

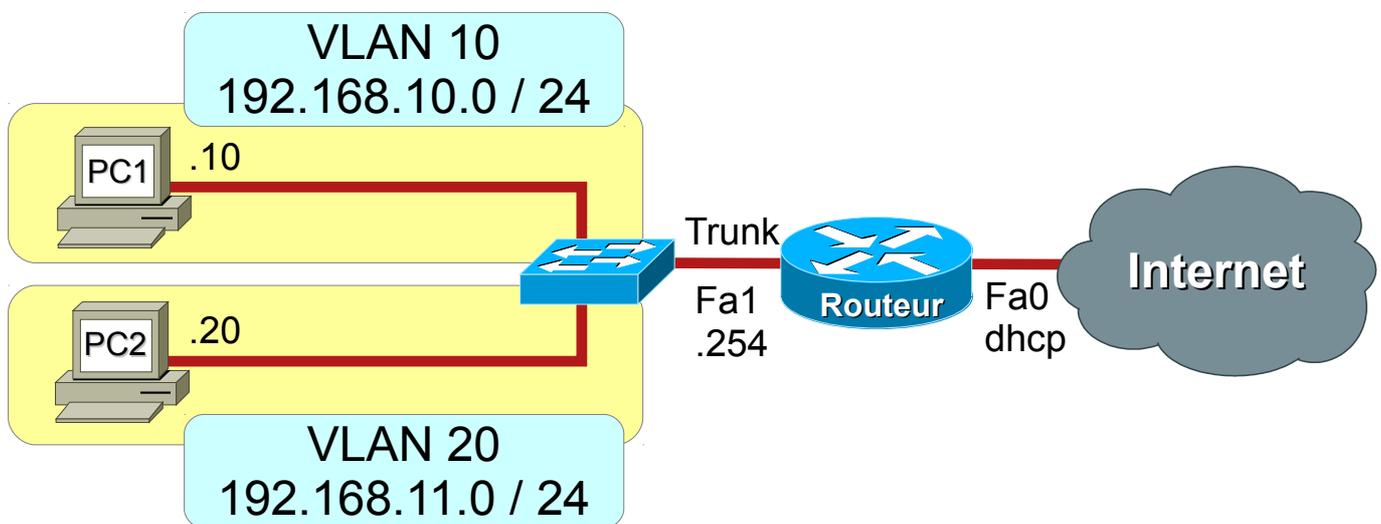
TP 1

Liste de contrôle d'accès

Réseaux et Télécoms – IUT d'Auxerre – Université de Bourgogne

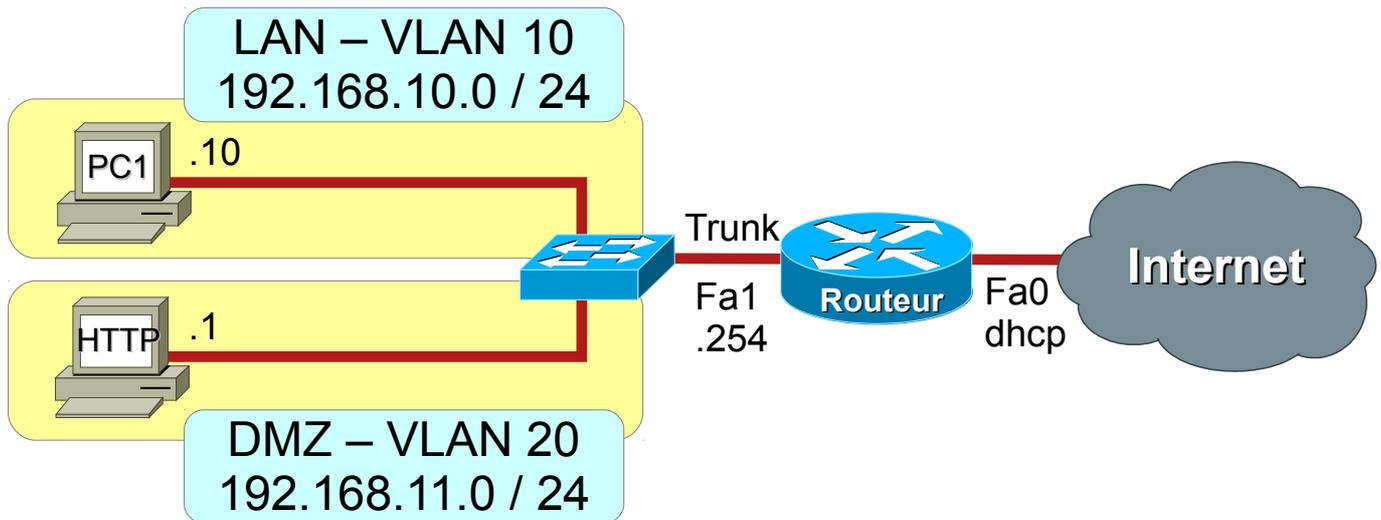
Exercice 1 :

Initialisez le matériel et câblez le schéma réseau ci-dessous.



- Configurez les différents éléments du réseau (sans ACL), et validez son fonctionnement.
- Configurez des ACL sur le routeur qui applique la stratégie de sécurité suivante :
 - Autorise les hôtes des VLAN avec une adresse IP paire à communiquer entre eux
- Validez le fonctionnement du réseau et de la stratégie de sécurité avec des commandes de diagnostic.
- Initialisez et désactivez les ACL du routeur, et validez le fonctionnement du réseau.
- Configurez des ACL sur le routeur qui applique la stratégie de sécurité suivante :
 - Autorise le VLAN 10 à accéder à Internet sauf le PC1
- Validez le fonctionnement du réseau et de la stratégie de sécurité avec des commandes de diagnostic.

Exercice 2 :



- a) Initialisez et désactivez les ACL sur le routeur, et configurez un serveur HTTP et SSH dans le VLAN 20. Validez le fonctionnement du réseau et du serveur.
- b) Configurez des ACL sur le routeur qui applique la stratégie de sécurité suivante :
 - Autorise le LAN à naviguer sur le Web (HTTP, DNS)
 - Autorise les connexions HTTP à destination du serveur de la DMZ
 - Autorise les requêtes `ping` à destination du serveur de la DMZ
 - Autorise le PC1 à se connecter en SSH sur le serveur de la DMZ
- c) Validez le fonctionnement du réseau et de la stratégie de sécurité avec des commandes de diagnostic.

Annexe

Configuration des ACL étendues nommées sur routeur Cisco

- **Syntaxe générale d'une ACL étendue**

```
ip access-list extended NOM_ACL
  {permit | deny | remark} protocole
  adresse_source masque_générique [opérateur port]
  adresse_destination masque_générique [opérateur port]
  [icmp-type] [established]
```

- **Configuration d'une ACL étendue**

```
! Crée une ACL étendue
ip access-list extended NOM_ACL

! Intègre un commentaire
remark Commentaire

! Autorise le trafic IP
permit ip adresse_source masque_générique
adresse_destination masque_générique

! Refuse le trafic IP
deny ip adresse_source masque_générique
adresse_destination masque_générique

! Autorise une connexion TCP
permit tcp adresse_source masque_générique [eq port]
adresse_destination masque_générique [eq port]

! Refuse une connexion TCP
deny tcp adresse_source masque_générique [eq port]
adresse_destination masque_générique [eq port]

! Autorise un connexion TCP établie
permit tcp adresse_source masque_générique [eq port]
adresse_destination masque_générique [eq port]
established

! Autorise les requêtes echo ICMP (ping)
permit icmp adresse_source masque_générique
adresse_destination masque_générique echo

! Autorise les réponses echo ICMP (ping)
permit icmp adresse_source masque_générique
adresse_destination masque_générique echo-reply
```

- **Configuration d'une interface avec une ACL nommée**

```
! Sélectionne une interface
interface nom_interface

! Active une ACL en entrée
ip access-group NOM_ACL in

! Active une ACL en sortie
ip access-group NOM_ACL out
```

- **Mots-clés**

```
any : 0.0.0.0 / 255.255.255.255
host adresse : adresse / 0.0.0.0
```

- **Protocoles**

```
icmp
ip
tcp
udp
```

- **Opérateurs**

```
lt : inférieur à
gt : supérieur à
eq : égal à
neq : non égal à
```

- **Diagnostic**

```
show access-lists [acl-name]
show ip access-lists [acl-name]
show ip interface [interface-name]
```

Configuration d'un commutateur Cisco

- **Configuration de VLAN**

```
! Création d'un VLAN
vlan numéro_vlan

! Affectation d'un VLAN à un groupe d'interfaces
interface range Fa0/min - max
  switchport mode access
  switchport access vlan numéro_vlan

! Configuration d'un port en agrégation de VLAN 802.1Q
interface nom_interface
  switchport mode trunk
```

- **Diagnostic**

```
! Affiche la liste des VLAN
show vlan

! Affiche les agrégations de VLAN
show interface trunk
```

Configuration d'un routeur Cisco

- **Configuration d'une interface avec agrégation de VLAN 802.1Q**

```
! Interface physique
interface nom_interface_physique
  no ip address
  no shutdown

! Interface VLAN
interface nom_interface_physique.numéro_vlan
  encapsulation dot1q numéro_vlan
  ip address adresse masque
  no shutdown
```

- **Configuration du NAT**

```
! Définit une interface dans le réseau interne
! LAN privé
interface nom_interface
  ip nat inside

! Définit une interface dans le réseau externe
! WAN public
interface nom_interface
  ip nat outside

! Autorise le LAN à être traduit
ip access-list standard ACL_NAT
  permit any

! Active la traduction NAT
ip nat inside source list ACL_NAT interface nom_interface_public overload
```

- **Configuration du transfert de port**

```
ip nat inside source static tcp adresse_interne port_interne
adresse_externe port_externe
```