

DHCP :

Conf t

Ip dhcp pool vlan1

Network 10.1.0.0 255.255.0.0

Default-router 10.1.0.254

Ip dhcp excluded-address 10.1.0.254

Ip dhcp pool vlan1

Ip dhcp excluded-address 10.1.0.53

Pour vlan :

Changer les vlan sur le switch et mettre le port relié au router en dot1q

Création du vlan 1 (SI) :

---

Conf t

Interface fastethernet 0/0

No shut

Exit

Interface fastethernet 0/0.1

Encapsulation dot1q 1

Ip addr 10.1.0.254 255.255.0.0

No shut

Exit

Interface fastethernet 0/0.2

Encapsulation dot1q 2

Ip addr 10.2.0.254 255.255.0.0

No shut

Exit

Interface fashethernet 0/0.3

Ip addr 10.3.0.254 255.255.0.0

No shut

Exit

---

Vlan 2 (administratif)

Vlan 3 (commerciaux)

Pour les autres vlan il faut changer les ip de réseau et de router par les bonnes ip (selon chaque vlan).

Les dns sont en .53 et router en .254

Vlan1=Service informatique

Vlan2=administratif

Vlan3=commerciaux

Ip dns : 10..53

Exemple acl pour config (donc a adapté avec nos nom de reseau et nos IP) :

On autorise la machine 192.168.2.12 à se connecter via ssh à toutes les machines du réseau 192.168.3.0/24 :

```
R2(config)#ip access-list extended reseau-secretariat
```

```
R2(config-ext-nacl)#permit tcp host 192.168.2.12 gt 1023 192.168.3.0 0.0.0.255 eq 22
```

```
R2(config-ext-nacl)#permit udp host 192.168.2.30 eq 53 192.168.3.0 0.0.0.255 gt 1023
```

```
R2(config-ext-nacl)#permit tcp any any established
```

```
R2(config-ext-nacl)#deny ip any any log
```

Commande pour interdire a un réseau(le 10.1.1.0 ici) de communiquer avec un autre (ici 10.1.2.0)

```
access-list 1 deny 10.1.2.0 0.0.0.255
```

Ensuite il faut se mettre sur l'interface que l'on veut (avec les vlans c'est les fa 0/0.x (x numéro de vlan)) et faire : `ip access-group 1 out`