
# TP2 Réseaux d'entreprise

*Antoine Laguette & Guillaume Tisserand & Juliette Bluem*

6 décembre 2022

# Table des matières

# 1 Introduction

Durant trois TP, nous allons mettre en place la topologie suivante.

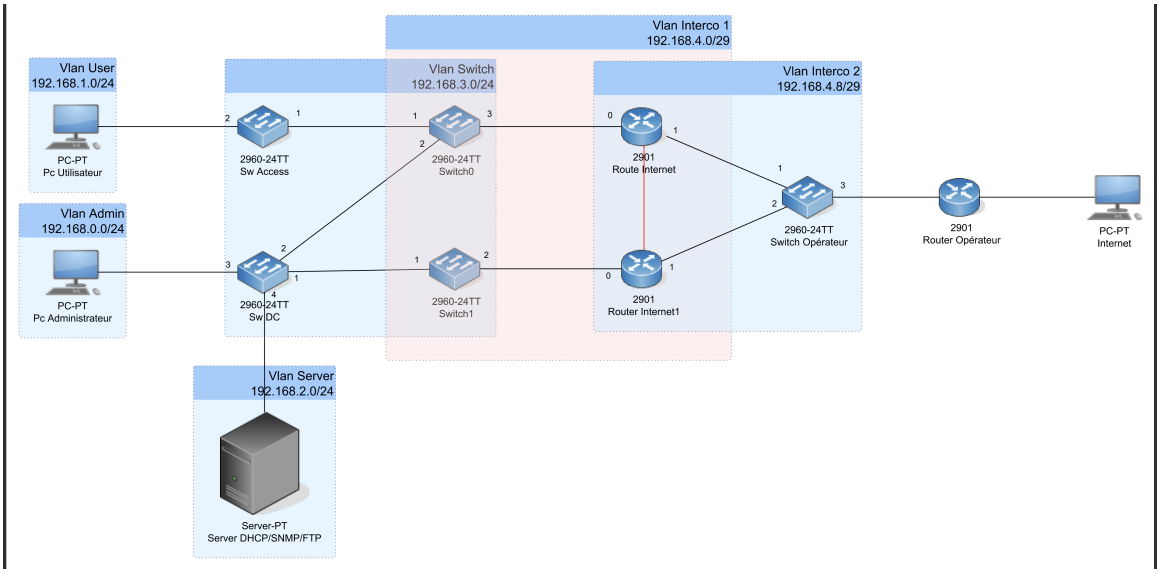


FIGURE 1 – Caption

Elle nous a servis dans la première séance à utiliser différent protocoles comme le VTP, le DHCP et le LACP, mais aussi des technologies comme la stackwise qui nous a permis de coupler deux switch pour n'en faire qu'un.

Elle va nous servir dans cette deuxième séance à mettre en place des pratiques connues et acquises, comme les ACL ou le SSH, mais aussi nous permettre de découvrir le DHCP snooping, le chiffrement de mots de passe et la sécurité de ports.

## 2 ACL étendues

Dans le but de développer d'avantage l'aspect sécurité et optimisation de l'utilisation des liens, nous mettons en place différentes ACL. Une ACL, pour Access-Control-List, est une règle que l'on injecte dans un routeur pour avoir une gestion plus fine des droits d'accès pour l'entrée et la sortie de trafic au niveau d'une interface.

Il existe deux types d'ACL, les ACL standard et les ACL étendues. Les ACL standard ne peuvent filtrer que par l'origine du trafic et peuvent être numérotées entre 1 et 99.
Les ACL étendues peuvent filtrer par protocole, par adresse IP source et de destination, et par port d'origine et de destination. Elles peuvent également être numérotés entre 100 et 199.

Les différents protocoles que nous souhaitons contrôler sont les suivants : DHCP (67 client, 68, serveur), ICMP, SSH, SNMP, RDP, SMB, FTP.

Pour anticiper la mise en place de ces ACL nous avions préparé les commandes en amont. Attention, nous n'avions pas pris en compte le fait que ce n'était pas des masques normaux à renseigner dans les commandes d'ACL mais des masques inversés. Voici donc les commandes initialement prévues :

```
ACCESS-LIST 100 PERMIT ICMP 192.168.0.0 255.255.255.0 ANY
ACCESS-LIST 110 PERMIT ICMP HOST 10.10.10.1 ANY
ACCESS-LIST 120 PERMIT ICMP ANY
ACCESS-LIST 130 PERMIT TCP 192.168.0.0 0.0.0.255 ANY EQ 22
ACCESS-LIST 140 PERMIT TCP ANY ANY EQ 22
ACCESS-LIST 150 PERMIT UDP 192.168.0.0 0.0.0.255 ANY EQ 161
ACCESS-LIST 160 PERMIT UDP ANY ANY EQ 161
ACCESS-LIST 170 PERMIT TCP ANY ANY EQ 445
ACCESS-LIST 180 PERMIT UDP ANY ANY EQ 68 67
ACCESS-LIST 190 PERMIT TCP ANY ANY EQ 3389
ACCESS-LIST 190 PERMIT UDP ANY ANY EQ 3389
```

On a pû vérifier la bonne configuration de nos ACLs avec la commande suivante : SHOW ACCESS-LIST

```
Stacked(config)#do show access-list
Extended IP access list 110
    10 permit icmp host 10.10.10.1 any
Extended IP access list 120
    10 permit icmp any any
Extended IP access list 130
    10 permit tcp 192.168.0.0 0.0.0.255 any eq 22
Extended IP access list 140
    10 permit tcp any any eq 22
Extended IP access list 150
    10 permit udp 192.168.0.0 0.0.0.255 any eq snmp
Extended IP access list 160
    10 permit udp any any eq snmp
Extended IP access list 170
    10 permit tcp any any eq 445
Extended IP access list 180
    10 permit udp any any eq bootpc
    20 permit udp any any eq bootps
Extended IP access list 190
    10 permit tcp any any eq 3389
    20 permit udp any any eq 3389
Stacked(config)#
```

FIGURE 2 – Vérification ACLs

Nous avions ensuite pour projet de faire correspondre les ACLs à chaque Vlan grâce à des access map en utilisant les commandes suivantes :

```
(config)# vlan access-map VACL_Users 10
(config-access-map)# match ip address DHCPAll ICMPAdmin ICMPExt SMBAll
(config-access-map)# action drop
(config-access-map)# exit
(config)# vlan access-map VACL_Admin 20
(config-access-map)# match ip address ICMPAll RDPALL SNMPAll
(config-access-map)# action drop
(config-access-map)# exit
(config)# vlan access-map VACL_Switch 40
(config-access-map)# match ip address ICMPAdmin SSHAdmin SNMPAdmin
(config-access-map)# action drop
(config-access-map)# exit
(config)# vlan access-map VACL_Server 30
(config-access-map)# match ip address DHCPAll SNMPAdmin
(config-access-map)# action drop
(config-access-map)# exit
```

Pour pour vérifier que nos ACLs sont bien placées au sein de nos VLANs : show vlan access-map

```
Stacked#show vlan access-map
Vlan access-map "VACL_Users"  10
  Match clauses:
    ip  address: 110 180 100 170
  Action:
    drop
Vlan access-map "VACL_Admin"  20
  Match clauses:
    ip  address: 120 190 160
  Action:
    drop
Vlan access-map "VACL_Switch"  40
  Match clauses:
    ip  address: 100 130 150
  Action:
    drop
Vlan access-map "VACL_Server"  30
  Match clauses:
    ip  address: 180 150
  Action:
    drop
Stacked#
```

Figure 3 – Modification des ACLs

Néanmoins nous avons par la suite appris que ce n'étais pas du tout une façon de faire. Nos ACLs n'étaient donc pas bien configurées, nous avons dû les modifier pour obtenir ceci :


FIGURE 4 – Vérification ACls VLAN

Nous voyons que pour chaque Vlan, nous avons plusieurs règles de protocoles et de ports. Nous ne créons donc pas une ACL pour un blocage, mais une ACL par vlan.
Nous comprenons maintenant que notre raisonnement était partit à l'envers, nous voulions attribuer plusieurs ACL à un Vlan, ce qui est impossible.

# 3 SSH

SSH, pour Secure SHell, est un protocole de communication sécurisé qui, dans ce cas, nous permet de configurer nos équipements à distance et en toute sécurité. Nous aurions pu utiliser Telnet mais c'est une solution très archaïque et absolument pas sécurisé qu'il faut à tout prix mettre de côté dans nos bonnes pratiques.
En effet, SSH utilise un algorithme pour chiffrer le trafic et n'est donc pas lisible par un agresseur qui tenterait une attaque de type Men-in-the-Midle.

Pour configurer le protocole sur chacun des switchs, il faut injecter les commandes suivantes :
(CONFIG)#IP HTTP SECURE-SERVER
(CONFIG)#CRYPTO KEY GENERATE RSA GENERAL-KEYS MODULUS 1024
(CONFIG)#AAA NEW-MODEL
(CONFIG)#AAA AUTHENTICATION LOGIN DEFAULT LOCAL
(CONFIG)#AAA AUTHORIZATION EXEC DEFAULT LOCAL
(CONFIG)#USERNAME ADMIN PASSWORD POLYTECH
(CONFIG)#LINE VTY 0 15
(CONFIG-LINE)#LOGIN LOCAL
(CONFIG-LINE)#TRANSPORT INPUT SSH
(CONFIG)#IP SSH VERSION 2

On peut vérifier la bonne configuration de SSH en s'y connectant à partir d'un ordinateur et en constatant sur un des switchs (celui sur lequel on s'est connecté) qu'une session IN/OUT est ouverte :

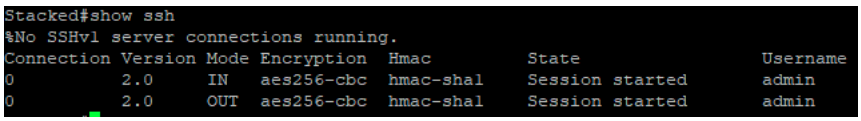


FIGURE 5 – Vérification ACls VLAN

Après modification de certains paramètres des ACLs nous nous sommes rendus compte que le SSH ne fonctionnait plus. Le problème était le suivant : nous avions réfléchi en session (comme pour un firewall) et non en IN & OUT comme le comprend un switch, même de niveau 3. De ce fait nous avions uniquement autorisé le IN pour le SSH sans autoriser le OUT donc la session SSH était impossible à établir. Pour pouvoir re-autoriser les sessions SSH il a fallu injecter une nouvelle ACLs autorisant le retour des hôtes :

Pour le vlan administrateur :
PERMIT TCP 192.168.0 0.0.0.255 192.168.3.0 0.0.0.255 EQ 22
Pour le vlan switch :
PERMIT TCP 192.168.3.0 0.0.0.255 EQ 22 192.168.0.0 0.0.0.255

Maintenant, si nous utlisons un PC sur le switch Access, il prend grace au DHCP une adresse IP utilisateur. Nous pouvons essayer d'ouvrir une session SSH sur un de nos switch, c'est impossible.
En revanche, si nous utilisons un PC sur le switch DC, nous lui attribuons une adresse dans le réseau Admin. Nous pouvons créer une session SSH sur un de nos switch afin de l'administrer.

# 4 DHCP snooping

Le service DHCP est très efficace pour adresser de grand réseau automatiquement, c'est beaucoup moins fastidieux que d'adresser chaque machine avec une @IP fixe. Cependant, cette solution est extrêment sujet aux cybercriminels qui, en se connectant simplement sur un port RJ45, obtiennent une adresse IP lié au réseau et d'entreprendre aisément des attaques sur ce dernier comme proposer d'autres serveur dhcp qui permettront l'injection de malwares.

Pour solutionner cela, le DHCP snooping a été créé. Cette fonction est intégrée dans le switch 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 switch. Seuls les paquets autorisés provenant de serveurs DHCP dignes de confiance sont transmis aux clients.

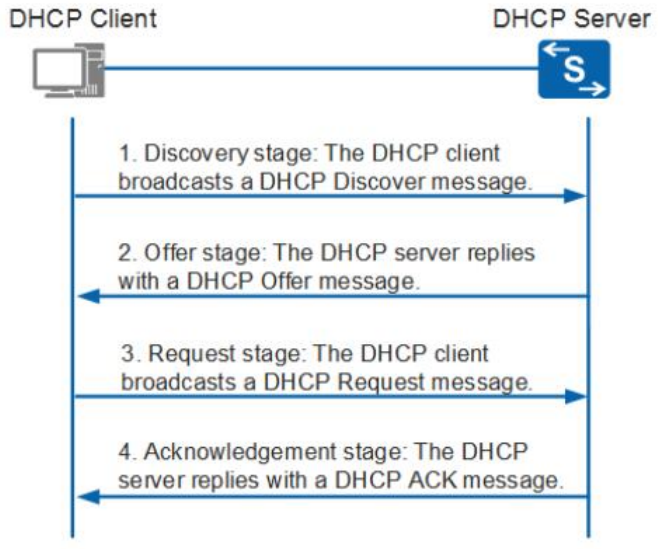


FIGURE 6 – Principe de fonctionnement du DHCP snooping

Nous avons configuré notre DCHP snooping ainsi :
SWDC(config)#ip dhcp snooping
SWDC(config)#ip dhcp snoop vlan ID1, ID2
SWDC(config)#int fa0/4
SWDC(config-if)#ip dhcp snooping trust

On peut vérifier la configuration de nos switchs :

```
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
FastEthernet0/7          yes        yes             unlimited
  Custom circuit-ids:
```

Figure 7 – Vérification DHCP snooping

Comme vous pouvez le constater, nous n'avons rencontré aucun problème lors ce cette implémentation.

# 5 Chiffrement mots de passe

Dans l'optique d'améliorer d'avantage notre sécurité, nous mettons en place le chiffrement de nos mots de passe, en effet ces derniers sont stockés en clair dans les switchs.

Nous l'activons de cette manière :
Définition d'un mot de passe sur la CTY (soit le lien direct (console))
(config)#service password-encryption
(config)#sh line
(config)#enable secret polytech
(config)#line con 0
(config-line)#password polytech
(config-line)#login
(config-line)#exit

Notons qu'il y en avait déjà un pour l'accès distant sur la VTY grâce à notre configuration SSH précédente.

Il y a maintenant un mot de passe à saisir pour l'accès au switch et un mot de passe à saisir pour l'accès au mode avec privilège.

De plus, ces mots de passe sont chiffrés : #show run

```
enable secret 5 $1$zOlq$OYvzGG8.hsoqZ7mudTf630
!
username admin secret 5 $1$6.w0$EEkh/iGiTGYXKBQXzGfnJ0
!
```

Figure 8 – Vérification DHCP snooping

# 6 Sécurité des ports

Ici, on souhaite filtrer par adresse mac certains ports de nos switchs. C'est à dire que les interfaces vont analyser l'adresse mac de l'hôte qui se connecte sur ce dernier, si l'adresse mac est connue alors elle pourra exploiter l'interface sinon, l'interface sera désactivé.

On en profitera pour ajouter quelques règles élémentaires comme le fait d'avoir au maximum un vlan par port.

On configure le filtrage MAC en spécifiant l'adresse MAC de l'un de nos utilisateurs.
Attention, pour cela, nous devons commencer par éteindre notre interface avant de rentrer nos commandes. Il faudra penser à la réactivier ensuite.

On peut alors vérifier quels sont les états des ports après configuration et on constate bien que l'ensemble de ces derniers sont bien downs suite à notre configurations.

```
DC#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              1            1                  1         Shutdown
      Fa0/2              1            0                  0         Shutdown
      Fa0/3              1            0                  0         Shutdown
      Fa0/4              1            0                  0         Shutdown
      Fa0/5              1            0                  0         Shutdown
      Fa0/6              1            0                  0         Shutdown
      Fa0/7              1            1                  0         Shutdown
      Fa0/8              1            0                  0         Shutdown
      Fa0/9              1            0                  0         Shutdown
     Fa0/10              1            0                  0         Shutdown
     Fa0/11              1            0                  0         Shutdown
     Fa0/12              1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

FIGURE 9 – Vérification des ports downs

Pour vérifier l'efficacité du filtrage mac, nous avons réaliser un test simple : en branchant un autre PC que celui renseigné, l'interface s'éteint et nous obtenons un message d'alerte sur notre équipement.

```
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
 switchport port-security maximum 1 vlan access
 switchport port-security
 switchport port-security mac-address 6c2b.59ea.3c54
 spanning-tree portfast
end

DC#
DC#
DC#
DC#
*Mar  1 04:16:15.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 04:16:16.049: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 04:16:20.050: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 04:16:20.059: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 6c2b.59e8.cd1a on port FastEthernet0/1.
DC#
```

FIGURE 10 – Filtrage MAC