Partie 1: Bloc Administration (4 pts)

1. Configurez les paramètres de base pour le comumutateur SA3, renseignez les commandes nécessaires:
2. **Configurez le nom du commutateur conformément à la topologie**

Enable

Configure terminal

hostname SA3

1. **Configurez ExamCS comme mot de passe sécurisé pour l'accès privilégié**

enable secret ExamCS

1. **Configurez ESPRIT2024 comme mot de passe pour l'accès console**

line console 0

password ESPRIT2024

login

1. **Désactiver la cherche du serveur DNS**

no ip domain-lookup

1. **Configurez l'interface virtuelle de gestion par défaut pour ce commutateur en utilisant l'adre 172.16.1.3/24**

interface vlan 1

ip address 172.16.1.3 255.255.255.0

no shutdown

1. **Configurez la passerelle par défaut pour ce commutateur en utilisant la première adrese même réseau**

ip default-gateway 172.16.1.1

1. **Sur le commutateur SA2, l'administrateur souhaite permettre l'accès uniquement au Pe Configurez le port approprié de sorte qu'il acquière l'adresse MAC de façon dynamiqu ignore le trafic en cas de violation.**

interface FastEthernet0/1 # Remplacez FastEthernet0/1 par le numéro de port approprié

switchport mode access

switchport port-security

switchport port-security violation restrict

1. **Quelle est la différence entre les modes Protect et Restrict en cas de violation ?**

Protect: En cas de violation, le mode "Protect" désactive le port sécurisé, ce qui signifie qu'aucun trafic n'est autorisé sur ce port tant que l'adresse MAC non autorisée n'est pas retirée.

Restrict: En cas de violation, le mode "Restrict" limite le trafic provenant de l'adresse MAC non autorisée, mais il ne désactive pas le port. Les paquets provenant de l'adresse MAC non autorisée sont ignorés et un compteur de violation est incrémenté.

**Partie 2: Bloc 1-VLAN**

1. **Au niveau du bloc 1, l'administrateur a correctement configure les VLANs commutateur S1-1 et S1-2. Faites le nécessaire sur le commutateur $1-3.**

vlan 10

name Scolarité

vlan 20

name Enseignant

vlan 30

name Etudiant

**Au niveau des commutateurs S1-2, faites-en sorte que les PCs (2, 3, 4, 5) soient da modes et leurs VLANs adéquats. On donne le tableau suivant:**

**PC2 PC3 PC4 192.168.10.24 192.168.131/24 192.168.120.24 Enseignant PC5 Renseignez les commandes faites sur S1-2 uniquement.**

|  |  |  |
| --- | --- | --- |
| **Terminal** | **VLAN** | **Réseau** |
| PC2 | Scolarité | 192.168.11.0 /24 |
| PC3 | Enseignant | 192.168.12.0/24 |
| PC4 | Enseignant | 192.168.12.0/24 |
| PC5 | Etudiant | 192.168.13.0/24 |

interface FastEthernet0/2 # PC2

switchport mode access

switchport access vlan 10

interface FastEthernet0/3 # PC3

switchport mode access

switchport access vlan 20

interface FastEthernet0/4 # PC4

switchport mode access

switchport access vlan 30

interface FastEthernet0/5 # PC5

switchport mode access

switchport access vlan 20

1. **Configurez les porta e ports epi relient les les commutatars 1-2 et 1-3 dans leurs modes appropriés en autorisant les Vians créés précédemment. Renseigner les commandes faites e 1-201**

interface FastEthernet0/1 # Port connecté à S1-2

switchport trunk encapsulation dot1q

switchport mode trunk

interface FastEthernet0/1 # Port connecté à S1-3

switchport trunk encapsulation dot1q

switchport mode trunk

1. **Quel est le rôle d'un VLAN natif dans un réseau? (1)**

Le VLAN natif (native VLAN) est un VLAN par défaut utilisé sur un port trunk. Son rôle principal est de transporter le trafic qui n'est pas étiqueté avec une information de VLAN spécifique. Les trames de ce VLAN natif ne sont pas taguées lorsqu'elles traversent un port trunk.

Le VLAN natif est important car il permet aux appareils qui ne comprennent pas les VLANs (comme les périphériques réseau plus anciens ou certains périphériques réseau grand public) de communiquer sur le réseau sans nécessiter de configuration VLAN spécifique.

**Partie 3: BLOC I-STP (3pt)**

1. **L'administrateur souhaite définir des ponts racines pour le bon fonctionnement du protocols PVST.**
2. **Définissez S1-1 comme pont racine pour tous les VLANs (0,5)**

spanning-tree vlan 1,10,20,30 priority 0

1. **Définissez $1-2 comme pont racine de secours pour les VLANs 1 et 11 (0,5)**

spanning-tree vlan 1,11 priority 4096

1. **Définissez S1-3 comme pont racine de secours pour les VLANs 12 et 13 (0,5)**

spanning-tree vlan 12,13 priority 4096

1. **Expliquez la différence entre les protocoles STP et PVST+2(0.5)**

STP (Spanning Tree Protocol): C'est un protocole standard qui permet d'éviter les boucles dans les réseaux LAN en désactivant sélectivement des ports pour créer un arbre de diffusion sans boucle.

PVST+ (Per-VLAN Spanning Tree Plus): C'est une extension Cisco du STP qui crée un arbre de diffusion distinct pour chaque VLAN. Cela signifie que plusieurs instances de STP (une par VLAN) peuvent s'exécuter simultanément sur le réseau, ce qui permet une meilleure utilisation de la bande passante.

1. **On souhaite à présent définir les ports 10/24 et 10/23 du switch 51-3 comme des ports EDGE Faites les configurations nécessaires. (Renseignez les commandes pour l'interface f0/24) (1)**

interface FastEthernet0/24

spanning-tree portfast

**Partie 4: Bloc 2- Routage InterVian (4 pt)**

1. **Citez les deux méthodes de communication inter-VLAN. Expliquez l'avantage de l'une par rapport à l'autre. (1)**

Les deux méthodes principales de communication inter-VLAN sont :

Routeur sur une interface physique (Router on a Stick) : Une seule interface physique d'un routeur est utilisée pour connecter le routeur à un commutateur, avec les différents VLANs configurés comme sous-interfaces logiques sur cette interface physique.

Couche 3 sur le commutateur (Layer 3 Switching) : Un commutateur de couche 3 est utilisé pour effectuer le routage entre les VLANs. Chaque VLAN a une interface virtuelle (SVI) configurée sur le commutateur, et le commutateur a une capacité de routage intégrée pour acheminer le trafic entre les VLANs.

L'avantage de la méthode "Couche 3 sur le commutateur" (Layer 3 Switching) est qu'elle permet un traitement plus rapide des paquets entre les VLANs car le routage est effectué au niveau du commutateur lui-même, évitant ainsi d'avoir à transférer chaque paquet vers un routeur externe pour le traitement inter-VLAN. Cela peut améliorer les performances du réseau et réduire la charge sur le routeur principal.

1. **Afin de pouvoir assurer la communication entre les différents réseaux virtuels, l'administrateur a commencé la configuration du routeur R2. Complétez la configuration de l'interface G0/0. (2,25)**

interface GigabitEthernet0/0

description Connexion vers le réseau local technique

ip address 192.168.1.1 255.255.255.0 # Remplacez par l'adresse IP et le masque appropriés

no shutdown

1. **Envoyer une PING depuis PC6 vers PC9, Proposez les corrections nécessaires en cas d'échec. (0,75)**

En cas d'échec d'un PING de PC6 vers PC9, voici les étapes de dépannage et de correction possibles :

Vérifiez les configurations IP :

Assurez-vous que PC6 et PC9 ont des adresses IP valides dans le même sous-réseau.

Vérifiez les masques de sous-réseau pour s'assurer qu'ils correspondent correctement.

Vérifiez les configurations de passerelle par défaut :

Assurez-vous que PC6 et PC9 ont correctement configuré leur passerelle par défaut pour atteindre les réseaux distants.

Vérifiez les règles de pare-feu :

Assurez-vous qu'aucun pare-feu n'interfère avec le trafic ICMP nécessaire pour le PING.

Vérifiez la connectivité physique :

Assurez-vous que les câbles Ethernet sont correctement connectés et que les interfaces des commutateurs et des routeurs sont activées.

Vérifiez les tables de routage :

Assurez-vous que les routeurs ont des entrées de routage appropriées pour acheminer le trafic entre les réseaux de PC6 et PC9.

**Partie 5: Interconnexion des Bloc 1 et 2-Etherchannel (2pt)**

**Pour assurer l'échange de données volumineuses entre le local technique et le local commercial, l'administrateur souhaite créer un lien agrégé entre S2-1 et S1-1 en utilisant le protocole propriétaire à Cisco.**

1. **Faites les configurations nécessaires de manière que les interfaces au niveau de $2-1 cherchent activement à établir l'agrégation et celles de $1-1 restent passives. Renseignez toutes les commandes (2pt).**

Sur le commutateur S2-1 (actif) :

interface range GigabitEthernet0/1 - 2 # Sélectionnez les ports à agréger

channel-group 1 mode active

Sur le commutateur S1-1 (passif) :

interface range GigabitEthernet0/1 - 2 # Sélectionnez les ports à agréger

channel-group 1 mode desirable

**Partie 6: HSRP (2,5 pt)**

1. **Afin de garantir que l'administration ait un accès en permanence à Internet, l'administratem doit faire les configurations nécessaires sur les routeurs R1 et R2. Quel protocole l'administrateur doit utiliser ? (0,5)**

Pour garantir l'accès Internet en permanence, l'administrateur doit utiliser le protocole HSRP (Hot Standby Router Protocol).

1. **Faites les configurations nécessaires afin que le routeur R1 soit actif avec une priorité supérieure à celle par défaut par 20. (Remarque: R2 a était correctement configure.) (1.25)**

interface GigabitEthernet0/0

standby version 2

standby 1 ip 192.168.1.254 # Adresse IP virtuelle du groupe HSRP

standby 1 priority 120 # Priorité supérieure à la valeur par défaut (100)

1. **Depuis PC0 el PC1, essayer d'ouvrir une page Web vers le serveur (Adresse 209.165.200.202). La page web ne s'ouvre pas, quel est le probléme ? Proposez les corrections nécessaires. (0,75)**

Vérifiez la connectivité IP :

Assurez-vous que PC0 et PC1 ont des adresses IP valides dans le même sous-réseau que le serveur (209.165.200.202).

Vérifiez les configurations de passerelle par défaut :

Assurez-vous que PC0 et PC1 ont correctement configuré leur passerelle par défaut pour atteindre le réseau où se trouve le serveur.

Vérifiez les règles de pare-feu :

Assurez-vous qu'aucun pare-feu ne bloque le trafic HTTP sortant depuis PC0 et PC1 vers le serveur.

Vérifiez les règles de routage :

Assurez-vous que les routeurs ont des entrées de routage appropriées pour acheminer le trafic vers le serveur (209.165.200.202).