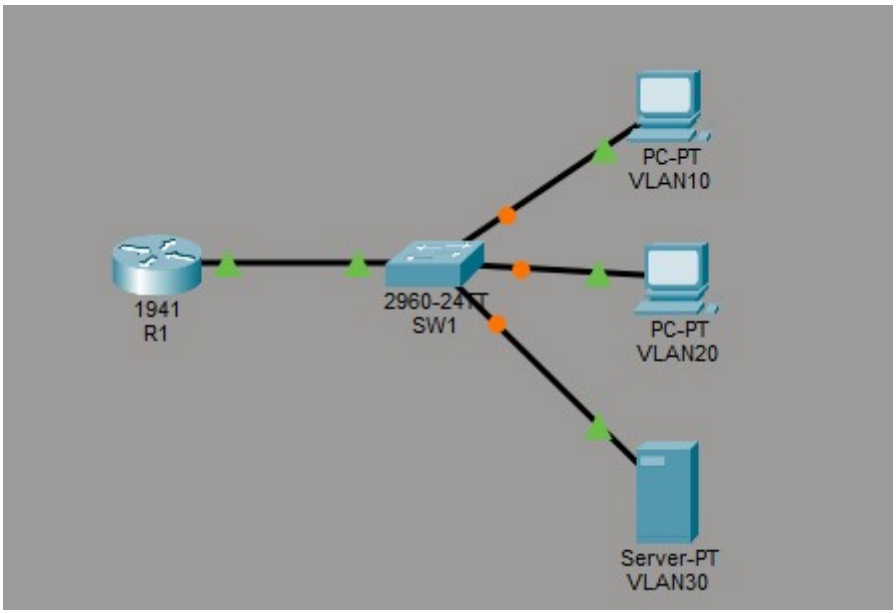
TP18 : Routage inter-vlan, dhcp, access-list

Sommaire

On commence tout d’abord par reproduire la topologie



1. Configuration du commutateur SW1

```
Switch(config)#no ip domain-lookup
Switch(config)#service password-encryption
Switch(config)#hostname SW1
SW1(config)#enable secret class
SW1(config)#int range f0/1 - 9
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW1(config-if-range)#switchport port-security
```

```
SW1(config)#int f0/10
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport port-security
```

Je me suis tromper j’avais mit jusqu’à la F0/9 alors que c’est jusqu’à la F0/10

```
SW1(config)#int range f0/11 - 20
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW1(config-if-range)#switchport port-security
```

```
SW1(config)#int range f0/21 - 24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW1(config-if-range)#switchport port-security
```

On fait un sh vlan br pour vérifier la création des vlan et l'affectation des ports

```
SW1#sh vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   VLAN0020                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
30   VLAN0030                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

On met l'interface G0/1 en mode TRUNK pour permettre le passage des VLANs vers le routeur

```
SW1(config)#int g0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#no shut
```

On shutdown l'interface G0/2

```
SW1(config)#int G0/2
SW1(config-if)#shut
```

On définit l'adresse IP du VLAN 1 pour permettre l'administration à distance du switch via telnet

```
SW1(config)#int Vlan1
SW1(config-if)#ip address 192.168.0.2 255.255.255.252
```

On définit la passerelle par défaut du switch

```
SW1(config)#ip default-gateway 192.168.0.1
```

On définie l'access-list 1 pour le management du switch via telnet

```
SW1(config)#access-list 1 permit 192.168.1.0 0.0.0.15
```

On configure l’accès console et telnet

```
SW1(config)#line con 0
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#logging synchronous
```

```
SW1(config)#line vty 0 15
SW1(config-line)#access-class 1 in
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#transport input telnet
```

2. Configuration du routeur R1

```
Router(config)#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#hostname R1
R1(config)#enable secret class
```

L'interface physique est utilisée pour le VLAN 1 qui n'est pas tagué avec 802.1X (VLAN natif)

```
R1(config)#int g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.252
R1(config-if)#no shut
```

Sous-interface pour le VLAN 10, encapsulation dot1Q

```
R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.1.1 255.255.255.240
```

Sous-interface pour le VLAN 20, encapsulation dot1Q

```
R1(config)#int g0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.1.17 255.255.255.240
```

Sous-interface pour le VLAN 30, encapsulation dot1Q. On y applique l'access list extended "server-access&retour" de manière à n'autoriser que le traffic ICMP et DNS pour les VLANs 10 et 20 et uniquement le trafic Web provenant du VLAN 20 vers le serveur Web/DNS

```
R1(config)#int g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.1.33 255.255.255.248
R1(config-subif)#ip access-group serve-access&retour out
```

```
R1(config)#int g0/1
R1(config-if)#no ip address
R1(config-if)#shut
```

On définie l'access-list 1 pour le management du routeur via telnet

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

On définie l'ACL étendue server-access&retour pour l'accès au serveur Web/DNS

```
access-list 1 permit 192.168.1.0 0.0.0.15
ip access-list extended server-access&retour
 permit tcp 192.168.1.16 0.0.0.15 host 192.168.1.34 eq www
 permit icmp 192.168.1.0 0.0.0.31 host 192.168.1.34 echo
 permit tcp 192.168.1.0 0.0.0.31 host 192.168.1.34 eq domain
 permit tcp any host 192.168.1.34 established
 permit icmp any host 192.168.1.34 echo-reply
 permit udp 192.168.1.0 0.0.0.31 host 192.168.1.34 eq domain
```

On exclut les adresses des sous-interfaces du routeur pour les pools DHCP

```
R1(config)#ip dhcp excluded-address 192.168.1.1
R1(config)#ip dhcp excluded-address 192.168.1.17
```

On définie des pools DHCP pour chaque VLAN

```
R1(config)#ip dhcp pool vlan10
R1(dhcp-config)#network 192.168.1.0 255.255.255.240
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 192.168.1.34
R1(dhcp-config)#exit
R1(config)#ip dhcp pool vlan20
R1(dhcp-config)#network 192.168.1.16 255.255.255.240
R1(dhcp-config)#default-router 192.168.1.17
R1(dhcp-config)#dns-server 192.168.1.34
```

On configure l’accès console

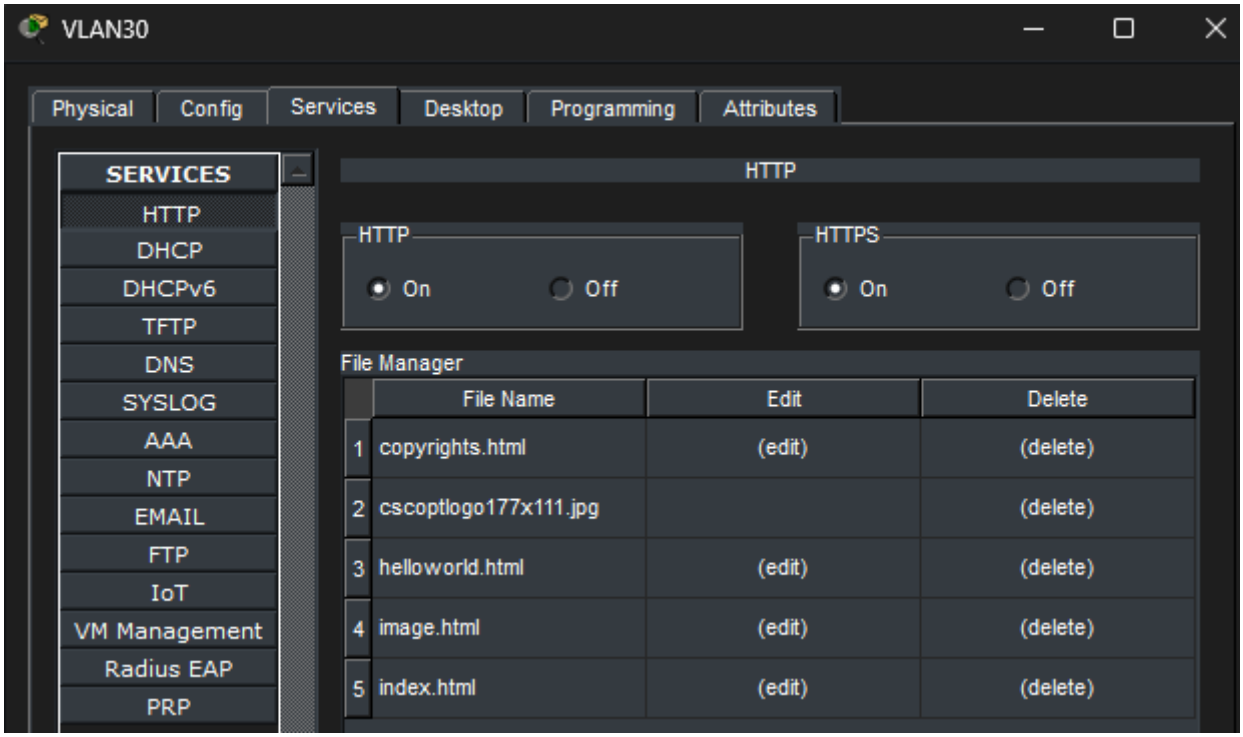
```
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
```

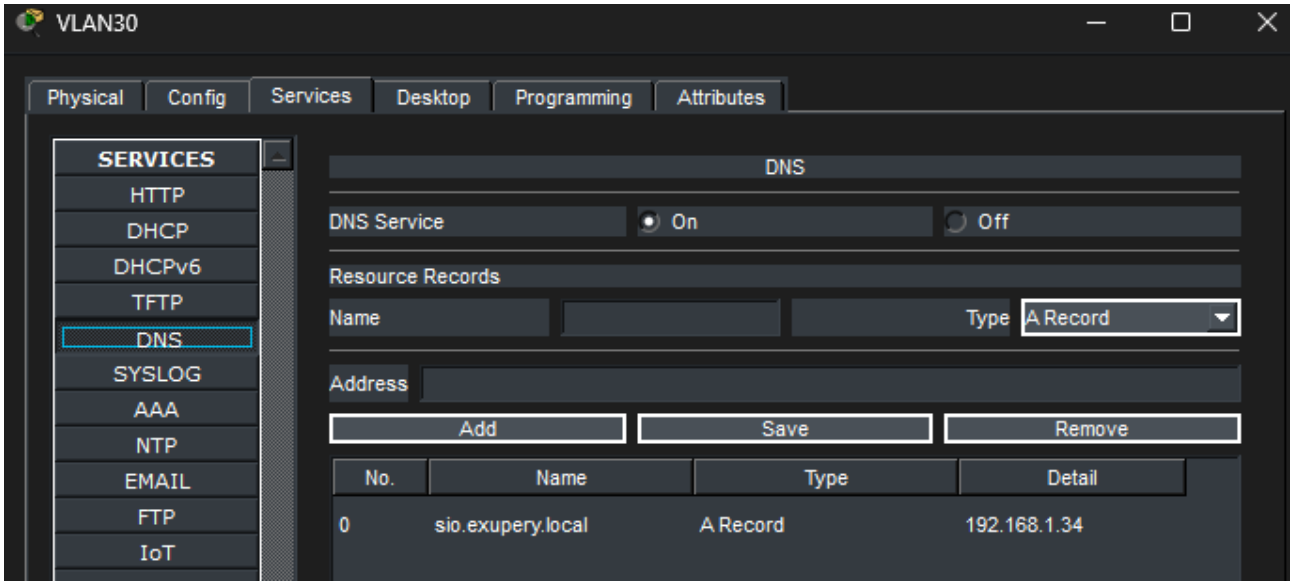
On applique l'access-list 1 aux lignes VTY pour n'autoriser que les connexions provenant du VLAN 10

```
R1(config)#line vty 0 4
R1(config-line)#access-class 1 in
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#transport input telnet
```

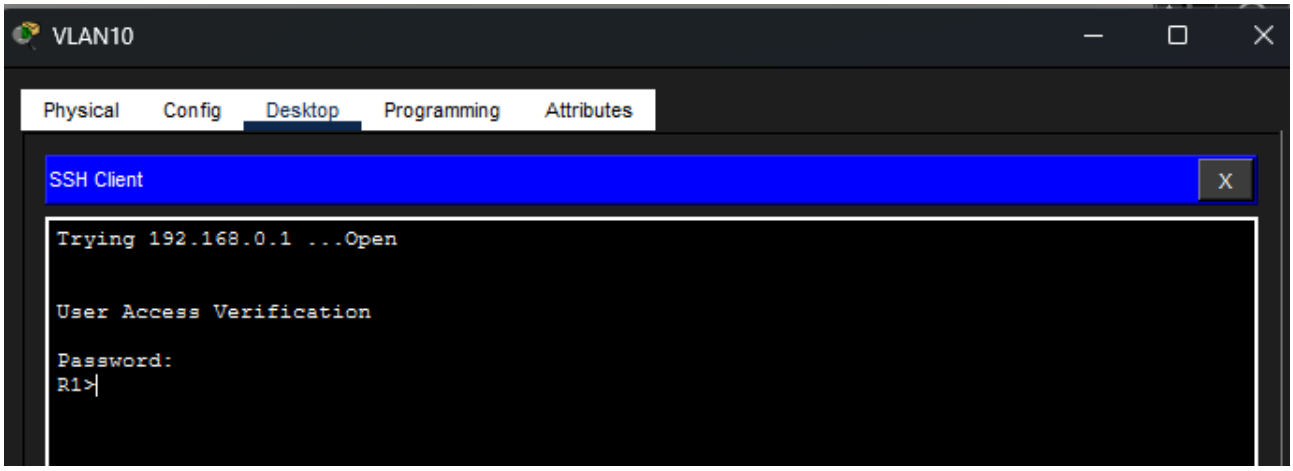
3. Travail à faire

1) On met en place le réseau et on configure les différents équipements. Le serveur présent dans le VLAN 30 héberge les services Web et DNS (onglet **Services**)

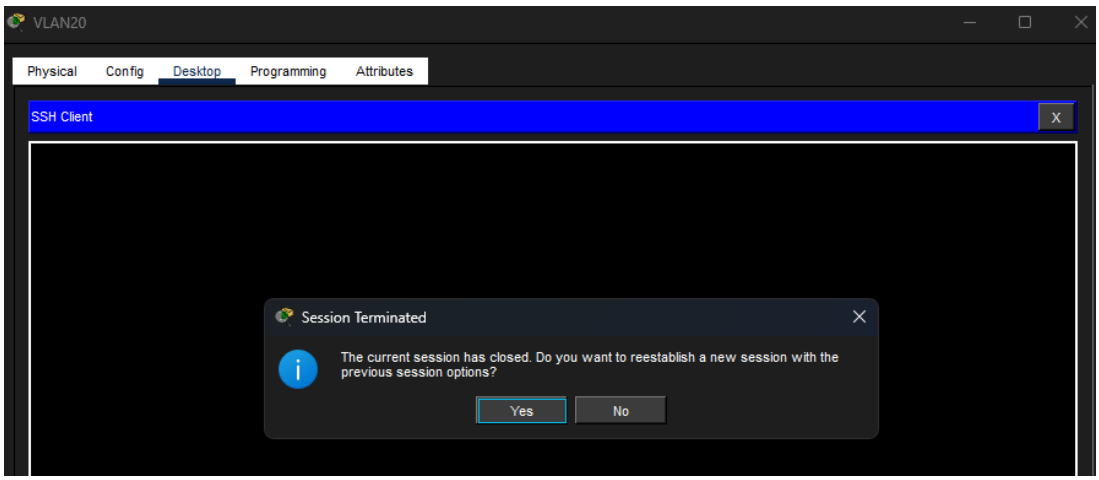




2) On vérifie que seuls les hôtes du VLAN 10 peuvent manager le switch ainsi que le routeur via telnet

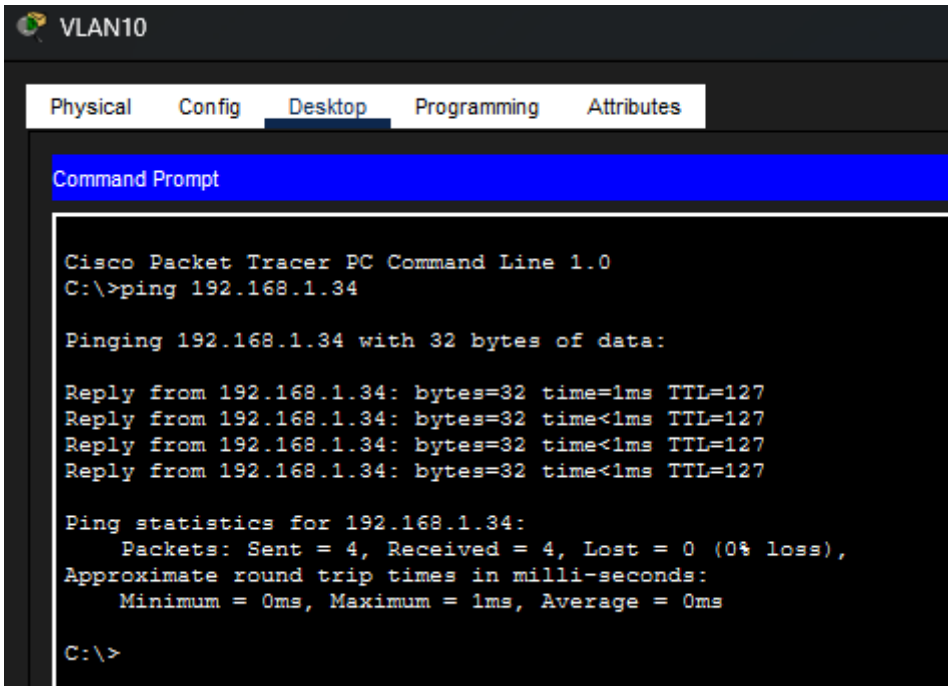


On peut bien voir que les hôtes du Vlan 10 peuvent manager le switch et le routeur via telnet alors que les hôtes des autres Vlan ne le peuvent pas

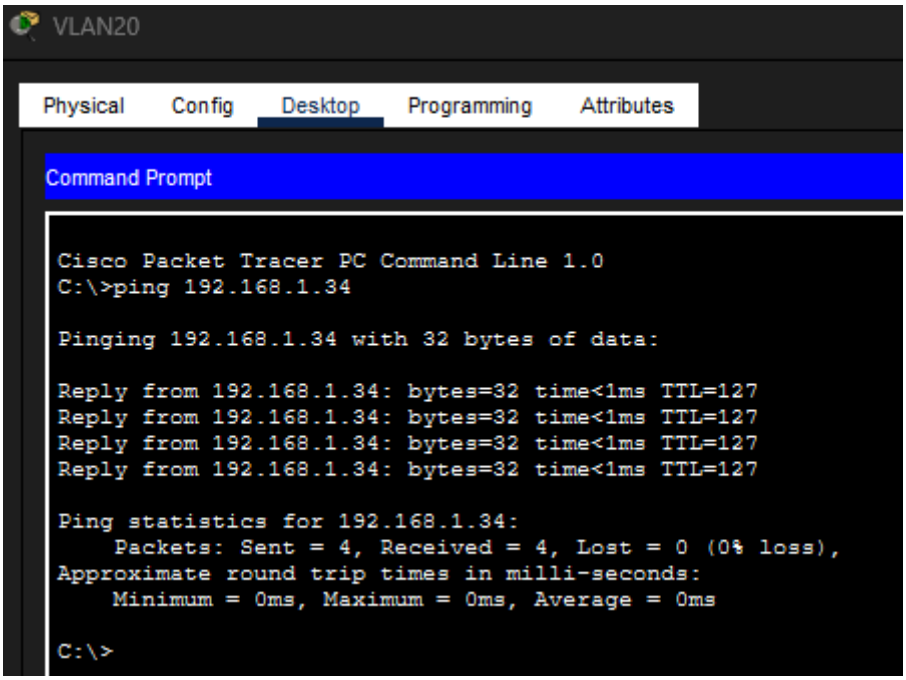


3) On vérifie que les machines des VLAN 10 et 20 peuvent « pinguer » le serveur du VLAN 30

Ping depuis Vlan10 :

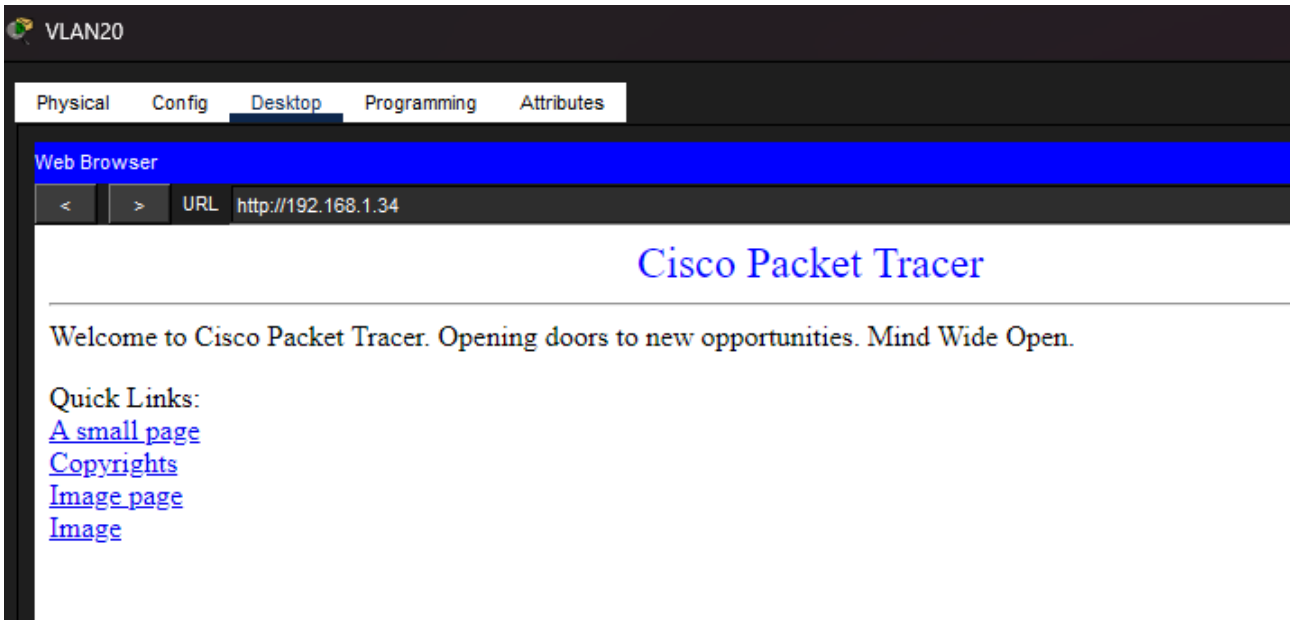


Ping depuis Vlan20 :



Les pings marchent les machines du Vlan10 et 20 peuvent bien pinguer le serveur du Vlan30

4) On vérifie que seuls les hôtes du VLAN 20 peuvent accéder à l’application Web de ce serveur


VLAN20
Physical
Config
Desktop
Programming
Attributes
Web Browser
<
>
URL
http://192.168.1.34
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