# Procédure d’installation et de configuration des équipements.

# Activer SSH

router> enable

router# configure terminal

router(config)# username **admin** password **admin**

router(config)# hostname **Ragence1**

RAgence1(config)# ip domain-name **cylon.com**

RAgence1(config)# crypto key generate rsa modulus 1024

The name for the keys will be: 2960-RG.mondomaine.fr

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RAgence1(config)#ip ssh version 2

RAgence1(config)#ip ssh time-out 60

RAgence1(config)#ip ssh authentication-retries 3

RAgence1(config)# line vty 0 4

RAgence1(config-line)# transport input ssh

RAgence1(config-line)# login local

RAgence1(config-line)# exit

RAgence1#show ip ssh

# Supprimer SSH

2960-RG(config)#crypto key zeroize rsa

% All RSA keys will be removed.

% All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no]: yes

# Filtrer l’accès au SSH

*Dans la commande suivante, la liste de contrôle d’accès a le numéro 10 et le réseau autorisé à se connecter en ssh est 192.168.100.0/24.*

Switch(config)#access-list 10 permit 192.168.100.0 0.0.0.255

*Ensuite, on autorise la connexion exclusive de ce réseau sur les terminaux virtuel avec la commande access-class:*

Switch(config)#line vty 0 15

Switch(config-line)#access-class 10 in

# Filtrer l’accès sur une interface

Sur un switch de niveau 3

Switch>enable

Switch#conf t

Switch(config)#vlan 10

Switch(config-vlan)#ex

Switch(config)#vlan 20

Switch(config-vlan)#ex

Switch(config)#int vlan 10

Switch(config-if)#ip add 10.0.0.254 255.0.0.0

Switch(config-if)#ex

Switch(config)#int vlan 20

Switch(config-if)#ip add 10.0.0.254

Switch(config-if)#ex

Switch(config)#int fa0/1

Switch(config-if)#switchport access vlan 10

Switch(config-if)#ex

Switch(config)#int fa0/2

Switch(config-if)#switchport access vlan 20

Switch(config-if)#ex

Switch(config)#ip routing

Switch(config)# access-list 1 deny 11.0.0.1 0.0.0.0

Switch(config)#access-list 1 permit any

Switch(config)#int vlan 10

Switch(config-if)# ip access-group 1 out

Switch(config-if)# ip access-group 1 in

Switch(config-if)#ex

# Création d’un vlan numéro 2 (switch)

Switch>enable

Switch#conf t

Switch(config)#vlan 2

Switch(config)#name vlan2

Switch(config)#exit

# Affecter un port à un vlan (switch)

Switch>enable

Switch#conf t

Switch(config)#interface fa0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 2

Switch(config-if)#exit

Switch(config)#exit

# Attribuer une plage d’adresse IP

Switch>enable

Switch#conf t

Switch(config)#int vlan 2

Switch(config-if)# ip add 192.168.0.254 0.0.0.255

Switch(config-if)#exit

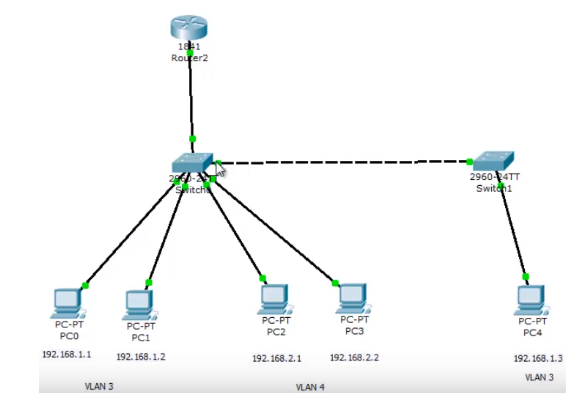
Switch(config)#exit

# Vérifier les vlans

Switch>enable

Switch# show vlan brief

# Configurer VTP



**Switch 1 : serveur (gauche) :**

Switch>enable

Switch#conf t

Switch(config)#int “nom de l’interface liée au switch client“

Switch(config-if)# switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

**Switch 2 : client (droite):**

Switch>enable

Switch#conf t

Switch(config)#int “nom de l’interface liée au switch serveur“

Switch(config-if)# switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

**Switch 1 : serveur (gauche) :**

Switch>enable

Switch#conf t

Switch(config)#vtp domain « nom de domaine »

Switch(config)#vtp mode server

Switch(config)#exit

**Switch 2 : client (droite):**

Switch>enable

Switch#conf t

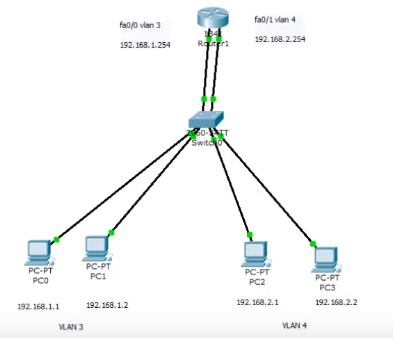
Switch(config)#vtp domain « nom de domaine »

Switch(config)#vtp mode client

Switch(config)#exit

(client : récupère la configuration du serveur et peut la retransmettre / transparent : transmet la configuration du server)

# Communication entre 2 vlans



**Configuration du routeur**

Configurer les adresses ip des interfaces

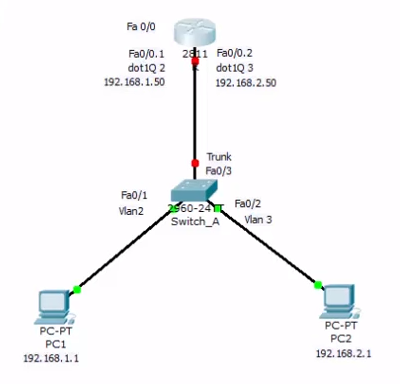
**Configuration du switch**

Ajouter les adresses de sortie aux VLANs correspondants (voir partie « Affecter un port à un VLAN page 1)

**Configuration des pcs**

Ajouter la passerelle aux différents pcs, la passerelle est l’adresse IP de l’interface du routeur relié au VLAN. (VLAN 3 : 192.168.1.254 / VLAN 4 : 192.168.2.254)

# Communication entre plusieurs vlans



Configuration du switch:

Switch>enable

Switch#conf t

Switch(config)#int “nom de l’interface liée au switch serveur“

Switch(config-if)# switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

Configuration du routeur:

Router>enable

Router #conf t

Router(config)# interface “nom de l’interface d’entrée du routeur“

(Exemple : pour le réseau 192.168.1.0/24 l’interface est : Fa0/0.1)

Router(config-if)# encapsulation dot1Q “numero du vlan“

Configurer l’adresse IP

Allumer l’interface physique (fa0/0)

# Configuration du firewall

ciscoasa>enable

ciscoasa#show run

ciscoasa#conf t

ciscoasa(config)#int vlan 1

ciscoasa(config-if)#no ip address

ciscoasa(config-if)#exit

ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside

ciscoasa(config)#end

ciscoasa#conf t

ciscoasa(config)#int vlan 1

ciscoasa(config-if)#ip address 192.168.1.1 255.255.254.0

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#ex

ciscoasa(config)#int e0/1

ciscoasa(config-if)#switchport access vlan 1

ciscoasa(config-if)#ex

ciscoasa(config)#int vlan 2

ciscoasa(config-if)#ip address 203.1.1.2 255.255.255.0

ciscoasa(config-if)#no sh

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#ex

ciscoasa(config)#int e0/0

ciscoasa(config-if)#switchport access vlan 2

# Config OSPF

ISP>en

ISP#conf t

ISP(config)#router ospf 1

ISP(config-router)#network 203.1.1.0 0.0.0.255 area 0

# Création objet network + Enable NAT

ciscoasa#conf t

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.1.1.1

ciscoasa(config)#object network LAN

ciscoasa(config-network-object)#subnet 192.168.0.0 255.255.254.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

# Create access-list

ciscoasa#conf t

ciscoasa(config)#access-list in\_to\_internet extended permit tcp any any

ciscoasa(config)#access-list in\_to\_internet extended permit icmp any any

ciscoasa(config)#access-group in\_to\_internet in interface outside

# Vérifier le NAT

ciscoasa#show xlate

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net

ICMP PAT from inside:172.16.1.5/13 to outside:203.1.1.2/23555 flags i idle 00:00:08, timeout 0:00:30

ciscoasa#show nat

Auto NAT Policies (Section 2)

1 (inside) to (outside) source dynamic LAN interface

translate\_hits = 144, untranslate\_hits = 142

# DMZ

ciscoasa(config)#int vlan 3

ciscoasa(config-if)#no forward interface vlan 1

ciscoasa(config-if)#ip address 10.10.10.1 255.255.255.0

ciscoasa(config-if)#no sh

ciscoasa(config-if)#nameif DMZ

INFO: Security level for "DMZ" set to 0 by default.

ciscoasa(config-if)#security-level 50

ciscoasa(config-if)#ex

ciscoasa(config)#int et0/2

ciscoasa(config-if)#switchport access vlan 3

ciscoasa(config-if)#end

ciscoasa#conf t

ciscoasa(config)#object network WEBSERVER

ciscoasa(config-network-object)#host 10.10.10.10

ciscoasa(config-network-object)#nat (dMZ,outside) static 203.1.1.3

ciscoasa(config-network-object)#ex

ciscoasa#conf t

ciscoasa(config)#access-list outtodmz extended permit tcp any host 10.10.10.10 eq www

ciscoasa(config)#access-group outtodmz in interface outside

ciscoasa(config)#object network DMZ-SUBNET

ciscoasa(config-network-object)#subnet 10.10.10.0 255.255.255.0

ciscoasa(config-network-object)#nat (dMZ,outside) dynamic interface

ciscoasa(config-network-object)#ex

# Création d’un hsrp

Sur le routeur principal:

router> enable

router# configure terminal

router(config)# int fa0/0

router(config-if)# standby 2 ip 192.168.10.1

router(config-if)# standby 2 priority 150

router(config-if)# standby 2 preempt

Sur le routeur de backup :

router> enable

router# configure terminal

router(config)# int fa0/0

router(config-if)# standby 2 ip 192.168.10.1

router(config-if)# standby 2 priority 90

router(config-if)# standby 2 preempt