Dersim Besiktas

configuration des fonctions de sécurité des commutateurs

SOMMAIRE

Partie 1 : Configuration de la topologie et initialisation des périphériques

Étape 1 : Câblez le réseau conformément à la topologie

Je câble le routeur,switch et PC-A conformément à la topologie

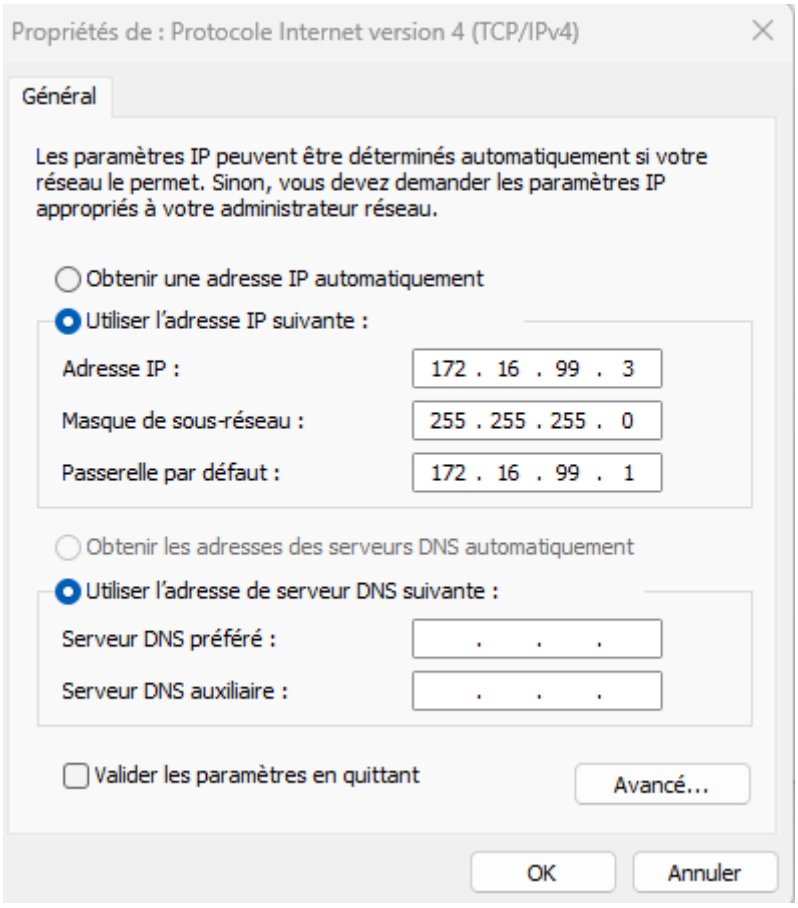
Étape 2 : Initialisez et redémarrez le routeur et le commutateur

Je supprime les configurations existantes

Partie 2 : Configuration des paramètres du périphérique de base et vérification de la connectivité

Étape 1 : Configurez une adresse IP sur PC-A

Je configure une adresse IP Sur PC-A



Étape 2 : Configurez les paramètres de base sur R1

Je configure l'adresse IP de l'interface indiqué dans la table d'adressage

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 172.16.99.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
```

```
Router#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down

GigabitEthernet0/0         unassigned      YES unset  administratively down down

GigabitEthernet0/1         172.16.99.1     YES manual up                    up

Serial0/0/0                unassigned      YES unset  administratively down down

Serial0/0/1                unassigned      YES unset  administratively down down

Router#
```

Étape 3 : Configurez les paramètres de base sur S1

Je configure le Switch avec les paramètres de base

Je supprime la configuration existante

```
Switch1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [con
firm]
[OK]
Erase of nvram: complete
Switch1#
```

Je change le nom du Switch

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
```

Je désactive la recherche DNS

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#no ip domain-lookup
SW1(config)#
```

J’attribue **class** comme mot de passe du mode d'exécution privilégié

```
SW1(config)#enable secret class
SW1(config)#
```

J’attribue **cisco** en tant que mots de passe de console et vty, puis activez la connexion

```
SW1(config)#line vty 0 15
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#
```

J’attribue comme mot de passe de console et vty cisco

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#line console 0
SW1(config-line)#password cisco
SW1(config-line)#exit
SW1(config)#
```

```
SW1(config)#line vty 0 15
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#
```

Je mets une passerelle par défaut sur S1

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int f0/5
SW1(config-if)#ip default-gateway 172.16.99.1
```

J’enregistre la configuration actuelle avec la commande copy run start

```
SW1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
0 bytes copied in 0.881 secs (0 bytes/sec)
SW1#
```

Je créer le vlan 99

```
SW1(config)#vlan 99
SW1(config-vlan)#name Management
SW1(config-vlan)#exit
SW1(config)#
```

Je configure le vlan 99

```
SW1(config-if)#ip address 172.16.99.11 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#end
SW1#
```

Je tape la commande sh vlan br et je vois que le vlan 99 est acif

```
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW1#
```

En tapant la commande sh ip int br je vois que l'état du protocol est en down

```
SW1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan99                 172.16.99.11    YES manual up                    down
```

J'attribue les ports F0/5 et F0/6 au VLAN 99 sur le commutateur

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int f0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 99
SW1(config-if)#interface f0/6
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 99
SW1(config-if)#end
SW1#
```

Étape 4 : Vérifiez la connectivité entre les périphériques

Je ping R1 depuis PC-A

```
C:\Users\dbesiktas>ping 172.16.99.1

Envoi d'une requête 'Ping'  172.16.99.1 avec 32 octets de données :
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=128
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=128
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=128
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.16.99.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Depuis Switch1 je ping ma passerelle par défaut sur R1

```
SW1#ping 172.16.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1006 ms
SW1#
```

Partie 3 : Configuration et vérification de l'accès SSH sur S1

J'ctive le SSH sur S1. À partir du mode de configuration globale, je créer un nom de domaine **CCNA-Lab.com**.

```
SW1(config)#ip domain-name CCNA-Lab.com
SW1(config)#
```

```
SW1(config)#username admin privilege 15 secret sshadmin
SW1(config)#
```

Je configure l'entrée de transport de telle sorte que les lignes vty permettent uniquement les connexions SSH

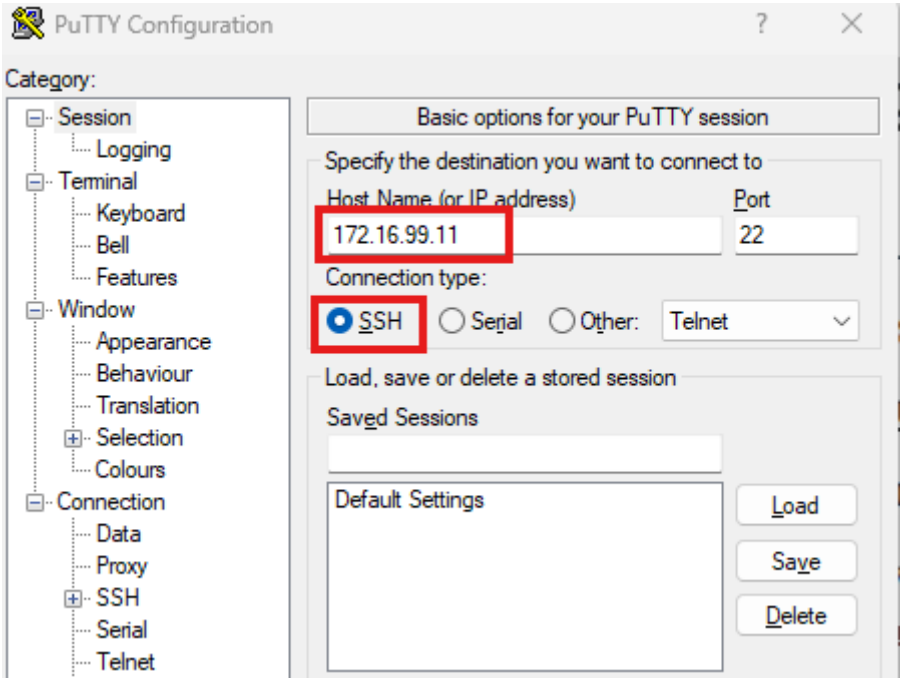
```
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#exit
SW1(config)#username admin privilege 15 secret sshadmin
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exit
SW1(config)#
```

Je génère une clé de chiffrement

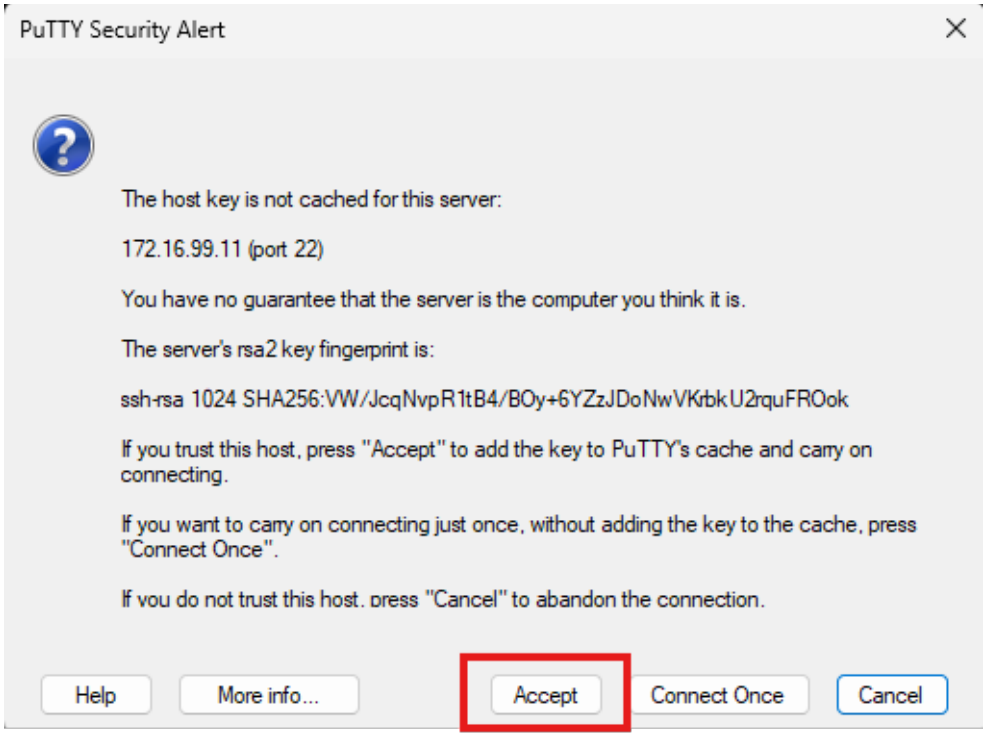
```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.CCNA-Lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW1(config)#
```

Étape 3 : Vérifiez la configuration de SSH sur S1

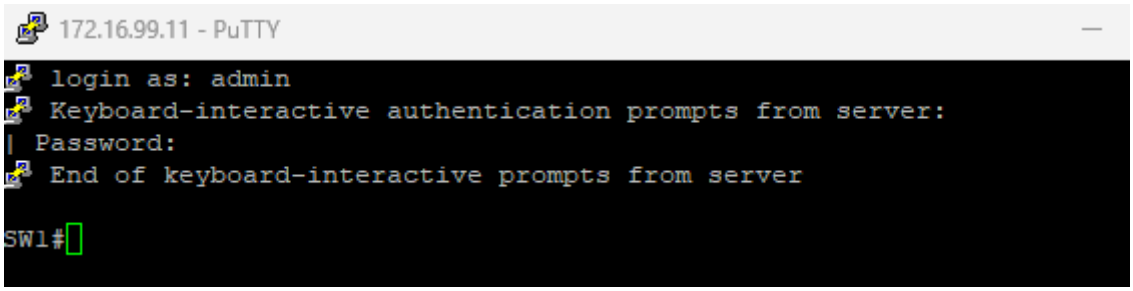
Depuis Putty sur PC-A je me connecte au Switch1 en SSH



J’accepte le message



Je me login avec admin et je tape le mot de passe sshadmin



Après avoir tapé la commande sh ip int br, je constate que les seules interfaces physiques actives sont F0/5 et F0/6

```
SW1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan99                 172.16.99.11    YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
```

Partie 4 :

Configuration et vérification des fonctions de sécurité sur S1

Étape 1 : Configurez les fonctions de sécurité générales sur S1.

```
SW1(config)#interface range f0/1 - 4
SW1(config-if-range)#shutdown
SW1(config-if-range)#
```

```
SW1(config-if-range)#interface range f0/7 - 24
SW1(config-if-range)#shutdown
```

```
SW1(config)#interface range g0/1 - 2
SW1(config-if-range)#shutdown
SW1(config-if-range)#
```

Je tape la commande sh ip int br

```
SW1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan99                 172.16.99.11    YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
```

Étape 2 : Configurez et vérifiez la sécurité des ports sur S1

Sur R1 je tape la commande show interface g0/1 pour regarder l'adresse mac

```
R1#sh int g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is e02f.6dee.f6a9 (bia e02f.6dee.f6a9)
  Internet address is 172.16.99.1/24
```

Je tape la commande show mac adress-table pour voir les adresses mac de F0/5 et F0/6

```
  99    40ae.30c2.00a8    DYNAMIC     Fa0/6
  99    e02f.6dee.f6a9    DYNAMIC     Fa0/5
Total Mac Addresses for this criterion: 22
SW1#
```

Sur S1 je passe en mode de configuration d'interface

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int f0/5
SW1(config-if)#
```

J’arrête le port avec la commande shutdown

```
SW1(config-if)#shutdown
SW1(config-if)#
```

J’active la sécurité des ports sur F0/5

```
SW1(config-if)#switchport port-security
SW1(config-if)#
```

Je configure une entrée statique pour l’interface G0/1 de R1

```
SW1(config-if)#switchport port-security mac-address e02f.6dee.f6a9
SW1(config-if)#
```

Avec la commande no shutdown j’active le port

```
SW1(config-if)#no shutdown
SW1(config-if)#end
SW1#
```

Je vérifie la sécurité des ports sur l’interface F0/5

```
SW1#show port-security  int f0/5
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   : 0000.0000.0000:0
Security Violation Count   : 0

SW1#
```

Depuis R1 je ping PC-A

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Je passe en mode de configuration d'interface pour G0/1 pour arrêter l'interface

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#shutdown
R1(config-if)#
```

Je configure une nouvelle mac adresses

```
R1(config-if)#mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown
R1(config-if)#
```

Je tape la commande show port-security sur S1 et je constate qu'il est en shutdown

```
SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Fa0/5              1            1                  1         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
SW1#
```

Je regarde l'état du Port Security

```
SW1#show port-security int f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
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   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

SW1#
```

Je tape la commande sh int f0/5 et je vois qu'il est en down

```
SW1#sh int f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 2401.c767.2385 (bia 2401.c767.2385)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
SW1#sh port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  99    e02f.6dee.f6a9    SecureConfigured              Fa0/5         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
SW1#
```

Je vais dans l'interface G0/1 pour supprimer la nouvelle mac adresse et remettre celle qui est légitime

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#shutdown
```

```
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown
R1(config-if)#end
R1#
```

Je constate qu'après avoir remis de nouveau l'adresse mac légitime de R1, l'état de S1 est toujours en Error-disabled

```
SW1#sh int f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 2401.c767.2385 (bia 2401.c767.2385)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

J'efface l'état Error Disabled

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int f0/5
SW1(config-if)#shutdown
SW1(config-if)#no shut
SW1(config-if)#
```

Je retape la commande sh int F0/5 et je vois que c'est bien en connected

```
SW1#sh int f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 2401.c767.2385 (bia 2401.c767.2385)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Je ping de nouveau PC-A depuis R1 et le ping fonctionne

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```