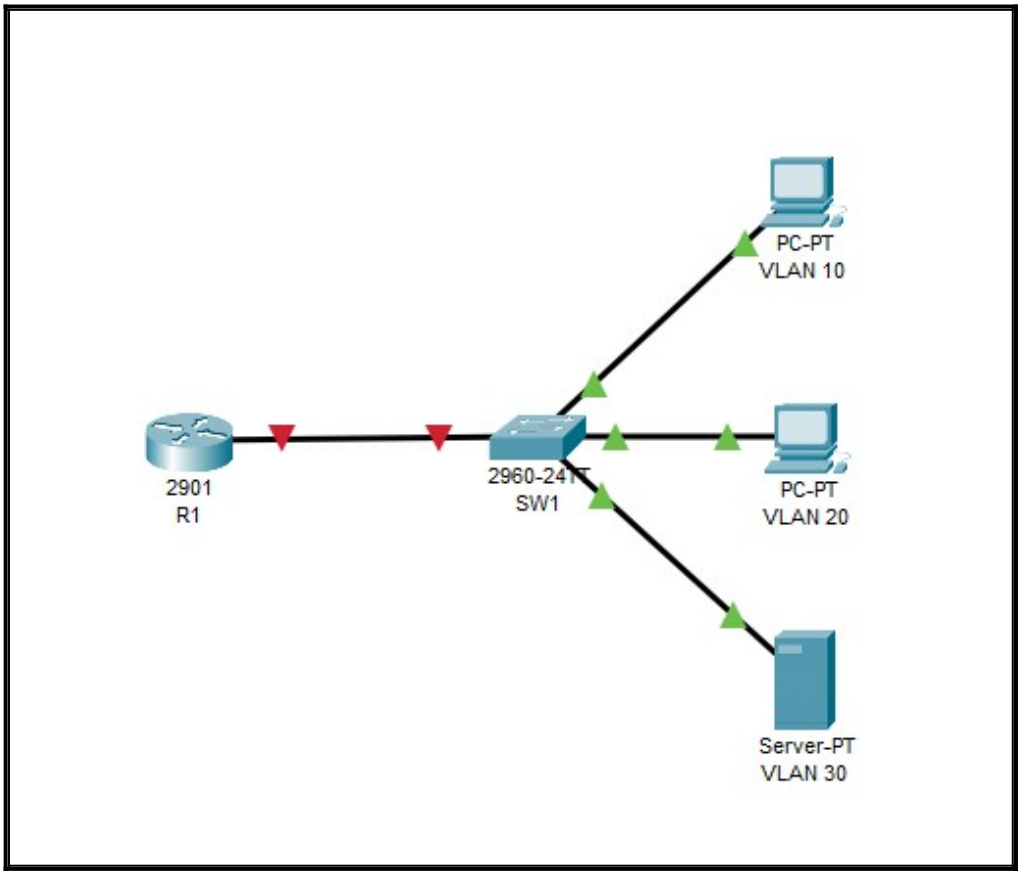
TP18 : Routage inter-vlan, dhcp, access-list

Sommaire :

Topologie :



1. Configuration du commutateur SW1

```
SW1#sh run
Building configuration...

Current configuration : 2349 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.0.2 255.255.255.252
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

1ère étape : Configuration du commutateur SW1.

2. Configuration du routeur R1

```
R1#sh run
Building configuration...

Current configuration : 1653 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
ip dhcp excluded-address 192.168.1.0
ip dhcp excluded-address 192.168.1.16
!
ip dhcp pool VLAN10
 network 192.168.1.0 255.255.255.240
 default-router 192.168.1.1
 dns-server 8.8.8.8
ip dhcp pool VLAN20
 network 192.168.1.16 255.255.255.240
 default-router 192.168.1.17
 dns-server 8.8.8.8
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX1524ORK
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.252
 ip access-group WEB in
 ip access-group WEB_RETOUR out
 duplex auto
 speed auto
```

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.240
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.17 255.255.255.240
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.33 255.255.255.248
 ip access-group WEB out
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended WEB
 permit ip 192.168.1.16 0.0.0.15 any echo
 permit tcp 192.168.1.16 0.0.0.15 any eq www
 permit tcp 192.168.1.16 0.0.0.15 any eq 443
 deny tcp 192.168.1.0 0.0.0.15 any eq www
 deny tcp 192.168.1.0 0.0.0.15 any eq 443
access-list 1 permit 192.168.1.0 0.0.0.15
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 1 in
 password cisco
 logging synchronous
 login
 transport input telnet
!
!
!
end
```

3. ACL

Définition de l'access-list 101 pour le management du switch via telnet :

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.15
```

```
R1(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.15 host 192.168.0.2
eq telnet
```

```
R1(config)#access-list 101 permit tcp any host 192.168.0.2 established
```

```
R1(config)#access-list 101 permit icmp any host 192.168.0.2  echo-reply
```

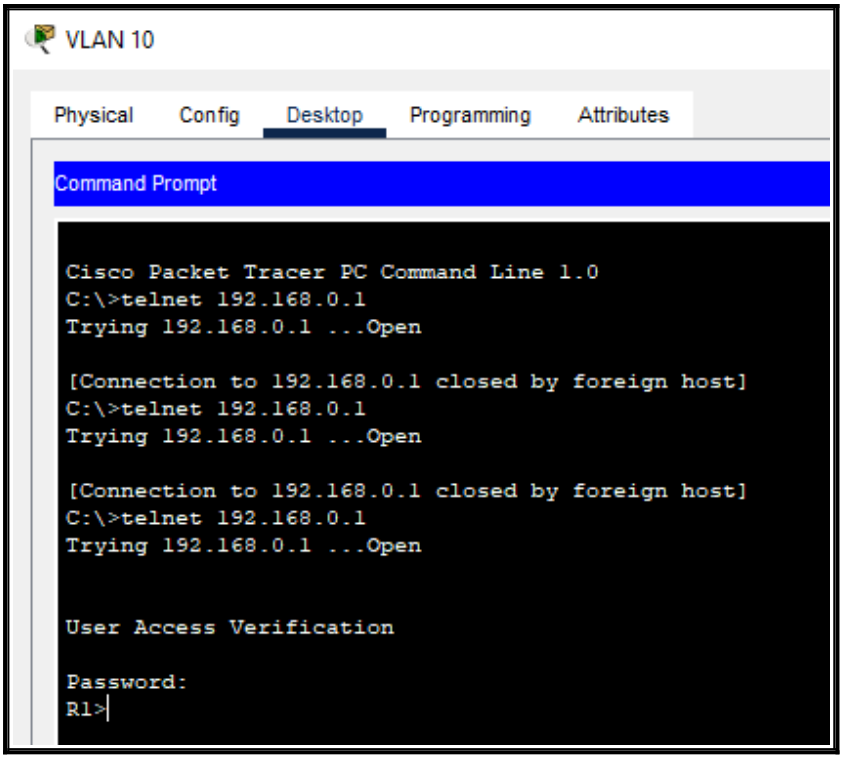
Définition de l'ACL étendue server-access pour l'accès au serveur Web/DNS :

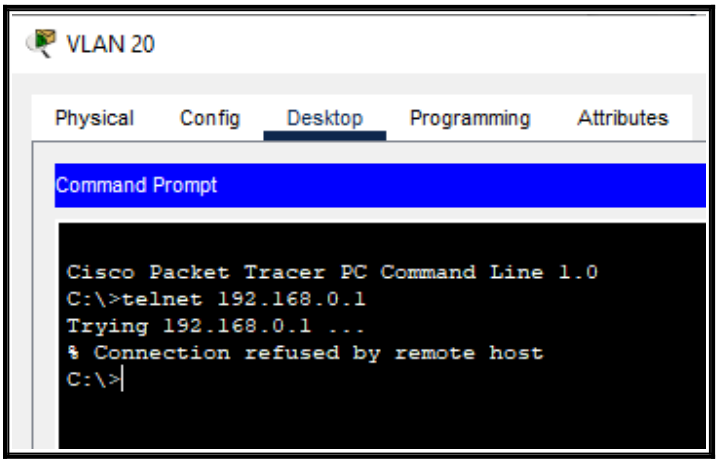
```
R1(config)#ip access-list extended server-access_retour
R1(config-ext-nacl)#permit tcp 192.168.1.16 0.0.0.15 host 192.168.1.34 eq www
R1(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.31 host 192.168.1.34 echo
R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.31 host 192.168.1.34 eq
domain
R1(config-ext-nacl)#permit udp 192.168.1.0 0.0.0.31 host 192.168.1.34 eq
domain
```

```
R1(config-ext-nacl)#permit tcp any host 192.168.1.34 established
R1(config-ext-nacl)#permit icmp any host 192.168.1.34 echo-reply
```

4. Travail à faire

2. Vérifier que seuls les hôtes du VLAN 10 peuvent accéder au VLAN de management via telnet :





3. Vérifier que les machines des VLAN 10 et 20 peuvent « pinguer » le serveur du VLAN 30 :

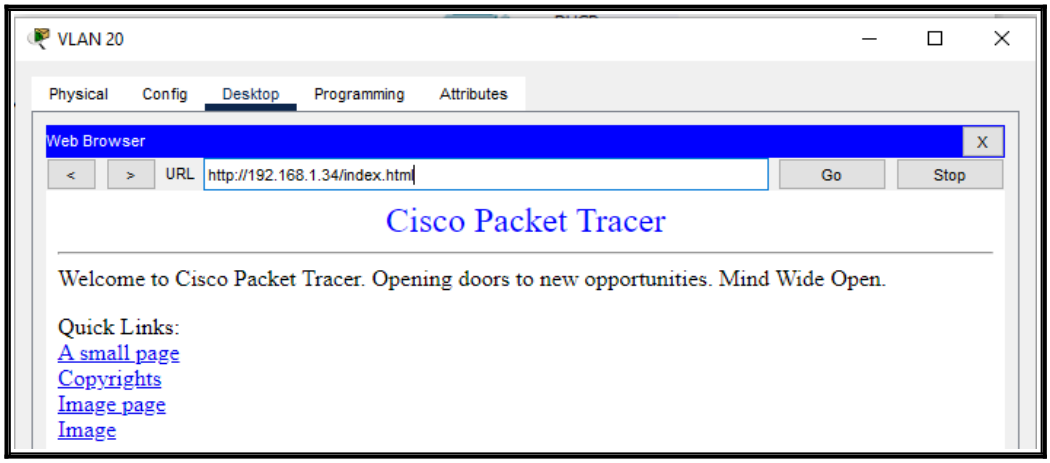
VLAN 10 vers VLAN 30

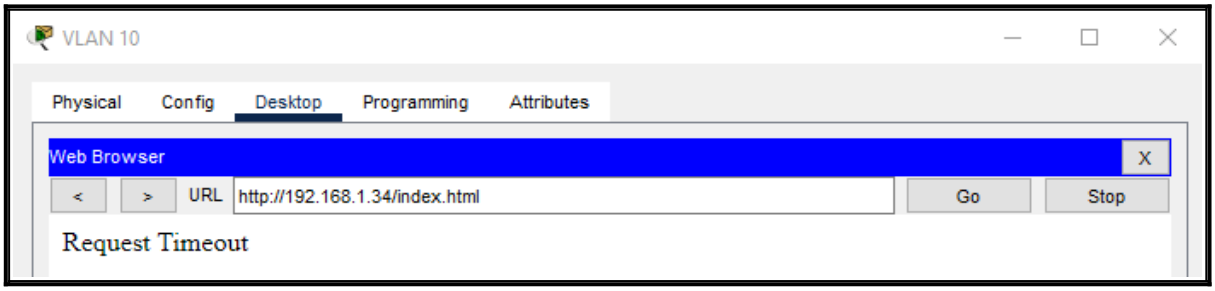
```
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=4ms TTL=127
Reply from 192.168.1.34: bytes=32 time<1ms TTL=127
Reply from 192.168.1.34: bytes=32 time<1ms TTL=127
Reply from 192.168.1.34: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

VLAN 20 vers VLAN 30

```
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time<1ms TTL=127
Reply from 192.168.1.34: bytes=32 time<1ms TTL=127
Reply from 192.168.1.34: bytes=32 time=1ms TTL=127
Reply from 192.168.1.34: bytes=32 time=5ms TTL=127

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

4. Vérifier que seuls les hôtes du VLAN 20 peuvent accéder à l'application Web de ce serveur :


VLAN 20
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.34/index.html
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


VLAN 10
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.34/index.html
Go
Stop
Request Timeout