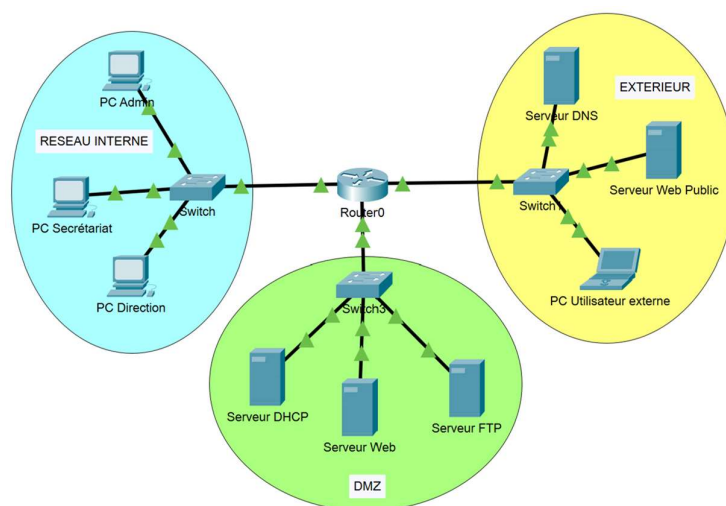


Travaux Pratiques R&T 1^{ère} année

Durée : 3 heures

SAE21

Cisco - Etude de cas



Nom :

Groupe de TP :

Date :

OBJECTIFS - TOPOLOGIE

⇒ Configuration d'un réseau d'entreprise avec VLAN et limitation des accès par ACL

Vous utiliserez pour ce TP le logiciel Cisco Packet Tracer.

Pour l'ensemble des questions suivantes vous décrirez votre façon de procéder dans le **compte rendu de TP** et vous joindrez également votre **fichier Packet Tracer** dans l'espace Cours en ligne.

-MANIPULATIONS

Partie 1 – Création du réseau de l'entreprise

Le réseau privé de l'entreprise (à gauche du schéma) comprend 2 VLAN : 1 pour l'administrateur du réseau (PC Admin), 1 pour le Personnel (PC Secrétariat et PC Direction).

1. Faites une proposition de découpage en sous-réseaux pour le réseau privé de l'entreprise (10.0.0.0/8), précisez les adresses attribuées aux 2 VLAN.

Réseau 10.0.0.0/10

Adresses Vlan :

ADMIN : Réseau 10.64.0.0/10

PERSONNEL : Réseau 10.128.0.0/10

2. Implémentez les VLAN sur le switch et configurez port par port l'affectation des VLAN (Mettre une adresse IP du sous réseau Admin sur l'interface VLAN Admin).

On créer les vlans :

```
Switch(config)#vlan 10
Switch(config-vlan)#name admin
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name personnel
```

On les affectes aux ports :

Vlan 20 :

```
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Vlan 10 :

```
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

On met une ip au vlan admin :

```
Switch(config-if)# ip address 10.0.0.10 255.192.0.0
```

3. Quel sera le type de liaison entre le switch et le routeur ? Expliquez.

Il y aura une liaison de type trunk entre le routeur et switch

4. Implémentez la configuration sur le routeur (routage inter-vlan).

On crée deux interfaces qui seront les passerelles de nos deux vlans :

```
Router(config)#int fa0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.1 255.192.0.0
Router(config-subif)#exit
Router(config)#int fa0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add
Router(config-subif)#ip address 10.64.0.1 255.192.0.0
Router(config-subif)#int fa0/0
Router(config-if)#no shut
```

Sur le switch, on active le mode trunk :

```
Switch(config)#int fa0/4
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,

Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#no shut
Switch(config-if)#exit
```

5. Testez avec la commande ping la communication inter-vlan via le routeur.

On ping pc direction vers pc admin :

```
C:\>ping 10.0.0.20

Pinging 10.0.0.20 with 32 bytes of data:

Reply from 10.0.0.20: bytes=32 time<1ms TTL=127
Reply from 10.0.0.20: bytes=32 time<1ms TTL=127
Reply from 10.0.0.20: bytes=32 time<1ms TTL=127
Reply from 10.0.0.20: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6. Configurez le switch afin que le PC-Admin puisse l'administrer via le protocole SSH.

On configure le switch pour le ssh :

```
Alexis(config)#hostname Alexis
Alexis(config)#ip domain-name alexis.com
```

```
Alexis(config)#enable password 123456
Alexis(config)#crypto key generate rsa
The name for the keys will be: Alexis.alexis.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

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

```
Alexis(config)#line vty 0 4
Alexis(config-line)#transport input ssh
Alexis(config-line)#transport output ssh
Alexis(config-line)#login local
Alexis(config-line)#exit
Alexis(config)#username alexis password 123456
```

Sur le pc admin on teste :

```
C:\>ssh alexis@10.0.0.10
Invalid Command.

C:\>ssh -l alexis 10.0.0.10

Password:

Alexis>enable
Password:
Alexis#
```

7. Mettez en place une ACL afin d'autoriser uniquement le PC-Admin à accéder à la configuration du switch par SSH (les requêtes SSH vers le switch doivent être bloquées pour les machines du personnel) .

```
Alexis(config-ext-nacl)#permit tcp 10.0.0.20 0.0.0.0 eq 22 0.0.0.0 0.0.0.0 eq 22
```

```
Alexis(config-line)#access-class 101 in
Alexis(config-line)#
```

Quand on tente de se connecter sur un pc du vlan personnel, ceci ne fonctionne pas

```
C:\>ssh -l alexis 10.0.0.10

% Connection timed out; remote host not responding
C:\>
```

Partie 2 – Ajout de la DMZ et du réseau extérieur

La DMZ de l'entreprise (en bas du schéma) comprend 3 serveurs (Web, DHCP, FTP). Le réseau extérieur (à droite du schéma) est représenté par deux serveurs publics (Web et DNS) ainsi que par un PC d'un utilisateur extérieur.

1. Configurez le serveur DHCP pour distribuer les IP sur l'ensemble du réseau de l'entreprise (sous-réseaux Admin et Personnel).

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool20	10.64.0.1	0.0.0.0	10.64.0.10	255.192.0.0	5	0.0.0.0	0.0.0.0
serverPool10	10.0.0.1	0.0.0.0	10.0.0.10	255.192.0.0	5	0.0.0.0	0.0.0.0
DMZ	172.25.0.1	0.0.0.0	172.25.0.20	255.255.0.0	20	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.25.0.0	255.255.0.0	512	0.0.0.0	0.0.0.0

2. Mettez en place une ACL afin d'autoriser les PC du sous-réseau Personnel à accéder aux serveurs de la DMZ.

On met en place ceci :

```
Router(config)#access-list 1 deny 10.0.0.0 0.0.0.255
Router(config)#acc
Router(config)#access-list 1 permit 10.64.0.0 0.0.0.255
Router(config)#int fa0/1
Router(config-if)#ip acc
Router(config-if)#ip access-group 1 out
Router(config-if)#ex
Router(config)#int fa0
Router(config)#int fa0/1
Router(config)#int fa0/0
Router(config-if)#ip
Router(config-if)#ip acc
Router(config-if)#ip access-group 1 in
```

Sur le pc personnel :

```
C:\>ping 172.25.0.12

Pinging 172.25.0.12 with 32 bytes of data:

Reply from 172.25.0.12: bytes=32 time<1ms TTL=127
Reply from 172.25.0.12: bytes=32 time<1ms TTL=127
Reply from 172.25.0.12: bytes=32 time<1ms TTL=127
Reply from 172.25.0.12: bytes=32 time<1ms TTL=127

Ping statistics for 172.25.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Sur le pc admin :

```
C:\>ping 172.25.0.12

Pinging 172.25.0.12 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
```

3. Mettez en place une ACL afin d'autoriser les PC du sous-réseau Personnel à accéder aux serveurs extérieurs.

```
Router(config)#access-list 2 permit 10.64.0.0 0.0.0.255
Router(config)#int fa0/4
%Invalid interface type and number
Router(config)#int eth0/1/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 2 out
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip
Router(config-if)#ip acc
Router(config-if)#ip access-group 2 in
Router(config-if)#
```

On ping depuis personnel :

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.12: bytes=32 time<1ms TTL=127
Reply from 192.168.1.12: bytes=32 time<1ms TTL=127
Reply from 192.168.1.12: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4. Depuis le PC Secretariat, vérifiez les accès vers les serveurs Web interne (HTTP) et externe (HTTPS).

5. Mettez en place une ACL afin d'autoriser le PC extérieur à accéder au serveur web de la DMZ en HTTPS.