

LAN SWITCHING

Spanning-Tree et Etherchannel

[François-Emmanuel Goffinet](#)

Formateur IT

Version 15.10

Disponibilité dans le LAN

Couche	Protocole/Solutions	Délais de reprise
L2	<u>Rapid Spanning Tree</u>	Quelques secondes
L2	<u>Etherchannel</u>	Plus ou moins 1 seconde pour rediriger le trafic sur un lien alternatif
L3	First Hop Redundancy Protocols comme HSRP, VRRP, GLBP	10 secondes par défaut (Cisco) mais le constructeur conseille 1s hello time, 3s Hold Time
L3	Protocoles de routage	En dessous de la seconde avec OSPF ou EIGRP bien configurés au niveau des compteurs

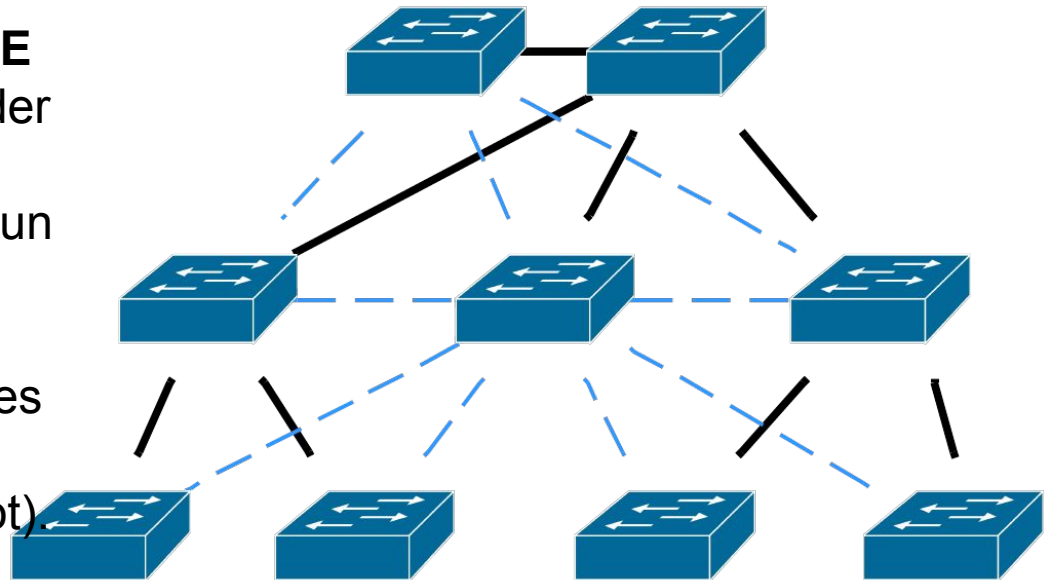
Sommaire

1. Protocoles Spanning-Tree
2. Technologies Etherchannel

1. Protocoles Spanning-Tree

Spanning-Tree

- Spanning-Tree est un protocole L2 formalisé **IEEE 802.1D** qui permet de garder une topologie physique redondante tout en créant un chemin logique unique.
- Spanning-Tree envoie régulièrement des annonces (BPDU) pour élire un commutateur principal (root).
- En fonction de cette information, les commutateurs "coupent" des ports et une topologie de transfert à chemin unique converge (de quelques secondes à 50 secondes selon les versions).



Variantes STP

Sur du matériel Cisco STP fonctionne en PVST+ ou en PVRST+

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

Protocoles 802.1

IEEE 802.1 est un groupe de travail du projet [IEEE 802](#). Ses thèmes d'étude sont (dans l'ordre où le groupe de normalisation les énumère) :

- Architecture [LAN/MAN](#) 802.
- Interconnexions avec les réseaux 802.
- Sécurité de la liaison 802.
- Gestion des réseaux 802.
- Couches de protocole au-dessus des couches [MAC](#) et [LLC](#).

Parmi les standards IEEE 802.1 les plus populaires

- 802.1D : MAC Bridges
- 802.1Q : Virtual LANs
- 802.1X : Port Based Network Access Control
- 802.1AB : Station and Media Access Control Connectivity Discovery ([LLDP](#))
- 802.1AE : MAC Security
- 802.1AX : Link Aggregation

Terminologie

Bridge, MAC bridges, BID, BPDU, Etats STP, commutateur Root, commutateur non-Root, port Désigné, port Root, port Non-désigné, délais, RSTP, PVST+, PVRST+, rapid-pvst

Problématique

Pour assurer la fiabilité des liaisons entre des commutateurs du LAN il est utile de multiplier les connexions physiques (redondance).

1. Si les commutateurs transfèrent le trafic de diffusion et multicast par tous les ports sauf celui d'origine
2. Si les trames Ethernet ne disposent pas de durée de vie

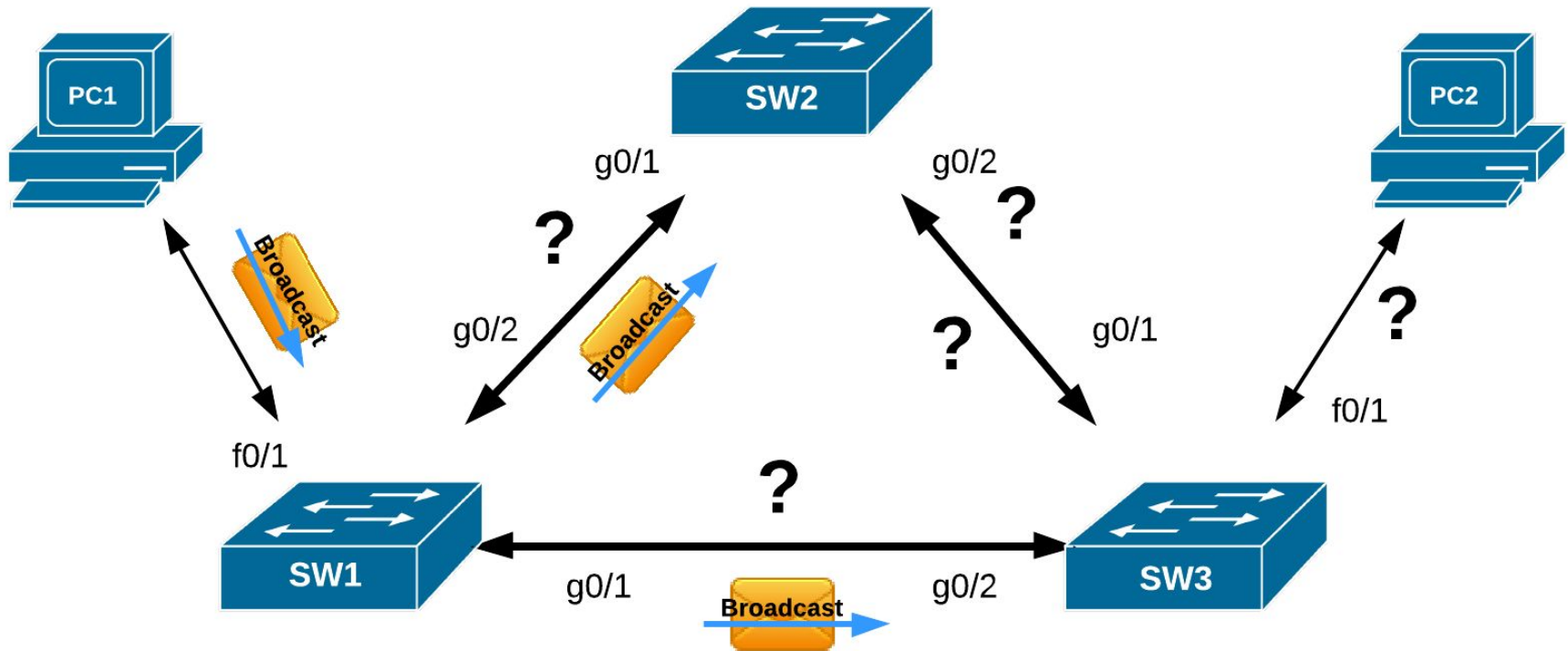
Plusieurs problèmes peuvent alors survenir :

1. Tempêtes de diffusion
2. Trames dupliquées
3. Instabilité des tables de commutation

Tempête de diffusion

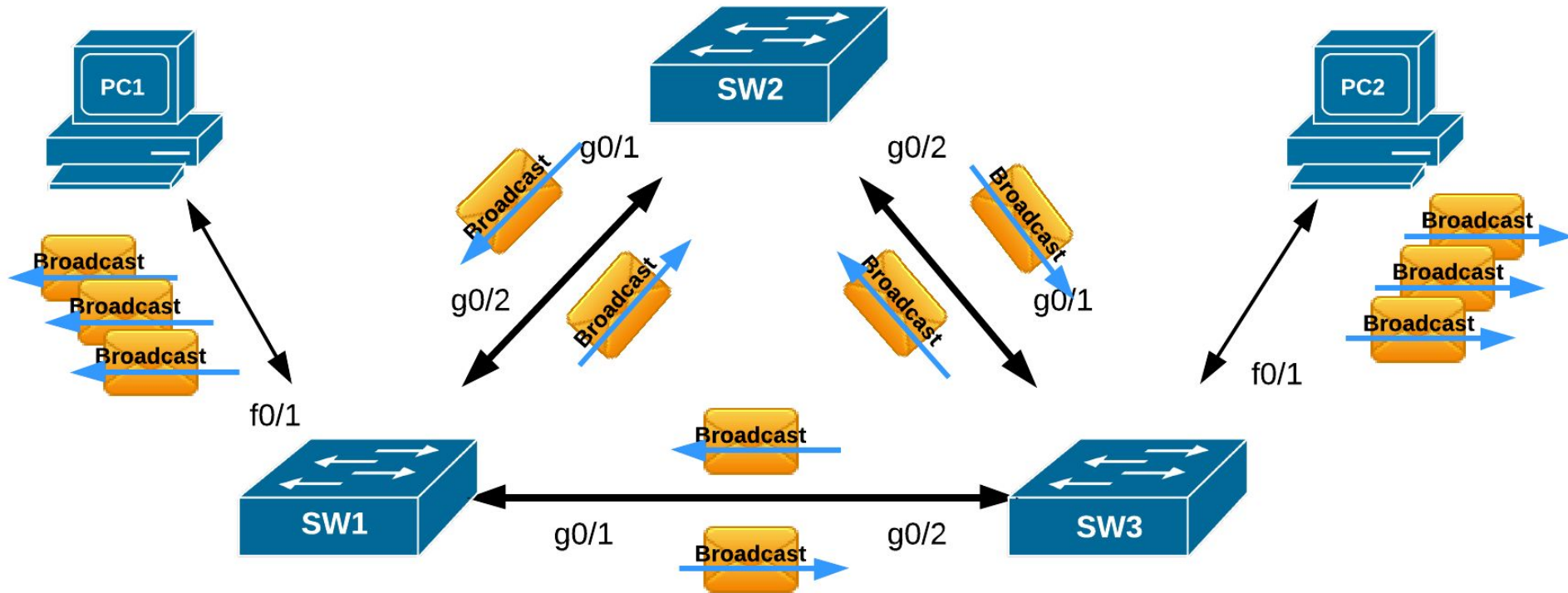
- Lorsque des trames de diffusion ou de multicast sont reçues (FF-FF-FF-FF-FF-FF en destination par exemple, du trafic ARP Req), les commutateurs les transfèrent par tous les ports.
- Les trames circulent en boucles et sont multipliées à chaque passage sur un commutateur.
- N'ayant pas de durée de vie (TTL comme les paquets IP), elles peuvent tourner indéfiniment.

Tempête de diffusion



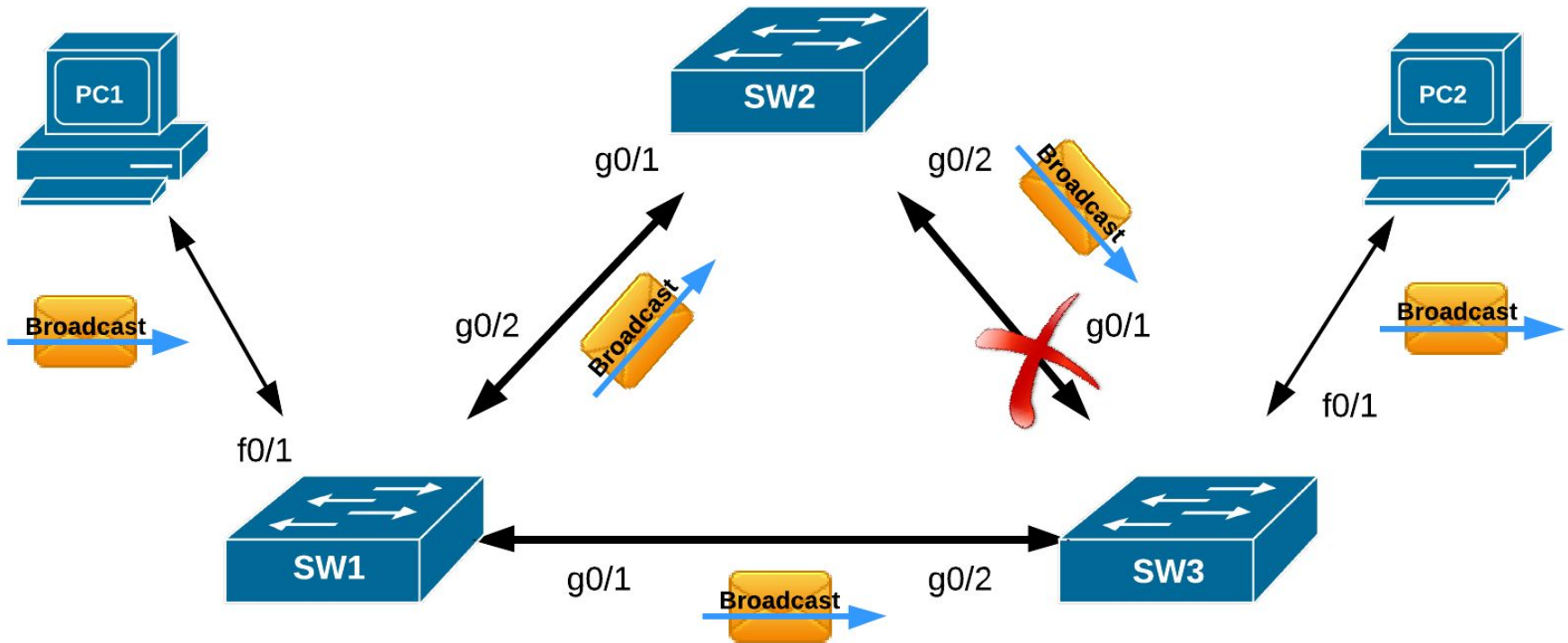
Quel est le sort réservé par les commutateurs à la trame dont la destination est une adresse de diffusion ou multicast ?

Tempête de diffusion



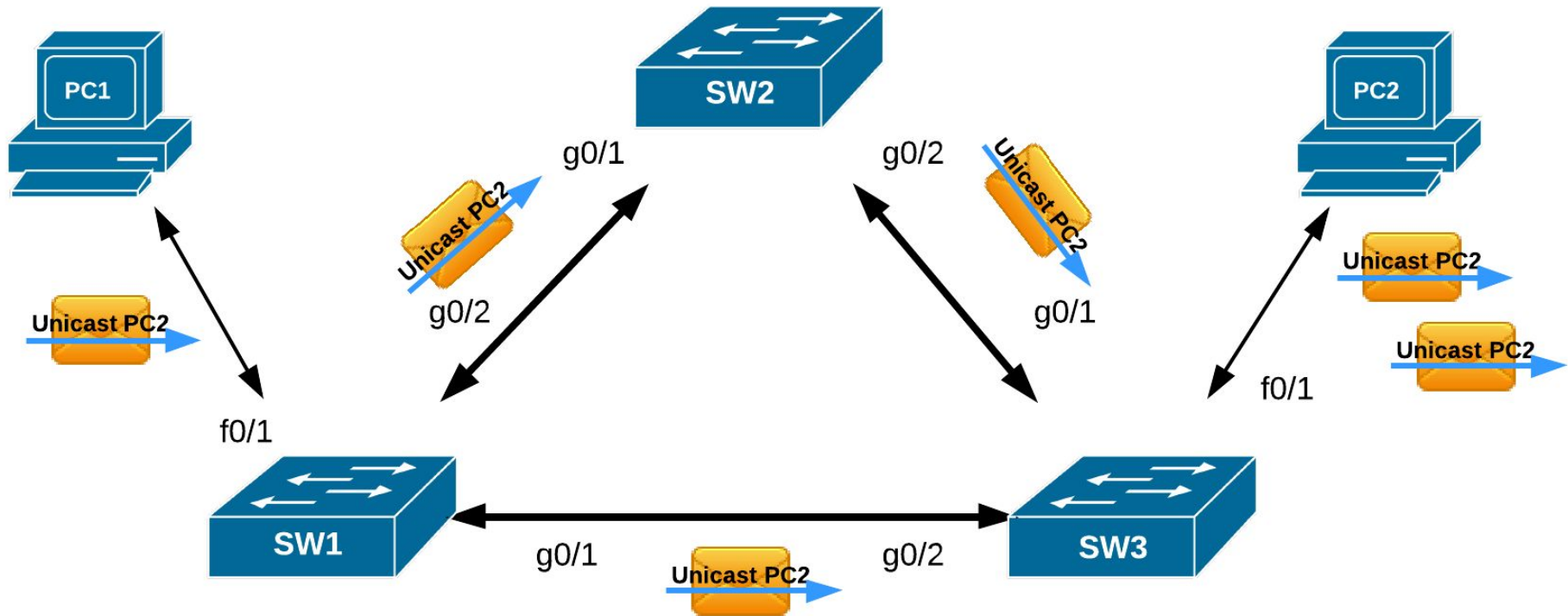
Une trame de diffusion est multipliée en boucle sur tous les ports jusqu'à rendre le réseau inutilisables. Comment mettre fin à ce phénomène ?

Couper la boucle de commutation



En coupant la boucle, un seul chemin est possible d'une extrémité à l'autre du réseau

Trames dupliquées



Dans cet autre exemple, PC1 envoie une trame à PC2, elle arrive en double exemplaire à sa destination.

STP : principe

- Afin de profiter de la redondance tout en évitant la problématique des boucles, Spanning-Tree crée un chemin sans boucle basé sur le chemin le plus court.
 - Ce chemin est établi en fonction de la somme des **coûts** de liens entre les commutateurs.
 - Ce coût est une valeur inverse à la vitesse d'un port, car un lien rapide aura un coût moins élevé qu'un lien lent.
- Aussi, un chemin sans boucle suppose que certains ports soient bloqués (**état Blocking**) et pas d'autres (**état Forwarding**).
- Les commutateurs STP échangent régulièrement (2s. par défaut, en Multicast) des informations (appelées des **BPDUs - Bridge Protocol Data Unit**) afin qu'une éventuelle modification de la topologie puisse être adaptée sans boucle.

BID : Bridge ID

Chaque commutateur prendra un identifiant unique appelé BID (Bridge ID) composé :

- d'une priorité configurable (4 bits, multiples de 4096), par défaut cisco 32768 (0111)
- d'une "Bridge System ID Extension" de 12 bits (numéros de VLAN)
- de l'adresse MAC du commutateur

Par exemple :

```
Bridge ID  Priority 32769  (priority 32768 sys-id-ext 1)
Address                0001.96C7.DC42
```

Le BID permet à STP de choisir un commutateur Root dans la topologie.

Algorithme STP

Spanning-Tree calcule une topologie sans boucle en 4 étapes :

1. Sélection d'**un commutateur Root**, un seul par topologie, qui sera le commutateur racine de la topologie, tous ses ports transfèrent le trafic (**ports Designated**). Le commutateur avec le BID le plus faible remporte l'élection.
2. Sélection d'un seul **port Root** sur les (autres) **commutateurs non-Root**, qui dispose de la liaison dont le coût vers le commutateur Root est le plus faible. Il est le seul à transférer du trafic.
3. Sélection d'**un port Designated pour chaque segment physique** qui connecte deux commutateurs quand c'est nécessaire. C'est le port qui a le coût vers le commutateur Root le plus faible qui est sélectionné, il est le seul à transférer le trafic.
4. Les **ports Root et Designated** transfèrent du trafic (état "Forwarding") et les autres coupent la liaison (état "Blocking")

1. Sélection d'un commutateur Root

- Le **commutateur Root** (principal) sera le point central de l'arbre STP. Le choix de celui-ci dans l'architecture du réseau peut avoir son importance. Idéalement dans la couche Distribution.
- Par défaut, le commutateur qui aura l'identifiant (**BID**) le plus faible sera élu Root.
- Si la **priorité STP du commutateur** reste à sa valeur par défaut (32768, 0x08), la valeur de l'adresse MAC du commutateur sera déterminante.
- Le commutateur Root est unique dans la topologie.
- Tous ses ports sont en état “Forwarding”, transfèrent du trafic.

Influencer la sélection du commutateur Root

- En fixant la priorité du commutateur (par VLAN) :

```
(config)#spanning-tree vlan vlan-id priority priority
```

- En laissant l'IOS fixer la meilleure priorité :

```
(config)#spanning-tree vlan vlan-id root  
[primary|secondary]
```

2. Sélection d'un seul port Root chaque commutateur non-Root

Les autres commutateurs non-Root vont sélectionner un seul port Root qui aura le chemin le plus court vers le commutateur Root.

Un port Root est en état « forwarding ».

Le coût est calculé inversement à la vitesse de la liaison :

Vitesse du lien	Coût	Plage de coût recommandée
10 Mbps	100	50 à 600
100Mbps	19	10 à 60
1Gbps	4	3 à 10
10Gbps	2	1 à 5

Coût des liaisons

Ce coût peut être modifié.

S'il s'agit d'un port configuré en mode Access (qui connecte un périphérique terminal), la commande de configuration est :

```
(config-if) #spanning-tree cost cost
```

S'il s'agit d'un port en mode Trunk (qui connecte un autre commutateur pour transporter du trafic de plusieurs VLANs), la commande de configuration est :

```
(config-if) #spanning-tree vlan vlan-id cost cost
```

Ports Root exaequo

Sur un commutateur non-Root, pour des interfaces STP en cas de coûts égaux vers le commutateur Root, c'est leur priorité la plus faible (d'une valeur de 0 à 255) qui emporte le choix du port Root (elle est de 128 par défaut) en déterminant l'ID du port composé de 2 octets (priorité + numéro STP du port) :

Sur un port en mode Access :

```
(config-if) #spanning-tree port-priority priority
```

Sur un port en mode trunk :

```
(config-if) #spanning-tree vlan vlan-id port-priority  
priority
```

3. et 4. Port Désigné par segment

Pour chaque segment physique, domaine de collision ou lien, il y a un **port Designated**.

Le **port Designated** d'un segment est celui qui a le chemin le plus court vers le commutateur Root.

Un port Designated est normalement en état “Forwarding”, autrement dit, envoie et reçoit du trafic de données.

Tous les autres sont des ports Non-Designated en état “Blocking”, c'est-à-dire bloquant tout trafic de données mais restant à l'écoute des BPDU.

STP en résumé

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

Port		⇔	Port	Etat		⇔	Etat	Commutateur		⇔	Commutateur
Root		⇔	Designated	Forwarding		⇔	Forwarding	Non-root		⇔	Root
Designated		⇔	Root	Forwarding		⇔	Forwarding	Non-root		⇔	Non-root
Designated		⇔	Non-Designated	Forwarding		⇔	Blocking	Non-root		⇔	Non-root

États STP

États	Délais	Transfert data	Apprentissage MAC	Envoi des BPDUs	A l'écoute des BPDUs, SNMP
Blocking	Max Age = 20 sec.	non	non	non	oui, en attente de BPDUs
Listening	Forwarding Delay = 15 sec.	non	non	oui	oui
Learning	Forwarding Delay = 15 sec.	non	oui	oui	oui
Forwarding		oui	oui	oui	oui

Un port démarre en état “Blocking” et peut atteindre l’état “Forwarding” en fonction des BPDUs reçus. L’état “Disabled” est une désactivation administrative ou fait suite à une erreur de sécurité.

Délais STP

- Âge maximum, délais avant lequel un port attend avant d'entrer en état "Listening" :

```
(config)#spanning-tree [vlan vlan-id] max-age seconds
```

6 à 200 secondes, 20 secondes par défaut

- Délais pour atteindre l'état "Forwarding" :

```
(config)#spanning-tree [vlan vlan-id] forward-time seconds
```

4 à 200 secondes, 15 secondes par défaut

- Fréquence des Hellos STP :

```
(config)#spanning-tree [vlan vlan-id] hello-time seconds
```

1 à 10 secondes, 2 secondes par défaut

Messages STP

Les commutateurs s'échangent des Bridge Protocol Data Units (BPDU) de deux types :

- type **Configuration** : utilisés lors des élections, pour maintenir la connectivité entre les commutateurs
- type **Topology Change Notification (TCN)** : envoyés auprès d'un commutateur Root pour signaler des ruptures de liens. Quand un commutateur reçoit un TCN, il l'accuse de réception.

Capture de trafic STP :

<https://www.cloudshark.org/captures/add9bb6a43f9>

Charge STP

IEEE 802.3 Ethernet

Logical-Link Control

Spanning Tree Protocol

Protocol Identifier: Spanning Tree Protocol (0x0000)

Protocol Version Identifier: Spanning Tree (0)

BPDU Type: Configuration (0x00)

BPDU flags: 0x00

Root Identifier: 32768 / 1 / 00:19:06:ea:b8:80

Root Path Cost: 0

Bridge Identifier: 32768 / 1 / 00:19:06:ea:b8:80

Port identifier: 0x8005

Message Age: 0

Max Age: 20

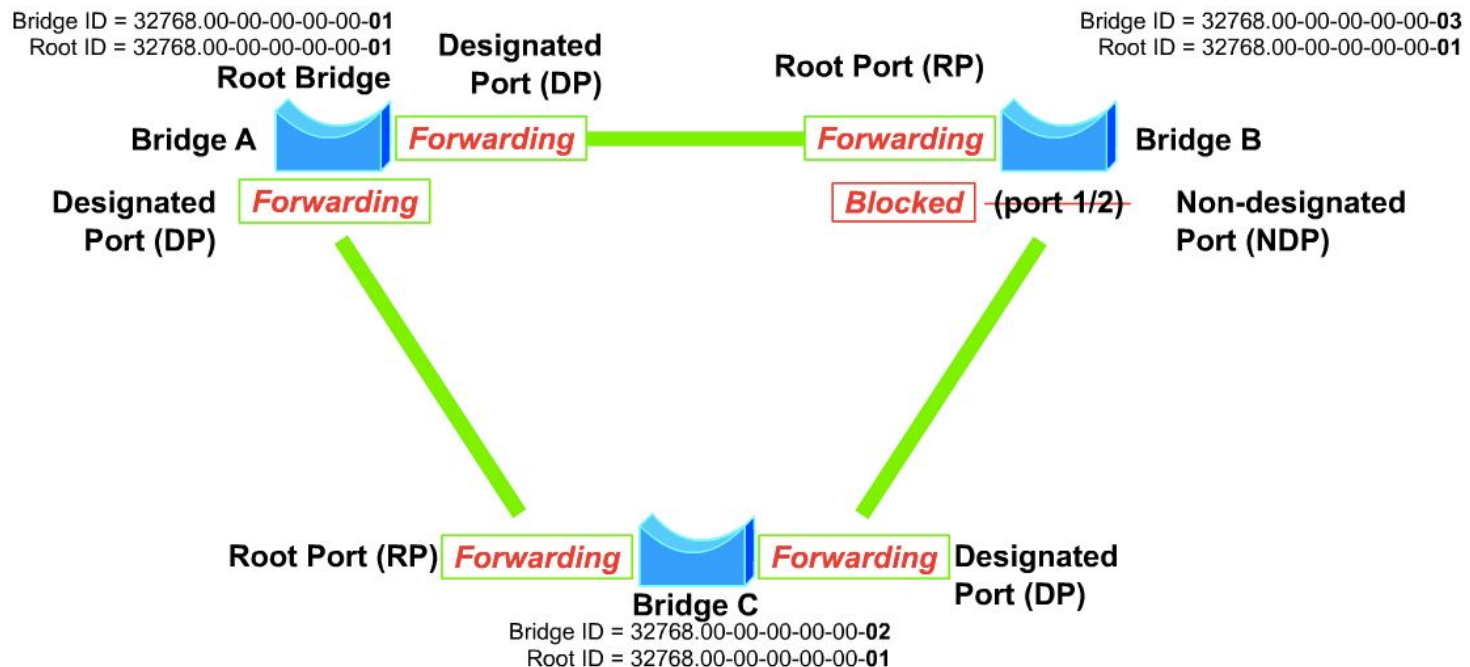
Hello Time: 2

Forward Delay: 15

Convergence STP

Cette animation illustre le fonctionnement de Spanning-Tree :

http://www.cisco.com/image/gif/paws/10556/spanning_tree1.swf



At this point Spanning tree has fully converged.

Portfast

La commande **Portfast** est une fonctionnalité propriétaire Cisco. Elle s'exécute uniquement sur des ports connectant des périphériques terminaux et dans une infrastructure VLAN uniquement sur des ports en mode Access.

Lorsqu'il est connecté, le port configuré en mode Portfast passe directement de l'état "Blocking" à l'état "Forwarding".

STP Portfast comporte aussi l'avantage de ne pas transférer de BPDUs TCN inutiles et de monter une interface sans passer par les délais STP.

La commande d'activation s'exécute en configuration d'interface :

```
(config-if) #spanning-tree portfast
```

Le message qui suivra indique la précaution d'usage afin d'éviter des boucles.

```
%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/X but will only have effect when the interface is in a non-trunking mode.
```

Portfast BPDU Guard

La fonctionnalité Portfast n'empêche pas de connecter un commutateur "pirate".

Afin de limiter plus strictement sa topologie STP, on peut utiliser le mode Portfast BPDU Guard :

le port Portfast qui reçoit des BPDU se mettra en mode "err-Disabled".

Ce mode est désactivé par défaut et s'active sur C2960:

```
(config-if) # spanning-tree bpduguard enable
```

Variantes STP

Protocole	Standard	Convergence	Instances /VLANs
Spanning-Tree (STP)	IEEE 802.1D	Lente	Unique
PVST+	STP Cisco	Lente	Multiple
Rapid Spanning-Tree (RSTP)	IEEE 802.1w	Rapide	Unique
PVRST+	RSTP Cisco	Rapide	Multiple
MIST	IEEE 802.1s	Rapide	Maulultiple

PVST+

- PVST+ est la version Cisco améliorée de STP IEEE 802.1D-2004.
- Avec PVST+, il y a une instance STP par VLAN.
- PVRST+ est la version améliorée de RSTP.
- MST est un standard IEEE 802.1s de l'implémentation propriétaire du Cisco Multiple Instances Spanning Tree Protocol (MISTP). MST distribue la charge de plusieurs VLANs sur plusieurs liens STP.

RSTP / PVRST+

RSTP / PVRST+ font fait passer le temps de convergence à 6 secondes maximum ce qui les rend beaucoup plus opérationnel que STP.

Pour l'activer, en mode de configuration globale :

```
(config)#spanning-tree mode rapid-pvst
```

En général, RSTP fonctionne de la même manière que STP :

1. Mêmes règles d'élection du commutateur Root
2. Mêmes règles de sélection d'un port Root sur un commutateur non-Root
3. Mêmes règles d'un unique port Designated sur un segment physique et les autres en état "Blocking".

Différences RSTP

Les différences par rapport à STP :

1. Il n'y a plus que **trois états** pour les ports RSTP :

- Discarding (au lieu de Disabled, Blocking et Listening)
- Learning et Forwarding (gardant la même fonction)

2. Les rôles **port Root** et **port Designated** subsistent. Les meilleurs ports alternatifs prennent le nom de lien de sauvegarde de ces derniers : **port Alternate** et **port Backup**. Ils prennent le rôle port Root et port Designated en cas de défaillance.

3. Types. Les ports connectant des périphériques terminaux s'appellent des **ports Edge** qui remplissent la même fonction que la fonction Portfast en PVST+. Les ports **Point-to-Point** connectent des commutateurs entre eux.

Alors que STP attend passivement des BPDUs pour agir, RSTP négocie le statut des liens rapidement (3 X le Hello Time = 6 secondes).

On peut voir des paquets RSTP ici : <https://www.cloudshark.org/captures/4d3b1f118872>

Diagnostic Spanning-Tree

1. Vérification du protocole *ieee* (pvst) ou *rstp* (rapid-pvst)
2. Identification du VLAN
3. Identification du BID du commutateur
- 4. Identification du Root ID**
5. Correspondance des délais (Hello Time, Forward Delay, Max Age)
- 6. État des ports**
7. Rôle des ports

Diagnostic de base

```
Switch#show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority      24577  
              Address      0001.96C7.DC42  
              Cost          4  
              Port          26(GigabitEthernet1/2)  
Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
```

```
Bridge ID   Priority      32769 (priority 32768 sys-id-ext 1)  
              Address      0001.4373.1102  
              Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec  
              Aging Time    20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/1	Altn	BLK	4	128.25	P2p
Gi1/2	Root	FWD	4	128.26	P2p
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

Commandes de diagnostic STP

Pour le diagnostic STP sur un VLAN :

```
#show spanning-tree vlan vlan-id
```

Pour le diagnostic STP d'une interface :

```
#show spanning-tree interface interface
```

Pour des informations détaillées :

```
#show spanning-tree detail
```

Pour vérifier uniquement les interfaces actives :

```
#show spanning-tree active
```

Références STP

- [IEEE 802.1D™-2004](#) IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges (Incorporates IEEE 802.1t™-2001 and IEEE 802.1w™)
- <http://packetlife.net/captures/protocol/stp/>
- [Understanding Multiple Spanning Tree Protocol \(802.1s\)](#)
- [Understanding Rapid Spanning Tree Protocol \(802.1w\)](#)
- [Understanding and Tuning Spanning Tree Protocol Timers](#)

2. Technologies Etherchannel

Technologie Etherchannel (1/2)

- EtherChannel est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet identiques en un lien logique.
- Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs.
- Un lien EtherChannel groupe de 2 à 8 liens actifs de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, plus éventuellement de 1 à 8 liens inactifs en réserve qui deviennent actifs quand des liens actifs sont coupés.

Technologie Etherchannel (2/2)

- EtherChannel est principalement utilisé sur la dorsale du réseau local, mais on peut aussi l'utiliser pour connecter des postes d'utilisateurs, des serveurs.
- La technologie EtherChannel a été inventée par la société Kalpana au début des années 1990. Cette société a ensuite été acquise par Cisco Systems en 1994. En 2000, l'IEEE a publié le standard 802.3ad, qui est une version ouverte de EtherChannel.
- Elle permet simplifier une topologie Spanning-Tree en diminuant le nombre de lien.

Configuration chez Cisco

Sur une interface, on indique à quel Groupe Etherchannel elle appartient. On trouvera des configurations :

- Statique
- Dynamique, via un protocole qui négocie l'aggrégation :
 - Port Aggregation Protocol (PAgP)
 - Link Aggregation Control Protocol (LACP).

EtherChannel et IEEE 802.3ad

Les protocoles EtherChannel et IEEE 802.3ad sont très semblables et accomplissent le même but.

Il y a néanmoins quelque différences entre les deux :

1. EtherChannel est un protocole propriétaire de Cisco, alors que 802.3ad est un standard ouvert
2. EtherChannel nécessite de configurer précisément le commutateur, alors que **802.3ad n'a besoin que d'une configuration initiale**
3. EtherChannel prend en charge plusieurs modes de distribution de la charge sur les différents liens, alors que 802.3ad n'a qu'un mode standard
4. EtherChannel peut être configuré automatiquement à la fois par LACP et par PAgP, tandis que **802.3ad ne peut l'être que par LACP.**

Configuration

```
Switch(config)# interface range fa0/1 - 4 {we can use the  
range or single interface}
```

```
Switch(config-if-range)# channel-group [1 - 6] mode [auto  
| desirable | on | active | passive]
```

- Le nombre de “channel-group” disponible dépend du type de commutateur.
- Les modes “auto” et “desirable” activent PAgP.
- “Active” et “passive” activent LACP.
- Le mode “on” force l’interface à se lier sans PAgP ou LACP

```
(config-if-range)#channel-group 1 mode ?  
active      Enable LACP unconditionally  
auto        Enable PAgP only if a PAgP device is detected  
desirable   Enable PAgP unconditionally  
on          Enable Etherchannel only  
passive     Enable LACP only if a LACP device is detected
```

Diagnostic

```
Switch# show interface etherchannel
```

```
Switch# show etherchannel [summary | load  
balance | port-channel]
```

Sources

<http://fr.wikipedia.org/wiki/EtherChannel>

Droits

Cisco Systems est une marque réservée.

Spanning-Tree et Etherchannel de goffinet@goffinet.eu est mis à disposition selon les termes de la [licence Creative Commons Attribution - Partage dans les Mêmes Conditions 4.0 International](#)