

Atelier Réseaux

I. Configurez les paramètres de base du commutateur

Commandes	Rôles	Commentaires
Enable	Mode d'exécution privilégié	
Conf t	Refléter le mode de configuration globale	
Hostname s1	Le nom d'hôte du commutateur	
service password-encryption	Le cryptage du mot de passe	
enable secret class	Mot de passe secret pour l'accès en mode EXEC privilégié	
no ip domain-lookup	Désactiver la recherche DNS indésirable	
banner motd # message #	Une bannière MOTD.	
interface vlan 1 ip address 192.168.1.2 255.255.255.0 no shutdown	Configuration de l'adresse IP de l'interface SVI du commutateur	
ip default-gateway 192.168.1.1	Configuration de la passerelle par défaut	
line con 0 password cisco login logging synchronous	Limiter l'accès au port de console	
line vty 0 15 password cisco login	Configuration des lignes de terminal virtuel (vty) de telle sorte que le commutateur autorise l'accès à Telnet.	
ping 192.168.1.2	Teste de la connectivité de bout en bout	
telnet 192.168.1.2	Vérification la gestion à distance de S1	
copy running-config startup-config	Enregistrement le fichier de configuration en cours du commutateur	

II. Gestion de la table d'adressage MAC

Commandes	Rôles	Commentaires
show mac address-table	Affichage des adresses MAC	
show mac address-table ?	Énumération des options	
show mac address-table dynamic	Affichage des adresses MAC acquises de façon dynamique.	
clear mac address-table dynamic	Supprimer les adresses MAC existantes	
mac address-table static 0050.56BE.6C89 vlan 1 interface fastethernet 0/6	Configuration d'une adresse MAC statique	
no mac address-table static 0050.56BE.6C89 vlan 1 interface fastethernet 0/6	Suppression de l'entrée MAC statique	

III. Configuration de la sécurité des ports

Commandes	Rôles	Commentaires
interface range f0/1 – 4 shutdown	Arrêt des ports physiques non utilisés sur le commutateur	
interface f0/6 shutdown switchport port-security switchport port-security maximum 1 switchport port-security mac-address xxxx.xxxx.xxxx switchport port-security violation shutdown no shutdown end	Configuration du port du commutateur FastEthernet 0/6 de sorte qu'il accepte un périphérique uniquement, acquière les adresses MAC de ces périphériques de façon statique et désactiver le port en cas de violation.	

IV. Création du VLAN et attribution des ports de commutateur

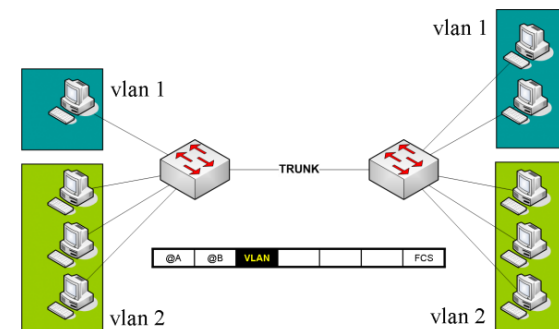
Commandes	Rôles	Commentaires
vlan 10 name Student	Création d'un VLAN	✓ la technologie actuelle des commutateurs ne nécessite plus l'exécution de la commande vlan pour l'ajout d'un VLAN à la base de données. En cas d'attribution d'un VLAN inconnu à un port, le VLAN s'ajoute à la base de données VLAN.
interface f0/6 switchport mode access switchport access vlan 10	Attribution d'un VLAN a une interface du commutateur	
interface vlan 1 no ip address interface vlan 99 ip address 192.168.1.11 255.255.255.0	Déplacez l'adresse IP de commutateur vers le VLAN 99 (de gestion)	
interface range f0/11-24 switchport mode access switchport access vlan 10	Attribution d'un VLAN à plusieurs interfaces	
interface range f0/11, f0/21 switchport access vlan 20	Réattribuer un VLAN à plusieurs interfaces	
interface f0/24 no switchport access vlan	Supprimer une attribution de VLAN de l'interface	
no vlan 30	Supprimez un ID de VLAN de la base de données VLAN	

V. Configuration d'un trunk 802.1Q entre les commutateurs

1. Trunk : Définition

Le trunk est le mécanisme qui permet d'**insérer l'identifiant du VLAN** sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN).

Dans ce schéma, on configure le lien inter-switch en Trunk. Toutes les trames qui sortiront sur ce lien (switch de droite ou de gauche), se verront appliquer une étiquette supplémentaire qui contient l'identifiant du VLAN (en **noir** sur la trame).



2. Le protocole DTP : Définition

DTP pour Dynamic Trunking Protocol, c'est un protocole propriétaire Cisco donc ne fonctionne qu'entre switchs 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.

Un port physique d'un switch peut avoir plusieurs état (ou mode) concernant le DTP.

Grâce au tableau ci-dessus, on voit que selon l'état choisi, le port *"souhaite"*, *"impose"* ou *"interdit"* de monter un trunk

Mode	Fonction
Dynamic Desirable	Annonce sa volonté de monter en trunk (négociation)
Dynamic Auto	Attends une sollicitation du voisin. Il n'envoie pas de requêtes mais répond aux requêtes d'en face
Trunk (on)	Le switch se met en mode trunk automatiquement et en informe le switch voisin
Nonegotiate	Le switch se met en mode trunk automatiquement sans en informer le switch voisin
Off	Désactivation du Trunk
Access	Désactivation du Trunk et prévient le 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

3. types de VLAN

- **VLAN de données**

Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN acheminant du trafic de voix ou de gestion ne peut pas faire partie d'un VLAN de données. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données. Un VLAN de données est parfois appelé un VLAN utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.

- **VLAN par défaut**

Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1.

Le VLAN 1 dispose de toutes les fonctions de n'importe quel VLAN, à l'exception du fait qu'il ne peut pas être **renommé** ni **supprimé**. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.

- **VLAN natif**

Un réseau local virtuel natif est affecté à un port trunk 802.1Q. Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN. Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »). Le trafic étiqueté est appelé ainsi en référence à l'étiquette de 4 octets ajoutée dans l'en-tête de trame Ethernet originale et spécifiant le VLAN auquel la trame appartient. Le port trunk 802.1Q place le trafic non étiqueté sur le VLAN natif, qui par défaut est le VLAN 1.

Les VLAN natifs sont définis dans la spécification IEEE 802.1Q pour assurer la compatibilité descendante avec le trafic non étiqueté qui est commun aux scénarios LAN existants. Un VLAN natif sert d'identificateur commun aux extrémités d'une liaison trunk.

Il est généralement recommandé de configurer le VLAN natif en tant que VLAN inutilisé, distinct du VLAN 1 et des autres VLAN. En fait, il n'est pas rare de dédier un VLAN fixe jouant le rôle de VLAN natif pour tous les ports trunk du domaine commuté.

- **VLAN de gestion**

Un VLAN de gestion est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion d'un commutateur. Le VLAN 1 est le VLAN de gestion par défaut. Pour créer le VLAN de gestion, l'interface virtuelle du commutateur (SVI) de ce VLAN se voit attribuer une adresse IP et un masque de sous-réseau, ce qui permet de gérer le commutateur via HTTP, Telnet, SSH ou SNMP. Sachant que la configuration initiale d'un commutateur Cisco utilise le VLAN 1 par défaut, il n'est pas judicieux de le choisir comme VLAN de gestion.

Commandes	Rôles	Commentaires
interface fa0/1 switchport mode trunk switchport trunk native vlan 99 no shutdown	imposer le trunking	
interface f0/1 switchport mode dynamic desirable	Utilisez le protocole DTP pour initier le trunking : Configuration de manière à négocier le mode trunk	

4. Le protocole VTP

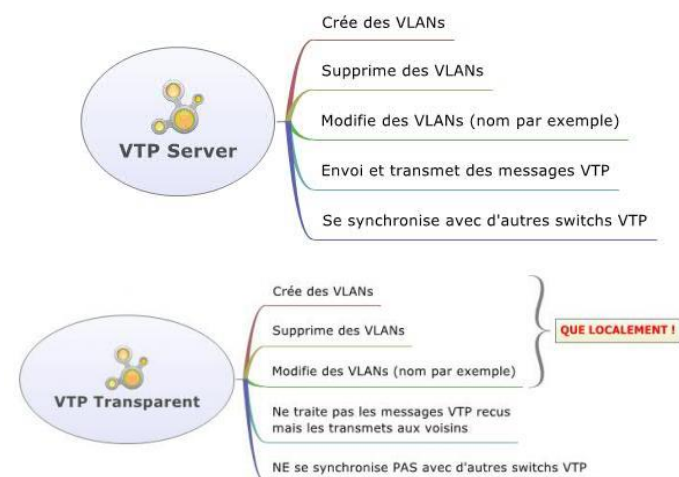
Fonctionnement :

Les messages VTP diffuse des annonces de création, de suppression ou de modification de VLAN. Cette diffusion s'effectue à travers tous les switchs grâce à une trame niveau 2 avec une adresse de destination MAC multicast bien particulière qui est 01-00-0C-CC-CC-CC.

Architecture du VTP :

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

- VTP Server: switch qui crée les annonces VTP
- VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP
- VTP Transparent: switch qui ne traite pas les annonces VTP



Configuration et vérification du protocole VTP

Commandes	Rôles	Commentaires
vtp mode server vtp domain CCNA vtp password cisco	Configurez S1 en tant que serveur VTP dans le domaine CCNA avec le mot de passe cisco	
vtp mode client vtp domain CCNA vtp password cisco	Configurez S2 en tant que client VTP dans le domaine VTP CCNA avec le mot de passe VTP cisco.	
vtp domain CCNA vtp password cisco	Configurez S3 de sorte qu'il soit dans le domaine VTP CCNA avec le mot de passe VTP cisco.	Le commutateur S3 restera en mode VTP transparent (par défaut)
vtp mode transparent	Modifier en mode transparent	

5. Le protocole STP :

Commandes	Rôles	Commentaires
show spanning-tree	Affichage des informations du mode Spanning Tree	
spanning-tree vlan 1-100 port-priority 1*4096		
spanning-tree vlan vlan_id root primary/secondary		
interface fa0/6 spanning-tree portfast	Configuration de PortFast	
interface fa0/6 spanning-tree bpduguard enable	Configuration de la protection BPDU	

6. configuration d'EtherChannel

Commandes	Rôles	Commentaires
interface range f0/3-4 channel-group 1 mode desirable no shutdown	Configurez les ports sur S1 avec l'option desirable mode PAgP	
interface range f0/3-4 channel-group 1 mode auto no shutdown	Les ports sur S3 avec l'option auto mode PAgP	

show run interface f0/3	Taatik el groupe	
show interfaces f0/3 switchport	Plus d'info sur f0 /3 -> plus d'info aal groupe	
interface port-channel 1 switchport mode trunk switchport trunk native vlan 99	Configuration d'un trunk sur un portChannel	
interface range f0/1-2 S1 switchport mode trunk switchport trunk native vlan 99 channel-group 2 mode <u>active</u> no shutdown	Configurez LACP sur S1	
interface range f0/1-2 switchport mode trunk switchport trunk native vlan 99 channel-group 2 mode <u>passive</u> no shutdown	Configurez LACP sur S1	
show etherchannel summary	Vérifiez que les ports ont été agrégés.	

7. configuration de HSRP

Commandes	Rôles	Commentaires
tracert 209.165.200.225	Envoyez une commande tracert a partir d'un pc	209.165.200.225 -> l'adresse de bouclage
ping -t 209.165.200.225	Démarrez une session ping	Ctrl+C
interface g0/1 standby version 2 standby 1 ip 192.168.1.254 standby 1 priority 150 standby 1 preempt	Configurer HSRP R1 devient le routeur actif	Par défaut priorité = 100
interface g0/1 standby version 2 standby 1 ip 192.168.1.254	Configurer HSRP	
show standby	Vérifiez HSRP	
show standby brief		

Vérifications :

Commandes	Rôles
show running-config	Le fichier de configuration en cours d'exécution
show startup-config	Le fichier de configuration initiale dans la mémoire vive non volatile
show interface vlan1	Les caractéristiques de l'interface SVI du VLAN 1.
show ip interface vlan1	Les propriétés IP de l'interface SVI du VLAN 1.
show version	Les informations relatives à la version de Cisco IOS du commutateur
show interface f0/6	Les propriétés de l'interface FastEthernet
show flash dir flash	Le contenu du répertoire flash
show run	La totalité de la configuration en cours
show mac address-table	Les adresses MAC
show mac address-table ?	Les options de la table d'adresses MAC
show mac address-table dynamic	Adresses MAC acquises de façon dynamique
show portsecurity interface	Vérifiez la sécurité des ports
show vlan show vlan brief	La liste des VLAN
show interface trunk	Les interfaces en mode trunk
show vtp status	Vérifier que le mode et le domaine VTP sont bien configurés
show vtp password	vérifier le mot de passe VTP