CHAPITRE 1: les réseaux commutés

LAN: il ont pensé au lan car le monde devient plus complexe et ce réseau va assurer l'intégration facile des services(il est sécurisé ,stable et disponible)/il est un réseau sans frontière (quelque soit la localisation de destination final on est capable de consommer le service)/accessible par tous les users/via les couches accès/distribution/réseau

les 4 critères de création d'un réseau sans frontière:

1-hiérarchique(pour identifier le rôle de chaque équipement et son emplacement)/2-Modularité:n'est pas fixe il est extensible/3-Resilience:assurer une haute disponibilité/4-Flexibilité:partages de charge entre les équipent

les couches:

Accès:la plus proche de user lui permet de se connecter(peut être sans fil ou filaire)

Distribution: permet d'acheminer le trafic /interface entre l'accès et le réseau/au niveau de ce couche on définit les vlans/organisé par vlan pour bien acheminer le trafic

Coeur de Réseau:connecté avec réseau de fait ou le réseau est externe /le débit dans cette couche doit être assez performant

⇒ **hiérarchie du réseau lan permet de:** assurer la qualité de service/la sécurité/la connexion peut être sans fil ou filaire et supporte les nouvelles technologies

⇒ le commutateur ne comprend pas les adresses ip il prend la décision pour commuter une trame via l'@ mac(car il est niveau 2)/donc il commute une trame en prenant en considération le port d'entrée et l'@mac/il connaît le port lequel il est

connecté la destination via le tabla mac(feha les @mac et les ports)==>auto apprentissage ou dynamique(il fait correspondance entre les ports et @ mac wa7do sans aide pour remplir table mac)/ou bien statique(l'admin va affecter la machine au port concerné)/dynamique est le mode par défaut il se fait chaque 5 minutes

⇒ si la source ne trouve pas l'adresse mac de destination il fait du broadcast càd il diffuse sur tous les ports sauf le port source(lui même)

Comment la switch va transférer les trames? il existe 2 façons:

1-Store and forward:exige que le switch récupère toute la trame ethernet en local et vérifie si la trame feha des erreurs ou non (checksum)et si la trame est correcte il commence la transfert/necessite le buffering(une mémoire temporaire pour stocker les info)/les inconvénient de cette méthode:lente/les avantages:stable et trame correcte envoyé

2-cut through:une fois le switch reçoit les 2 premier champs (@mac de destination)il commence le transfert sans faire la vérification/il est rapide mais il peut envoyer des trames erronés/pour remedier au probleme d'envoi des trames erronés il utilise le mode fragment free(envoyer les trames après 64 octets pour vérifier qu'il nya pas de collisions)

Communication entre 2 switches:tha9afa 3ama ma3ana manendbo beha

1-communication full duplex:faire l'envoi et la réception simultanément

2-communication hard duplex: soit envoyer soit recevoir

==>Domaine de collision:2 trames endommagé car ils sont envoyés sur le même support physique au même temps d'ou il ya un signal bruit d'où on doit avoir un arbitre qui va gérer cette communication qui est le switch (concentrateur) c lui qui va ségmenter les domaines de collision en les séparant d'où chaque interface de switch va être un domaine de collision.

⇒ **Domaine de diffusion:**une trame envoyé à tous le monde/le switch quand il reçoit une trame en diffusion il va la diffuser à tous les port car le switch ne peut pas arrêter la diffusion d'où c le routeur (équipement niveau 3)qui peut arrêter et diviser les domaine de diffusion

⇒ kol manzid switches kol mayzid f paquets envoyé en diffusion w la solution c le routeur

⇒ fl collision le switch haja positif mais fl diffusion howa haja négatif

Atelier Réseaux

I. Configurez les paramètres de base du commutateur

⇒ les interfaces de routeurs peuvent avoir des @ip d'où l'accès à distance est garantit en activant les lignes vty

==>on ne peut pas attribuer une @ ip à un interface du commutateur d'où l'accès à distance est non possible et pour remédier à ce problème on crée des interfaces virtuelles(SVI) et on les affecte au switch pour assurer sa gestion (interface de gestion:VLAN)

⇒ l'adresse de passerelle ou gateway est importante à la configurer dans le cas ou le switch va être géré à partir d'un autre réseau distant

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. Configuration de la sécurité des ports

⇒ très importante sur les réseaux sans frontière

⇒ une fois on connecte un pc et switch via un câble les boutons vont être verts cad la connexion est établie car le switch ne fait pas un contrôle il ne vérifie pas qui est en train d'accéder pour cela on fait la partie de sécurité des ports

⇒ les ports de switch sont toujours actif

⇒ **violation**: une machine non connus veut se connecter sur ce port

⇒ on remarque qu'il ya une violation au cas ou le nombre des @mac autorisés à se connecter à un port donné est dépassé/ou si une machine qui est autorisé à se connecter vient de se connecter via 2 ports différents pour cela on peut faire soit Protect soit Restrict soit shutdown (a7sen wahda shutdown car elle va arrêter l'interface mouch ki lokhrin juste yblokiw l'accès)==> différence entre restrict w protect c que restrict yab3ath des notifications de syslog ===> en cas de violation le port devient désactivé cad en mode shutdown

la sécurité des ports se fait de 3 façons : sécurité des @ mac

1-en mode statique

Commandes	Rôles	Commentaires
interface range f0/1 – 4 shutdown	Arrêt des ports physiques non utilisés sur le commutateur	
interface f0/6 shutdown switchport mode access switchport port-security switchport port-security maximum 1 switchport port-security mac-address xxxx.xxxx.xxxx switchport port-security violation shutdown no shutdown end	premièrement on désactive l'interface activer l'accès à l'interface activer la sécurité du port 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.	

2-en mode dynamique

S1(config)#interface fastethernet 0/18	identifier l'interface
S1(config-if)#switchport mode access	autoriser l'accès au niveau de cette interface pour pouvoir envoyer du

	trafic
S1(config-if)#switchport port-security	activer la sécurité des ports

3-en mode sticky

Commandes	Rôles	Commentaires
interface range f0/1 – 4 shutdown	Arrêt des ports physiques non utilisés sur le commutateur	
interface f0/6	kifkif	
switchport mode access Switchport mode access Switchport port-security Switchport port-security maximum 1 Switchport port-security mac-address sticky Switchport port-security violation shutdown no shutdown end		

===> show port-security interface : pour vérifier la sécurité du port

⇒ sauf les modes sticky et static récupèrent les @mac des machines explicitement mais dans le mode dynamique les @mac sont récupéré implicitement cad automatiquement

III. Gestion de la table d'adressage MAC d'une manière statique(par défaut il se remplit dynamiquement on va le remplir statiquement)

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.	
show mac address-table static	Affichage des adresses MAC acquises de façon statique.	
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	

CHAPITRE 2: VLAN: virtual local area network dans le LAN et le TRUNK

⇒ c le routeur qui permet de diviser un rx en sous rx ⇒ une segmentation physique

-vlan: c le faite de ségmenter un rx ip en des sous réseaux virtuelles l'un distant de l'autre à travers des switches car les routeurs sont coûteux ⇒ segmentation logique

Avantages des vlan: moins coûteux /amélioration de sécurité séparation de flux kol vlan ala rouo/meilleure performance/etc....

1. types de VLAN

- **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 ou par défaut 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 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. il est créé par l'administrateur pour permettre l'échange des informations

- **VLAN natif**
  permet d'acheminer les informations ou le trafic non tagué , il est par défaut est le VLAN 1. mais il est modifiable

  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(ses configurations). Le VLAN 1 est le VLAN de gestion par défaut.aussi il va permettre l'accès à distance au switch pour le configurer. il est modifiable 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.

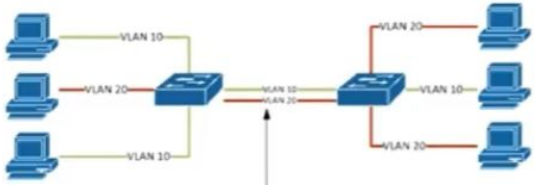
IV. Création du VLAN et attribution des ports de commutateur

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. **range de vlan: de 1==>1005** **⇒ au début on trouve le vlan1 et 1002==>1005 cad 5 vlan par défaut**
interface f0/6 switchport mode access switchport access vlan 10	Attribution d'un VLAN à 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(svi) de vlan 1 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	

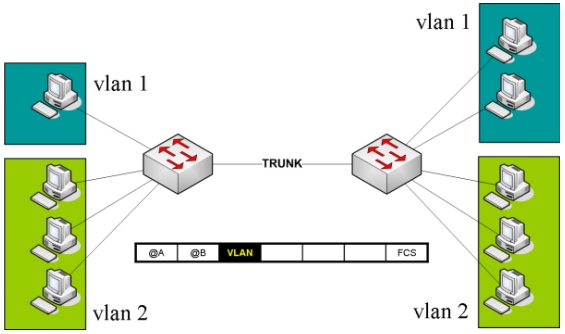
interface f0/24 no switchport access vlan	Supprimer une attribution de VLAN de l'interface	**Dans ce cas l'interface va être affecté au vlan par défaut**
no vlan 30	Supprimez un ID de VLAN de la base de données VLAN	**Les informations liés aux vlan sont stockés dans un fichier nommé flash:vlan:dat**

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

2. Trunk : Définition



(si on a 10 vlan il faut 10 liaison et c trop pour le switch alors le trunk est la solution cad une seule liaison partagé par tous les vlan)



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).

Dans le trunk on parle de l'encapsulation 802.1q et on va modifier au niveau de la trame ethernet car elle va

ajouter une tag ou étiquette

⇒ après avoir configuré les vlan et le trunk on va pouvoir contrôler les diffusion d'où chaque vlan est considéré comme domaine de diffusion séparé de l'autre

⇒ quand on a un trafic non tagué (cad il n'appartient à aucun vlan) dans ce cas il va circuler sur le vlan natif

==>trunk=aggregation

⇒ Remarque importante: une trame tagué n'a pas le droit de circuler sur un vlan natif

⇒ les ports connecté aux terminaux(aux pc) vont être en mode access(acheminement)

⇒ il y a 2 méthodes pour activer le trunk soit statiquement explicitement avec une commande donné soit avec le **DTP**

⇒ si on a un switch qui n'est pas cisco on utilise le mode statique

3. Le protocole DTP : Définition

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

Il est un protocole de négociation

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 ne 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.

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

Quelque a remarque liés aux tableau ci dessus:

switchport mode access: supporte uniquement le flux qui provient d'un seul vlan==>mode non trunk(access howa 3aks trunk) meme si le voisin en mode trunk il ne peut pas basculer vers le mode trunk car il est l'inverse de trunk

dynamic auto:mode par défaut sur les interfaces internet

nonegotiate: désactiver les négociation sur les interface alors si le voisins n'est pas cisco je dois arrêter les négociation car l'interface voisin ne peut pas supporter ce flux

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

? = limited connectivity=access+truk car il sont 2 modes contradictoires

access+ ay mode= access (sauf avec trunk=limited)

desirable +ay mode sauf access=trrunk

trunk+ay mode sauf access=trrunk

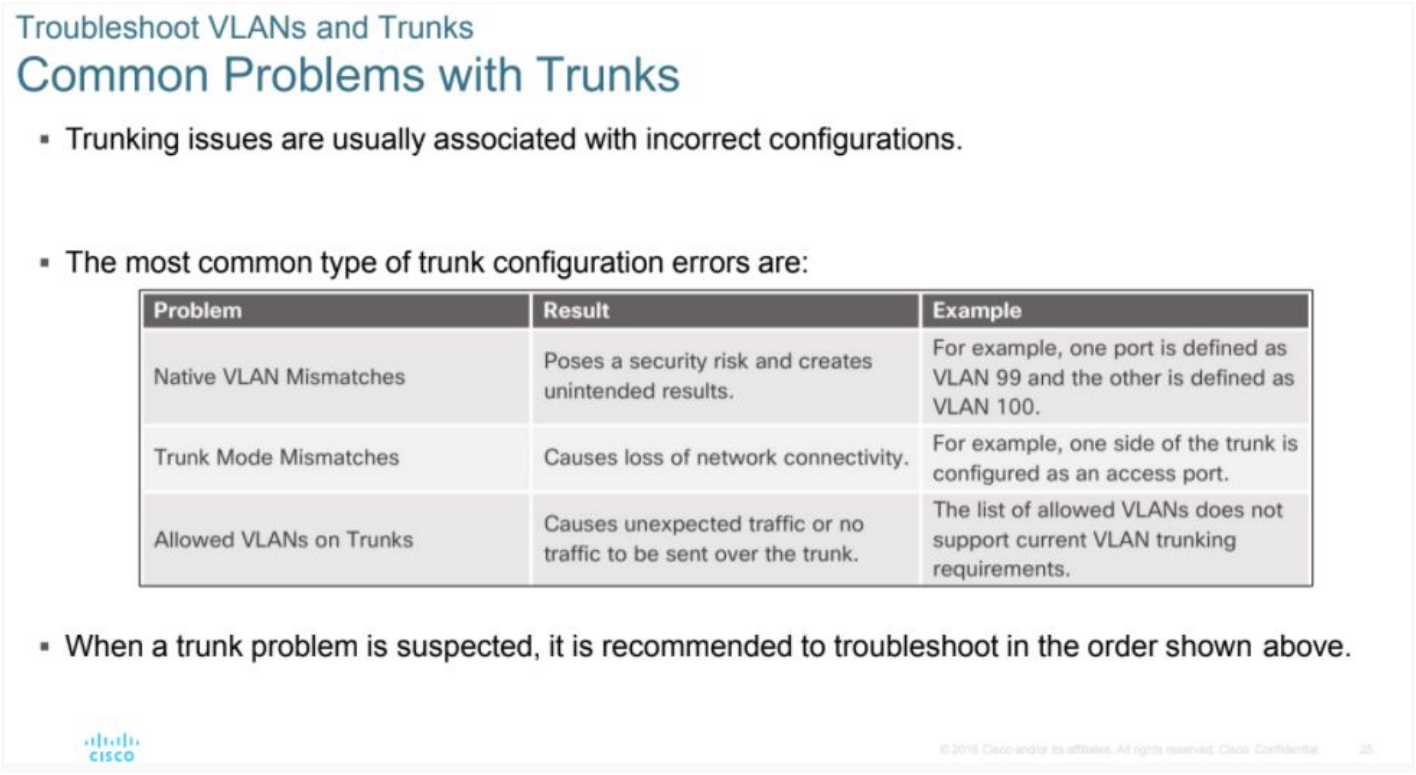
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	?
Access	Access	Access	?	Access

Commandes	Rôles	Commentaires
interface fa0/1 switchport mode trunk switchport trunk native vlan 99 no shutdown	imposer le trunking statiquement et explicitement 99 est le vlan native pour les trames non tagués	
interface f0/1 switchport mode dynamic desirable	**Utilisez le protocole DTP(dynamique) pour initier le trunking :** Configuration de manière à négocier le mode trunk	
no switchport trunk native vlan	réinitialiser le vlan natif par défaut	To configure the allowed VLANs for a virtual Ethernet interface, use the **switchport trunk allowed vlan** command. To remove the configuration, use the **no** form of this command. **switchport trunk allowed vlan**
no switchport trunk allowed vlan	(voir commentaire)	
show vlan	voir la base des vlan	
show interface trunk	oir l'etat des interface en mode trunk	

⇒ Tous les périphériques d'un VLAN doivent faire partie du même réseau IP pour communiquer.(exemlpe zouz youfew b .10 sinon ynajmouch ycommunikiw)

⇒ diapo 24:Dans cet exemple, le VLAN natif doit être le VLAN 99 cependant, la sortie de la commande identifie le VLAN 2 comme

le VLAN natif. Pour résoudre ce problème, configurez le même VLAN natif sur les deux côtés.==> car lezem même vlan native w meme base de vlan



Troubleshoot VLANs and Trunks

Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations.
- The most common type of trunk configuration errors are:

Problem	Result	Example
Native VLAN Mismatches	Poses a security risk and creates unintended results.	For example, one port is defined as VLAN 99 and the other is defined as VLAN 100.
Trunk Mode Mismatches	Causes loss of network connectivity.	For example, one side of the trunk is configured as an access port.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic to be sent over the trunk.	The list of allowed VLANs does not support current VLAN trunking requirements.

- When a trunk problem is suspected, it is recommended to troubleshoot in the order shown above.

les problèmes rencontré : voir les derniers pages du chap2

Chapitre 3: VTP : VLAN TRUNKING PROTOCOL

4. Le protocole VTP

Fonctionnement :

Utilisé par l'administrateur pour faciliter la gestion des vlan

Problématique: imaginez qu'on a 10 vlan alors on 'est obligé de configurer les 10 vlan sur tous les switch(risque d'erreur)

solution: configurer le vtp sur un seul switch qui va prendre le rôle d'un serveur et va transmettre la base sur le reste des switch dynamiquement

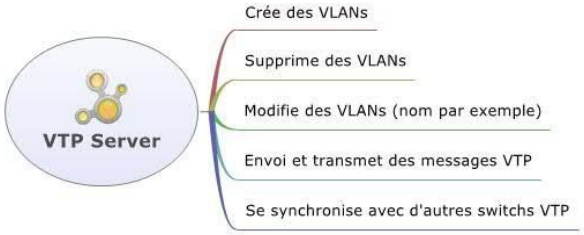
⇒ le passage de ce base doit être sur une liaison trunk alors il faut et c obligatoire d'activer le mode trunk dans la liaison entre les switchs

Les messages VTP diffusent des annonces de création, de suppression ou de modification de VLAN. Cette diffusion s'effectue à travers tous les switchs grâce à un équipement niveau 3, une trame niveau 2 avec une adresse de destination MAC multicast bien particulière qui est 01-00-0C-CC-CC-CC.

Les composants du VTP	Définitions
VTP Domain	pour chaque réseau on doit affecter un vtp domain qui peut être préciser à travers un équipement niveau 3 (routeur))
VTP advertisement	les messages envoyés par le vtp server à fin d'assurer la synchronisation et la distribution de la base des vlans (msg envoyé chaque 5 minute et compris que par les switch qui ont activé le vtp)
VTP modes	chaque switch a un role : server/client/transparent
VTP password	chaque vtp domain crée est protégé par un mot de passe

Architecture du VTP :

⇒ server et client sont obligatoire à faire mais transparent nn



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

- **VTP Server:** switch qui crée les annonces VTP/configurer les vlan qui vont être stocké dans la mémoire nvram/envoie des informations aux autres switches(advertisement)/on peut avoir plusieur vtp server sur le même réseau
- **VTP Client:** switch qui reçoit, se synchronise et propage les annonces VTP/fonctionne comme LE server sauf que la base des vlans est sauvegardé dans RAM cad f redemarrage donnés ydhi3o/attend vtp advertisement pour faire la mise à jour/participe à l'advertisement
- **VTP Transparent**: switch qui ne traite pas les annonces VTP/il reçoit l'advertisement mais il ne participe pas et ne prend pas en considération l'advertisement du serveur /mise à jour des vtp se fait en local manuellement/stockage en NVRAM /son rôle c faire des tests

VTP Advertisements

Ce sont les messages envoyés entre le serveur et le client et il existe 3 types:

***Summary advertisement:**msg contient le nom du domain du vtp et le numéro de révision et le mdp⇒ config de base du domain

***Advertisement request:**msg de réponse au cas où le client il dispose un numéro de révision supérieur à celui de serveur

***Subset advertisement:**msg qui contient des information sur la base des vlans

⇒ le vtp serveur et le vtp client doivent avoir le même numéro de révision et au cas ou le cas et contraire le client doit informer le serveur qu'il ne dispose le même numéro que lui/aussi meme domain et même mdp

⇒ et pour remédier à ce problème soit je change le domain name par un domain inexistant après nraja3 le domaine original ou soit je change le mode en transparent et après nraj3o fl mode mte3o lasleni

⇒ le numero de vtp transparent toujours = 0

=> nb vlan par défaut=5

⇒ exemple après faire config de 3 vlan le num revision=6(3 num vlan et 3 nom vlan)

⇒ le numéro de révision est par défaut 0 pour tout le monde il va s'incrémenter après avoir faire des configurations

⇒ le num de configuration ne prend pas en considération le config des mdp , il prend en considération que la config de gestion des vlans(ajout,modif ,suppression)

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)

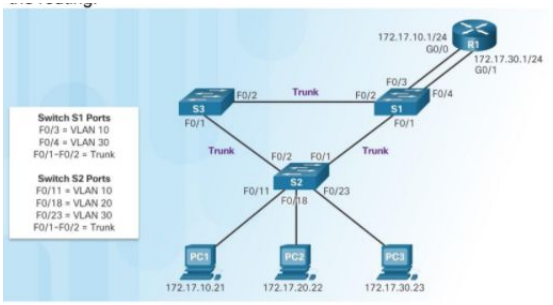
vtp mode transparent	Modifier en mode transparent	
show vtp status	verifier que le vtp est bien configué	

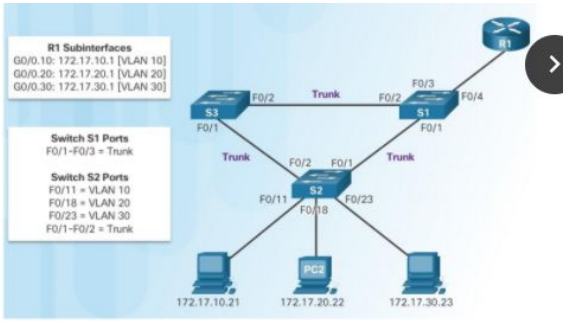
chapitre 4:Routage inter vlan

Problématique: si on a 2 PC qui appartiennent à 2 vlan différents alors ils ne peuvent pas communiquer

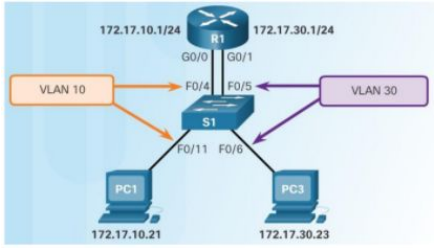
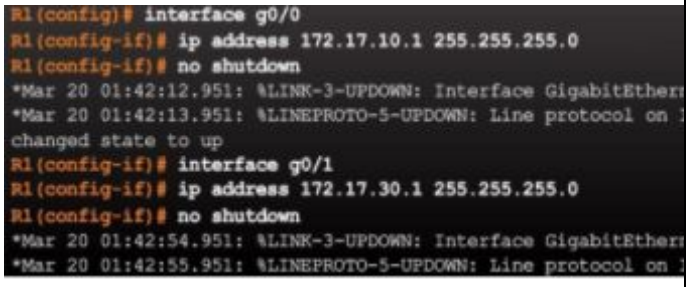
Solution: Routage inter vlan en utilisant un routeur(couche 3 du modèle osi) puisque le switch(niveau 2) ne peut pas assurer la communication entre les vlan

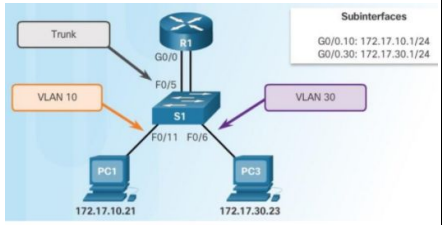
il existe 3 type de routage intervlan:1- Legacy inter-VLAN routing /2-Router-on-a-Stick /3-Layer 3 switching using SVIs

1- Legacy inter-VLAN routing: classique	Avoir 2 liaison physique est chaque liaison est dédié à un vlan donné(exemple liaison pour vlan 10 et vlan 30) mais le problème c qu e si on a 3 vlan alors le 3ème vlan ne puisse pas communiquer avec les pc d'autres vlan puisque le nb d'int dispo sur le routeur est limité ==>l les liaisons vont être en mode access car kol wehed lehi b un seul vlan	

2-Router-on-a-Stick : routage par sous interface	Avoir une seule liaison(mode trunk) pour tous les vlans en créant des sous interface logique cad virtuelle qui se base une seule interface physique exemple inte physique=G0/0 int logique G0/0.10 172.17.10.1pour vlan 10 G0/0.20 172.17.20.1 pour vlan 20 G0/0.30 172.17.30.1pour vlan 30 ils sont le gateway	

Configuration

1- Legacy inter-VLAN routing: classique 	1-Créer les vlans et attribuer chaque vlan à l'interface donné 2-Configurer les interfaces du routeurs par les @ du gateway(.1)	 

2-Router-on-a-Stick : routage par sous interface 	1-Créer la base des vlans et mettre l'interface lié à la switch en mode trunk 3-on crée un sous interface pour chaque vlan et on active le mode trunk sur chaque sous interface on écrivant encapsulation dot1q numvlan et on active l'interface physique ==>on peut aussi ajouter une sous interface pour les flux non tagué(native) lié au vlan 1 g0/10.1	S1(config)# vlan 10 S1(config-vlan)# vlan 30 S1(config-vlan)# interface f0/5 S1(config-if)# switchport mode trunk S1(config-if)# end S1# R1(config)# interface g0/0.10 R1(config-subif)# encapsulation dot1q 10 R1(config-subif)# ip address 172.17.10.1 255.255.255.0 R1(config-subif)# interface g0/0.30 R1(config-subif)# encapsulation dot1q 30 R1(config-subif)# ip address 172.17.30.1 255.255.255.0 R1(config)# interface g0/0 R1(config-if)# no shutdown *Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEth *Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEther *Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on changed state to up

Chapitre 5: STP:Spanning tree protocole

Problématique: redondance des chemins /tempête de diffusion/table mac instable/Transmission de trames multiples /bouclage

Solution:⇒ Le Spanning Tree permet d'éviter les boucles réseau, en plaçant certains ports dans un état de blocage, pour n'avoir qu'un seul chemin d'un point à un autre.

⇒ Le Spanning tree, utilise des **BPDU** pour la communication entre les switchs

⇒ **Les BPDU** sont des trames qui sont échangées régulièrement, à peu près environ toutes les 2 secondes, et permettent aux switches de garder une trace des changements sur le réseau afin d'activer ou de désactiver les ports des équipements

⇒ le BDU est composé de plusieurs champs mais le champs le plus important est le **Bridge identifier(bridge id)**

⇒ **Bridge identifier=Priorité +@mac**.

L'algorithme du spanning-tree procède en plusieurs Étapes :

1-Élection du commutateur racine :

Le commutateur avec **la priorité la plus basse(par défaut=32768 et on peut la modifier)** devient le **pont racine(appelé aussi root bridge**), et en cas d'égalité, c'est l'adresse MAC la plus basse qui l'emporte

2-Déterminer les ports racines :
Cette élection porte sur la distance la plus courte vers le commutateur racine.
Pour ça, il se base sur le « coût » de chaque lien traversé. Et la valeur du coût dépend de la bande passante du lien.
Le « port racine » sera celui qui mène le plus directement et plus rapidement au commutateur racine.(le port le plus proche à la racine)
⇒ Il ne peut y avoir qu'un seul root port(port racine) par commutateur.
En cas d'égalité, c'est-à-dire que 2 switchs ont le même coût vers le Bridge ID, alors ce sera **le port ayant le port ID le plus faible** qui sera élu.

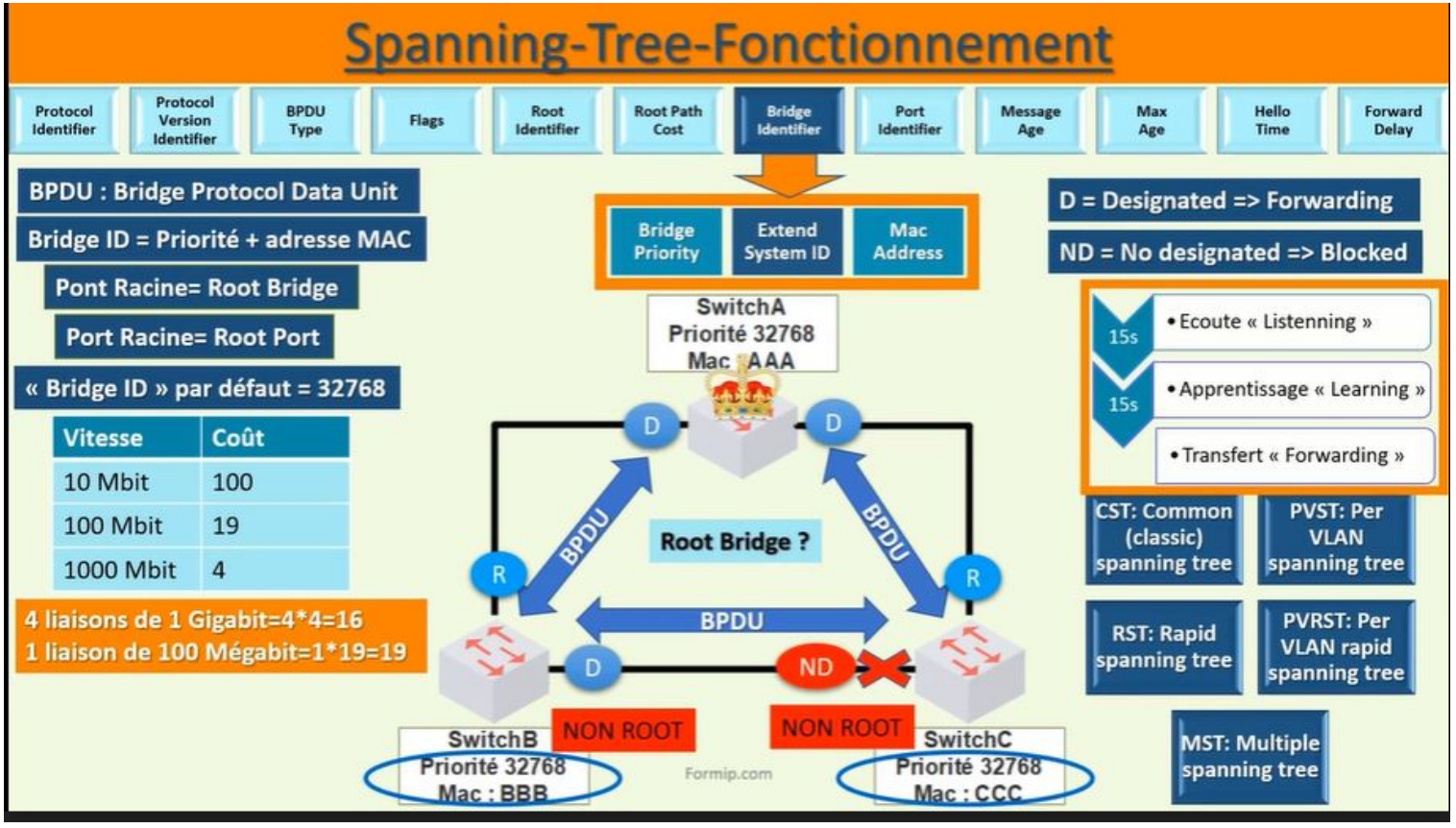
3-Sélectionner les ports désignés :
Pour chaque segment réseau qui relie des commutateurs, un **« port désigné »** est sélectionné par le spanning tree.

Il s'agit du port relié au segment, qui mène le plus directement à la racine.
==>Remarque importante: Un switch élue root bridge, aura systématiquement des ports désignés !
En cas d'égalité sur un segment, la sélection se fera aussi sur la **priorité et la Mac-adresse la plus basse.**

4-Blocage des autres ports:

Les ports qui ne sont ni racine, ni désignés sont bloqués.
Un port bloqué peut recevoir des paquets BPDU mais ne peut pas en émettre.

Image récapitulative du stp



Type de Spanning-Tree	VariÉTÉs de STP
• **Le spanning tree classique.** • **Le spanning tree par Vlan** • **Le spanning tree rapide** • **Le spanning tree par Vlan Rapide** • **Et le spanning tree multiple** ⇒ nchouf tp ken makhdemnech config mteeha so mch dekhla	• **STP** : permets simplement une redondance sans boucle. • **RSTP :** C'est l'évolution du STP, car il offre une convergence plus rapide. • **PVST et le PVST + :** permets de mettre en place un spanning tree différent par vlan. • **Rapid-PVST+ :** Amélioration du spanning tree par vlan. • **Multiple STP :** C'est une extension du Rapid spanning tree.

Portfast

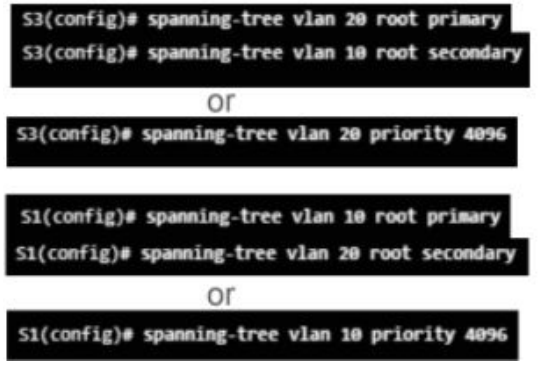
Chaque fois que l'on connecte un câble à une interface, il reste 15 secondes en écoute et 15 secondes en apprentissage, avant de pouvoir se retrouver en mode « Transfert », pour fonctionner correctement.
Au total il aura passé 30 secondes avant d'être complètement fonctionnel.
Ce fonctionnement est indispensable quand on branche plusieurs switchs sur ces ports, afin d'éviter les boucles.
Mais qu'en est-il si on branche un simple PC, ou bien tout autre équipement de terminaison.
Comme le pc c'est un équipement en bout de chaîne, il ne peut pas y avoir de boucle.

Dans ce cas, il n'est pas utile d'écouter les BPDU, car sinon le PC mettrait 30 secondes avant de pouvoir être utilisé et ce serait une perte de temps .Pour contourner ça, il existe une solution qui s'appelle **« Portfast »**
Les interfaces avec le mode « portfast » activées passeront immédiatement en mode de transfert, c'est-à-dire en mode forwarding ! Il sautera donc l'état d'écoute et d'apprentissage
.Il est important d'activer ce mode sur toutes les interfaces qui seront connectées à des hôtes !
⇒ Il se configure uniquement sur les ports du switch qui sont déjà en mode « access ».

BPDUGUARD

Généralement on combine le portfast avec la fonction « BPDUGUARD » qui permet de désactiver le port sur lequel le portfast est configuré immédiatement, dès qu'il reçoit des BPDU's.

5. Configuration de stp , portfast, bpduguard :

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 10 root primary/secondary	pour forcer l'élection du pontracine en choisissant le vlan du switch racine ou secondaire	
spanning-tree vlan 10 priority x	forçer l'élection du pont racine en changeant la priorité	
spanning-tree port-priority	modifier la valeur de la priorité du port.	
spanning-tree cost	modifier le coût d'une interface	
interface fa0/6 spanning-tree portfast	Configuration de PortFast	
interface fa0/6 spanning-tree bpduguard enable	Configuration de la protection BPDU	
# spanning-tree portfast bpduguard default **#spanning-tree portfast default**	configurer les fonctions sur toutes les interfaces du switch	**BPDU:** **+1 car vlan 1** **+10 car vlan 10** **+99 car vlan 99**

CHAPITRE 6:EtherChannel: agrégation de lien

EtherChannel est une technologie d'agrégation de liens utilisée principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique. Le but est d'augmenter la vitesse(augmenter la bande passante), la disponibilité et la tolérance aux pannes (au cas ou une liaison tombe panne on bascule vers une autre liaison)entre les commutateurs, les routeurs et les serveurs.Elle permet de simplifier une topologie Spanning-Tree en diminuant le nombre de liens et en assurant l'équilibrage de charge.

⇒ on peut regrouper les liens physique : soit des liens fast ethernet (maximum 800 Mbps Par s)ou bien des liens gigabit ethernet(8Gbps par s) mais non pas les deux ensemble c interdit

⇒ minimum 2 liens maximum 8 mais considéré comme un seul lien logique

⇒ Etherchannel peut être effectué soit entre 2 switch soit entre un serveur et switch

⇒ il faut faire le mode trunk

⇒ les configurations sont faites sur les ports logiques et ils sont affectés automatiquement sur les ports physique

⇒ Etherchannel peut être effectué en utilisant 2 protocoles: **Pagp et LACP**

1-Pagp: fonctionne que sur les équipements cisco

les mode de configuration de Pagp sont :

On:'interface ne va établir les négociations⇒ manuellement sans le pagp et lacp(lezem on des 2 côtés)

Désirable:il fait la demande avec le switch d'en face pour créer l'agrégation de lien

Auto:va attendre la négociation pour devenir une agrégation de lien

S1	S2	Channel Establishment
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not Configured	No
On	Desirable	No
Auto/On	Auto	No

2-LACP:fonctionne sur tout type d'équipements

les mode de configuration de lacp sont :

On:'interface va établir les négociations⇒ manuellement sans le pagp et lacp(lezem on des 2 côtés)

Active:il fait la demande avec le switch d'en face pour créer l'agrégation de lien

Passive:va attendre la négociation pour devenir une agrégation de lien

S1	S2	Channel Establishment
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

⇒ Dans les 2 modes:le mode on n'a pas une relation ni avec le pagp ni avec lacp il se fait manuellement

<u>Les règles de configuration de l'Etherchannel</u>(si ces règles ne sont pas respecté le etherchannel ne sera pa établie):

1-les interfaces des switchs doivent avoir le même débit et le même mode de duplex

-2les 2 switch doivent avoir les même vlan et le même vlan native

3 -le trunk doit être établi dans les 2 sens avec le même vlan native

6. configuration d'EtherChannel

Commandes	Rôles	Commentaires
interface range f0/1-2 S1 **channel-group 2 mode desirable** **interface port-channel 1** switchport mode trunk switchport trunk allowed vlan 1,2,20 switchport trunk native vlan 99 no shutdown	Configurez les ports sur S1 avec l'option desirable mode **PAgP**	
interface range f0/1-2 S1 **channel-group 2 mode auto** **interface port-channel 1** switchport mode trunk switchport trunk allowed vlan 1,2,20 switchport trunk native vlan 99 no shutdown	Les ports sur S3 avec l'option auto mode **PAgP**	
show run interface f0/3	Taatik configuration de l'interface	
show interfaces f0/3 switchport	Plus d'info sur f0 /3 -> plus dinfo aal groupe	**7atetha tofla li aamla résumé w mch met2akda menha mnin jebetha**
interface **port-channel 1** switchport mode trunk switchport trunk native vlan 99	Configuration d'un trunk sur un port-Channel	
interface range f0/1-2 S1 **channel-group 2 mode active** **interface port-channel 1** switchport mode trunk switchport trunk allowed vlan 1,2,20 switchport trunk native vlan 99 no shutdown	Configurez **LACP** et trunk sur S1 en mode active spécifier le range d'interfaces physique sur lesquels on va faire le etherchannel spécifier le mode utilisation du port logique portchannel 1 activation du trunk spécifier les vlans	
interface range f0/1-2 S1 **channel-group 2 mode passive**	Configurez **LACP** sur S2 en mode passive	

interface port-channel 1 switchport mode trunk switchport trunk allowed vlan 1,2,20 switchport trunk native vlan 99 no shutdown		
show etherchannel summary	Vérifier les ports sur lesquels nous avons appliqué le etherchannel et leurs informations	**⇒ si on trouve po1(SD) c qu'il ya un problème est il est down** **⇒ il faut trouver PO1(SU)**
show interfaces port-channel 1	vérifier le status et les caractéristiques du port-channel1	
show etherchannel port-channel	plus d'informations sur les port-channel	
show interfaces f0/1 etherchannel	vérifier sur l'interface physique	

⇒ dans pagp on fait le trunk sur l'interface logique alors que dans lacp sur l'interface physique avant de créer le channel groupe

CHAPITRE 7: HSRP

Hot Standby Router Protocol (HSRP) est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service. **HSRP** est principalement utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.

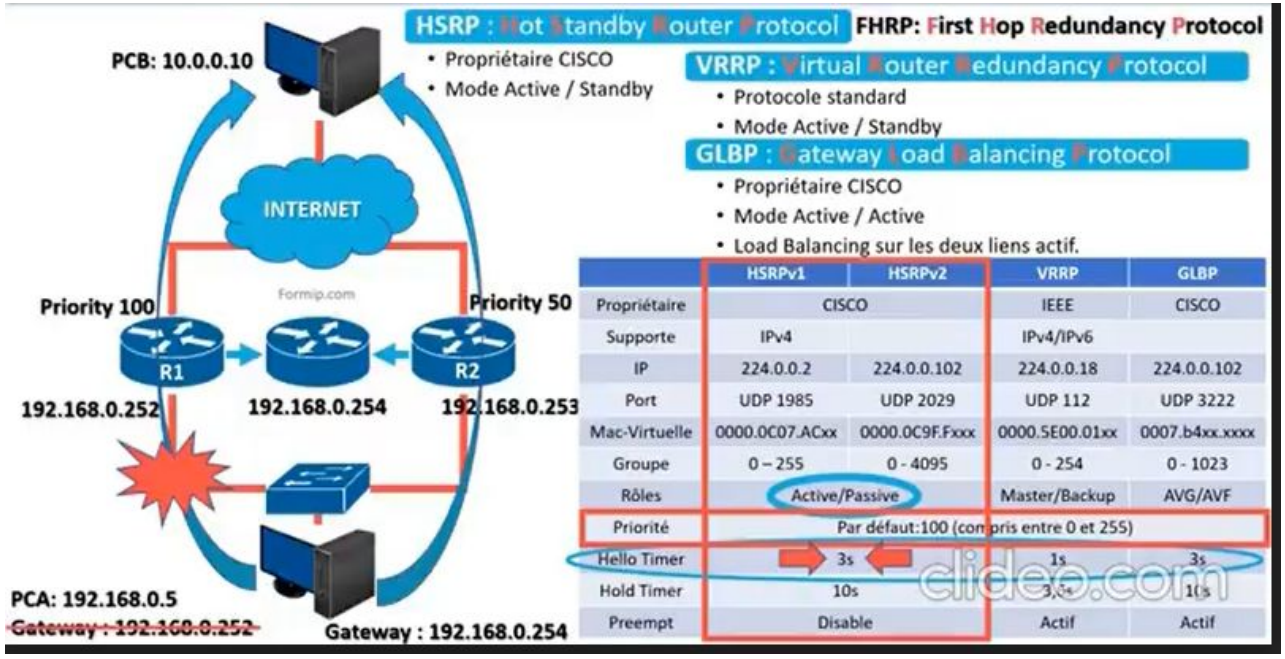
⇒ le choix d'un routeur actif et d'un routeur en stand bye se fait par une élection de HSRP

⇒ priorité par défaut d'un routeur = 100

⇒ le routeur qui a le priorité la plus haute sera en mode actif et l'autre en stand by et au cas ou ils sont égaux le choix se fait l'@ip la plus haute

⇒ kif yti7 panne l'actif tsir election okhra w yched blassto lekher

https://drive.google.com/file/d/1EHZxDhvGiwd74ncL3YX5xiFgeZEngJSS/view tfarjo fi video wlh fih kol chay kima fasret madame fl classe



==>créer un routeur virtuelle qui partagé entre les routeurs physique / le passerelle du pc doit être l'@ du routeur virtuelle

HSRP⇒ pour ipv4

FHRP⇒ pour ipv6

HSRP⇒ pour les équipements cisco

VRRP ⇒ pour tous les équipements

Version de HSRP:

Version	HSRP V1 (Default)	HSRP V2
Group numbers	0 to 255	0 to 4095
Multicast address	224.0.0.2	224.0.0.102 or FF02::66
Virtual MAC address	0000.0C07.AC00 - 0000.0C07.ACFF (last two digits group number)	**IPv4** 0000.0C9F.F000 to 0000.0C9F.FFFF **IPv6** 0005.73A0.0000- 0005.73A0.0FFF (last three digits group number)
Support for MD5 authentication	No	Yes

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(loopback)
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	Configurer HSRP	

standby version 2 standby 1 ip 192.168.1.254		
show standby	Vérifiez HSRP	
show standby brief	Vérifiez HSRP brièvement	
debug standby?	Pour afficher les changements d'état du protocole HSRP	**commande de débogage** **⇒ c pas important de les apprendre juste pour la verification**
debug standby packets	pour afficher les informations de débogage des paquets liés au protocole HSRP	
debug standby terse	pour voir que le r1 est off alors que l'autre routeur a pris sa place comme un routeur actif	

Commande de Vérification : Tous les chapitres

Commandes	Rôles
show running-config	Le fichier de configuration en cours d'exécution ou actuelle
show startup-config	Le fichier de configuration initiale dans la mémoire vive non volatile nvram
show ip interface brief	afficher les informations relatives aux interfaces
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 mémoire flash qui contient le SE

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 port-security interface ou show port-security address	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 interface f0/15 status	verifier la status ou l'etat de cette interface
show vtp password	vérifier le mot de passe VTP
show ip route C ⇒ @RX L⇒ @ip	afficher table de routage