# Protocoles de switch

### Découverte des voisins

### CDP – Cisco Discovery Protocol

CDP (Cisco Discovery Protocol) est un protocole propriétaire de découverte de périphériques réseau indépendant des medias et protocoles utilisés qui fonctionne au niveau de la couche 2. L'utilisation de CDP permet à un équipement de signaler son existence à ses voisins (nom, modèle, version, adresse IP, …).

## Fonctionnalités

**Vérifier l'état** de fonctionnement d'une liaison.
**Obtenir des informations** sur l'équipement voisin. son adresse IP par exemple.
**Découvrir et tracer** la topologie du réseau.
**Utiliser** pour la ToIP.

## Utilisation

**Activer ou désactiver CDP**
cdp run / no cdp run
**Activer ou désactiver CDP sur une interface spécifique**
cdp enable / no cdp enable

**Afficher les infos de fonctionnement de CDP**
show cdp

**Afficher un résumé des équipements voisins connectés**
show cdp neighbors

sw1#show cdp neighbors
**Device ID Local Intrfce Holdtme Capability Platform Port ID**

- **Device ID** : le nom configuré sur l'équipement
- **Local Intrfce** : l'interface de l'équipement sur lequel on travaille, laquelle est connectée l'autre équipement.
- **HoldTme** : Temps restant avant que cette entrée ne soit oubliée au cas ou aucune mise à jour n'est reçue.
- **Capability** : Fonctionnalités de l'équipement voisin.
- **Platform** : Type de l'équipement voisin.
- **Port ID** : Port sur l'équipement voisin auquel est rattaché la machine sur laquelle on se trouve.

**Afficher les informations détaillées sur chaque équipement voisin connecté**
show cdp neigbors detail

- Les informations affichées dépendent de la nature de l'équipement voisin.

**Afficher les informations détaillées d'un voisin spécifique**
show cdp entry <nom>
**Afficher les informations CDP concernant l'interface donnée**
show cdp interface <type> <numéro>

**Effacer la table CDP**
clear cdp table

Lorsque l'on modifie les connexions entre deux équipements, il est pratique de vider la table de CDP de manière à ne pas avoir de fausses informations, le temps que les anciennes entrées soient considérées comme périmées.

## Holdtime et interval des packets CDP

Le Holdtime est la durée de vie de l'information envoyée dans le message CDP.
L'interval est le temps qui s'écoule entre deux envois de message CDP.

**cdp holdtime <x>**
Défini la durée de vie en secondes de l'information envoyée. Valeur comprise entre 10 et 255 secondes. Par défaut la valeur est définie à 180.

**cdp timer <x>**
Fréquence à laquelle l'équipement doit renvoyer les messages CDP. Valeur comprise entre 5 et 254 secondes. Par défaut, la valeur est définie à 60.

**Note**
*Si on configure un holtime plus court que le timer, les infos CDP ne seront pas renouvelées à temps et le voisin aura une table CDP incomplète.*

## LLDP – Link Layer Discovery Protocol

LLDP est un protocole standardisé (IEEE 802.1ab) utilisé dans la découverte des topologies réseau et l'échange de configuration et des capacités des périphériques d'équipements directement connectés.
Il permet de d'effectuer un inventaire précis de la topologie physique et des équipements pour simplifier la gestion et la maintenance.

**Activer LLDP**

```
Sw1(config)#lldp run
Sw1(config)#lldp timer 30
Sw1(config)#lldp holdtime 60
```

**show lldp neighbors**
Affiche les informations des voisins

**show lldp entry <nom>**
Affiche les informations détaillées d'un voisin spécifique.

**lldp timer 10**
Configurer l'intervalle entre deux LLDPDU (Valeur comprise entre 5 et 65534 secondes)

**Recevoir et transmettre sur une interface spécifique**

```
Sw1(config)# interface GigabitEthernet 1/1
Sw1(config-if)# lldp transmit
Sw1(config-if)# lldp receive
```

Par défaut LLDP transmet tous les TLVs (*Type, Length, value*) disponibles. Vous pouvez choisir de restreindre cela en définissant ceux à propager.
Il faut répéter la commande pour chaque TLV. Une fois un TLV choisi, l'équipement ne propagera plus que lui (et ceux que vous configurerez après).

```
Sw1(config)#lldp tlv-select ?
mac-phy-cfg
management-address
port-description
port-vlan
power-management
system-capabilities
system-description
system-name
```

Vous pouvez également choisir les MED-tlv (*Media Endpoint Discovery*)

```
Sw1(config-if)#lldp med-tlv-select ?
inventory-management
location
network-policy
power-management
```

## Gestion des vlan dynamiques – DTP

### Définition

**DTP** pour **Dynamic Trunking Procotol**, c'est un protocole propriétaire Cisco. Le principe est très simple, lorsqu'un port monte, des annonces DTP sont envoyées;

- si le port est connecté à un switch voisin, ce dernier va recevoir l'annonce DTP et y répondre. Des deux côtés, l'activation du Trunk s'effectue;
- si le port est connecté à un PC, ce dernier ne répondra pas à l'annonce car il comprend pas le protocole. Sur le port du switch, le Trunk n'est pas activé et donc reste en mode **Access.**

### Fonctionnement

Un port physique d'un switch peut avoir plusieurs état (ou mode) concernant le DTP. Ces états sont très importants à connaitre car selon le modèle de votre switch, l'état par défaut n'est pas le même.

- **Dynamic desirable** = annonce sa volonté de monter en trunk
- **Dynamic auto** = écoute, réponse mais pas d'annonce
- **Trunk on** = se met automatiquement en trunk et annonce à son voisin
- **Nonegociate** = se met automatiquement en trunk et n'annonce pas à son voisin
- **Trunk off** = désactive le trunk
- **Access** = désactive le trunk et annonce à son voisin

| | Dynamic auto | Dynamic desirable | Trunk | Access |
|---|---|---|---|---|
| **Dynamic auto** | Access | Trunk | Trunk | Access |
| **Dynamic desirable** | Trunk | Trunk | Trunk | Access |
| **Trunk** | Trunk | Trunk | Trunk | ***** |
| **Access** | Access | Access | ***** | Access |

### Les combinaisons possibles

Les cases où il y a des "*****" sont les cas où le comportement des 2 switches est incertain car la configuration est incohérente: d'un côté on configure le port en **Access** et de l'autre en **Trunk** donc ça ne fonctionnera pas.

## Configuration

Prenons l'exemple des switchs 1 et 2 connectés entre eux via leur port gi1/0/1 respectifs. Configurons le switch 1 pour qu'il soit en mode **dynamic desirable**

```
Sw1(config)# interface gi1/0/1
Sw1(config-if)# shut
Sw1(config-if)# switchport mode dynamic desirable
Sw1(config-if)# no shut
Sw1> sh dtp
```

Et sur le switch 2, on configure le port gi1/0/1 en mode **auto**:

```
Sw2(config)# interface gi1/0/1
Sw2(config-if)# shut
Sw2(config-if)# switchport mode dynamic auto
Sw2(config-if)# no shut
Sw2> sh dtp
```

**Démonstration :**

- le switch 1 est en mode **dynamic desirable** donc il envoi des invitations au switch B pour monter un lien Trunk;
- le switch 2 est en mode **dynamic auto** donc il attend une invitation de son voisin, qu'il reçoit d'ailleurs. Une fois recue, il active le trunk et répond au switch A;
- le lien Trunk entre les 2 switches est monté

**Note**
**Il est conseillé de désactiver le DTP et de forcer le lien Trunk entre 2 switches.**

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

## VTP

Le protocole VTP (Vlan Trunk Protocol) réduit la gestion dans un réseau commuté. Quand vous configurez un nouveau VLAN sur un serveur VTP, le VLAN est distribué par tous les commutateurs dans le domaine. Ceci réduit la nécessité de configurer le même VLAN dans tous les switches.
VTP est un protocole propriétaire de Cisco qui est disponible sur la plupart des produits de la gamme Cisco Catalyst.

**Le switch possède 3 modes VTP : client, transparent ou server (actif par défaut) :**

**VTP Server**
Le switch en mode Server permet à l'administrateur de faire toute modification sur les vlan et de propager automatiquement ses modifications vers tous les switches du réseau.

- Crée des vlan
- Supprime des vlan
- Modifie des vlan
- Envoi et transmet des messages VTP
- Se synchronise avec les autres switches du même domaine VTP

**Le Serveur VTP est le mode par défaut.**

### VTP Client

Le switch en mode *Client* **ne permet pas** à l'administrateur de faire des modifications sur les VLAN. Un message d'erreur apparait lorsque vous essayez de créer un VLAN.

- Ne peut pas créer de vlan
- Ne peut pas supprimer des vlan
- Ne peut pas modifier des vlan
- Traite les messages reçus et les transmet aux voisins
- Se synchronise avec les autres switches du même domaine VTP

### VTP Transparent

Le switch en mode *Transparent* permet à l'administrateur de faire toute modification sur les VLAN en **local uniquement** et donc **ne propage pas** ses modifications vers tous les switches du réseau.

- Crée des vlan
- Supprime des vlan
- Modifie des vlan (le nom par exemple)
- Ne traite pas les messages reçus mais transmet des messages VTP
- Ne se synchronise pas avec les autres switches du même domaine VTP

### MOT DE PASSE VTP

Si vous configurez un mot de passe pour le VTP, vous devez configurer le mot de passe sur tous les commutateurs dans le domaine VTP. Le mot de passe doit être le même mot de passe sur tous ces commutateurs. Le mot de passe VTP que vous configurez est traduit par algorithme dans un mot de 16 octets (valeur MD5) qui est porté dans tous les paquets VTP d'annonce résumée.

## Pruning VTP

Le pruning VTP est une fonctionnalité permettant d'éliminer le trafic inutile.

**Explication**: imaginons qu'un switch reçoit les VLANs 1 et 2 mais qu'aucunes de ses interfaces appartiennent au VLAN 2. Lorsque le switch voisin lui enverra des trames du VLAN 2, ce switch les supprimera car aucune de ses interfaces appartiennent à ce VLAN. Il est donc inutile que le switch voisin lui envoi du trafic pour le VLAN 2.

On active alors la fonction VTP pruning pour avertir le switch voisin de ne pas lui envoyer de trafic pour ce VLAN. La fonction s'active à partir du switch Server.

## Configuration VTP

Il y a 5 étapes pour la configuration VTP :

- Configurez le serveur VTP.
- Configurez le nom de domaine et le mot de passe VTP.
- Configurez les clients VTP.
- Configurez les VLAN sur le serveur VTP.
- Vérifiez que les clients VTP ont reçu les nouvelles informations VLAN.

### Le protocole MVRP (anciennement GVRP)

La création dynamique des vlan et l'affectation dynamique des ports se fait via le protocole MVRP (Multiple VLAN Registration Protocol – 802.1ak). Si le protocole est activé, tous les ports participent.

Le protocole MVRP est fourni spécifiquement pour la diffusion automatique des informations relatives à l'appartenance aux VLAN entre les ponts compatibles VLAN.

Le protocole MVRP permet aux ponts compatibles VLAN d'apprendre automatiquement l'adressage des ports VLAN sans avoir à configurer individuellement chaque pont et à enregistrer l'appartenance à un VLAN.

**Exemple de Configuration**

```
(config)# mvrp global
(config)# interface FastEthernet 1/1
```

(config-if)# mvrp
**Définition du mode choisi pour les interfaces**
(config)# interface FastEthernet 1/1
(config-if)# mvrp registration normal
**L'apprentissage MAC automatique n'est pas activé par défaut.**
(config)# mvrp mac-learning auto
**Pour créer dynamiquement des VLAN, il faut configurer le matériel en mode transparent.**
(config)# vtp mode transparent
(config)# mvrp vlan create

## Optimiser et sécuriser les LAN

### Etherchannel

Etherchannel est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet **identiques** en un seul lien logique.

Le but est d'**augmenter la vitesse** et la **tolérance aux pannes** entre les commutateurs, les routeurs et les serveurs. Elle permet également de simplifier une topologie Spanning-Tree en diminuant le nombre de liens.

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.

L'IEEE a publié le standard **802.3ad**, qui est une version ouverte de Etherchannel.

## Configuration Cisco

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

**Statique**
**Dynamique**, via un protocole qui négocie l'agrégation :

1. Port Aggregation Protocol (PAgP)
2. Link Aggregation Control Protocol (LACP).

## Etherchannel et IEEE 802.3ad

- Etherchannel est un protocole propriétaire de Cisco, alors que 802.3ad est un standard ouvert.
- Etherchannel nécessite de configurer précisément le commutateur, alors que 802.3ad n'a besoin que d'une configuration initiale.
- 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.
- Etherchannel peut être configuré automatiquement à la fois par LACP et par PAgP, tandis que 802.3ad ne peut l'être que par LACP.

> La configuration des paramètres Duplex, vitesse, Spanning-Tree, Access ou Trunk doivent être identiques sur les interfaces physiques du channel-group et l'interface Port-Channel.

| Interface A | Interface B | Protocole |
|---|---|---|
| `Desirable` | `Desirable` | PAgP |
| `Desirable` | `Auto` | PAgP |
| `Active` | `Active` | LACP |
| `Active` | `Passive` | LACP |

Tableau des valeurs

## Etherchannel en mode trunk

### Configuration d'un etherchannel dans un environnement de vlan

**Activer LACP sur un switch niveau 2**

Sw2(config)#interface range gigabitEthernet 0/1 – 2
Sw2(config-if-range)#channel-group 1 mode active
Sw2(config-if-range)#channel-protocol lacp (facultatif)
Sw2(config)#interface port-channel 1
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#no shutdown

**Activer LACP sur un switch niveau 3**

Sw3(config)#interface range gi0/1 – 2
Sw3(config-if-range)channel-group 1 mode passive (ou active)
Sw3(config-if-range)switchport trunk encapsulation dot1q
Sw3(config-if-range)switchport mode trunk
Sw3(config-if-range)switchport mode nonegociate (désactive DTP si besoin)

**Vérifier etherchannel**

show etherchannel summary

## CISCO Virtual Switching System (VSS)

VSS est une technologie de clustering qui permet de regrouper deux switch Catalyst CISCO 4500 (ou 6500) en un seul commutateur virtuel.
Dans un VSS, le plan de données des deux commutateurs en cluster est actif en même temps dans les deux châssis.
Les membres VSS sont connectés par des liaisons de commutation virtuelles (VSL) à l'aide de connexions Gigabit Ethernet standard ou 10 Gigabit Ethernet entre les membres VSS.
Les VSL peuvent transporter un trafic utilisateur régulier en plus de la communication du plan de contrôle entre les membres VSS.

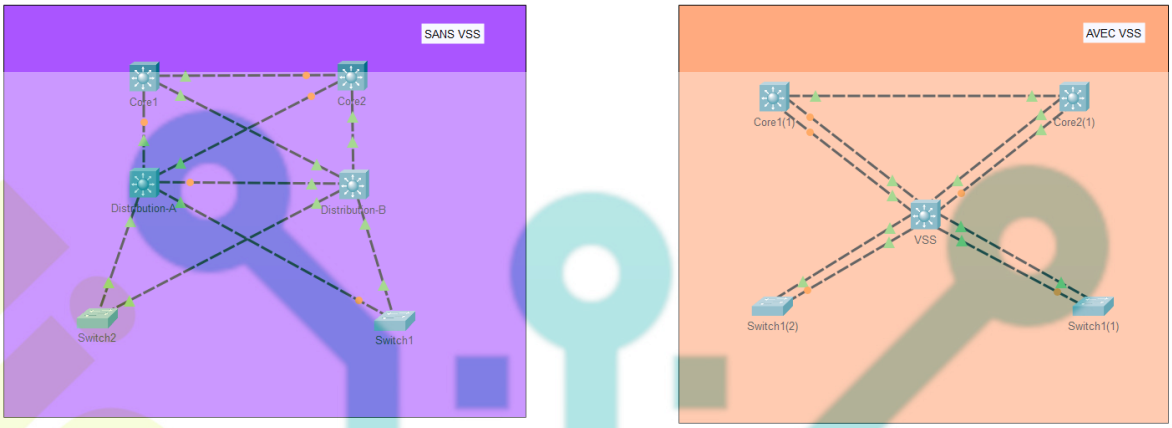


Schéma VSS

## Architecture VSS

Les deux commutateurs sont reliés par au moins deux liens agrégés 10G. On appelle cette connexion lien VSL (Virtual Switch Link).

Il est conseillé de configurer un troisième lien réservé à la détection de scénario actif/actif. Ce scénario peut se produire si la connexion du lien VSL est rompue.

### Activation du mode VSS

**Switch 1**

```
Sw-1(config)#switch virtual domain 100
Sw-1(config-vs-domain)# switch 1
```

**Switch 2**

```
Sw-2(config)#switch virtual domain 100
Sw-2(config-vs-domain)# switch 2
```

### Configuration des deux interfaces 10G utilisées pour le lien VSL

**Switch 1**

```
Sw-1(config)# interface port-channel 1
Sw-1(config-if)# switchport
Sw-1(config-if)# switch virtual link 1
Sw-1(config-if)# no shut
```

**Switch 2**

```
Sw-2(config)# interface port-channel 2
Sw-2(config-if)# switchport
Sw-2(config-if)# switch virtual link 2
Sw-2(config-if)# no shut
```

**Configuration du port-channel sur les liens dédiés VSL.**

```
Switch 1
Sw-1(config)# interface range tengigabitethernet 1/1-2
Sw-1(config-if)# channel-group 1 mode on
Switch 2
Sw-2(config)# interface range tengigabitethernet 1/1-2
Sw-2(config-if)# channel-group 2 mode on
```

**Conversion des deux switches en mode VSS**

```
Switch 1
Sw-1# switch convert mode virtual
Switch 2
Sw-2# switch convert mode virtual
```

Il n'y a maintenant plus qu'un seul fichier de configuration. Les interfaces sont nommées ainsi:
**numéro du switch/numéro du module/numéro du port.**

**Vérification après redémarrage du switch**

```
Switch-VSS#show switch virtual
Switch-VSS#show switch virtual role
```

## Détection d'un mode actif/actif

Si le lien VSL est coupé, un système de détection de l'état des deux switches qui composent le VSS doit être mis en place pour éviter que les deux switches soient actifs en

même temps.

Il y a plusieurs possibilités pour détecter cette situation:

- Lien fast-hello,
- Bidirectional Forwarding Detection (BFD)
- Lien etherchannel PAgP.

Lors de la détection d'un scénario actif/actif, l'ancien switch actif désactive ses interfaces ainsi que les instances de routage et de spanning tree. L'ancien switch passif reste donc le seul actif sur le réseau.

### Mise en place d'un lien fast-hello

Un lien doit être dédié pour le système fast-hello.
Si le lien VSL est tombé et si le lien fast-hello est toujours opérationnel, un scénario actif/actif est détecté.

```
Switch-VSS(config)# switch virtual domain 100
Switch-VSS(config-vs-domain)# dual-active detection fast-hello
Switch-VSS(config)# int gi1/2/2
Switch-VSS(config-if)# dual-active fast-hello
Switch-VSS(config)# int gi2/2/2
Switch-VSS(config-if)# dual-active fast-hello
Vérification
```

### Vérification

```
Switch-VSS#sh switch virtual dual-active fast-hello
```

### Connexion d'un commutateur au switch VSS

Pour assurer la haute disponibilité, le commutateur sera connecté au deux routeurs physiques. Les deux interfaces seront configurées avec le protocole LACP.

NB : la configuration des interfaces agrégées avec LACP doit être identique. une fois les deux interfaces configurées en agrégation de lien, il faudra entrer les commandes de configuration des interfaces sur l'interface port-channel et non sur les interfaces physiques.

### Configuration du switch VSS

```
Switch-VSS(config)# int gi1/4/2
Switch-VSS(config-if)# channel-group 10 mode active
Switch-VSS(config)# int gi2/4/2
Switch-VSS(config-if)# channel-group 10 mode active
Switch-VSS(config-if)# int port-channel 10
Switch-VSS(config-if)# switchport mode trunk
```

### Configuration du switch d'extrémité

```
Switch-2960(config)# int gi1/0/49
Switch-2960(config-if)# channel-group 1 mode passive
Switch-2960(config)# int gi2/0/49
Switch-2960(config-if)# channel-group 1 mode passive
Switch-2960(config-if)# int port-channel 1
Switch-2960(config-if)# switchport mode trunk
```

### Vérification:

```
Switch-VSS#show etherchannel summary
```

### Résumé

- Etherchannel regroupe plusieurs liaisons commutées pour équilibrer la charge sur des chemins redondants entre deux périphériques. Tous les ports d'un Etherchannel doivent avoir la même vitesse, les mêmes paramètres de duplex et les mêmes informations VLAN sur toutes les interfaces des périphériques aux deux extrémités.

PAgP est un protocole propriétaire de Cisco qui facilite la création automatique de liens Etherchannel.
LACP fait partie d'une spécification IEEE qui permet également de regrouper plusieurs ports physiques dans un canal logique. Les modes LACP sont LACP actif et LACP passif.
Le PAgP et le LACP n'interagissent pas.

- L'empilement de commutateurs permet de configurer jusqu'à neuf commutateurs Catalyst 3750 et de les présenter au réseau comme une seule et même entité. STP considère la pile de commutateurs comme un commutateur unique. Cet avantage supplémentaire permet de garantir le diamètre maximal recommandé de sept commutateurs selon l'IEEE.
- Le principe de VSS est d'associer deux switches Cisco catalyst 4500 ou 6500 physiques pour qu'ils forment un switch virtuel. Il n'y a qu'un seul fichier de configuration.
  Un seul des deux commutateurs contrôle le management, la supervision et le routage. Ce switch est appelé le commutateur actif. L'autre switch étant en mode standby à ces niveaux. Par contre, les deux commutateurs sont actifs sur le plan de la commutation.
  L'avantage principal est la haute disponibilité. Les switches d'extrémités sont connectés à chacun des routeurs via deux liens agrégés configurés en port-channel. Ainsi, les deux liens sont actifs et si un des liens tombe, le temps de convergence est beaucoup plus rapide qu'avec l'utilisation du protocole spanning-tree. On garde quand même le protocole spanning tree actif sur les matériels.
  La haute disponibilité du routage est assurée sans l'usage des protocoles VRRP ou HSRP. On gagne donc aussi en temps de configuration au niveau du routage.
  La supervision est également simplifiée puisqu'il n'y a plus qu'un seul fichier de configuration pour deux switchs configuré en VSS.