TP-INTERVLAN

Axel Hespel SIO1

Configuration général

Dans un premier temps, je vais connecter tous les câbles et configurer mes switches et routeurs de la manière suivante :

- Nommer le switch SX et le routeur RX.
- Ajouter un mot de passe pour l'accès en mode d'administration : enable password azerty.
- Configurer l'accès via Telnet : line vty 0 15, puis définir le mot de passe : password qwerty.
- Activer le chiffrement des mots de passe : service password-encryption.
- Ajouter une bannière d'accueil avec le mot de passe (pour les tests) : banner motd n.

Une fois cette configuration de base réalisée, je passerai à la configuration spécifique de chaque élément.

Configuration port trunk

Avant de pouvoir activer mon VTP, je dois configurer les ports où sont connectés mes switchs et mon routeur en mode trunk :
En mode de configuration :

interface fa X/X (dans notre cas fa0/24)
switchport mode trunk

Je réalise la même opération sur le S2 et sur la connexion entre le Switch 1 et le routeur.

Configuration S1-server VTP / S2-client

Dans un premier temps j’active le VTP sur S1 en temps que server:

vtp mode server
vtp domain axel

et sur mon S2

vtp mode client
vtp domain axel

Configuration S1 Vlan + Administration

Je vais maitenant réaliser quatre vlan:
sur mon server:
vlan 2; name SISR
vlan 3; name SLAM
vlan 4; name profs
vlan 50; name admin

Je vais affecter un port sur le S1 au vlan admin:
interface fa0/23
swithport acces vlan 50
Je vais maitenant ajouter des IP a mon vlan50 sur S1 et S2 puis quand nous configurons notre switch également
S1(conf)#vlan 50; ip addresse 192.168.10.2 255.255.255.0 // X2 sur S2

Configuration Attribution PORT

Je vais maitenant attribuer chaque port au bon VLAN

interface fa 0/X (le port)
switchport acces vlan X (sont vlan)

Je repete pour chaque port

une fois que tous les ports sont attribués je vais passer a la configuration du routeur

Configuration Routeur

Je vais montrer l’exemple de création de une sous interface:
Attention ne pas oublier d’allumer l’interface et de bien trunker le port venant du switch !

int fa0/0
no sh

int fa0/0.2 (création sous interface pour mon vlan 2 SISR)
encapsulation dot1q 2 (j’autorise les trams du VLAN 2)
ip address 192.168.2.254 255.255.255.0 (et j’affecte une ip a mon interface, de préférence en 254)
Je repete pour chaque sous interface et j’oublie pas pour mon administrateur,
une fois réalisé tous les vlans peuvent communiquer et mon Administrateur peux égalment se connecter en telnet a chaque machine

Configuration Routeur / ACL

Une contrainte nous est imposée : seuls les VLAN 2 et 4 doivent communiquer et non le VLAN 3. La solution facile serait de ne pas mettre de sous-interface, mais dans ce cas, on ne peut pas activer un DHCP qui sera activé après la mise en place de l'ACL.

Qu'est-ce qu'une ACL ?

Une ACL (ou liste de contrôle d'accès) est une liste de règles que l'on peut attribuer à un port d'un routeur. Il existe des ACL standard, des ACL basées sur les adresses MAC et des ACL étendues. Dans notre cas, nous allons utiliser une ACL standard. Simplement, nous voulons une règle qui empêche la sortie des VLAN 2 et 4 vers le VLAN 3.

Comment faire ?

Création de la règle :

access-list 1 deny 192.168.2.0 0.0.0.255

access-list 1 deny 192.168.4.0 0.0.0.255

attention si il y a une ACL il faux autorisé qui passe sinon toute demande sera refusé

acces-list 1 permit 192.168.3.0 0.0.0.255

Configuration Routeur / ACL

Que venons-nous de faire ? Nous avons d'abord créé la règle 1, puis nous avons interdit (deny) les machines avec l'adresse IP 192.168.2/3.0. Vous avez sûrement remarqué que le masque était différent car il ne s'agit pas du masque classique mais d'un masque inversé. En résumé, cela signifie que le routeur doit comparer les trois premiers octets (là où il y a un zéro) et ne pas regarder là où il y a 255. Ainsi, nous vérifions ici si les trois premiers octets correspondent à la règle mise en place mais pas le dernier. Peu importe si nous avons une IP en 2.23 ou 2.24, nous ne regarderons que 192.168.2 <--
Une fois la règle créée, nous allons l'appliquer à notre interface de sortie :
#int fa0/0.3
#ip access-group 1 out (ou in si nous voulons une ACL à l'entrée)
Et voilà, notre ACL a été mise en place. Note : les règles d'ACL sont appliquées dans l'ordre de leur création. Dans notre cas, nous vérifions d'abord si l'IP est dans le VLAN 2, PUIS dans le VLAN 4, et ensuite nous acceptons si on a le vlan 3 ou vlan 50

Configuration Routeur / DHCP

On a maintenant toutes nos connexions établies, nos règles mises en place et nos sous-interfaces configurées. Alors, nous voulons que tout le monde communique maintenant, donc nous allons réaliser des serveurs DHCP sur nos sous-interfaces :
Tout d'abord, nous n'allons autoriser que 10 adresses IP par DHCP :
ip dhcp excluded-address 192.X.X.1 192.X.X.9
ip dhcp excluded-address 192.X.X.21 192.X.X.254
Je crée ma première pool :
ip dhcp pool vlan2-SISR
network 192.168.2.0 255.255.255.0 (je lui dis sur quel réseau agir)
default-router 192.168.2.254 (et je lui donne son interface et la passerelle)
Je répète cette opération pour chaque réseau.

Mes config - S1

Telnet + Banner

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 ip address 192.168.10.1 255.255.255.0
!
banner motd ^C
Bienvenue sur le switch 1 SIO SAINT-LUC
^C
!
!
!
line con 0
!
line vty 0 4
 password 7 08305B4B1B0D1C
 login
line vty 5 15
 password 7 08305B4B1B0D1C
 login
```

Vlan

```
SW1#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/7, Fa0/9, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                   Fa0/22, Gig0/1, Gig0/2
2    SISR                                active    Fa0/5, Fa0/6
3    SLAM                                active    Fa0/8, Fa0/10
4    profs                               active
100  admin                               active    Fa0/23
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Mes config - S2

Telnet + Banner

```
interface Vlan100
 ip address 192.168.10.2 255.255.255.0
!
banner motd ^C
Bienvenue sur le routeur SIO SAINT-LUC
^C
!
!
!
line con 0
!
line vty 0 4
 password 7 08305B4B1B0D1C
 login
line vty 5 15
 password 7 08305B4B1B0D1C
 login
!
!
!
!
end
```

Vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/8, Fa0/10, Fa0/11
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    SISR                              active    Fa0/7
3    SLAM                              active    Fa0/9
4    profs                             active    Fa0/12
100  admin                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Mes config - R1

MDP + DHCP

```
enable password 7 0820564B1B0D1C
!
!
ip dhcp excluded-address 192.168.2.1 192.168.2.9
ip dhcp excluded-address 192.168.2.21 192.168.2.254
ip dhcp excluded-address 192.168.3.21 192.168.3.254
ip dhcp excluded-address 192.168.3.1 192.168.3.9
ip dhcp excluded-address 192.168.4.1 192.168.4.9
ip dhcp excluded-address 192.168.4.21 192.168.4.254
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.21 192.168.10.9
ip dhcp excluded-address 192.168.10.21 192.168.10.255
!
ip dhcp pool vlan2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.254
ip dhcp pool vlan3
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.254
ip dhcp pool vlan4
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.254
```

Mes interfaces

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.254 255.255.255.0
 ip access-group 102 in
 ip access-group 1 out
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.254 255.255.255.0
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.10.254 255.255.255.0
!
```

ACL + Banner + telnet

```
access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 deny 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
!
banner motd ^C
Bienvenue sur le routeur SIO SAINT-LUC
^C
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 password 7 08305B4B1B0D1C
 login
line vty 5 15
 password 7 08305B4B1B0D1C
 login
```

Test - vlan 2 -->

Ping depuis Vlan 2 vers 3 et 4 : Réussite vers 4 et échec vers 3

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.2.254: Destination host unreachable.
Reply from 192.168.2.254: Destination host unreachable.
Reply from 192.168.2.254: Destination host unreachable.

Ping statistics for 192.168.3.10:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.4.10: bytes=32 time<1ms TTL=127
Reply from 192.168.4.10: bytes=32 time<1ms TTL=127
```

Test - Pc admin -->

Je teste avec mon pc Admin;
j’ai accès a tout

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.10:
    Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Reply from 192.168.4.10: bytes=32 time<1ms TTL=127
Reply from 192.168.4.10: bytes=32 time<1ms TTL=127
```

Test - vlan 3 -->

ping pc dans vlan 3 vers autre impossible d’avoir une réponse

```
   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:63FF:FED5:1797
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.3.12
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.3.254

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.

Ping statistics for 192.168.2.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Request timed out.
```

Test - vlan 3 - probléme

Attention il y a ici une faille dans ma configuration car effetivement le vlan 2 et 4 ne peuvent pas sortir du port 0/0.3 par contre le vlan 3 peux communiquer avec eux il n’auras juste pas de réponse car les pings ne peuvent pas revenir, cependant il a quand meme une connexion, je vais donc appliquer une regle a la sortit des interfaces 0/0.2 et 0/0.4 pour corriger ce probleme

Test - vlan 3 - probléme

ici on voit les régles aplliquer en sortit des interfaces

```
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.254 255.255.255.0
 ip access-group 2 out
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.254 255.255.255.0
 ip access-group 102 in
 ip access-group 1 out
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.254 255.255.255.0
 ip access-group 2 out
```

La regle qui est: interdir 192.168.3.0 et aroriser tout le reste

```
R0(config)#access-list 2 deny 192.168.3.0 0.0.0.255
R0(config)#acces
R0(config)#access-list per
R0(config)#access-list permi
R0(config)#access-list 2 per
R0(config)#access-list 2 permit any
```

Test - vlan 3 - probléme

Et voila quand je ping on vois la différence, il ne dit pas que il a pas de réponse mais que il n’a pas accès !

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.3.254: Destination host unreachable.
Reply from 192.168.3.254: Destination host unreachable.

Ping statistics for 192.168.2.10:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
```

Dans une prod je pourait donc également interdir la communication de mes vlan vers l’admin et autoriser le vlan admin a communiquer avec le reste, ce que je n’ai pas fait pour pouvoir réaliser mes tests facilement !