UA#2\_V1

Une image contenant diagramme, ligne

Description générée automatiquement

**TABLEAU D’ADDRESSAGE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Appareil | Interface | Adresse IP / Préfixe | Passerelle |
|  | C1 | G1/0/1 | 10.10.5.1/30 | N/A |
|  | C1 | G1/0/2 | 10.20.5.1/30 | N/A |
|  | C1 | G1/0/3 | 10.30.5.1/30 | N/A |
|  | C1 | G1/0/4 | 10.40.5.1/30 | N/A |
|  | C1 | Lo0 | 100.100.100.100/32 | N/A |
|  | C1 | G1/0/24 | 209.165.200.2/30 | N/A |
|  | ISP/FAI | G1/0/24 | 209.165.200.1/30 | N/A |
|  | A1 | Vlan 10 | 192.10.5.5 | 192.10.5.1 |
|  | R1 | G1/0/1 | 10.10.5.2/30 | N/A |
|  | R1 | G1/0/2 | 10.12.5.1/30 | N/A |
|  | R1 | G1/0/3 | 10.13.5.1/30 | N/A |
|  | R1 | Lo0 | 1.1.1.1/32 | N/A |
|  | R2 | G1/0/1 | 10.20.5.2/30 | N/A |
| R2 | | G1/0/2 | 10.12.5.2/30 | N/A |
| R2 | | G1/0/3 | 10.24.5.1/30 | N/A |
|  | R2 | Lo0 | 2.2.2.2/32 | N/A |
| R3 | | G1/0/1 | 10.30.5.2/30 | N/A |
| R3 | | G1/0/2 | 10.34.5.1/30 | N/A |
| R3 | | G1/0/3 | 10.13.5.2/30 | N/A |
|  | R3 | Lo0 | 3.3.3.3/32 | N/A |
| R4 | | G1/0/1 | 10.40.5.2/30 | N/A |
| R4 | | G1/0/2 | 10.34.5.2/30 | N/A |
|  | R4 | G1/0/3 | 10.24.5.2/30 | N/A |
|  | R4 | Lo0 | 4.4.4.4/32 | N/A |
|  | DHCP | NIC | 192.69.5.10/24 | A déterminer |
|  | DNS | NIC | 192.69.5.20/24 | A déterminer |
|  | SYSLOG | NIC | 192.69.5.30/24 | A déterminer |

**TABLEAU DES VLANS**

|  |  |  |  |
| --- | --- | --- | --- |
|  | NOM | Sous-réseau | attribution |
| 10 | VLAN\_10 | 192.10.5.0/24 | R1(.1) |
| 20 | VLAN\_20 | 192.20.5.0/24 | R1(.1) |
| 30 | VLAN\_30 | 192.30.5.0/24 | R2(.1) |
| 40 | VLAN\_40 | 192.40.5.0/24 | R2(.1) |
| 50 | VLAN\_50 | 192.50.5.0/24 | R3(.1) |
| 60 | VLAN\_60 | 192.60.5.0/24 | R3(.1) |
| 69 | VLAN\_69 | 192.69.5.0/24 | DC1(.1),DC2(.2), DC3(.3), DC4(.4), R4(.254) |
| 999 | NATIVE |  |  |
| 404 | BLACKHOLE |  | Les ports inutilisés |

**TABLEAU D’ETAT DES PORTS**

|  |  |  |
| --- | --- | --- |
| **SWITCH** | **Ports** | **Vlans autorisés** |
| Entre A1 et R1 | F0/24 🡪G1/0/24 | A determiner |
| Entre A2 et R2 | F0/24 🡪G1/0/24 | A determiner |
| Entre A3 et R3 | F0/24 🡪G1/0/24 | A determiner |
| Entre R(1-4) et R(1-4) | G1/0/2-3 🡪G1/0/2-3 | N/A (routed) |
| Entre R(1-4) et C1 | G1/0/1 🡪G1/0/1-4 | N/A (routed) |
| Entre les DC(1,2,3,4) | F0/1-4 🡪F0/1-4 | A determiner |
| Entre DC1 et R4 | F0/24 🡪 G1/0/24 | A determiner |
| A1 | F0/5 | VLAN\_10 |
| F0/10 | VLAN\_20 |
| A2 | F0/5 | VLAN\_30 |
| F0/10 | VLAN\_40 |
| A3 | F0/5 | VLAN\_50 |
| F0/10 | VLAN\_60 |
| DC2 | F0/5 | VLAN\_69 |
| DC3 | F0/5 | VLAN\_69 |
| DC4 | F0/5 | VLAN\_69 |

**Étape1 : adressage IP**

1. Configurez l’adressage ip comme c’est indiqué sur le tableau

NB :XX dernier chiffre de votre numéro d’étudiant

**Étape 2 : Configuration de base**

* Configurez le nom d’hôte approprié selon le tableau.
* Configurez un mot de passe pour le mode d’exécution (privilégié) de **cisco**
* Configurez un mot de passe pour les connexions de consoles et VTY de **class**
* Activez la synchronisation des messages de la console
* Désactivez le délai d’attente de la console
* Désactivez la recherche DNS
* Configurez sur les entrées DNS suivantes sur le serveur DNS:

-DNS.local (associé à l’adresse IP du Serveur DNS)

-DHCP.local (associé à l’adresse IP du Serveur DHCP)

-SYSLOG.local (associé à l’adresse IP du Serveur SYSLOG)

* Configurez la résolution DNS sur les commutateurs A\_1, A\_2, A\_3

**Étape 3 : Configuration de SSH**

Configurer SSH Sur le commutateurs A\_1

* Désactiver telnet. Pour s’authentifier, il faut utiliser une base de données locale.
* Configurer le nom de domaine à prénom.local
* SSH version 2
* créer une clé RSA 2048 bits,
* Configurer un nom d’utilisateur admin et un mot de passe chiffré cisco111

**Étape 4 : configuration VLAN**

Sur tous les appareils concernés configurez :

-tous les vlans pertinents uniquement

-configurez les ports trunks et autorisez les VLANs adéquats uniquement

-utilisez le VLAN NATIF selon le tableau

-configurez les ports ACCESS

-mettez les ports non utilisés dans le VLAN 404 et désactivez les

-désactivez la négociation DTP sur tous les ports

- configurez Portfast sur tous les ports d’accès

- activer la protection BPDU (BPDU guard) sur tous les ports d’accès

**Étape 5 : configuration de la sécurité**

1- Configurez les port d’accès sur A\_1, A\_2, A\_3 avec les paramètres suivants :

● Limitez à 2 le nombre d’adresse MAC permise

● Activez l’apprentissage rémanent dynamique(sticky) des adresses MAC

● Changer la violation de sorte que le port ne soit pas désactivé lorsqu’une violation se produit, mais qu’une notification de la violation de sécurité soit générée et que les paquets de source inconnue soit rejeté.

2- Configurez seulement le port d’accès branché au 3 serveurs avec les paramètres suivants :

* Configurez la sécurité des ports avec une adresse MAC statique
* Limitez à 2 le nombre d’adresse MAC permise
* Changer la violation de sorte que le port soit désactivé lorsqu’une violation se produit

**Étape 6 : routage statique**

-Configurez le routage statique afin de répondre au besoin suivant :

-les LAN des PCs peuvents communiquer entre eux

-les LAN des PCs peuvents communiquer avec les serveurs

-les LAN des PCs et des serveurs peuvent communiquer avec ISP (internet)

-assumez qu’on ne connait pas les réseaux au-delà de ISP

**Étape 7: Configuration du serveur DHCPv4**

1. Configurez le service DHCPv4 pour les VLAN 10 à 60 selon les paramètres suivants

-Exclure les 10 premières adresses du réseau

* + Nommez le pool VLANXX
  + Définir l’adresse adéquate pour la passerelle par défaut
  + Définir l’adresse adéquate pour le serveur DNS

**Étape 8: sécurité DHCP**

-sur les commutateurs A\_1,A\_2,A\_3 activez DHCP snooping spécifiquement pour les VLANs pertinents

-limitez les paquets DHCP à 5 par secondes sur les ports des PC

-assurez de faire confiance (TRUST) aux ports nécessaires au bon fonctionnement du DHCP

**Étape 9: Configuration du serveur SYSLOG**

-activez le service SYSLOG sur le serveur SYSLOG

-Configurez tous les routeurs et les commutateurs afin d’Effectuer la journalisation vers le serveur SYSLOG