# SOMMAIRE



# 1. Création du réseau et configuration des paramètres de base des périphériques

Étape 2 : Configurez les paramètres de base du commutateur.

```
Current configuration : 1383 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
ip domain-name sio-exupery.local
!
username admin secret 5 $1$mERr$89oFbVUY9tU/mdjv3ClG3.
!
!
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan39
 ip address 192.168.39.6 255.255.255.248
!
ip default-gateway 192.168.39.1
!
!
!
line con 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

Étape 3 : Configurez les paramètres de base du routeur.

```
no service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin privilege 15 password 0 adminclass
!
!
license udi pid CISCO2901/K9 sn FTX1524X8G5-
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name sio-exupery.local
```

```
interface GigabitEthernet0/0
 ip address 172.17.110.201 255.255.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.250.3
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
```

# 2. Configuration des VLAN et du trunking

### Étape 1 : Créez et nommez les VLAN sur S1.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
30   util_serv_1                       active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18
32   util_serv_2                       active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
34   serveurs                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12
39   admin                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6
1002 fddi-default                      active
```

### Étape 2 : Configurez les ports trunk.

```
S1#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

S1#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,30,32,34,39

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none

S1#
```

### Étape 3 : Configurez les ports d'accès en fonction du tableau de description.

```
!
interface FastEthernet0/1
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/7
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 34
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 32
 switchport mode access
!
```

# 3. Configuration du routage inter-VLAN basé sur un trunk

Étape 1 : Créez et configurez les sous-interfaces pour les différents VLAN.

```
R1(config)#interface g0/1
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface g0/1.39
R1(config-subif)#encapsulation dot1Q 39
R1(config-subif)#ip address 192.168.39.1 255.255.255.248
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface g0/1.32
R1(config-subif)#encapsulation dot1Q 32
R1(config-subif)#ip address 192.168.0.1 255.255.255.224
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface g0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.0.33 255.255.255.240
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface g0/1.34
R1(config-subif)#encapsulation dot1Q 34
R1(config-subif)#ip address 192.168.0.49 255.255.255.248
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#no interface g0/0.30
```

### Étape 2 : Vérifiez la connectivité.

a. A partir de PCAdmin, est-il possible d'envoyer une requête ping à la passerelle par défaut du VLAN39 ?

```
C:\>ping 192.168.39.1

Pinging 192.168.39.1 with 32 bytes of data:

Reply from 192.168.39.1: bytes=32 time<1ms TTL=255
Reply from 192.168.39.1: bytes=32 time<1ms TTL=255
Reply from 192.168.39.1: bytes=32 time<1ms TTL=255
Reply from 192.168.39.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.39.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

b. A partir de PCAdmin, est-il possible d'envoyer une requête ping à S1 ? Oui
L'échange de trames passe-t-il par la passerelle du VLAN 39 ?non

```
C:\>ping 192.168.39.6

Pinging 192.168.39.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.39.6: bytes=32 time<1ms TTL=255
Reply from 192.168.39.6: bytes=32 time<1ms TTL=255
Reply from 192.168.39.6: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.39.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

c. A partir de PCAdmin, est-il possible d'envoyer une requête ping au serveur 192.168.0.50 ?

```
C:\>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

# 4. Configuration du serveur DHCP

### Étape 1 : Configurez les adresses à exclure des pools d'adresses.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.0.33
R1(config)#ip dhcp excluded-address 192.168.0.1
R1(config)#
```

### Étape 2 : Paramétrez les pools DHCP pour les VLANs 30 et 32.

a. Créez les pools **dhcpvlan30** et **dhcpvlan32**.

```
R1(config)#ip dhcp pool dhcpvlan30
R1(dhcp-config)#network 192.168.0.32 255.255.255.240
R1(dhcp-config)#default-router 192.168.0.33
R1(dhcp-config)#dns-server 172.17.254.5
R1(dhcp-config)#domain-name sio-exupery.local
R1(dhcp-config)#exit
R1(config)#
```

b. Chaque pool donne l'adresse du serveur DNS Aviateur, le suffixe DNS (sio-exupery.local) avec l'option **domain-name** ainsi que la passerelle par défaut du VLAN.

```
R1(config)#ip dhcp pool dhcpvlan32
R1(dhcp-config)#network 192.168.0.0 255.255.255.224
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#dns-server 172.17.254.5
R1(dhcp-config)#domain-name sio-exupery.local
R1(dhcp-config)#exit
R1(config)#
```

### Étape 3 : Configurez PC30 en tant que client DHCP.

a. PC30 peut-il contacter sa passerelle par défaut, le serveur 192.168.0.50 ou PCAdmin ?oui

```
C:\>ping 192.168.39.2

Pinging 192.168.39.2 with 32 bytes of data:

Reply from 192.168.39.2: bytes=32 time<1ms TTL=127
Reply from 192.168.39.2: bytes=32 time=13ms TTL=127
Reply from 192.168.39.2: bytes=32 time=1ms TTL=127
Reply from 192.168.39.2: bytes=32 time<1ms TTL=127
```

b. PC30 peut-il contacter l'interface externe du routeur ?

```
C:\>ping 172.17.110.201

Pinging 172.17.110.201 with 32 bytes of data:

Reply from 172.17.110.201: bytes=32 time<1ms TTL=255
Reply from 172.17.110.201: bytes=32 time=5ms TTL=255
Reply from 172.17.110.201: bytes=32 time<1ms TTL=255
Reply from 172.17.110.201: bytes=32 time=40ms TTL=255

Ping statistics for 172.17.110.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 40ms, Average = 11ms
```

c. PC30 peut-il contacter le serveur Aviateur ? Pourquoi ?

```
C:\>ping 172.17.254.5

Pinging 172.17.254.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.254.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

**Non**, ça ne fonctionne pas encore. Parce que le **NAT/PAT n'est pas encore configuré**. PC30 a une adresse privée et le routeur ne traduit pas encore ces adresses vers l'extérieur.

# 5.Configuration du NAT/PAT

**Étape 1 : Désignez les interfaces du routeur participant à la traduction d'adresse.**

```
R1(dhcp-config)#exit
R1(config)#interface g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
R1(config)#interface g0/1.30
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#
R1(config)#interface g0/1.32
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#
R1(config)#interface g0/1.34
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#
R1(config)#interface g0/1.39
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#
```

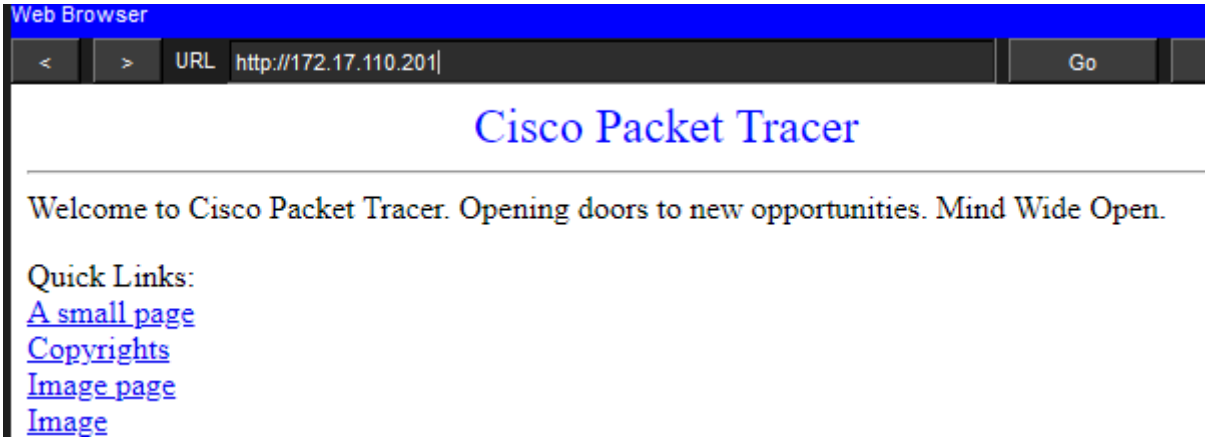
**Étape 2 : Mettez en œuvre la traduction d'adresse dynamique avec la fonction PAT permettant de traduire les adresses en provenance des réseaux 30, 32, 34 et 39 afin de recevoir les réponses des machines extérieures.**

```
R1(config)#access-list 1 permit 192.168.0.32 0.0.0.15
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.31
R1(config)#access-list 1 permit 192.168.0.48 0.0.0.7
R1(config)#access-list 1 permit 192.168.39.0 0.0.0.7
R1(config)#
R1(config)#ip nat inside source list 1 interface g0/0 overload
R1(config)#
```

**Étape 3 : Mettez en œuvre une traduction d'adresse statique de 172.17.110.201 (interface outside) vers le serveur 192.168.0.50 permettant d'accéder aux sites web de ce dernier depuis l'extérieur**

```
R1(config)#ip nat inside source static 192.168.0.50 172.17.110.201
R1(config)#
```

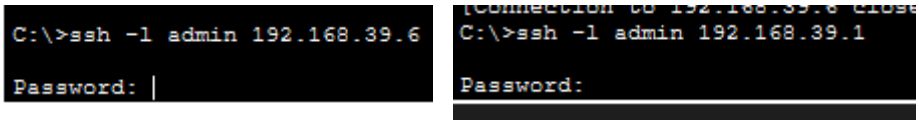
Teste de la traduction



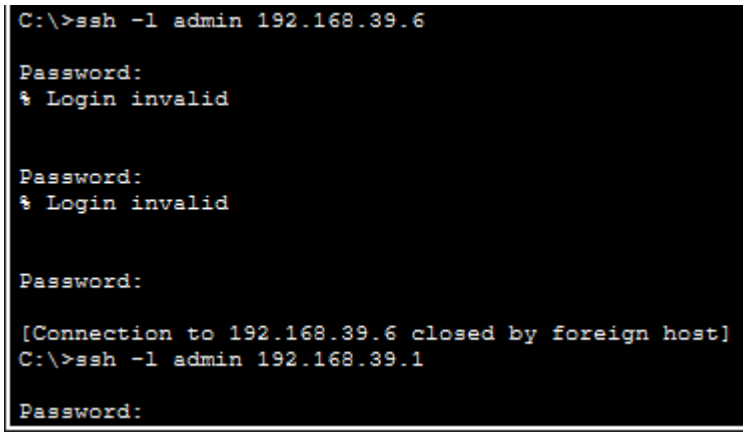

## 6. Mise en place d'ACL

**Etape 1 : testez l'accès SSH au switch ainsi qu'au routeur depuis une machine des VLAN 39, 30 et 32 (éventuellement depuis VLAN 34).**

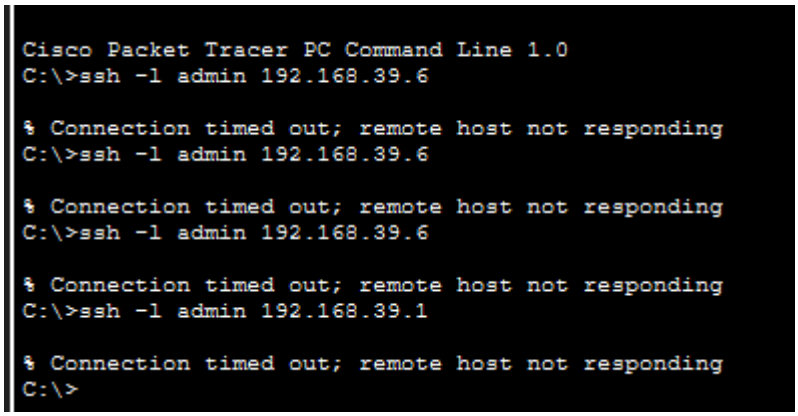
PC admin




Pc30




**PC32 (VLAN 32)** l' SSH bloqué)



**Etape 2 : sécurisez l'accès au switch.**

```
S1(config)#access-list 10 permit 192.168.39.0 0.0.0.7
S1(config)#line vty 0 15
S1(config-line)#access-class 10 in
S1(config-line)#exit
S1(config)#
```

**Etape 3 : sécurisez l'accès au routeur**

```
R1(config)#ip access-list standard R1_SSH
R1(config-std-nacl)#permit 192.168.39.0 0.0.0.7
R1(config-std-nacl)#exit
R1(config)#
R1(config)#line vty 0 15
R1(config-line)#access-class R1_SSH in
R1(config-line)#exit
R1(config)#
```

**Etape 4 : limiter les accès depuis le réseau VLAN 32**

```
R1(config)#ip access-list extended VLAN32_IN
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.31 192.168.0.32 0.0.0.15
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.31 192.168.0.48 0.0.0.7
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.31 192.168.39.0 0.0.0.7
R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.31 host 172.17.254.5
R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.0.31 host 172.17.254.5 eq 80
R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.0.31 host 172.17.254.5 eq 443
R1(config-ext-nacl)#permit udp 192.168.0.0 0.0.0.31 host 172.17.254.5 eq 53
R1(config-ext-nacl)#permit udp 192.168.0.0 0.0.0.31 any eq 67
R1(config-ext-nacl)#exit
R1(config)#
R1(config)#interface g0/1.32
R1(config-subif)#ip access-group VLAN32_IN in
R1(config-subif)#exit
R1(config)#
```

pc admin peut ce connecte en ssh pas les autre pc

```
[Connection to 192.168.39.1 closed by foreign host]
C:\>ssh -l admin 192.168.39.6

Password:
```

```
C:\>ssh -l admin 192.168.39.6

% Connection refused by remote host
C:\>
```

# 7. Hypothèse d'un serveur DHCP situé dans le réseau 172.17.0.0/16

Les commandes àque ont doit saisir sur R1 sont uniquement les ip helper-address sur chaque sous-interface des VLAN:

```
interface g0/1.30
ip helper-address 172.17.254.5
exit

interface g0/1.32
ip helper-address 172.17.254.5
exit
```