partie 2 : configuration de VLAN, de VLAN natifs et de trunks
Partie 3 : configuration du pont racine et examen de la convergence PVST+

26

Sécurisation de l'accès aux ports

- Protection des commutateurs

Adresse MAC spécifique	Limitation du nombre d'adresses MAC
'Static secure MAC address' **Configuration manuelle des adresses MAC autorisées par port**	**'Dynamic secure MAC address'** **Limitation du nombre maximal d'adresses MAC de la table CAM par port** **'Sticky secure MAC address'** **Apprentissage dynamique des adresses MAC et configuration persistante de ces adresses**

Act

27

27