- Toujours commencer par rappeler la demande (Cahier des charges)
- Toujours présenter un schéma de l'architecture à mettre en place avec les composants, services essentiels et les paramètres TCP/IP

1) Configuration du switch CISCO

a) Activation du mode SSH :

Afin de pouvoir administrer librement le switch sans avoir besoin d'utiliser le ~~cable~~ câble console il faut activer le protocole SSH.

Pour ce faire il faut tout d'abord brancher le ~~cable~~ câble console et se connecter ~~grace~~ grâce au logiciel putty sur le port COM3.
Une fois sur l'interface il faut saisir les commandes suivantes :

Switch> enable → Pour passer en mode admin.
Switch# configure terminal → *Pour entrer en mode configuration.*
Switch(config) #hostname SW1 → *Nom donné au switch.*
SW1 (config) #ip domain-name esicad.local → Nom de domaine adressé.
SW1 (config) #crypto key generate rsa general-key modulus 1024 → Générations des clés RSA nécessaire au SSH.
SW1 (config) #ip ssh version 2 → Commande pour activer le SSH

Ensuite il faut créer l'utilisateur pour le SSH :

SW1 (config) #username Esicad31 password cisco
SW1 (config) #enable password cisco

Pour finir il faut désactiver le protocole Telnet :

SW1 (config) #line vty 0 5
SW1 (config) #login local
SW1 (config) #transport input ssh

Tbien c'est succinct mais cela suffit !

b) Mise en place des VLANS :

Les VLANS permettent la configurations de plusieurs réseaux logiques séparés les uns des autres sur le même switch. Pour cet exercice (il fat le penser comme un projet mais pas un exercice scolaire !) j'ai donc créé 3 VLANS. Le 1er allant du port 1-5, le 2ème allant du port 6-10, le 3ème allant du port 11-15.

Création des vlans :

On donne un nom à nos VLANS :

```
SW1(config)#vlan 10
SW1(config-vlan)#name administration
SW1(config)#vlan 20
SW1(config-vlan)#name eleves
SW1(config)#vlan 30
SW1(config-vlan)#name serveurs
```

Affectation des ports à chaque Vlan correspondant :

```
SW1(config)#interface range fastEthernet 0/1-5
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#interface range fastEthernet 0/6-10
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
SW1(config)#interface range fastEthernet 0/11-15
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
```

Je vérifie alors que mes VLANS sont créés avec la commande : Show vlan

Ensuite je passe le port 0/24 en mode TRUNK : (pourquoi, en une phrase)

```
SW1(config)#interface fastEthernet 0/24
SW1(config-if)#switchport mode trunk
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#exit
```

Pour finir je n'oublie pas de sauvegarder avec la commande *copy run start.*

Le switch et mes VLANS sont désormais configurés. Je passe donc à la configuration du routeur.

2)Configuration du routeur CISCO

a)Activation du protocole SSH :

Configuration du nom du routeur et du nom de domaine

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#ip domain-name esicad.local
R1(config)#exit
R1#wr
```

On crée alors la clé RSA :

```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.esicad.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Jul 28 23:09:37.291: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
```

On active SSH :

```
R1(config)#ip ssh version 2
```

On ajoute le compte administrateur :

```
R1(config)#username Esicad31 password cisco
R1(config)#enable password cisco
```

b) Création des sous interfaces : pourquoi ? Expliquer pourquoi on y a recours à la place des interfaces physiques

Choix des IP :

Fa0/0.1 Adresse IP : 192.168.1.10

Fa0/0.2 Adresse IP : 192.168.2.10

Fa0/0.3 Adresse IP : 192.168.3.10

On rajoute aussi la commande *ip helper-address* qui permet d'activer l'agent de relais DHCP.

Rappeler aussi comment est fait le lien de chaque sous-interface avec son vlan.

```
R1(config)#interface fastEthernet 0/0.1
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#ip helper-address 192.168.3.100
R1(config-if)#exit

R1(config)#interface fastEthernet 0/0.2
R1(config-if)#ip address 192.168.2.10 255.255.255.0
R1(config-if)#ip helper-address 192.168.3.100
R1(config-if)#exit

R1(config)#interface fastEthernet 0/0.3
R1(config-if)#ip address 192.168.3.10 255.255.255.0
R1(config-if)#ip helper-address 192.168.3.100
R1(config-if)#exit
```

Et on N'oublie pas de sauvegarder comme vu plus haut. (*wr).*

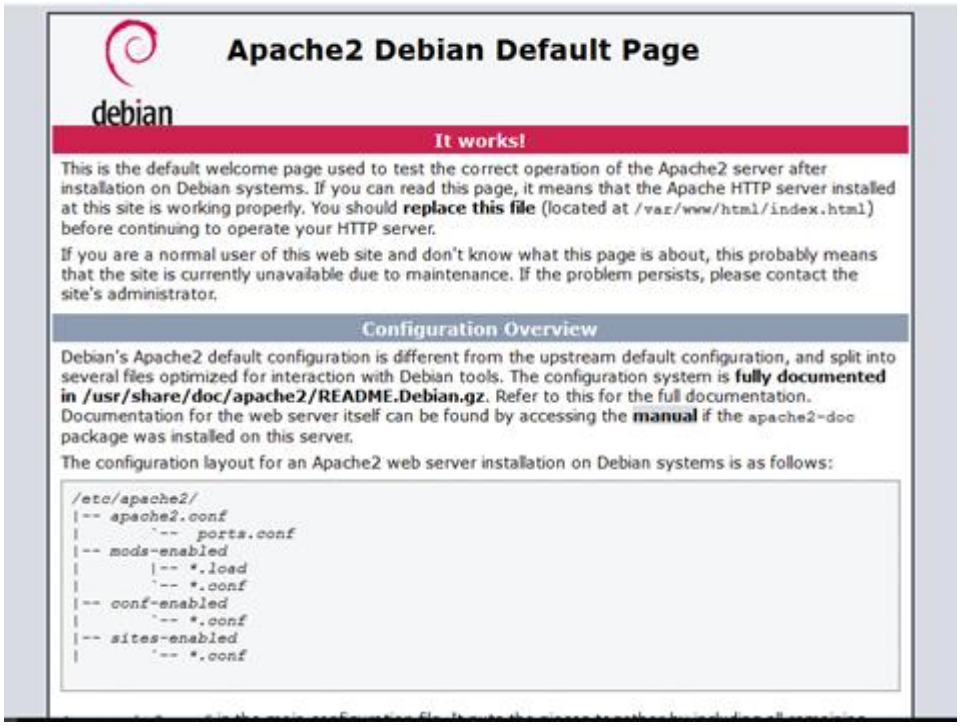
3) Le Serveur WEB :

Pour Installer ~~le serveur web est très simple, il suffit d'installer~~ le paquet apache2 sur ~~son~~ le debian 8 dont l'IP est 192.168.3.100 Les commande sont les suivantes :

apt-get update

apt-get install apache2

En suite si vous vous rendez sur l'adresse de votre serveur web (192.168.3.100) vous devriez voir apparaitre cette page :



4) Le serveur DHCP :
Puisque on n'a pas un schéma récapitulatif on a l'impression d'aligner des services sans avoir une vision globale du sujet à traiter.

On installe le paquet isc-dhcp-server :

apt-get update

apt-get install isc-dhcp-serve

Une fois installé on rentre dans le fichier de config : nano /etc/dhcp/dhcpd.conf

Il faut alors modifier les lignes :

option domain-name «esicad.local» ;

option domain-name-servers 192.168.3.101 ;

On déclare alors les sous réseaux ~~que l'on va impacter par le~~ auxquels le DHCP attribuera une adresse.

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.11 192.168.1.254;
option routeurs 192.168.1.10;
option broadcast address 192.168.1.255; }

subnet 192.168.2.0 netmask 255.255.255.0 {
range 192.168.2.11 192.168.2.254;
option routeurs 192.168.2.10;
option broadcast address 192.168.2.255; }

On modifie alors le fichier : *nano /etc/default/isc-dhcp-server*

On renseigne l'interface d'écoute :

INTERFACES="eth0"

On redémarre alors le serveur DHCP :

/etc/init.d/isc-dhcp-server restart

Configuration du fichier des interfaces réseaux :

nano /etc/network/interfaces

On affecte a notre serveur une IP fixe, ici 192.168.3.100

Si tout se passe bien lorsque vous connectez un ordinateur sur un de ces 2 VLANS, une adresse IP sera automatiquement attribué dans la range correspondante.

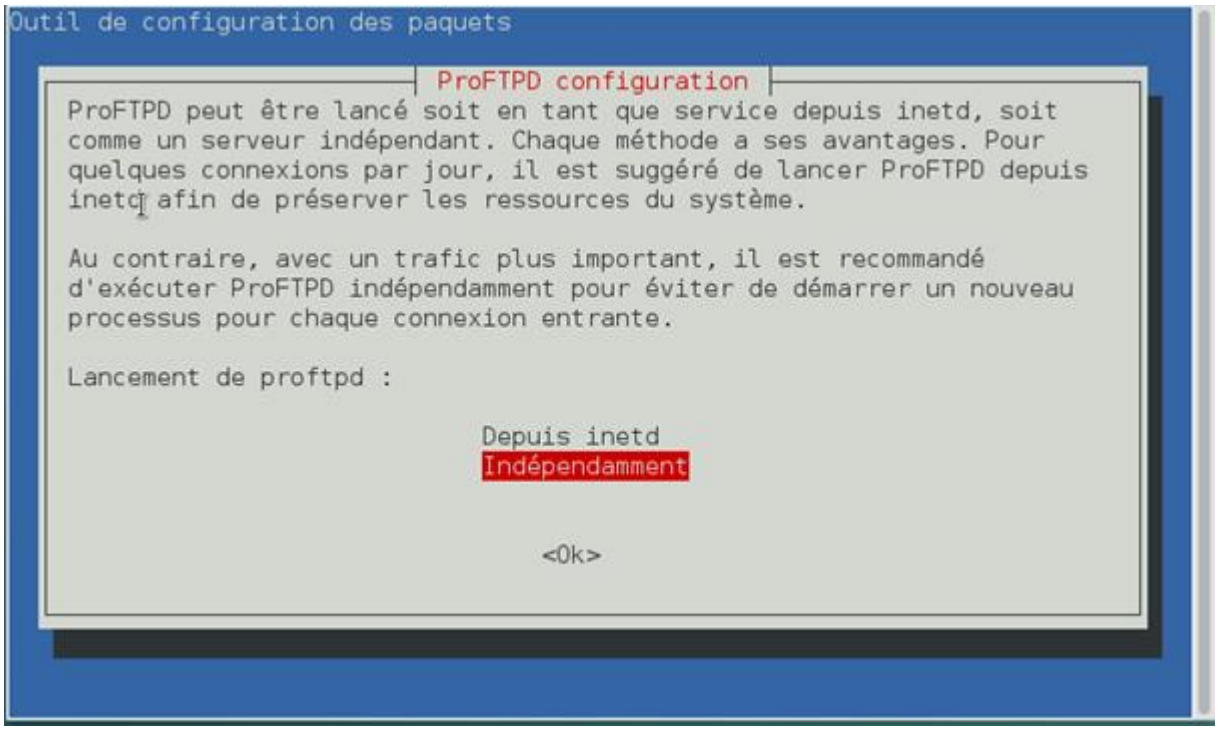
5) Le serveur FTP :

Installation du paquet :

apt-get update *(mise à jour des sources de téléchargements)*

apt-get install proftpd-basic *(installation du service FTP)*

Configuration :



Tout d'abord il faut choisir "Depuis inetd".

On entre alors dans le fichier de configuration *nano /etc/proftpd/proftpd.conf*

On change les paramètres IP du serveur :

Adresse IP : 192.168.3.101

Masque de sous-réseau : 255.255.255.0

Passerelle : 192.168.3.10

On crée ensuite un utilisateur pour l'accès FTP :

```
root@Tom:/etc/proftpd# adduser ftp-esicad31
Ajout de l'utilisateur « ftp-esicad31 » ...
Ajout du nouveau groupe « ftp-esicad31 » (1001) ...
Ajout du nouvel utilisateur « ftp-esicad31 » (1001) avec le groupe « ftp-esicad3
1 » ...
Création du répertoire personnel « /home/ftp-esicad31 »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur ftp-esicad31
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
        Nom complet []:
        N° de bureau []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]
root@Tom:/etc/proftpd#
```

Nous allons donc chiffrer ces informations avec une sécurisation TLS.

Création du certificat SSL auto-signé :

sudo openssl req -new -x509 -days 365 -nodes -out /etc/ssl/certs/proftpd.cert -keyout /etc/ssl/private/proftpd.key

Configurer le serveur FTP à utiliser TLS pour générer une connexion chiffrée.

Créer le fichier tls.conf :

nano /etc/proftpd/conf.d/tls.conf

<IfModule mod_tls.c>

TLSEngine on

TLSLog /var/log/proftpd/tls.log

 # Utilisation du protocol TLSv1 Uniquement

TLSProtocol TLSv1

 # N'autorise que les connexions sécurisées

TLSRequired on

 # Renseigne l'emplacement des certificats

TLSRSACertificateFile /etc/ssl/certs/proftpd.cert

TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key

TLSVerifyClient off

TLSRenegotiate none

</IfModule>

Redémarrer le serveur FTP :

/etc/init.d/proftpd restart

4) Configuration des ACL :

Encore une fois, on ne sait même pas pourquoi tu vas faire des ACL. Il manque la spécification de la demande.

R1#conf t

R1(config)#ip access-list extended accesftp-noping

R1(config-ext-nacl)#deny tcp 192.168.2.0 0.0.0.255 host 192.168.3.10 eq ftp

R1(config-ext-nacl)#deny icmp 192.168.2.0 0.0.0.255 192.168.0.0 0.0.255.255

R1(config-ext-nacl)#exit

R1(config)#interface fastEthernet 0/0.3

R1(config-if)#ip access-list extended accesftp-noping out

Et il manque aussi la validation

Pourtant il y a de très bonnes choses dans ta façon de rédiger, c'est simple, concis et sans fioritures 😉

Mais, il faudrait rajouter

- Rappel du cahier des charges
- Schéma récap du réseau à mettre en place avec les composants
- Un document avec des titres et sous-titres pour générer un sommaire
- Et puis une validation complète

Note : 13/20