

Compte-rendu

Contexte :

L'association M2L a sollicité notre expertise pour la mise en place d'une architecture réseau qui garantira la redondance et la sécurité.

Pour cela, nous proposons un réseau composé de trois routeurs Cisco 1841 configurés avec les protocoles de routage RIP et HSRP pour assurer une disponibilité optimale. Trois commutateurs Catalyst 3750 seront utilisés pour connecter les différents réseaux entre eux, en veillant à sécuriser les ports des commutateurs reliés aux ordinateurs pour renforcer la sécurité des réseaux. Un serveur web sera accessible pour les utilisateurs et des tests seront effectués sur l'infrastructure à partir d'un poste client.

Sommaire:

- 1 - Configuration des cartes réseaux de la machine cliente et du serveur
- 2 - Configuration des interfaces des routeurs
- 3 - Mise en place du protocole RIP sur les routeurs
- 4 - Mise en place de la redondance avec HSRP sur les routeurs
- 5 - Sécurisation des ports des commutateurs
- 6 - Configuration NAT sur les routeurs
- 7 - Mise en place du serveur web
- 8 - Test de la redondance et de la sécurisation des ports

Prérequis :

- Trois commutateurs Catalyst 3750
- Trois routeurs Cisco 1841
- Un Serveur Web
- Deux Stations clientes Windows 10
- Un accès Administrateur au serveur
- Le logiciel VMware Workstation pro 2016

Explication :

L'infrastructure décrite comporte plusieurs composants permettant de fournir une haute disponibilité avec HSRP, sécurisation des ports et du routage dynamique avec RIP. Voici une explication détaillée de chaque élément :

La haute disponibilité se fera avec deux routeurs (router0 et router1), ils garantissent une disponibilité si un des routeurs tombent.

Le routage dynamique RIP permettra de faire communiquer les tables de routage entre les différents routeurs afin de faire communiquer les trois réseaux.

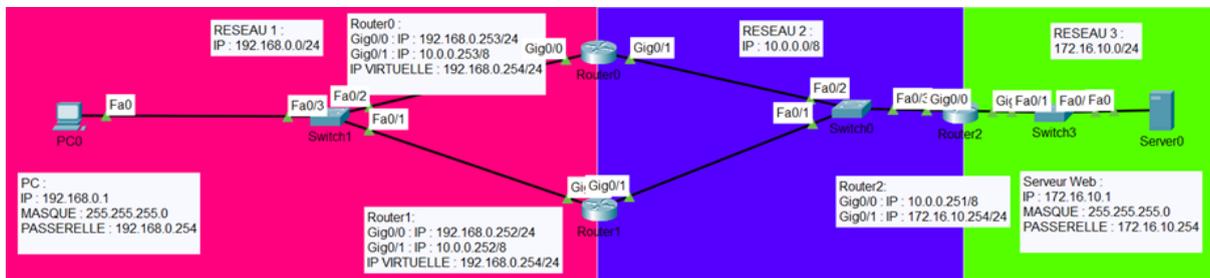
Une sécurisation des ports avec l'adresse MAC des hôtes est mise en place sur les commutateurs afin de garantir notre réseau.

Un serveur web avec une page web sera présent pour être accessible depuis une machine cliente.

Le but est de garantir un accès à ce serveur web lorsqu'un routeur tombe en panne.

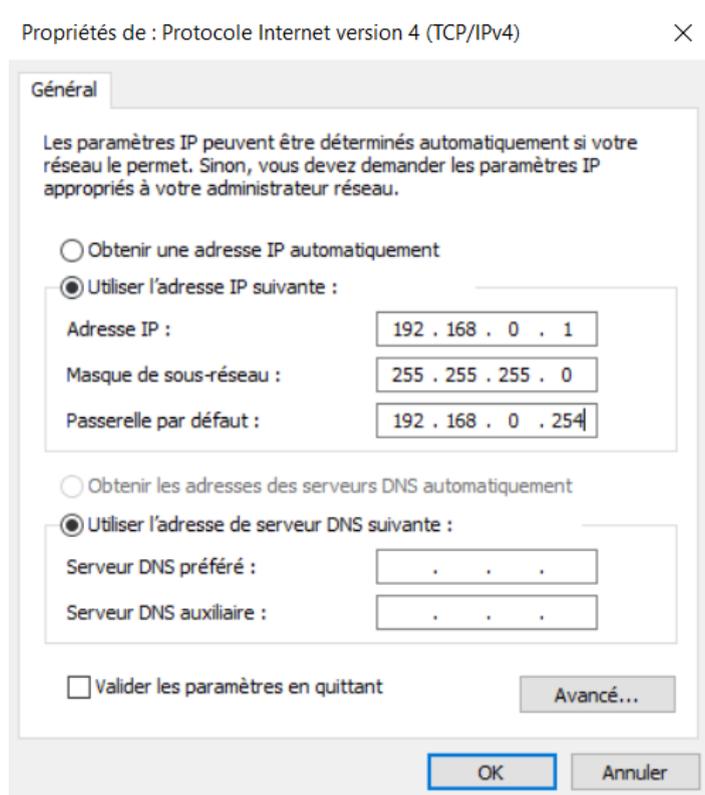
Enfin, le protocole NAT sera utilisé ici de manière à masquer l'adresse venant de la machine client vers le serveur web pour ne pas savoir quel hôte envoie des requêtes.

Schéma de la mission :



Tutoriel :

1- Configuration des cartes réseaux de la machine cliente et du serveur



On vient de modifier la configuration ip de la carte réseau de la machine cliente.

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses: [172.16.10.1/24]
      routes:
        - to: default
          via: 172.16.10.254
  version: 2
```

On modifie la configuration ip du serveur web.

2- Configuration des interfaces des routeurs

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#ip address 192.168.0.253 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
Jan 2 12:10:06.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#
```

On donne une adresse à l'interface Fa0/0 du routeur0 puis on active l'interface.

Amine Boukherouba BTS SIO SISR

```
Router(config-if)# interface FastEthernet0/1
Router(config-if)# ip address 10.0.0.253 255.0.0.0
Router(config-if)# no sh
Router(config-if)#
Jan 2 12:12:17.215: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Jan 2 12:12:18.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

On fait de même avec l'interface Fa0/1.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)# ip address 192.168.0.252 255.255.255.0
Router(config-if)# no sh
Router(config-if)#
Jan 2 12:14:16.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

On donne une adresse à l'interface Fa0/0 du routeur1 puis on active l'interface.

```
Router(config-if)# interface FastEthernet0/1
Router(config-if)# ip address 10.0.0.252 255.0.0.0
Router(config-if)# no sh
Router(config-if)#
Jan 2 12:15:09.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

On fait de même avec l'interface Fa0/1.

```
Router(config)#interface FastEthernet0/0
Router(config-if)# ip address 10.0.0.251 255.0.0.0
Router(config-if)# no sh
Router(config-if)#
Jan 2 12:15:45.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

On donne une adresse à l'interface Fa0/0 du routeur2 puis on active l'interface.

```
Router(config-if)#interface FastEthernet0/1
Router(config-if)# ip address 172.16.10.254 255.255.255.0
Router(config-if)# no sh
Router(config-if)#
Jan 2 12:16:35.887: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Jan 2 12:16:36.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

On fait de même avec l'interface Fa0/1.

3- Mise en place du protocole RIP sur les routeurs

```
Router(config-if)#router rip
Router(config-router)# version 2
Router(config-router)# network 10.0.0.0
Router(config-router)# network 192.168.0.0
Router(config-router)# no auto-summary
```

On active RIP puis on déclare nos réseaux sur les routeur0 et routeur1.

```
Router(config-if)#router rip
Router(config-router)# version 2
Router(config-router)# network 10.0.0.0
Router(config-router)# network 172.16.0.0
Router(config-router)# no auto-summary
```

Puis, on fait de même avec le routeur2.

4- Mise en place de la redondance avec HSRP sur les routeurs

```
Router(config-router)#interface FastEthernet0/0
Router(config-if)#standby 10 ip 192.168.0.254
Router(config-if)# standby 10 priority 105
Router(config-if)# standby 10 preempt
Router(config-if)#
```

On met en place une ip virtuelle qui sera 192.168.0.254 avec une priorité de 105 sur le routeur0.

```
Router(config-router)# interface FastEthernet0/0
Router(config-if)#standby 10 ip 192.168.0.254
Router(config-if)# standby 10 preempt
Router(config-if)#
```

On met aussi cette ip virtuelle sur le routeur1.

5- Sécurisation des ports des commutateurs

```
interface FastEthernet1/0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address fc3f.dbf9.94ac
```

On se connecte à l'interface Fa1/0/3 sur le switch1 puis on active la sécurité sur le port avec l'adresse mac du PC CLIENT.

```
Switch(config)#exit
Switch#show port-security interface FastEthernet1/0/3
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : fc3f.dbf9.94ac:1
Security Violation Count : 0
```

On remarque que l'interface se retrouve avec le port sécurité activé avec un shutdown en cas de violation.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet2/0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address 2C-F0-5D-FC-E1-13
Switch(config-if)#switchport port-security mac-address 00-0C-29-BA-82-38
Switch(config-if)#switchport port-security violation shutdown
```

On se connecte à l'interface Fa2/0/2 sur le switch3 puis on active la sécurité sur le port avec l'adresse mac du serveur web et du pc qui sert à virtualiser (machine VM).

```
Switch#show port-security interface FastEthernet2/0/2
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses    : 2
Configured MAC Addresses : 2
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Switch#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       000c.29ba.8238   SecureConfigured    Fa2/0/2  -
1       2cf0.5dfc.e113   SecureConfigured    Fa2/0/2  -
-----
Total Addresses in System (excluding one mac per port)  : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

On remarque que l'interface se retrouve avec le port sécurité activé avec un shutdown en cas de violation. On retrouve bien les deux adresses mac.

6- Configuration NAT sur les routeurs

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
```

On souhaite masquer les adresses ip privé venant de l'interface fa0/0 (PC). Cela permet d'avoir une protection supplémentaire.

```
Router(config-if)# interface FastEthernet0/1
Router(config-if)# ip nat outside
```

Normalement , on fait cela sur une interface publique mais étant donné que c'est un réseau privé n'allant pas sur internet on fait cela en privé. On affiche donc une seule adresse ip

7- Mise en place du serveur web

```
serverlinux@serverlinux:~$ sudo apt update
```

```
serverlinux@serverlinux:~$ sudo apt upgrade
```

On met à jour à jour la liste des packages puis on les met à niveau vers la nouvelle version.

```
serverlinux@serverlinux:~$ sudo apt install apache2_
```

On installe Apache2 pour mettre en place un serveur web.

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses: [172.16.10.1/24]
      routes:
        - to: default
          via: 172.16.10.254
      version: 2
```

On configure la carte réseau de notre serveur web.

8- Test de la redondance et de la sécurisation des ports

```
C:\Users\utilisateur>ping -t 192.168.0.254

Envoi d'une requête 'Ping' 192.168.0.254 avec 32 octets de données :
Réponse de 192.168.0.254 : octets=32 temps=1 ms TTL=255
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 192.168.0.254 : octets=32 temps=1 ms TTL=255
```

On remarque que lorsqu'on fait un ping infini, et qu'on éteint le routeur maître, le routeur esclave prend le relais.

```
Switch(config)#
*Mar 1 01:06:49.880: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa2/0/2, putting Fa2/0/2 in err-disable state
*Mar 1 01:06:49.888: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address fc3f.dbf9.94ac on port FastEther
net2/0/2.
*Mar 1 01:06:50.886: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0/2, changed state to down
*Mar 1 01:06:51.885: %LINK-3-UPDOWN: Interface FastEthernet2/0/2, changed state to down
```

On remarque que lorsqu'on connecte un autre pc qui possède une adresse mac différente de celle renseignée pour sécuriser le commutateur. Celui-ci désactive l'interface automatiquement car il subit une violation de sécurité.