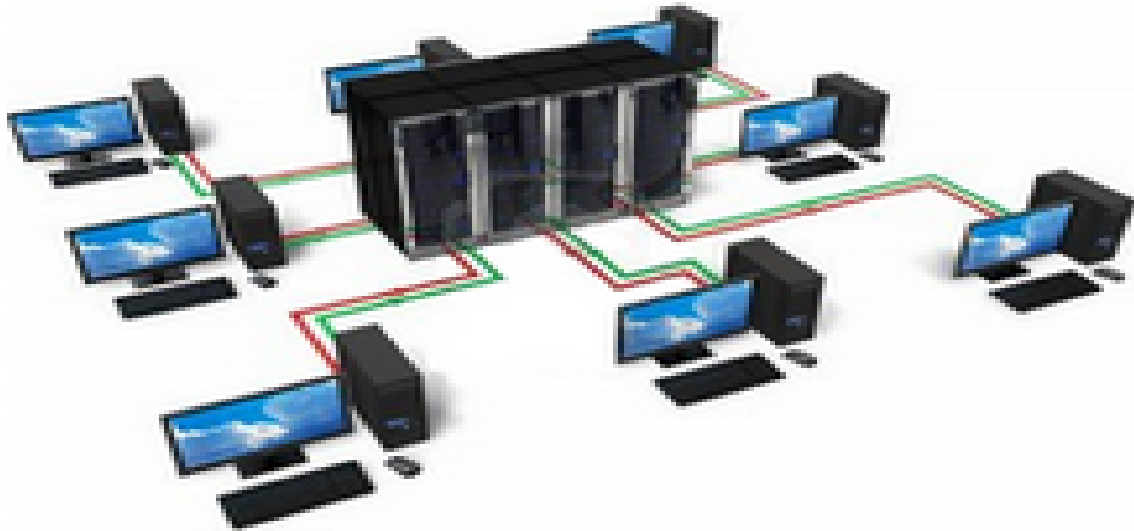


## Travaux pratiques : Sécurité des équipements Réseaux

LA FILIÈRE : SYSTÈMES UBIQUITAIRES ET DISTRIBUÉS CLOUD ET IoT



*Réaliser par :*  
HAJJAJI Ayyoub

*Professeur :*  
EL YAHYAOUI Ahmed

17 OCTOBRE 2020

# Sommaire

<b>1</b>	<b>Configuration de base des équipements réseau</b>	<b>2</b>
1.1	Introduction . . . . .	2
1.2	Câblage réseau et mise en place d'infrastructure . . . . .	2
1.3	Configuration basique des routeurs . . . . .	3
1.4	Configuration de base des switches et du point d'accès . . . . .	4
1.5	Configuration des paramètres IP des PCs et du laptop . . . . .	6
1.6	Vérification de la connectivité entre les différents PCs . . . . .	7
<b>2</b>	<b>Sécurité d'accès aux routeurs</b>	<b>9</b>
2.1	Configuration de paramètres pour R1 et R3 . . . . .	9
2.2	Configurez le serveur SSH sur R1 et R3 . . . . .	11
2.3	Sécuriser contre les attaques de connexion et sécuriser l'IOS et le fichier de configuration de R1 . . . . .	11
2.4	Configurer une source de temps synchronisée à l'aide de NTP . . . . .	13
2.5	Configurer la prise en charge de Syslog sur R3 et un serveur Syslog . . . . .	14
<b>3</b>	<b>Configuration de la sécurité des switches.</b>	<b>16</b>
<b>4</b>	<b>Configuration de la sécurité WPA2-PSK sur le point d'accès</b>	<b>19</b>
<b>5</b>	<b>Filtrage ACL et contrôle d'accès</b>	<b>21</b>
5.1	Routeur R3 : Autoriser l'accès à partir du réseau 172.16.3.0/24 . . . . .	21
5.2	Switch S3 : Autoriser l'accès juste à partir de la machine PC-C . . . . .	22
<b>6</b>	<b>Configurer une ZPF et un IPS</b>	<b>23</b>
6.1	Configurer une ZPF sur R3 à l'aide de la CLI . . . . .	23
6.2	Configuration de IPS sur R3 à l'aide de CLI . . . . .	24
6.3	Conclusion . . . . .	25

# Partie 1

## Configuration de base des équipements réseau

### 1.1 Introduction

Comme des informations confidentielles circulent dans les réseaux, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. Par ailleurs, dans cette TP on va mettre en place une infrastructure réseau constitué des différents équipements et faire la configuration de base pour ces dernières.

### 1.2 Câblage réseau et mise en place d'infrastructure

Dans de cette partie j'ai commencé par la mise en place de toutes les équipements dont on est besoin comme vous allez voir dans l'image qui suit, puis j'ai fais le câblage on suivant le tableau d'adressage donné.

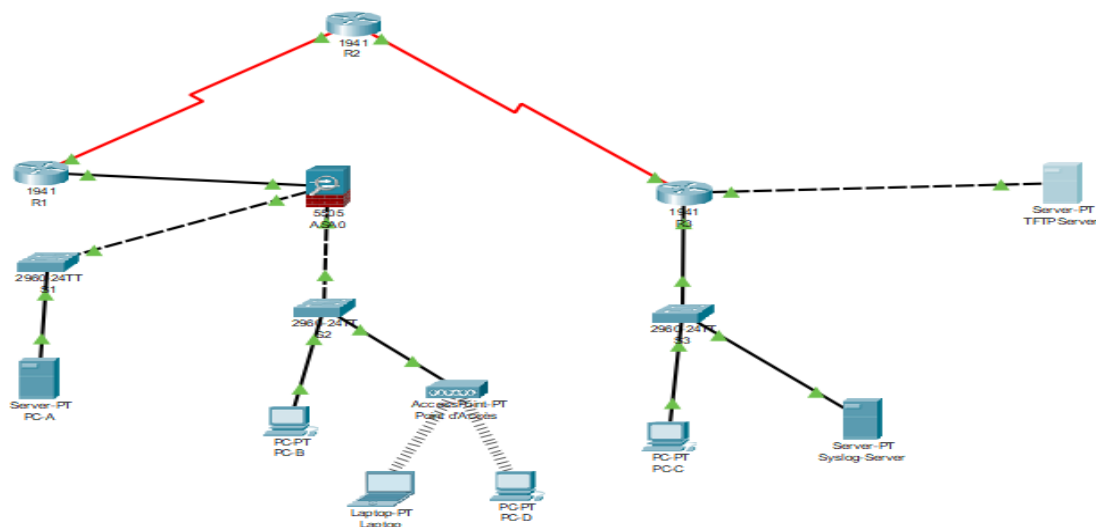


FIGURE 1.1 – Topologie du Réseau

Lors de cette partie j'ai eu l'occasion de mettre en place des carte wifi pour le laptop et le PC-D en plus de l'interface de type HWIC-2T pour chaque routeur



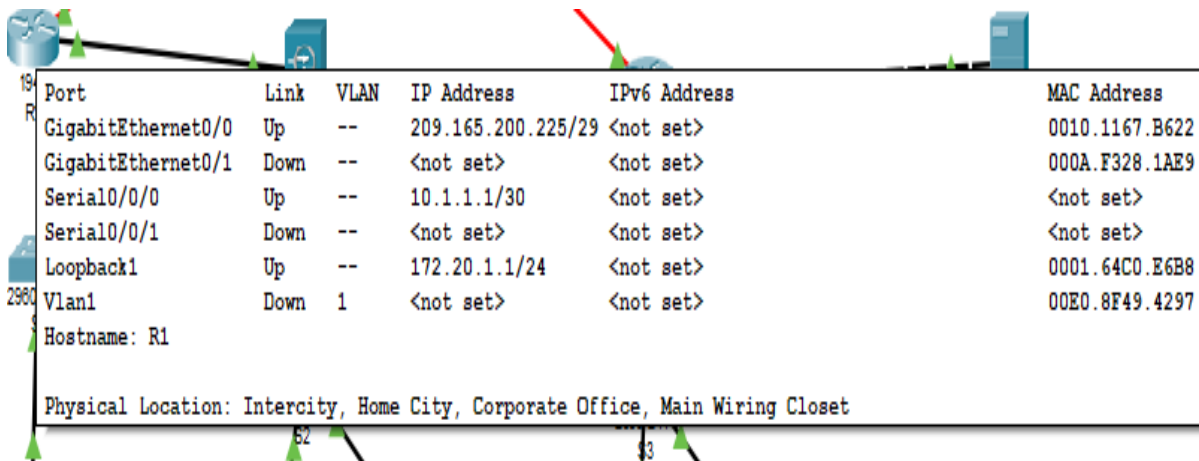
### 1.3 Configuration basique des routeurs

Après avoir mise on place de toute les équipement j'ai commencé à les configurer. On commençant par les routeurs, il suffit de suivre les commandes suivant pou configurer toutes les interfaces des routeurs.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#
```

FIGURE 1.2 – configuration de l'interface serial0/0/0 de R2

Après la configuration de toute les interface de R1 j'ai eu le résultat suivant :



Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	209.165.200.225/29	<not set>	0010.1167.B622
GigabitEthernet0/1	Down	--	<not set>	<not set>	000A.F328.1AE9
Serial0/0/0	Up	--	10.1.1.1/30	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Loopback1	Up	--	172.20.1.1/24	<not set>	0001.64C0.E6B8
Vlan1	Down	1	<not set>	<not set>	00E0.8F49.4297

Hostname: R1

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

FIGURE 1.3 – configuration de R1

Puis j'ai désactivé le DNS lookup sur chaque routeur, par la command suivant : ***no ip domain-lookup*** et pour finir j'ai Configuré une route statique par défaut de R1 à R2 et de R3 à R2. et des routes statiques de R2 vers le sous-réseau de R1 Fa0/0-to-ASA et vers le réseau LAN de R3.

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
R3(config)#
```

FIGURE 1.4 – Route statique par défaut de R3 à R2.

## 1.4 Configuration de base des switches et du point d'accès

Dans cette partie, il suffit de suivre le tableau d'adressage pour Configurer l'adresse de management du VLAN 1 sur chaque switch

```
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.11 255.255.255.0
S2(config-if)#
```

FIGURE 1.5 – configuration de S2

Puis j'ai configuré la passerelle IP par défaut pour chacun des trois switches, et on utilisant la même commande utilisé pour les routeurs on a désactivé le DNS lookup sur chaque switch

```
S3>enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#ip default-gateway 172.30.3.1
S3(config)#
```

FIGURE 1.6 – Default Gateway de S3

Et se qui concerne le point d'accès j'ai Configuré le port 1 avec un SSID=masterips

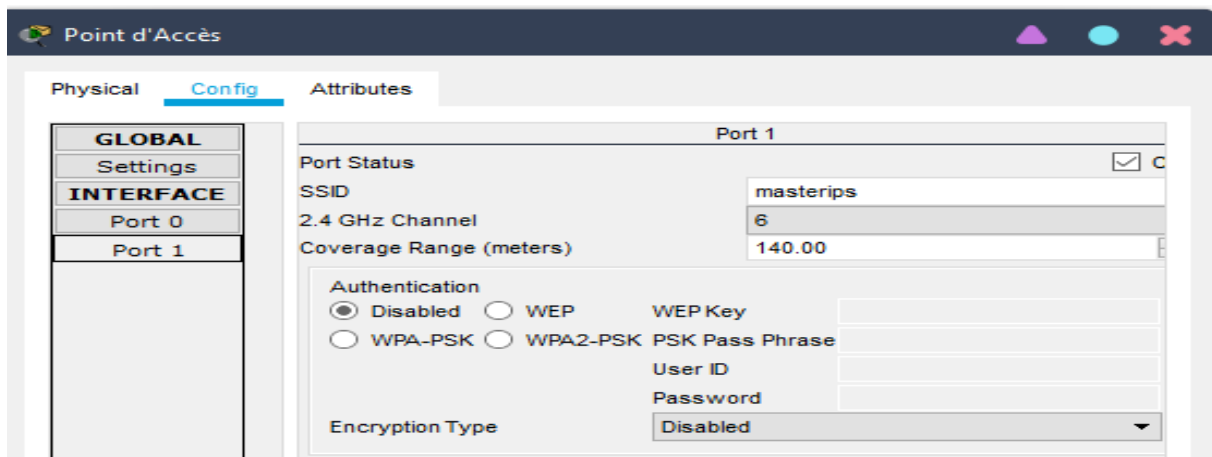


FIGURE 1.7 – configuration du point d'accès

## 1.5 Configuration des paramètres IP des PCs et du laptop

Finalement j'ai configuré tout les PCs avec ses adresse IP et ses gateway comme montre les figures suivant :

Port	Link	IP Address	IPv6 Address	MAC Address
Wireless0	Up	192.168.1.2/24	<not set>	0010.1136.5E50
Bluetooth	Down	<not set>	<not set>	0001.9629.7D43
Gateway: 192.168.1.1				
DNS Server: <not set>				
Line Number: <not set>				
Wireless Best Data Rate: 54 Mbps				
Wireless Signal Strength: 70%				
Physical Location: Intercity, Home City, Corporate Office				

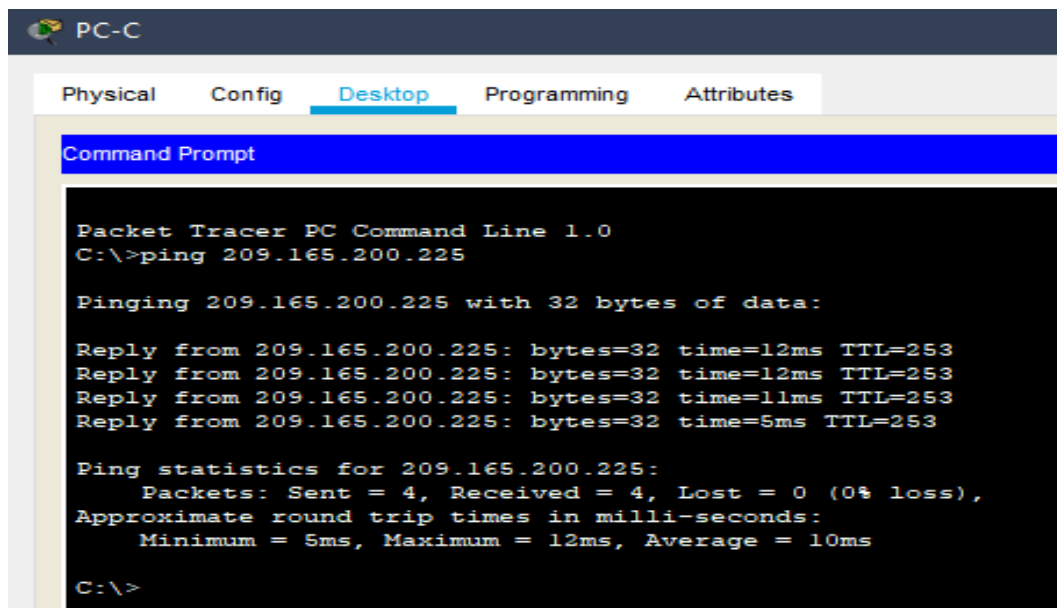
FIGURE 1.8 – configuration du laptop

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	172.16.3.3/24	<not set>	0000.0C53.8EA6
Bluetooth	Down	<not set>	<not set>	0030.F20A.4102
Gateway: 172.16.3.1				
DNS Server: <not set>				
Line Number: <not set>				
Physical Location: Intercity, Home City, Corporate Office				

FIGURE 1.9 – configuration du PC-C

## 1.6 Vérification de la connectivité entre les différents PCs

Après toute configuration fait, il ne reste que tester la connectivité entre les différents PCs, comme montre les figures suivants :



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225

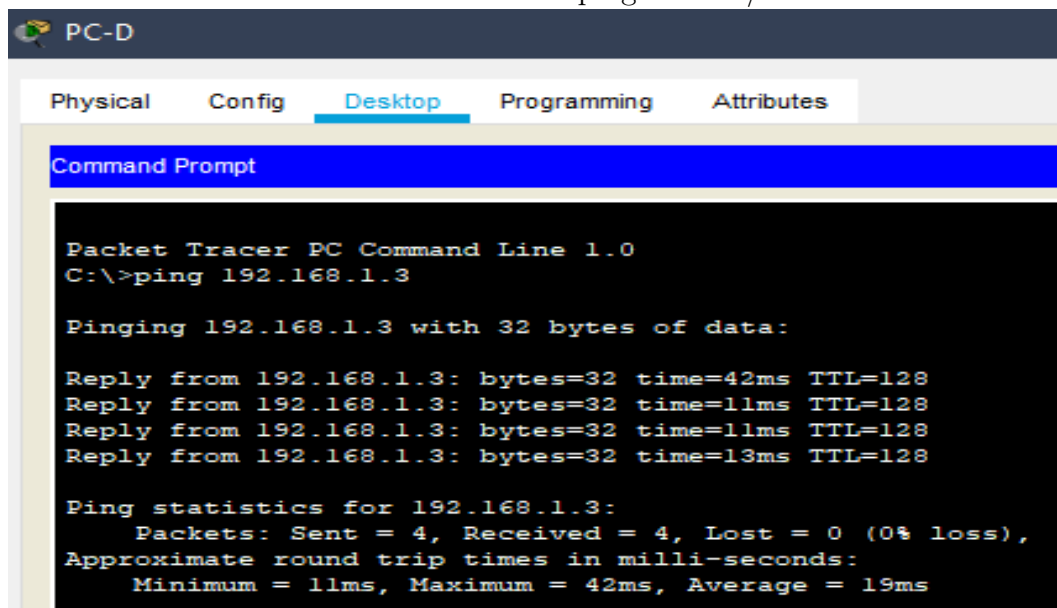
Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=12ms TTL=253
Reply from 209.165.200.225: bytes=32 time=12ms TTL=253
Reply from 209.165.200.225: bytes=32 time=11ms TTL=253
Reply from 209.165.200.225: bytes=32 time=5ms TTL=253

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 12ms, Average = 10ms

C:\>
```

FIGURE 1.10 – PC-C ping R1 G0 / 0.



```
PC-D
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

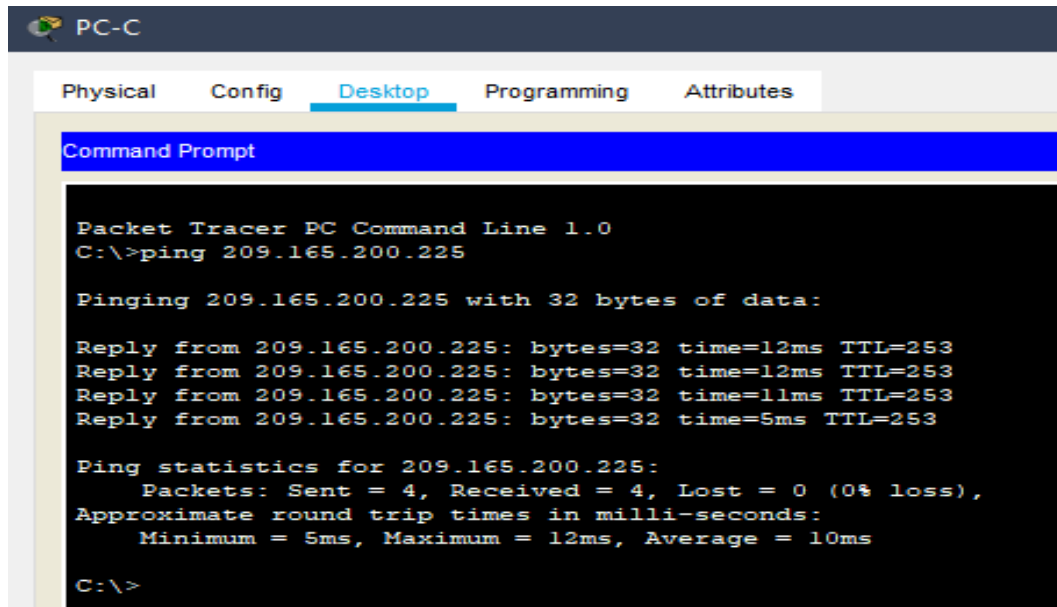
Reply from 192.168.1.3: bytes=32 time=42ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 42ms, Average = 19ms
```

FIGURE 1.11 – PC-D ping PC-B.



Mais quand j'ai essayé de tester la communication entre le PC-C et le laptop toutes les paquets ont été perdu, puis j'ai essayé de communiquer PC-B et PC-A J'ai eu le même problème, je pense qu'il me manque la configuration du firewall ASA



The screenshot shows the 'PC-C' configuration window in Packet Tracer, with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the results of a ping command to the IP address 209.165.200.225. The output shows four successful replies with varying round-trip times (12ms, 12ms, 11ms, 5ms) and a TTL of 253. The ping statistics indicate 0% loss of packets.

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=12ms TTL=253
Reply from 209.165.200.225: bytes=32 time=12ms TTL=253
Reply from 209.165.200.225: bytes=32 time=11ms TTL=253
Reply from 209.165.200.225: bytes=32 time=5ms TTL=253

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 12ms, Average = 10ms

C:\>
```

FIGURE 1.12 – PC-C ping laptop

## Partie 2

# Sécurité d'accès aux routeurs

### 2.1 Configuration de paramètres pour R1 et R3

Dans cette partie on a commencé par configurer des mots de passe pour sécuriser l'accès aux routeurs R1 et R3

- J'ai Configuré une longueur de mot de passe minimale de 10 caractères, puis je fais le chiffrement de ce mot de passe en clair, après j'ai Configuré un avertissement destiné aux utilisateurs non autorisés avec une bannière MOTD. J'ai commit une erreur au niveau du message afficher, il suffit d'utiliser la commande suivante :

*banner motd \$Unauthorized access strictly prohibited and prosecuted to the full extent of the law !\$*

- Puisque mon version de l'IOS est 15.1 je n'ai pas pu utiliser algorithm-type scrypt

- Puis j'ai Créé un compte d'utilisateur local Admin01 et finalement j'ai Activé les services aaa

```
R3>en
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#security passwords min-length 10
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized access strictly prohibited!$
R3(config)#enable secret cisco12345
R3(config)#username Admin01 privilege 15 algorithm-type scrypt secret
% Invalid input detected at '^' marker.
R3(config)#Admin01pa55
% Invalid input detected at '^' marker.
R3(config)#username Admin01 privilege 15 secret Admin01pa55
R3(config)#aaa new-model
R3(config)#aaa authentication login default local-case enable
R3(config)#line con 0
R3(config-line)#privilege level 15
R3(config-line)#exec-timeout 15 0
R3(config-line)#logging synchronous
R3(config-line)#
```

Dans le même endroit J'ai configurer la ligne de console et les lignes VTY comme montre la figure suivante :

```
R3(config)#aaa authentication login default local-case enable
R3(config)#line con 0
R3(config-line)#privilege level 15
R3(config-line)#exec-timeout 15 0
R3(config-line)#logging synchronous
R3(config-line)#line vty 0 4
R3(config-line)#privilege level 15
R3(config-line)#exec-timeout 15 0
R3(config-line)# transport input SSH
R3(config-line)#exit
R3(config)#login on-success log
R3(config)#login on-failure log
R3(config)#exit
R3#
```

Comme vous pouvez voir dans cette image, après la configuration des lignes j'ai Configuré le routeur pour enregistrer les activités de connexion.

La commande show login nous montre que toutes les succès et les échecs sont enregistrer.

```
R3#sh login
  A default login delay of 1 seconds is applied.
  No Quiet-Mode access list has been configured.
  All failed login is logged.
  All successful login is logged.

  Router NOT enabled to watch for login Attacks
```

## 2.2 Configurez le serveur SSH sur R1 et R3

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip domain-name computersecurity.ma
R3(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: R3.computersecurity.ma

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:53:12.644: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#ip ssh version 2
R3(config)# ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
```

Dans cette partie j'ai commencé par configurer le nom de domaine computer-security.ma, puis générer la paire de clés RSA avec un modulus size de 2048 bits, finalement configurer SSH version 2.

Après toute configuration faites j'ai vérifié la connectivité SSH vers R1 et R3 en exécutant la commande : ssh -l username ip

```
C:\>ssh -l Admin01 10.1.1.1

Password:
R1#sh run
Building configuration...

Current configuration : 1416 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$WvpW0nSHghRrqnrxXCUU1.
!
!
!
!
--More-- |
```

## 2.3 Sécuriser contre les attaques de connexion et sécuriser l'IOS et le fichier de configuration de R1

Dans cette partie on a essayé de configurer une sécurité de connexion avancée, par exemple si un utilisateur fait deux tentatives de connexion infructueuses dans un

délai de 30 secondes, on va désactiver les connexions pendant une minute. Puis on a sécurisé l'image de Cisco IOS et archivé une copie de la configuration en cours en utilisant les commandes `secure boot-image` et `secure boot-config`

```
User Access Verification

Username: Admin01
Password:
R1#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source:
0.0.0.0] [localport: 0] at 01:01:39 UTC Mon Mar 1 1993


R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#login block-for 60 attempts 2 within 30
R1(config)#login on-failure log
R1(config)#secure boot-image
%IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully secured running
image
R1(config)#secure boot-config
%IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured config
archive [flash:.runcfg-19930301-010429.ar]
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

---

Comme vous pouvez remarquer quand j'ai essayé d'accéder au CLI de R1 j'ai passé la vérification ce qui assure le fonctionnement de la partie 2.1

La commande `show secure bootset` nous permet de Vérifier que notre image et notre configuration sont sécurisées.

le nom du fichier de configuration en cours d'exécution archivé est *runcfg-19930301-010429.ar*, ce nom est basé sur la date du ios

```
R1#sh secure bootset
IOS resilience router id FTX1111W0QT

IOS image resilience version 15.1 activated at 01:03:45 UTC Mon Mar 1
1993
Secure archive flash:/c1900-universalk9-mz.SPA.151-4.M4.bin type is
image (elf) []
  file size is 33591768 bytes, run size is 33591768 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 15.1 activated at 01:04:29 UTC
Mon Mar 1 1993
Secure archive flash:/runcfg-19930301-010429.ar type is config
  configuration archive size 1594 bytes


R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no secure boot-image
%IOS_RESILIENCE-5-IMAGE_RESIL_INACTIVE: Disabled secure image
archival
R1(config)#no secure boot-config
%IOS_RESILIENCE-5-CONFIG_RESIL_INACTIVE: Disabled secure config
archival [removed flash:/runcfg-19930301-010429.ar]
R1(config)#
```

Et finalement on a utilisé les commandes `no secure boot-config` et `no secure boot-image` pour restaurer les paramètres par défaut de ces fichiers.

## 2.4 Configurer une source de temps synchronisée à l'aide de NTP

On commence cette partie par la configuration de R2 en tant que serveur NTP comme montre l'image suivante :

```
R2>en
R2#sh clock
*1:9:28.394 UTC Mon Mar 1 1993
R2#clock set 11:41:30 Nov 9 2020
R2#sh clock
11:41:41.522 UTC Mon Nov 9 2020
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp authentication-key 1 md5 NTPpassword
R2(config)#ntp trusted-key 1
R2(config)#ntp authenticate
R2(config)#ntp master 1
```

Puis on passe à la Configuration de R1 et R3 en tant que clients NTP en suivant les étapes mentionné dans le TP :

```
User Access Verification

Username: Admin01
Password:
R3##SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source:
0.0.0.0] [localport: 0] at 01:19:33 UTC Mon Mar 1 1993


R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp authentication-key 1 md5 cisco12345
R3(config)#ntp trusted-key 1
R3(config)#ntp authenticate
R3(config)#ntp server 10.2.2.2
R3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

R3(config)# ntp update-calendar
```

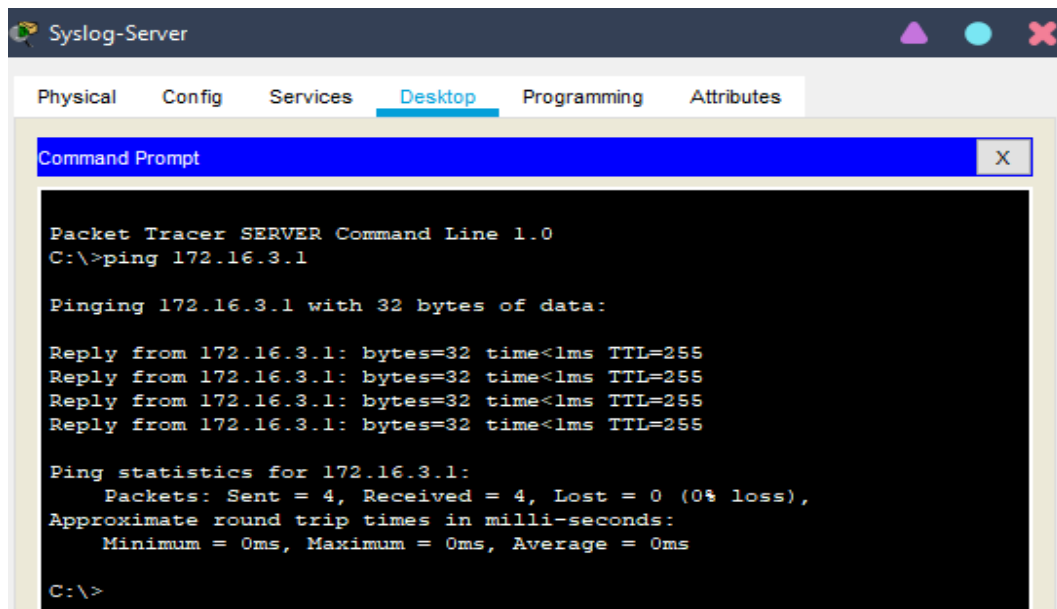
Finalement on Utilise la commande show ntp associations pour vérifier que R1 a établi une association avec R2.

```
R1#sh ntp associations

address          ref clock      st  when    poll   reach  delay
offset           disp
*~10.1.1.2       127.127.1.1    1   5       16     1      10.00
-2.00            0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
R1#
```

## 2.5 Configurer la prise en charge de Syslog sur R3 et un serveur Syslog

On commence par vérifier le ping entre le serveur syslog et l'interface d'adresse IP 172.16.3.1 du routeur



J'ai vérifié que le service d'horodatage pour la journalisation n'est pas activé sur le routeur à l'aide de la commande show run.

```
R3#sh run
Building configuration...

Current configuration : 1500 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R3
!
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$WvpW0n5HghRrqn timerwXCUU1.
!
!
!
!
!
--More--
```

Donc j'ai suivi les commandes de TP pour activer le service d'horodatage, puis j'ai configuré le service syslog sur le routeur pour envoyer des messages syslog au serveur syslog, et finalement j'ai défini le niveau de gravité de R3 sur 7 (debugging).

*j'ai oublié de prendre des capture d'écran pour cette étape.*

La commande show logging nous a aidé à voir le type et le niveau de journalisation activés.

```
R3#sh logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 8 messages logged, xml
disabled,
                  filtering disabled
Monitor logging: level debugging, 8 messages logged, xml
disabled,
                  filtering disabled
Buffer logging: disabled, xml disabled,
                  filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level debugging, 8 message lines logged
Logging to 172.16.3.4 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
8 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled

R3#
```



## Partie 3

# Configuration de la sécurité des switches.

Ce qui concerne les switches il suffit de procéder comme pour les routeur

```
S1>en
S1#conf t
S1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip http server
^
% Invalid input detected at '^' marker.

S1(config)#enable secret cisco12345
S1(config)#service password-encryption
S1(config)#banner motd $Unauthorized access strictly prohibited!$
S1(config)#ip domain-name computersecurity.ma
S1(config)#username Admin01 privilege 15 secret Admin01pa55
S1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: S1.computersecurity.ma

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 2 2:11:15.297: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh version 2
S1(config)# ip ssh time-out 90
S1(config)#ip ssh authentication-retries 2
S1(config)#line con 0
S1(config-line)#login local



---


S1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: S1.computersecurity.ma

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 2 2:11:15.297: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh version 2
S1(config)# ip ssh time-out 90
S1(config)#ip ssh authentication-retries 2
S1(config)#line con 0
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#interface F0/1
S1(config-if)#switchport mode access
S1(config-if)#spanning-tree portfast
```

Finalement on configure la sécurité du port F0/1 et on désactive les ports inutilisés.

```
S1(config)#interface F0/1
S1(config-if)#switchport mode access
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
```

Pour finir avec les switches on doit refaire le même travail de cette partie pour les switches S2 et S3.

```
S3(config-line)#login local
S3(config-line)#privilege level 15
S3(config-line)#exec-timeout 5 0
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#login local
S3(config-line)#privilege level 15
S3(config-line)#exec-timeout 5 0
S3(config-line)#transport input ssh
S3(config-line)#exit
S3(config)#interface F0/1
S3(config-if)#switchport mode access
S3(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION
|
%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
S3(config-if)#spanning-tree bpduguard enable
```

```

S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#enable secret cisco12345
S2(config)#service password-encryption
S2(config)#banner motd $Unauthorized access strictly prohibited!$
S2(config)#ip domain-name computersecurity.ma
S2(config)#username Admin01 privilege 15 secret Admin01pa55
S2(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: S2.computersecurity.ma

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:5:15.518: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#ip ssh version 2
S2(config)#ip ssh time-out 90
S2(config)#ip ssh authentication-retries 2
S2(config)#line con 0
S2(config-line)#login local
S2(config-line)#privilege level 15
S2(config-line)#exec-timeout 5 0
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#privilege level 15
S2(config-line)#exec-timeout 5 0
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#interface F0/1
S2(config-if)#switchport mode acces
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

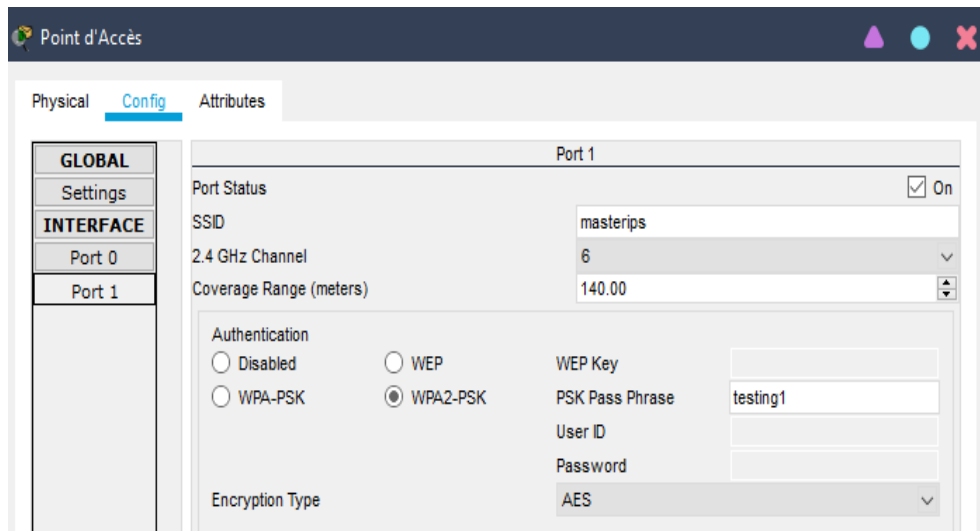
%Portfast has been configured on FastEthernet0/1 but will only

```

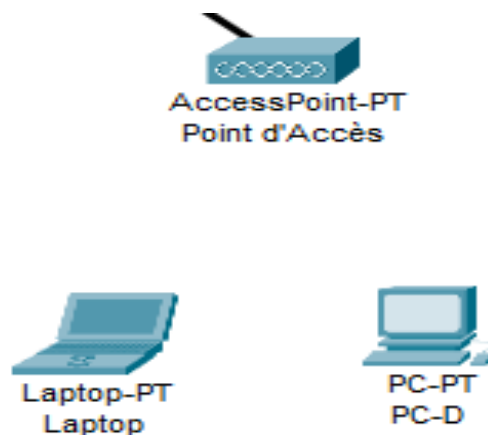
## Partie 4

# Configuration de la sécurité WPA2-PSK sur le point d'accès

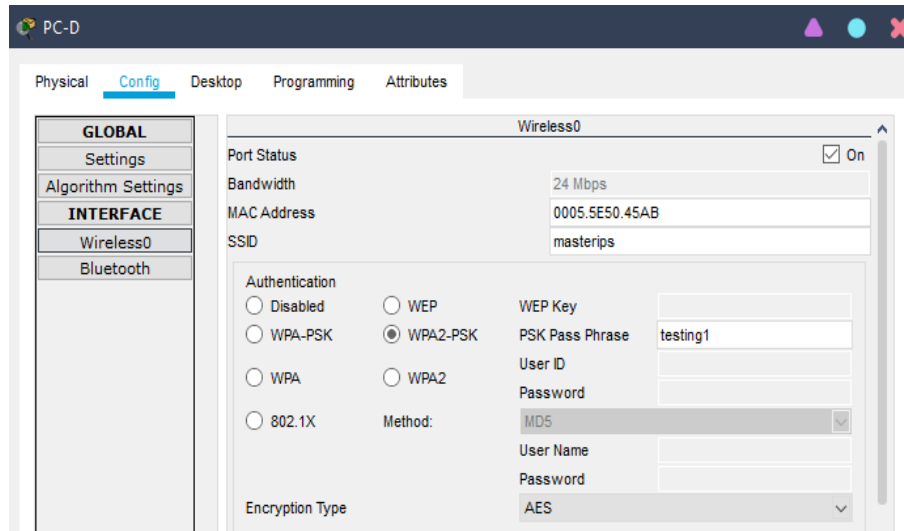
Dans cette partie j'ai commencé par Configurer le SSID : masterips, puis J'ai configuré le cryptage AES avec testing1 comme clé.



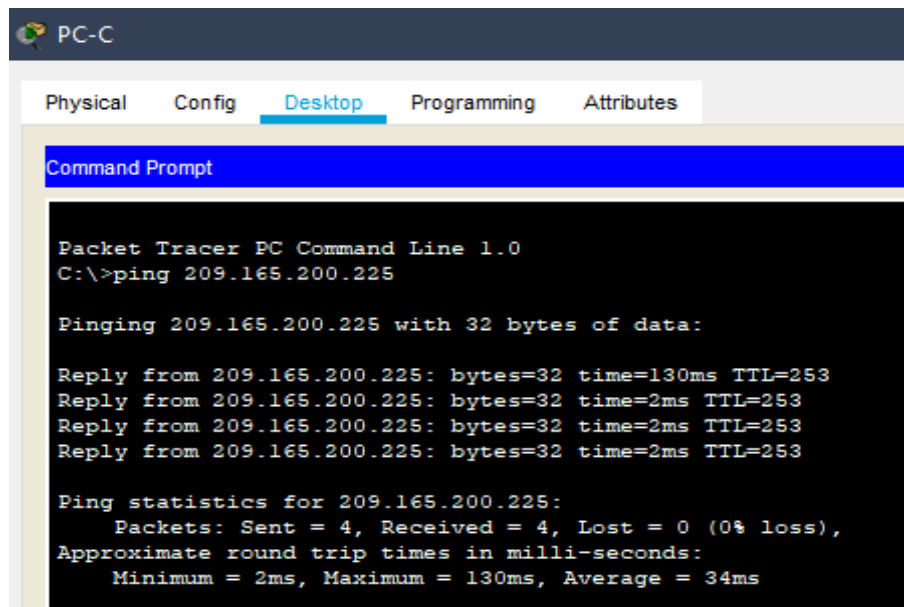
Après cette configuration le PC-D et le laptop ne sont plus connectés



Finalement j'ai adapté les paramètres de sécurité sur les deux machines wireless comme suit :



Voila le test du ping de la partie 1.6 :



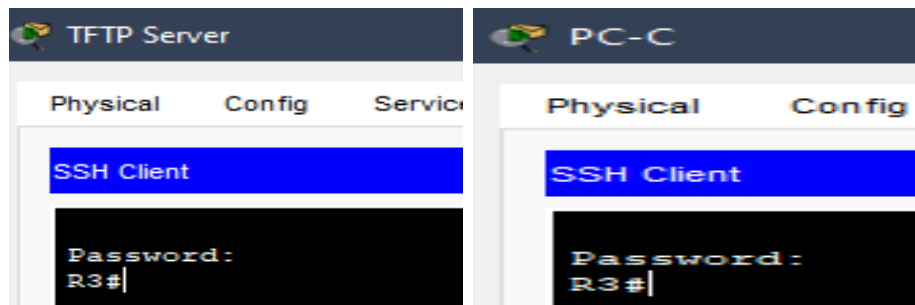
## Partie 5

# Filtrage ACL et contrôle d'accès

Dans cette partie on a limité l'accès SSH au routeur R3 et au Switch S3 en configurant les ACL standards.

### 5.1 Routeur R3 : Autoriser l'accès à partir du réseau 172.16.3.0/24

On a commencé cette partie par vérifier qu'on est capable de se connecter en SSH au routeur R3 à partir du serveur TFTP et de la machine PC-C.



Après cette vérification on a créé une ACL standard numérotée 1 permettant d'autoriser le réseau 172.16.3.0/24, puis on l'a appliqué pour ne permettre l'accès SSH au routeur R3 qu'à partir du réseau 172.16.3.0/24.

```
R3(config)#access-list 1 permit 172.16.3.0 0.0.0.255
R3(config)#line vty 0 15
R3(config-line)#access-class 1 in
```

Enfin on a essayé de se connecter de nouveau en SSH à partir du serveur TFTP(1.1.1.2), mais on a pas pu se connecter à cause de la dernière configuration de R3 qui ne permet l'accès SSH au routeur R3 qu'à partir du réseau 172.16.3.0/24.

Mais R3 peut se connecter en SSH à partir de PC-C même après la configuration

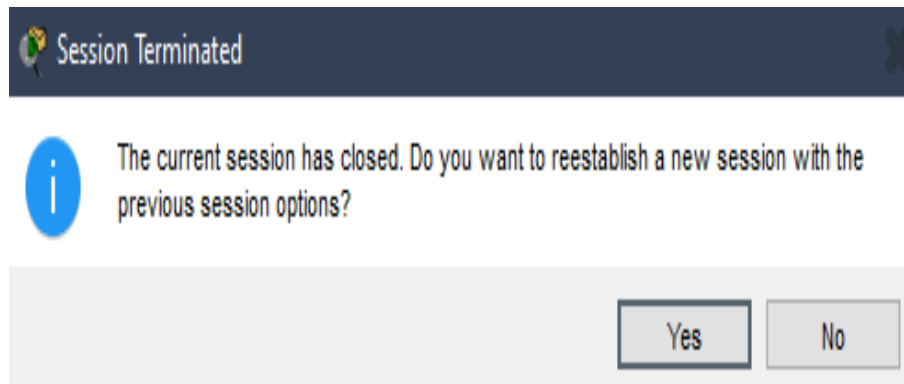


FIGURE 5.1 – message après avoir essayer de se connecter en SSH à partir du TFTP

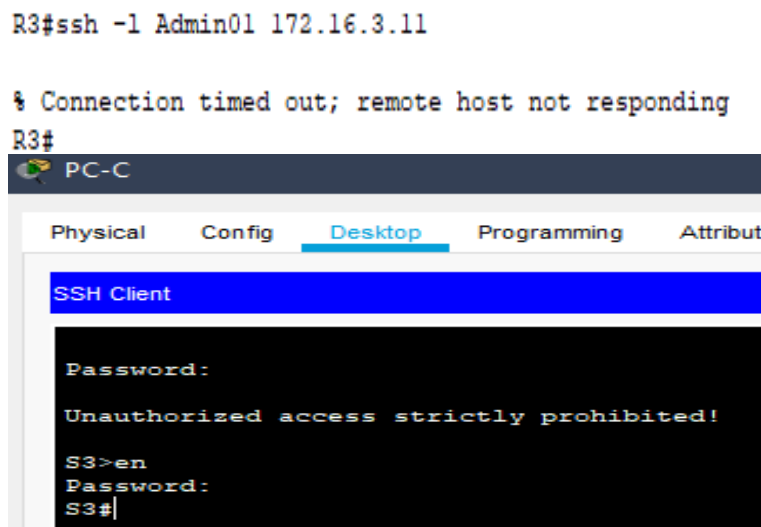
## 5.2 Switch S3 : Autoriser l'accès juste à partir de la machine PC-C

De même pour le switch S3 on a suivi le même enchaînement de commande utiliser en 5.1 pour autoriser l'accès à S3 juste à partir de la machine PC-C.

```
S3(config)#access-list 2 permit host 172.16.3.3
S3(config)#line vty 0 15
S3(config-line)#access-class 2 in
S3(config-line)#
```

Après la configuration de S3 j'ai essayer de se connecter en SSH à partir du routeur R3 et de PC-C.

Comme vous pouvez voir dans les images suivants on a pas pu se connecter en SSH à partir de R3, mais on a pu se connecter en SSH à partir de PC-C.



## Partie 6

# Configurer une ZPF et un IPS

Dans cette partie, on a configuré une ZPF et un IPS sur R3 à l'aide de la CLI

### 6.1 Configurer une ZPF sur R3 à l'aide de la CLI

J'ai pas pu utilisé la commande zone security puisque la technologie sécurité a été désactiver

Technology	Technology-package Current	Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	disable	None	None
data	disable	None	None

FIGURE 6.1 – Avant l'activation

Technology	Technology-package Current	Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	disable	None	None
data	disable	None	None

FIGURE 6.2 – Après l'activation

Pour configurer une ZPF sur R3 on a commencé par Créer des zones de sécurité INSIDE et OUTSIDE.



Ensuite on a créé une class-map on autorisant tous les protocoles principaux pour la zone INSIDE puisque on fait confiance à cette zone, dans la même commande on a indiqué au routeur que les instructions de protocole de correspondance suivantes seront considérées comme une correspondance, on utilisant le mot clé **match-any**, puis on match les paquets TCP, UDP ou ICMP.

Après on a créé une policy-map d'inspection nommée INSIDE-TO-OUTSIDE-POLICY pour inspecter tous les paquets correspondants à la class-map INSIDE-PROTOCOLS.

Puis on a créé une zone de paire appelée INSIDE-TO-OUTSIDE qui autorise le trafic initié du réseau interne vers le réseau externe mais ne permet pas au trafic en provenance du réseau externe d'atteindre le réseau interne.

Finalement on a appliqué la policy-map à la zone-pair et on a Attribué l'interface G0/1 de R3 à la zone de sécurité INSIDE et l'interface S0/0/1 à la zone de sécurité OUTSIDE.

```
R3(config)#zone security OUTSIDE
R3(config-sec-zone)#exit
R3(config)#class-map type inspect match-any INSIDE-PROTOCOLS
R3(config-cmap)#match protocol tcp
R3(config-cmap)#match protocol udp
R3(config-cmap)#match protocol ICMP
R3(config-cmap)#exit
R3(config-cmap)#exit
R3(config)#policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
R3(config-pmap)#class type inspect INSIDE-PROTOCOLS
R3(config-pmap-c)#inspect
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE
destination OUTSIDE
R3(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
R3(config-sec-zone-pair)#exit
R3(config)#int g0/1
R3(config-if)#zone-member security INSIDE
R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#zone-member security OUTSIDE
```

En fin on a vérifié notre configuration ZPF à l'aide des commandes **show zone-pair security**, **show policy-map type inspect zone-pair sessions**, et **show zone security**, le résultat a montré exactement la configuration qu'on a entré.

## 6.2 Configuration de IPS sur R3 à l'aide de CLI

Puisque le répertoire IPS n'existe pas dans la mémoire flash j'ai commencé par le créer en mode d'exécution privilégié à l'aide de la commande **mkdir**.

Puis j'ai défini l'emplacement de stockage de la signature IPS sur le répertoire IPSDIR que j'ai créé dans la mémoire flash, après avoir Créer une règle IPS et nommé IOSIPS.

Ensuite on a configuré IOS IPS pour utiliser l'une des catégories de signature prédéfinies.

Pour finir par l'application de la règle IPS au trafic entrant vers l'interface S0/0/1 de R3.

```
R3#mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash:IPSDIR

R3#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ips name IOSIPS
R3(config)#ip ips config location flash:IPSDIR
R3(config)#ip ips signature-category
R3(config-ips-category)#category all
R3(config-ips-category-action)#retired true
R3(config-ips-category-action)#exit
R3(config-ips-category)#category ios_ips basic
R3(config-ips-category-action)#retired false
R3(config-ips-category-action)#exit
R3(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this
engine will be scanned

R3(config)#interface s0/0/1
R3(config-if)#ip ips IOSIPS in
```

Et finalement on a utilisé la commande `show ip ips all` pour afficher le résumé de l'état de la configuration IPS, et elle a montré exactement ce qui dans le tp.

## 6.3 Conclusion

Dans le TP3 on a commencé par limiter l'accès SSH au routeur R3 et au Switch S3 en configurant les ACL standards.

Puis on a eu l'occasion de configurer une ZPF et un IPS sur R3 à l'aide de la CLI.

Dans cette dernière étape on a pu distinguer entre deux zone interne et externe, ensuite on a autorisé le trafic initié du réseau interne vers le réseau externe mais ne permet pas au trafic en provenance du réseau externe d'atteindre le réseau interne.

Pour voir le projet toute entier en cisco packet tracer visiter ce lien :

<https://github.com/ayy-oub/Security>