# **RESTRUSTUCTURATION DE RESEAU**

# **PAR VLAN**



CUENCA Teva SIO 2

**SOMMAIRE**

1 – Prérequis…………………………………………………………………………………………………………………………..

2 – Création des VLAN……………………………………………………………………………………………………………..

3 – Configuration des VLAN……………………………………………………………………………………………………..

4 – Configuration du routage et des ports……………………………………………………………………………….

5 – Configuration des Services…………………………………………………………………………………………………

6 – Test des accès et services………………………………………………………………………………………………….

7 – Conclusion……………………………………………………………………………………………………………………….

**1 – Prérequis :**

* Posséder un switch de niveau 3 (Toutes les commandes s’appliquent à ce switch)
* Posséder une VM sous Debian
* Installer le terminal PUTTY pour configurer le switch niveau 3

Nous devons configurer un Serveur FTP / WEB et un serveur DHCP.

* Le serveur DHCP devra distribuer des IP correspondantes à l’IP de chaque VLAN. - Nous devons avoir 3 VLAN.
* -Le serveur Web doit être accessible depuis tous les VLAN.
* Et le port 21 ne doit pas pouvoir accéder au FTP.
* Il faut aussi tester le routage inter VLAN.

**Le switch utilisé est un cisco business 350 series de niveau 3 les commandes sont donc spécifiques à ce switch.**

****

**Architecture réseau de notre travail :**

Une image contenant texte, diagramme, ligne, capture d’écran

Description générée automatiquement

**2 – Création des VLAN**

Se connecter à Putty :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

**3 - Configuration des VLan :**

Ajout d’une IP sur le VLAN 1 :

* Interface VLAN1
* Ip address
* 192.168.1.1 255.255.255.0

La commande pour nommer les VLAN :

* Interface VLAN X
* Hostname X

Commande pour ajouter les ports dans les VLANs :

* Interface VLAN X
* Switchport mode access
* Switchport access VLAN X

Vlan 1

192.168.1.1 255.255.255.0

Interfaces : 1, 9, 10

Vlan 10 interfaces 2/3

Formation

192.168.10.254 255.255.255.0

Interfaces 2, 3

Vlan 20 interfaces 4/5

Personnel

192.168.20.254 255.255.255.0

Interfaces : 4, 5

Vlan 30 interfaces 6/7

Serveur

168.168.30.254. 255.255.255.0

Interfaces : 6, 7

Domaine :

Esicad.lan

**4 - CONFIGURATION DU ROUTAGE ET DES PORTS**

**Configuration d’un accès SSH :**

Via la commande

* Interface VLAN 1
* Ip ssh
* Ip ssh pasword – auth

Activation du routage :

* Ip routing

Test de l’accès SSH :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Ensuite cliquer sur Open :

Une image contenant texte, capture d’écran, noir, Police

Description générée automatiquement

L’accès SSH fonctionne donc correctement.

**Il faut maintenant vérifier que le routage inter VLAN fonctionne en faisant des tests de ping depuis des VLAN différents :**

Ping d’un poste du VLAN 10 au VLAN 20 :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ping d’un poste du VLAN 20 au VLAN 10 :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On observe que les VLAN communiquent correctement entre eux ce qui prouve que notre routage est effectif et correctement configuré.

**5 - CONFIGURATION DES DIFFERENTS SERVICES SOUS LINUX :**

Configuration du DNS :

Ces commandes nous permettrons d’installer les différents services de bind9 qui nous permettrons de faire fonctionner notre DNS.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Configuration des fichiers de zone :

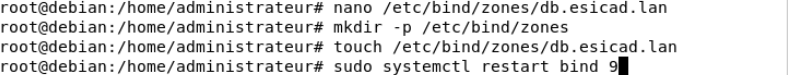
Nano /etc/bind/named.conf.local

Une image contenant texte, logiciel, Page web, Site web

Description générée automatiquement

Configuration des enregistrements DNS :

Création du répertoire db.esicad.lan



Nano /etc/bind/zones/db.esicad.lan

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Notre DNS a donc été changé en db.esicad.lan ce qui permet aux utilisateurs d’accéder aux différents service en tapant ce nom plutôt que l’IP.

Configuration du serveur WEB :

Nous aurons besoin d’installer Apache.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Installation d’apache :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Test d’accès à Apache 2

Une image contenant texte, Police, logiciel, nombre

Description générée automatiquement

Configuration d’apache :

Ici on modifie le fichier /var/www/html/index.html afin d’avoir un site fonctionnel plutôt que l’interface de configuration d’apache.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Test d’accès au site après modification on peut voir que notre modification a bien été prise en compte par apache.

Une image contenant texte, logiciel, nombre, capture d’écran

Description générée automatiquement

Configuration du serveur DHCP :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Configuration du serveur DHCP et ajout de la range IP à distribuer.

nano /etc/dhcp/dhcpd.conf

On cherche à faire en sorte que le DHCP distribue des IP correspondantes à chaque VLAN, donc on modifie la plage IP distribués par le DHCP pour chaque VLAN, voici la configuration.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Configuration de l’interface réseau :

* nano /etc/default/isc-dhcp-server
* interface v4 « ens33 »

Redémarrage des services :

* systemctl restart isc-dhcp-serv

Installation du Serveur FTP:

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Configuration de Pro FTPD :

* sudo nano /etc/proftpd/proftpd.conf

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Configuration des ACL afin de bloquer le port 21 :

* sudo iptables -L
* sudo iptables -A INPUT -p tcp --dport 21 -j DROP

(DROP) est en fait le rejet des paquets entrants et sortants sur ce port

Afin de sauvegarder cette règle on utilise la commande :

* sudo iptables-save > /etc/iptables/rules.v4

Pour activer le routage il faut utiliser la commande :

* ip helper

Test d’attribution d’ip via le serveur DHCP :

* Afin de pouvoir vérifier que nos VLAN distribuent correctement les adresses IP donné par le serveur DHCP nous allons effectuer différents Test :

Attribution d’ip du VLAN 10 sur le poste test :

Il faut d’abord passer notre carte réseau Ethernet en DHCP :

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

Ensuite ouvrir une invite de commande via Window + R / CMD

* Taper IPCONFIG et vérifier que l’adresse IP est correcte :

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

Test sur le VLAN 20 :

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

Les adresses distribuées par le DHCP sont correctes on peut voir que les adresses distribuées par le DHCP correspondent bien à chaque VLAN.

Test d’accès au serveur web :

Pour rappel tous les VLAN doivent accéder au service WEB depuis leur poste :

https://db.esicad.lan

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On observe que j’accède bien au serveur web depuis mon poste étant donné que je n’ai pas configuré de règle l’empêchant d’y accéder depuis un VLAN différent, tous les VLAN y ont accès.

**Test de l’accès au serveur FTP :**

Une image contenant texte, Police, capture d’écran, algèbre

Description générée automatiquement

L’accès au serveur FTP ne doit pas fonctionner depuis le port 21 :



Voici le résultat lors du test d’accès au serveur FTP.

Pour conclure les différents test effectués nous ont montrés que le routage inter vlan était fonctionnel via des test de ping, on observe aussi que tous les VLAN ont accès au serveur web et que le port 21 n’a pas accès au FTP.