TP 1 Port-Security : Manipulation de la fonction Port-Security, cette dernière permet de contrôler les adresses MAC autorisées sur un port. En cas de "*violation*", c'est-à-dire en cas d'adresses MAC non autorisées sur le port, une action est prise

-Activation

```
(config)#interface G0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
```

On peut fixer le nombre d'adresses MAC autorisées, ici par exemple 1

```
(config-if)#switchport port-security maximum 1
(config-if)#switchport port-security mac-address sticky
(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

Les adresses MAC apprises peuvent être **inscrites dynamiquement dans la configuration courante (**running-config**) avec le mot clé "**sticky**"** :

```
(config-if)#switchport port-security mac-address sticky
```

Les adresses MAC autorisées peuvent être fixées :

```
(config-if)#switchport port-security mac-address 0000.0000.0003
```

Une "Violation" est une action prise en cas de non-respect d'une règle port-security.

```
(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

Diagnostic port-security

```
#show port-security
```

TP 2 Storm-control

Le contrôle de tempête empêche le trafic tel qu'une émission, une Multidiffusion, ou une tempête d'unicast sur une des interfaces physiques du commutateur.. Le trafic excessif dans le RÉSEAU LOCAL, désigné sous le nom d'une tempête de RÉSEAU LOCAL, mènera à une dégradation des performances du réseau.

```
Switch(config-if)#storm-control unicast level 85
Switch(config-if)#storm-control broadcast level 30
Switch(config-if)#storm-control action shutdown
```

TP 3 DHCP Snooping

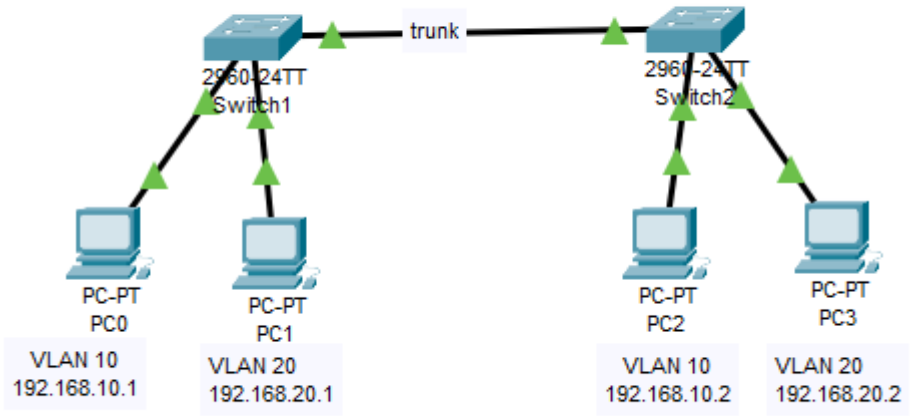
Le DHCP snooping est une fonction de sécurité intervenant au deuxième niveau du modèle OSI. Cette fonction est intégrée dans le **commutateur** connectant les clients aux serveurs DHCP. En d'autres termes, il s'agit d'un protocole qui contrôle tout d'abord l'ensemble des informations DHCP passant par le commutateur. Seuls les paquets autorisés provenant de serveurs dignes de confiance sont transmis aux clients.

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10,20

Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
```

TP4 Trunk :

L'objectif de ce TP est de faire communiquer les machines issues du même vlan même si elles sont sur deux switches différents

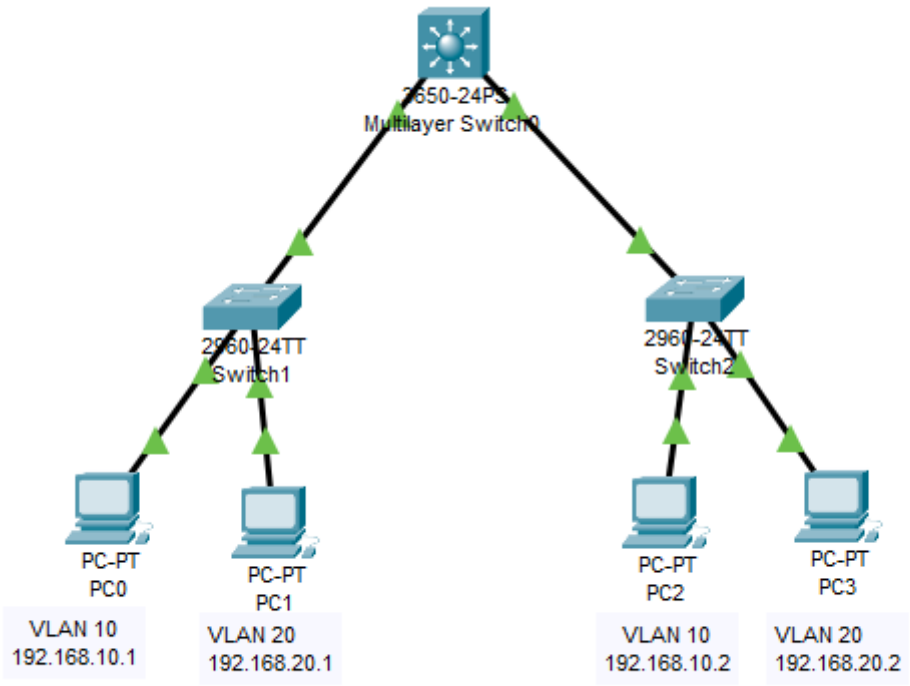


Configuration des switchs sw1 et sw2

interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20
switchport mode trunk
!

TP5 Routage inter-vlan :

L'objectif de ce tp est de faire communiquer les machines issues de deux vlan différents



Configuration des switchs sw1 et sw2

interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20
switchport mode trunk
!

Configuration DS

ip dhcp pool rsd
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
dns-server 8.8.8.8

ip dhcp pool mmi
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
dns-server 8.8.8.8

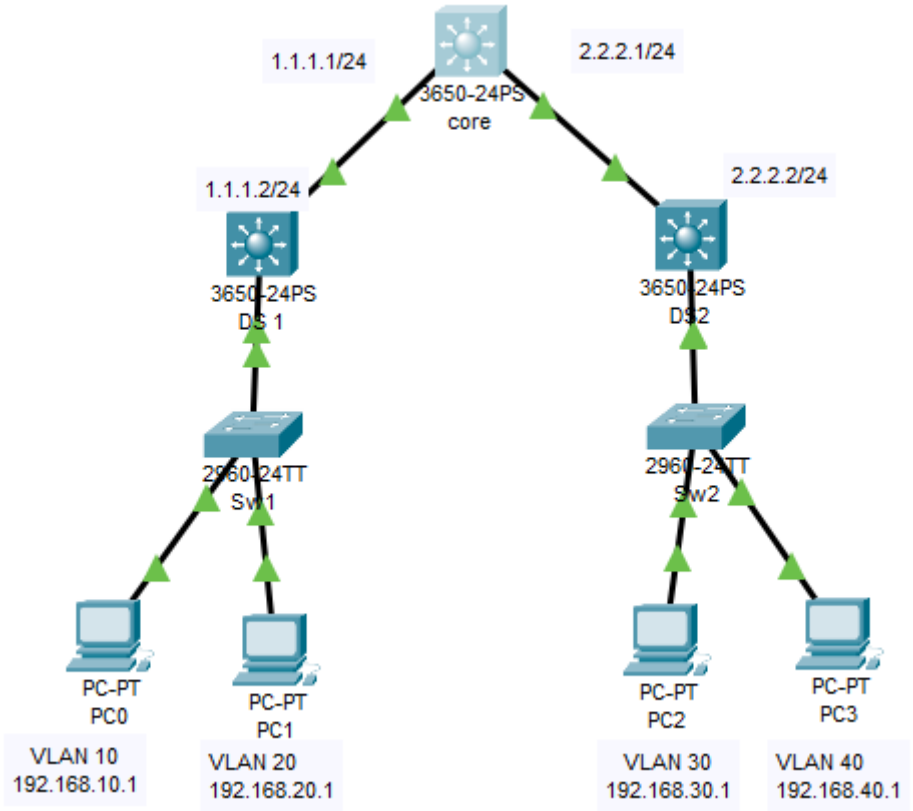
ip routing

interface GigabitEthernet1/0/1

switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk

interface GigabitEthernet1/0/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk

TP6 Schéma global core-distribution-access :



Config DS1

ip dhcp pool rsd

```
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
dns-server 8.8.8.8
!
ip dhcp pool mmi
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
dns-server 8.8.8.8
!
ip cef
ip routing
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/24
no switchport
ip address 1.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan10
mac-address 000b.beeb.9701
ip address 192.168.10.254 255.255.255.0
!
interface Vlan20
mac-address 000b.beeb.9702
ip address 192.168.20.254 255.255.255.0
!
router rip
version 2
network 1.0.0.0
network 192.168.10.0
network 192.168.20.0
no auto-summary
```

Config DS2

```
ip dhcp pool vlan30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.254
dns-server 8.8.8.8
!
ip dhcp pool vlan40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.254
dns-server 8.8.8.8
!
```

```
ip routing
!
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 30,40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/24
no switchport
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan30
mac-address 0001.63ad.6c01
ip address 192.168.30.254 255.255.255.0
!
interface Vlan40
mac-address 0001.63ad.6c02
ip address 192.168.40.254 255.255.255.0
!
router rip
version 2
network 2.0.0.0
network 192.168.30.0
network 192.168.40.0
no auto-summary
!
```

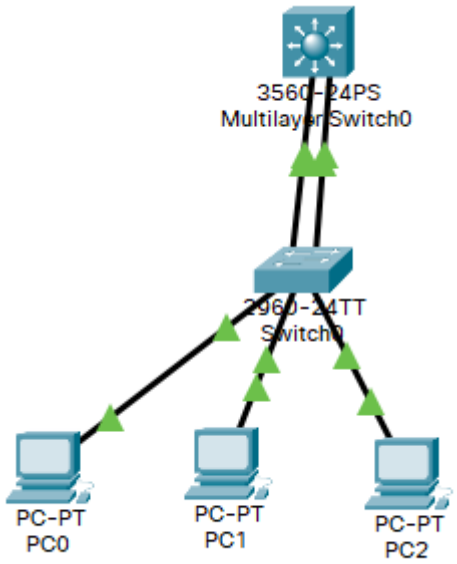
Config CS

```
!
ip routing
!
interface GigabitEthernet1/0/1
no switchport
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
no switchport
ip address 2.2.2.1 255.255.255.0
duplex auto
speed auto
!
!
router rip
version 2
```

network 1.0.0.0
network 2.0.0.0
!

TP6 ETherchannel :

L'objectif de cette agrégation (Etherchannel) est d'augmenter la bande passante et d'assurer la tolérance aux pannes en fusionnant plusieurs liens physiques par un seul lien logique.



Config Switch0

```
Switch0(config)#interface range g0/1-2
Switch0(config-if-range)#channel-group 1 mode auto
```

Config MultilayerSwitch0

```
MultilayerSwitch0(config)#interface range g0/1-2
MultilayerSwitch0(config-if-range)#channel-group 1 mode desirable
```

Pour vérifier votre configuration d'agrégation faites comme suit:

```
MultilayerSwitch0#show etherchannel summary
```

```
MultilayerSwitch0#sh interfaces port-channel 1
```

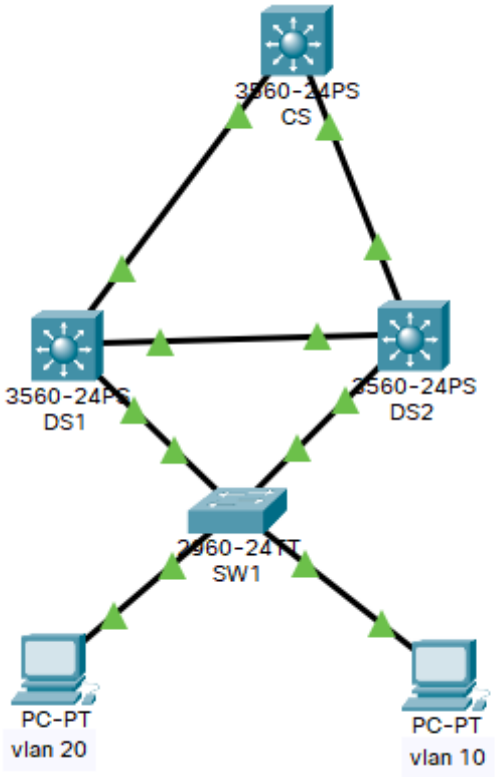
Pour configurer le port agrégé faites comme suit :

```
SW1(config)#interface port-channel 1
```

TP7 HSRP :

HSRP (Hot Standby Routing Protocol) est utilisé pour assurer une disponibilité accrue de la passerelle d'un réseau. L'adresse IP de la passerelle est configurée sur deux routeurs différents. Une seule de ces deux interfaces est active. Si l'interface active n'est plus accessible, l'interface passive devient active.

Dans ce TP nous allons réaliser la redondance des passerelles du routage inter-VLAN



Config DS1

```
DS1(config)#interface Vlan10
DS1(config-if)#ip address 192.168.10.252 255.255.255.0
DS1(config-if)#standby 1 ip 192.168.10.254
DS1(config-if)#standby 1 priority 150
DS1(config-if)#standby 1 preempt
!
DS1(config)#interface Vlan20
DS1(config-if)#ip address 192.168.20.252 255.255.255.0
DS1(config-if)#standby 2 ip 192.168.20.254
DS1(config-if)#standby 2 priority 150
DS1(config-if)#standby 2 preempt
```

Config DS2

```
DS2(config)#interface Vlan10
DS2(config-if)#ip address 192.168.10.253 255.255.255.0
DS2(config-if)#standby 1 ip 192.168.10.254
!
DS2(config)#interface Vlan20
DS2(config-if)#ip address 192.168.20.253 255.255.255.0
DS2(config-if)#standby 2 ip 192.168.20.254
```

Verification de la configuration:

```
DS2#show standby
```