Universidad de Los Andes

Infraestructura de Comunicaciones – 202220

Laboratorio 5 - Administración de Switches, VLANs y WLANs

Juan Alegría – 202011282

Juan Andrés Romero – 202013449

4.1 Configuración básica de dispositivos de red

4.1.1 Configuración básica de Switch

Configuración Switch 1

```
SW2(config)#hostname SW1
SW1(config)#interface vlan1
SW1(config-if)#ip address 192.168.0.2 255.255.255.0
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
SW1(config)#ip default-gateway 192.168.0.1
SW1(config)#interface range fastEthernet 0/6-23
SW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
```

Configuración Switch 2

```
SW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#interface vlan1
SW2(config-if)#ip address 192.168.0.3 255.255.255.0
```

```
SW2(config-if)#no shutdown

SW2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW2(config-if)#exit
SW2(config)#ip default-gateway 192.168.0.1
SW2(config)#interface range fastEthernet 0/6-23
SW2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
```

Comprobación configuración VLAN

SW1

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW1#
```

```
SW1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/3       1-1005
Fa0/4       1-1005
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1
Fa0/4       1
Fa0/5       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       none
Fa0/4       none
Fa0/5       1

SW1#
```

SW2

```
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW2#
```

```
SW2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/2       1-1005
Fa0/3       1-1005
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/2       1
Fa0/3       1
Fa0/4       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       none
Fa0/3       1
Fa0/4       none
```

4.1.2 Configuración básica de enrutador

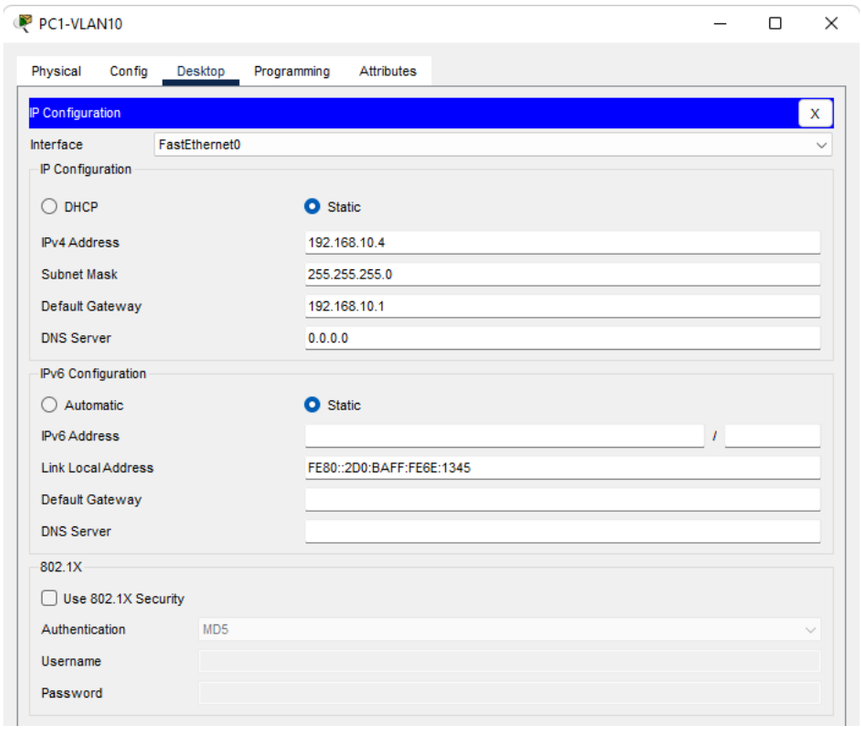
R1

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#exit
R1#
```

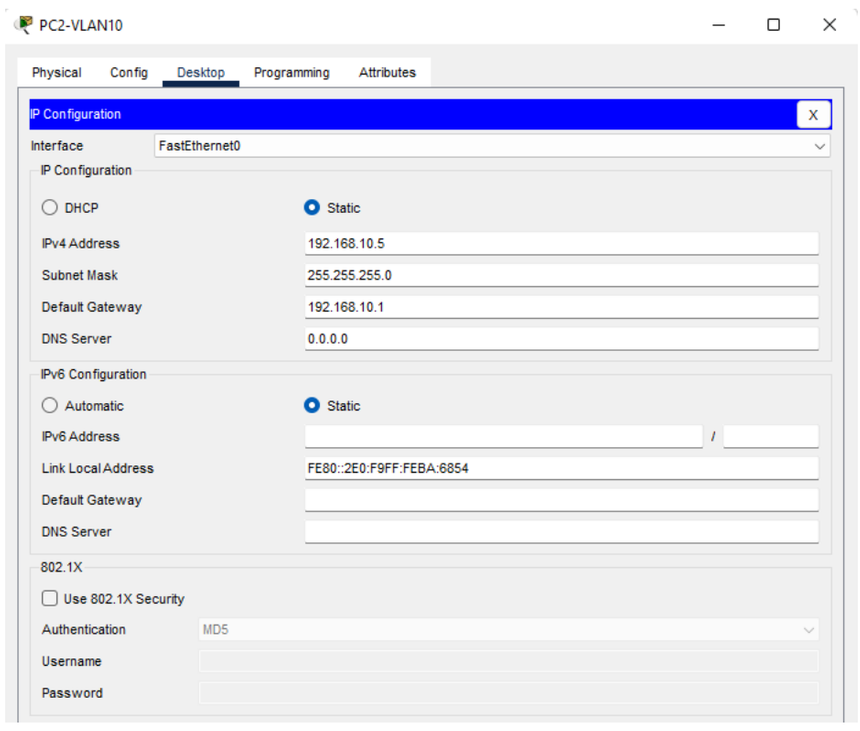
```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

4.1.3 Configuración básica equipos PCs

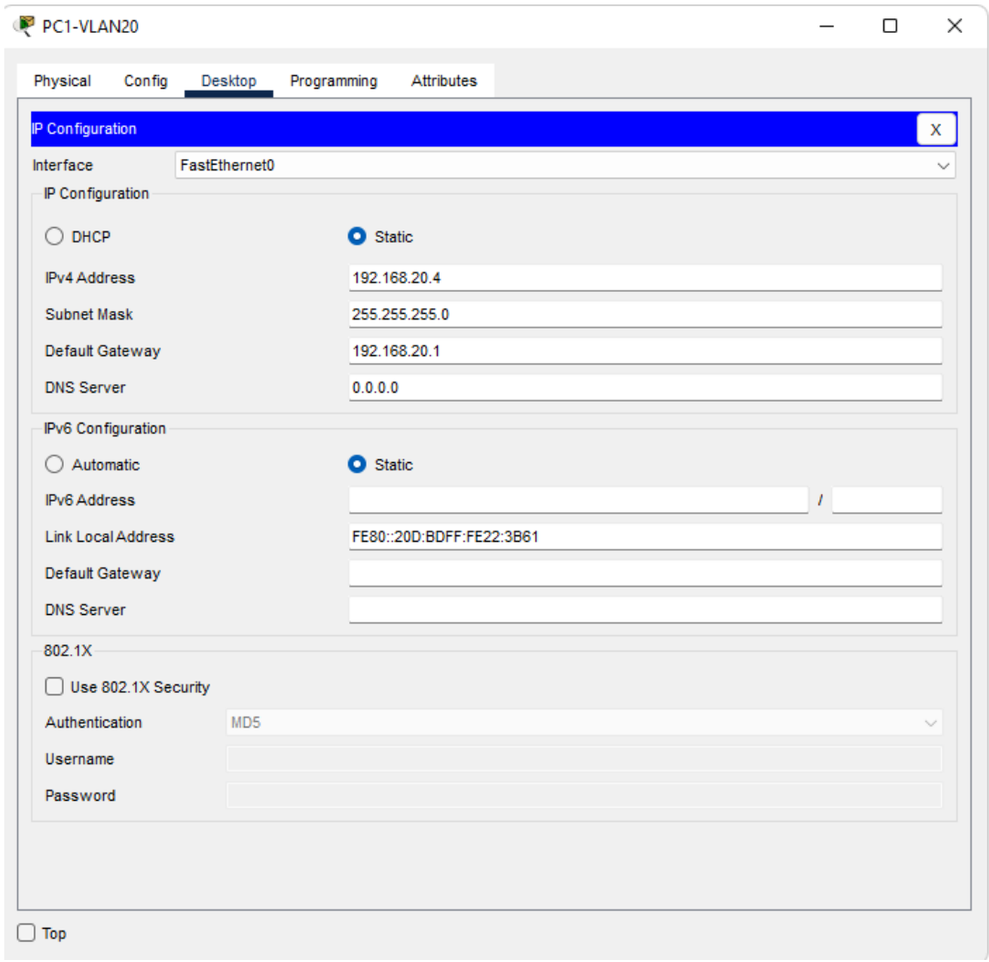
PC1-VLAN10



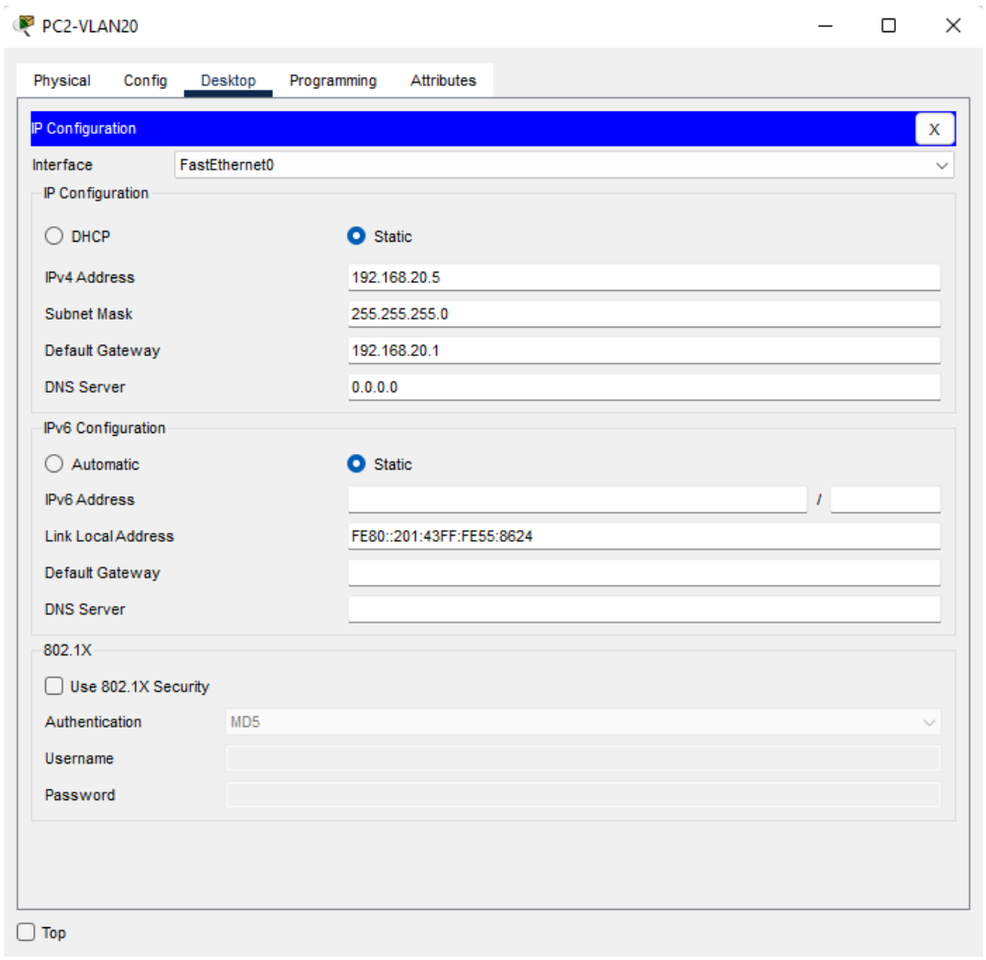
PC2-VLAN10



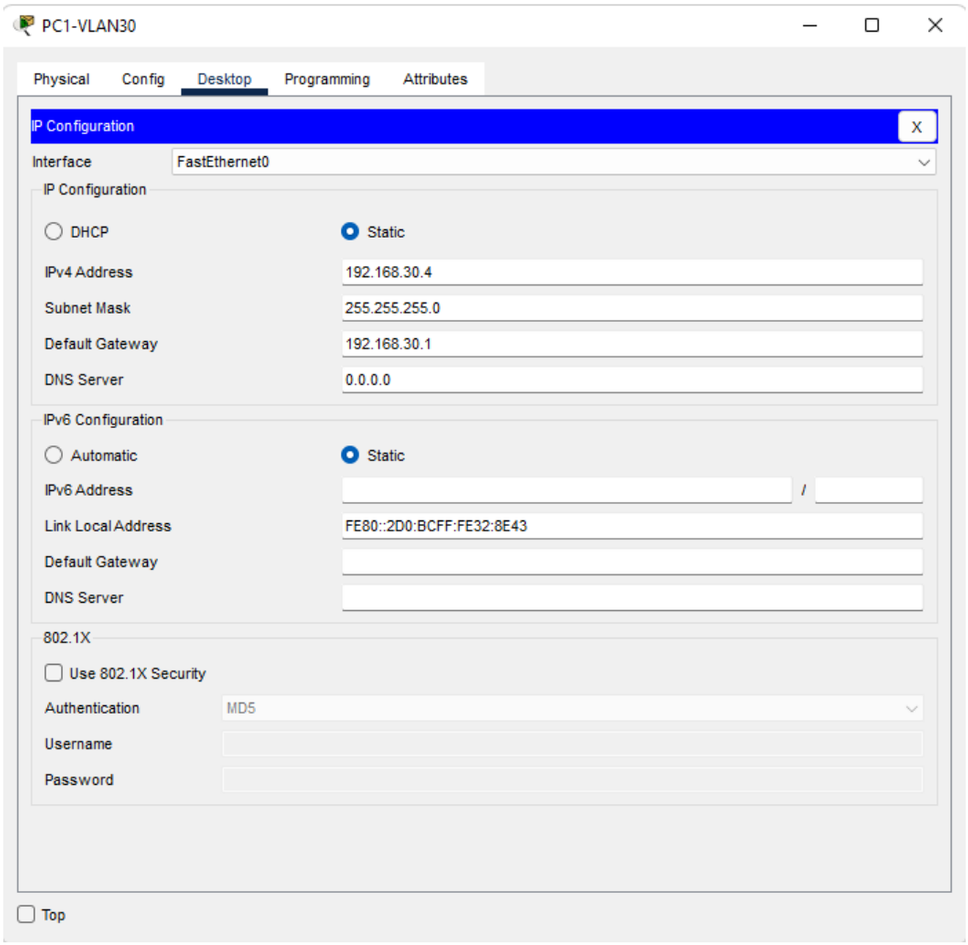
PC1-VLAN20



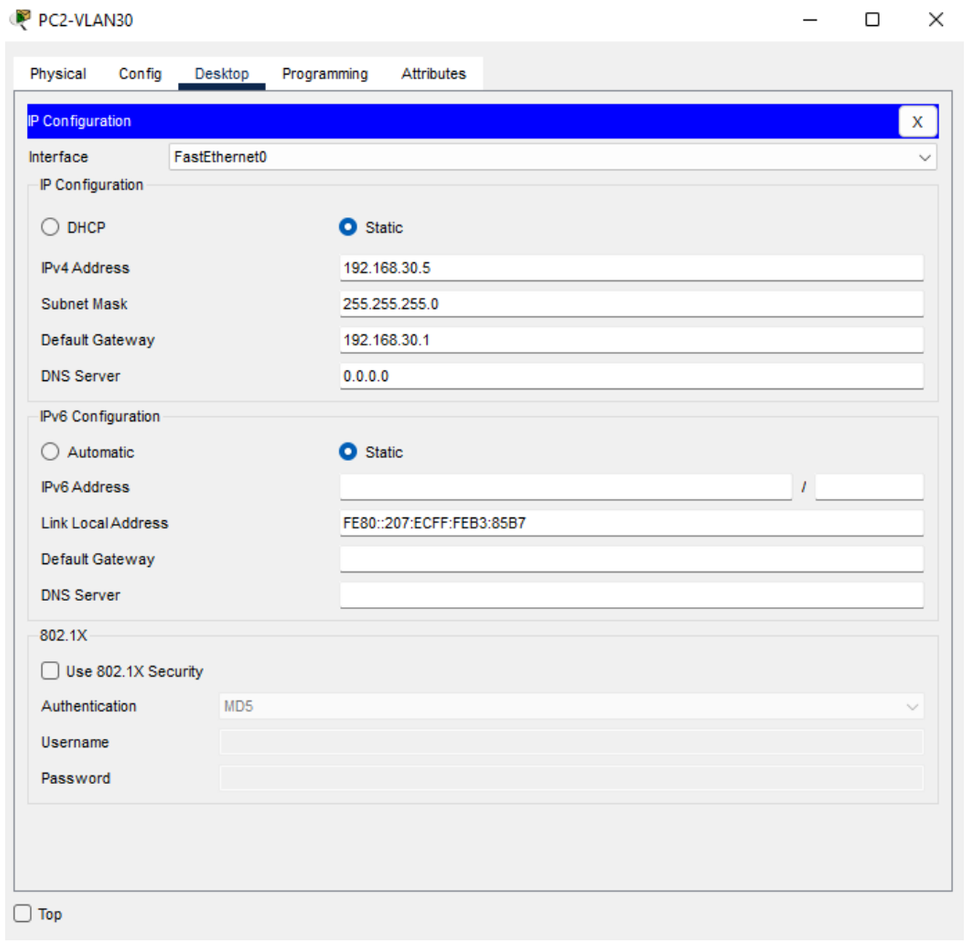
PC2-VLAN20



PC1-VLAN30



PC2-VLAN30



4.2 Configuración de VLANs y enrutamiento entre VLANs

4.2.1 Configuración de VLANs y enlace troncal

Creación de VLAN 10, 20 y 30 en SW1

```
SW1>enable
SW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#vlan 10
SW1(config-vlan)#name Administrativos
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name Preventa
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name Operaciones
SW1(config-vlan)#exit
```

Creación de VLAN 10, 20 y 30 en SW2

```
SW2>enable
SW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#vlan 10
SW2(config-vlan)#name Administrativos
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name Preventa
SW2(config-vlan)#exit
SW2(config)#vlan 30
SW2(config-vlan)#name Operaciones
SW2(config-vlan)#exit
SW2(config)#
```

Configuración enrutamiento en SW1

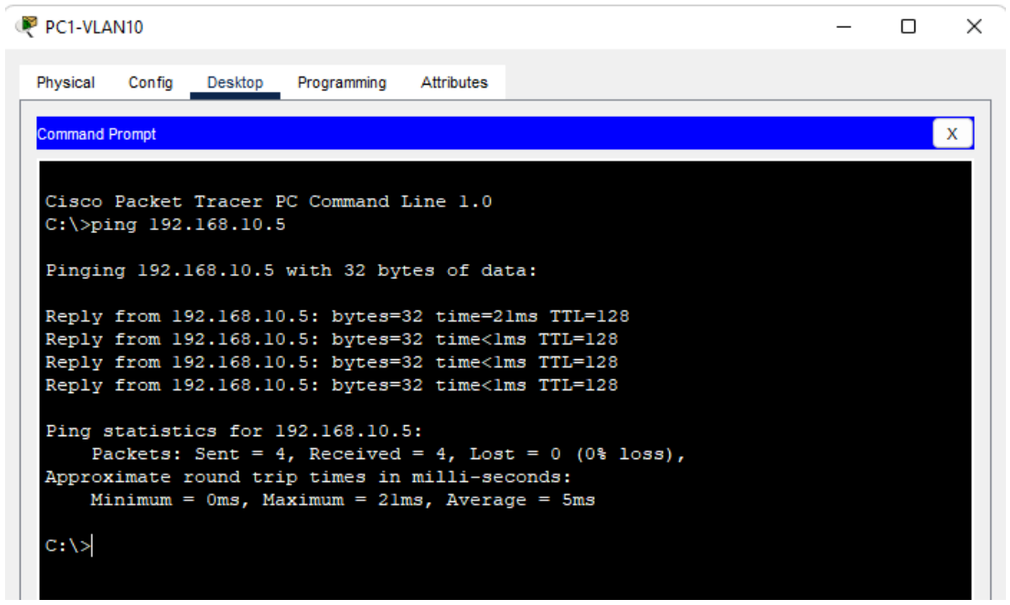
```
SW1(config-if)#interface Fa0/4
SW1(config-if)#switchport access vlan 20
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 1
SW1(config-if)#interface Fa0/3
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 1
SW1(config-if)#interface Fa0/5
SW1(config-if)#switchport access vlan 30
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 1
SW1(config-if)#
```

Configuración enrutamiento en SW2

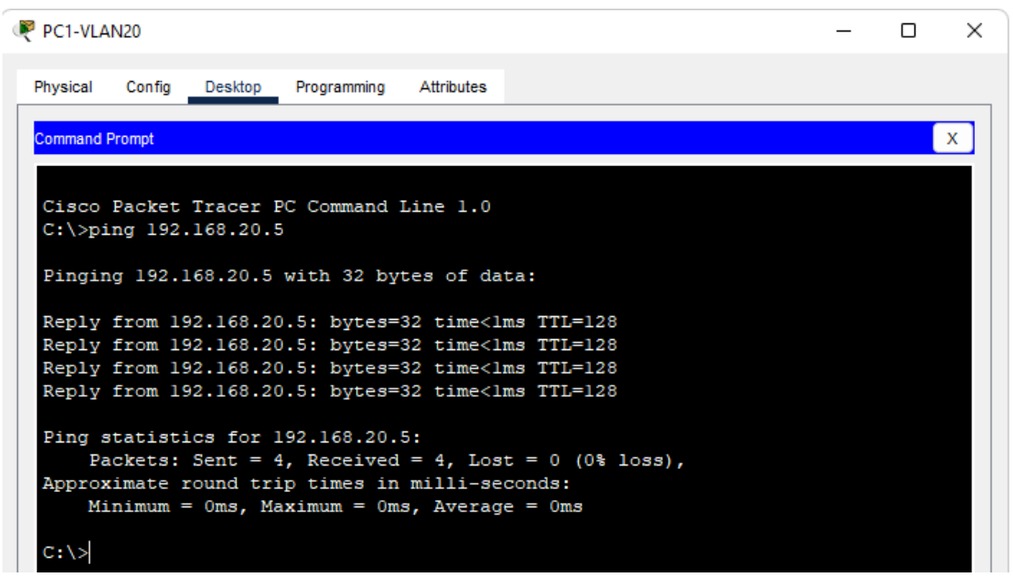
```
SW2(config)#interface Fa0/4
SW2(config-if)#switchport access vlan 30
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk native vlan 1
SW2(config-if)#interface Fa0/3
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk native vlan 1
SW2(config-if)#interface Fa0/2
SW2(config-if)#switchport access vlan 10
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk native vlan 1
SW2(config-if)#
```

Prueba de conectividad dentro de las mismas VLANs

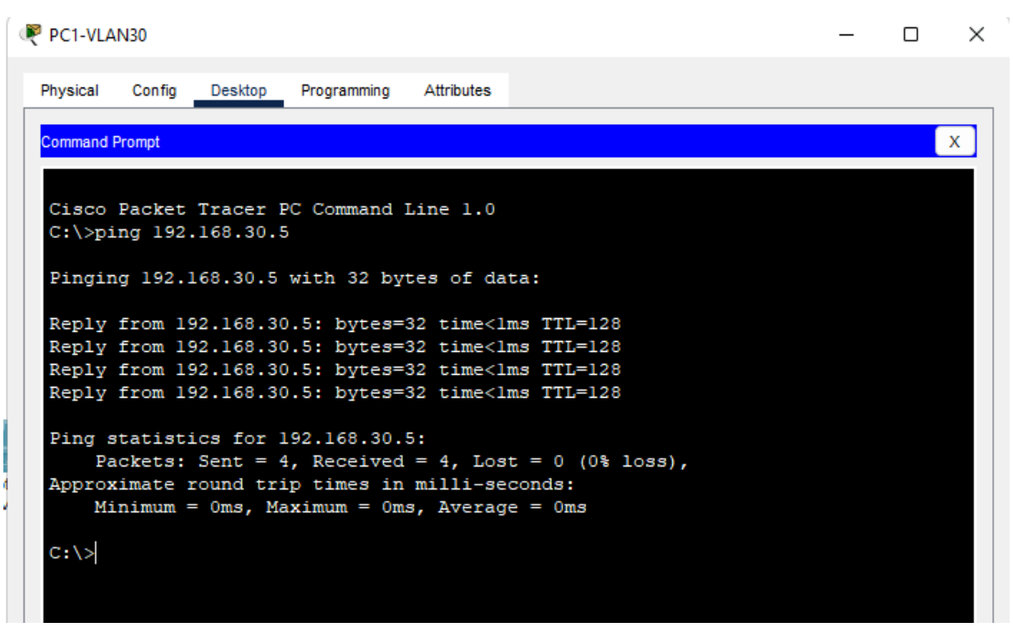
VLAN 10



VLAN 20



VLAN 30



4.3 Configuración de Router-on-stick

4.3.1 Configurar una subinterfaz para la VLAN 1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface G0/0.1
R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#ip address 192.168.0.1 255.255.255.0
R1(config-subif)#
```

4.3.2 Configurar una subinterfaz para la VLAN 10

```
R1(config)#interface G0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#exit
```

4.3.3 Configurar una subinterfaz para la VLAN 20

```
R1(config)#interface G0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#exit
```

4.3.4 Configurar una subinterfaz para la VLAN 30

```
R1(config)#interface G0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#exit
```

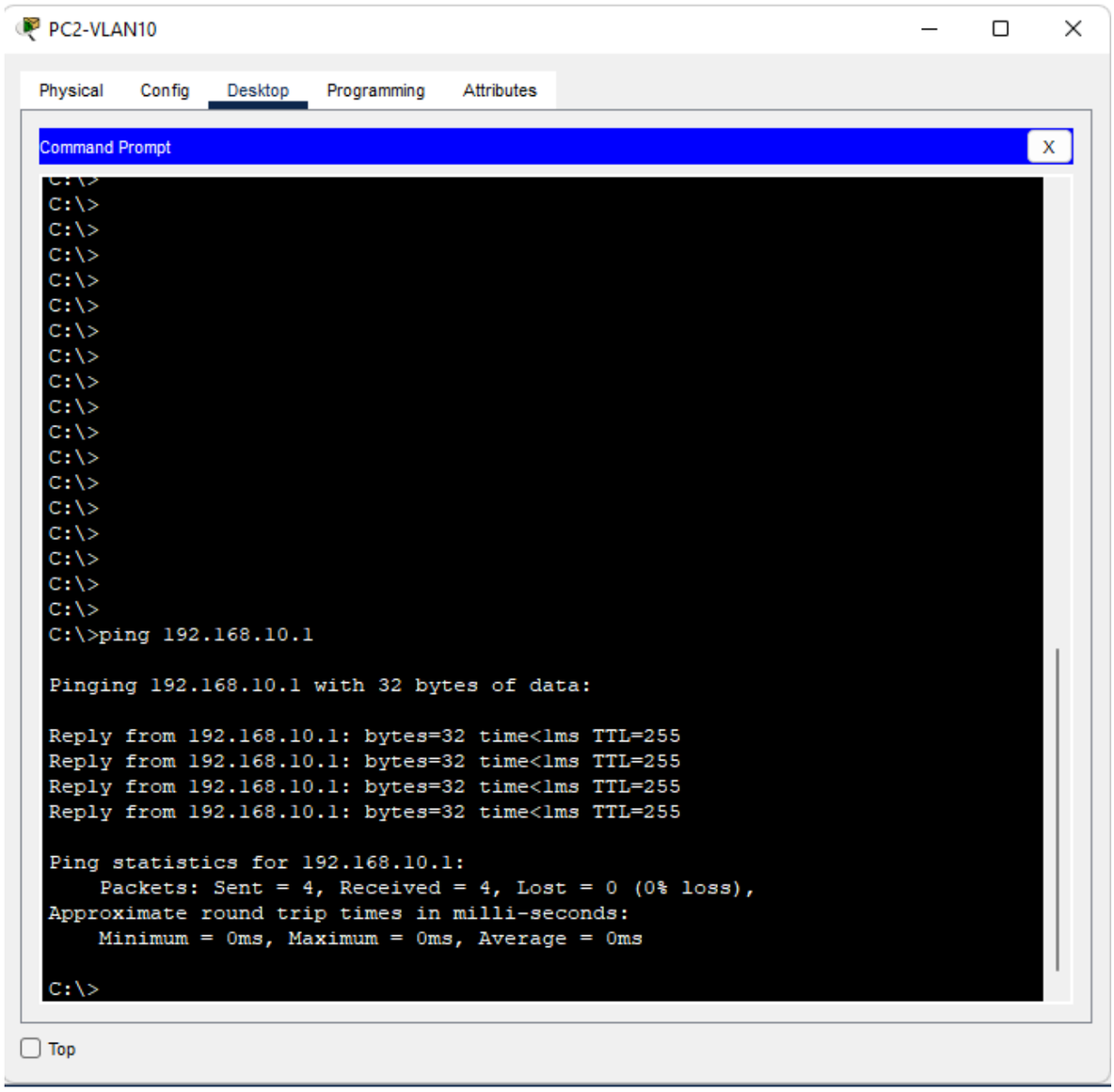
4.3.5 Habilitar la interfaz G0/0 y verificación de conectividad entre VLANs

Encendido de interfaz G0/0

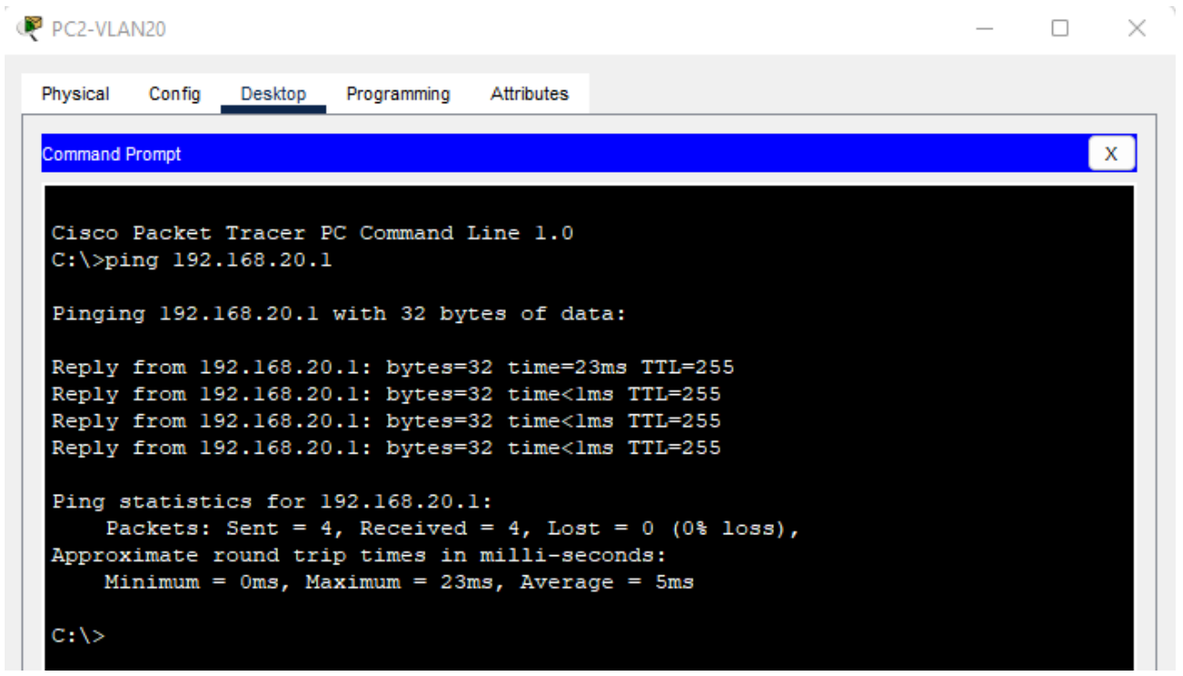
```
R1(config)#interface G0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up

R1(config-if)#
```

Verificación de conectividad entre VLAN y Gateway predeterminado

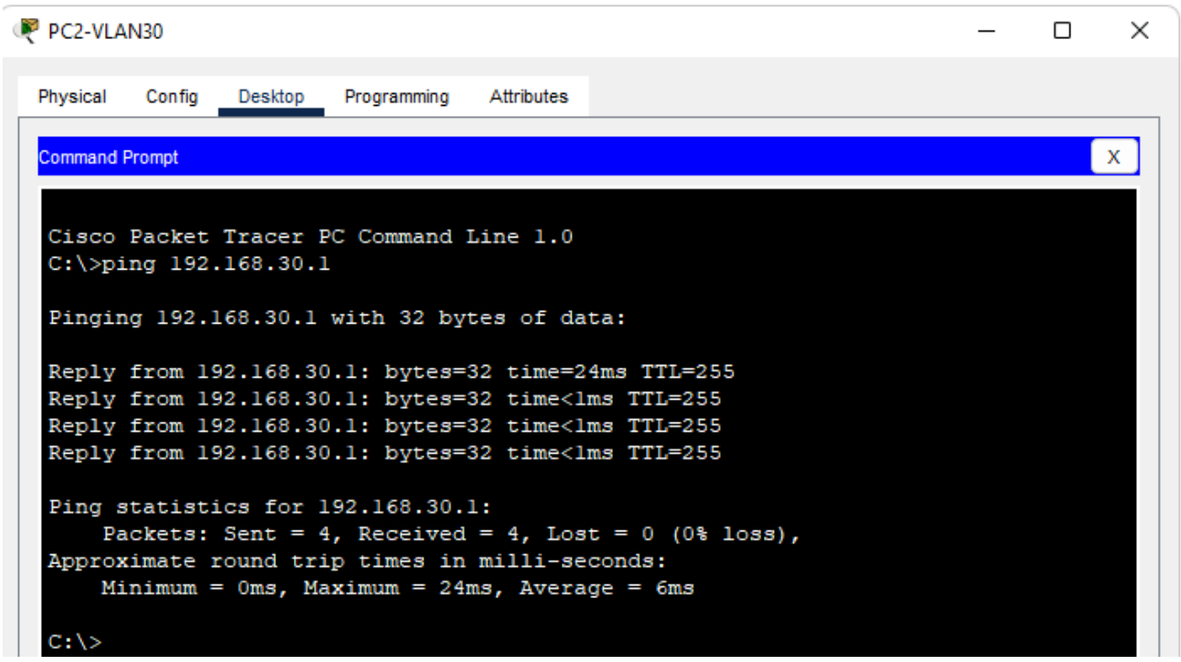
VLAN 10



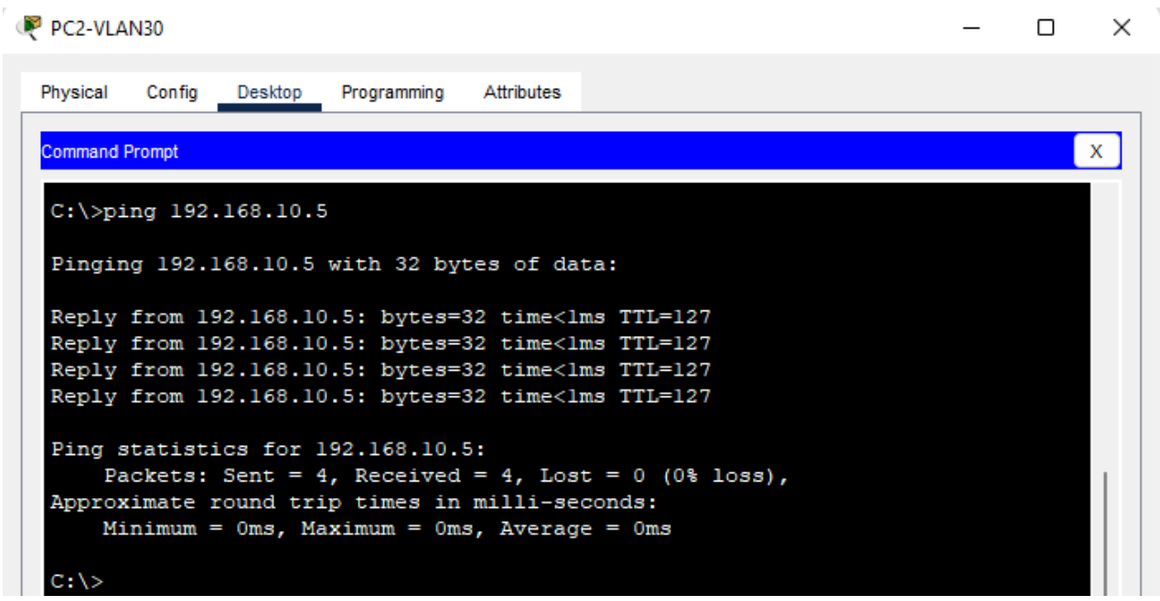
VLAN 20



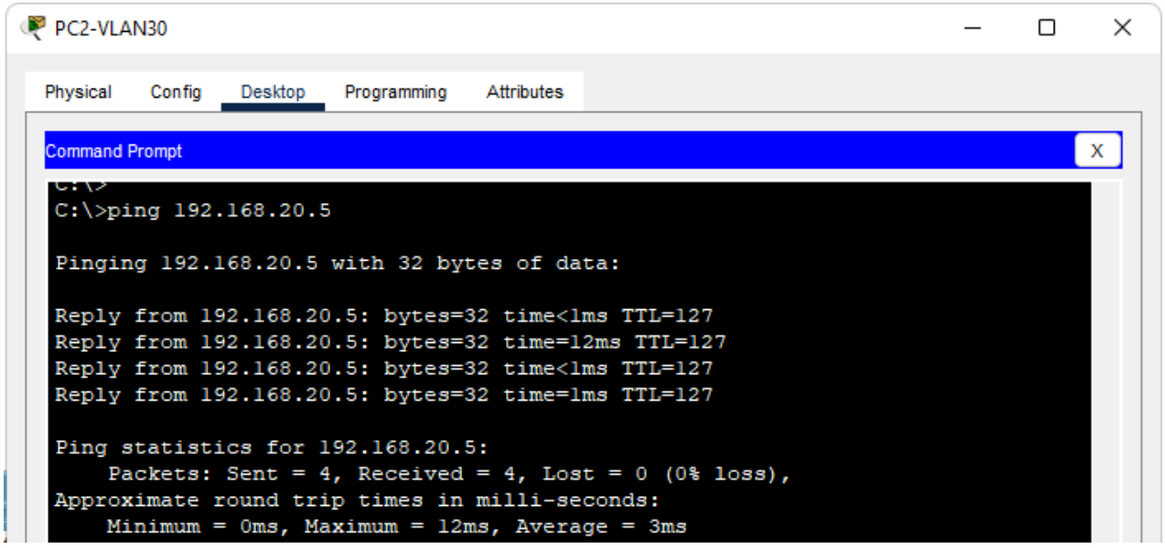
VLAN 30



VLAN 30 a VLAN 10

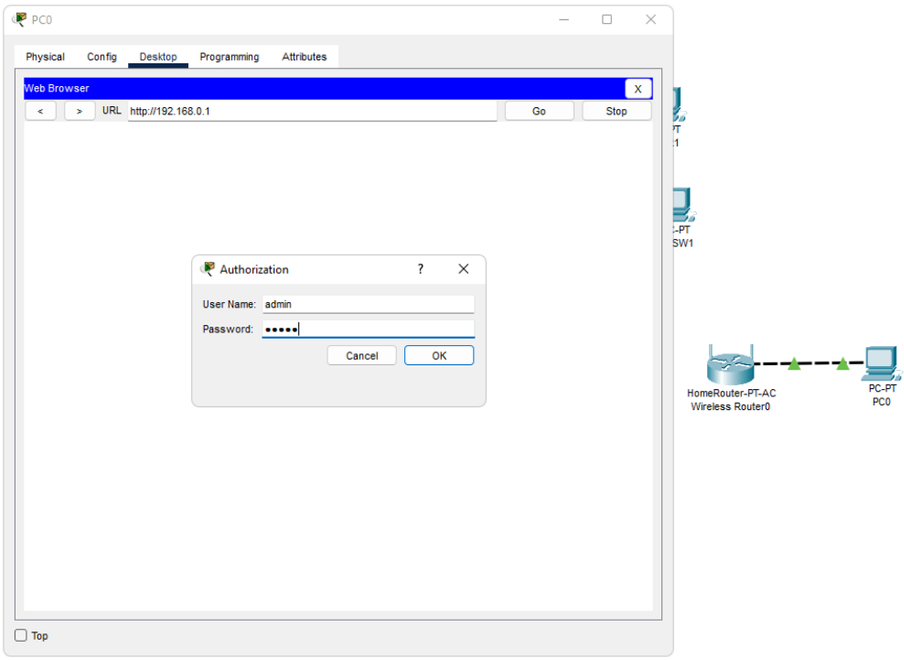


VLAN 30 a VLAN 20

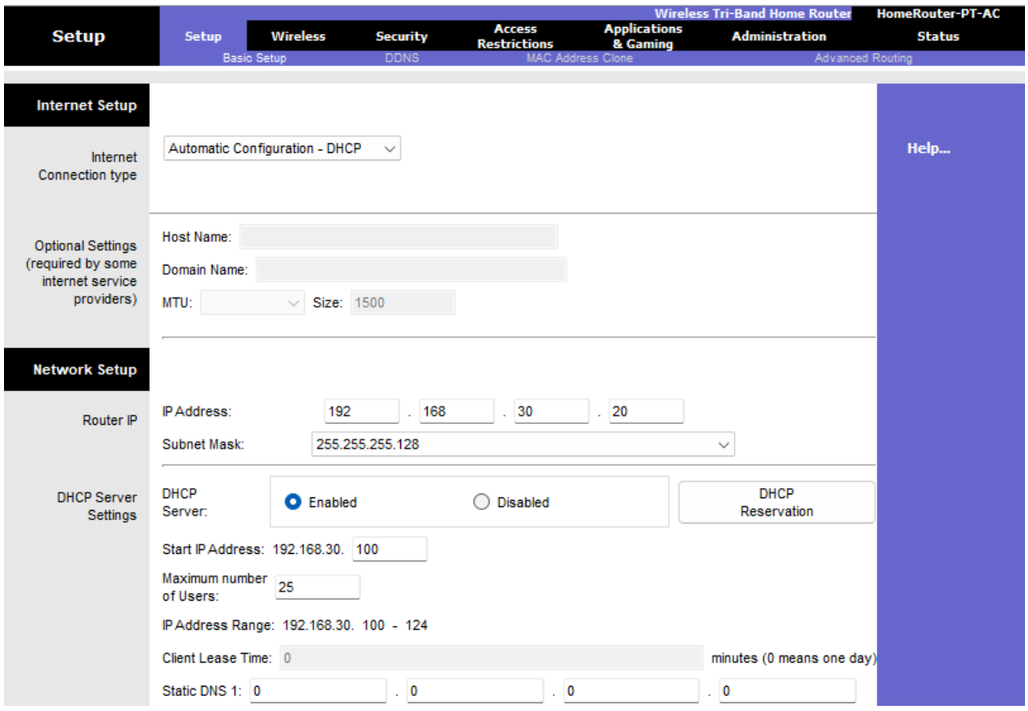


4.4 Configuración Home router

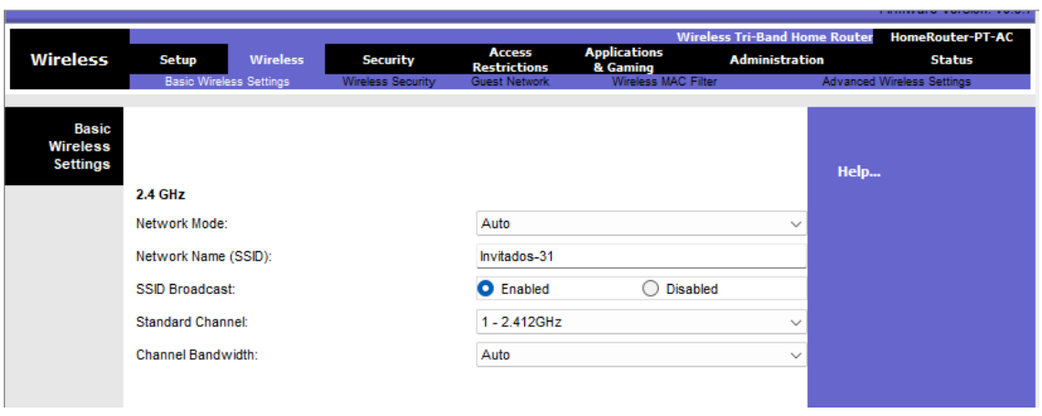
Configuración y acceso a Home Router



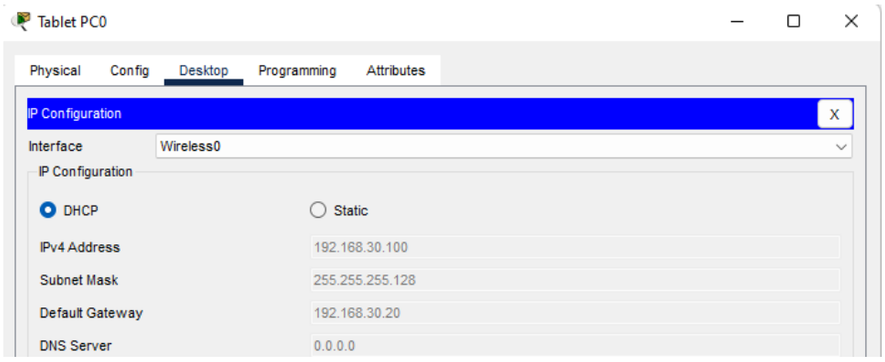
Configuración IP y DHCP



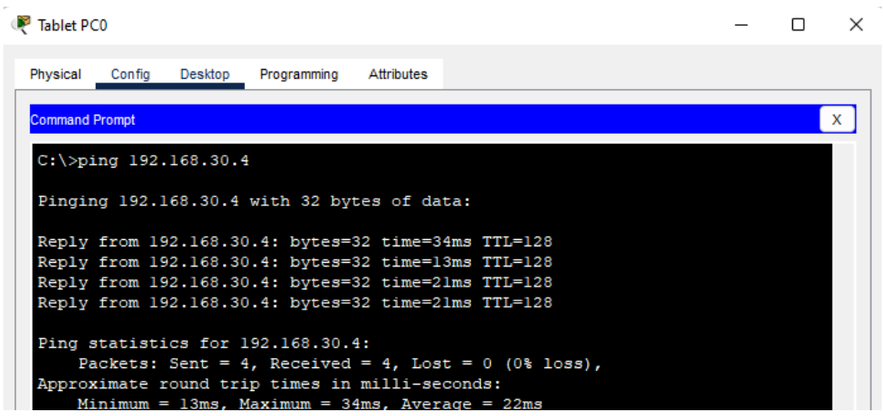
Configuración WiFi



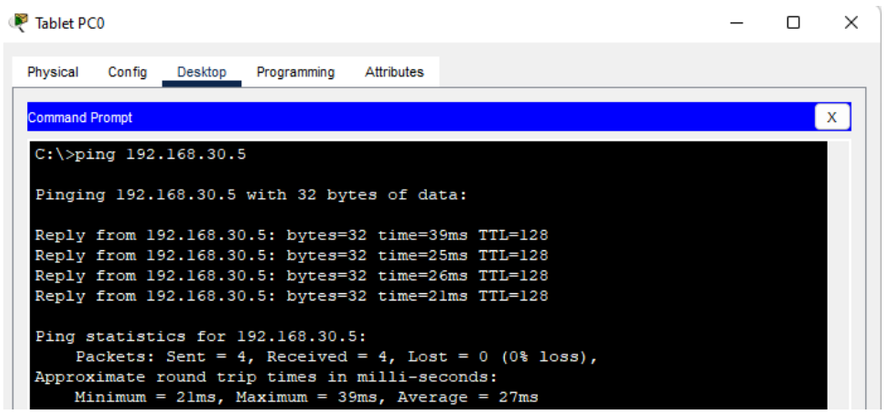
Agregando dispositivos inalámbricos y revisando su conexión por WiFi



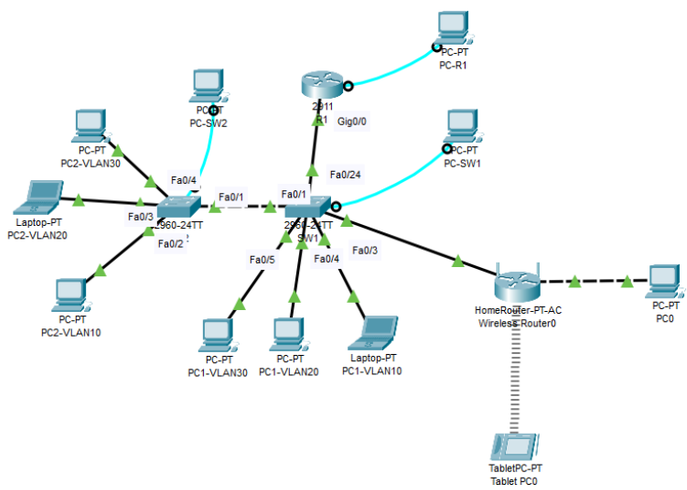
Ping de Tablet0 a PC1 VLAN30



Ping de Tablet0 a PC2 VLAN30



Topología Final



4.5 Preguntas

1. ¿Qué es VTP y cuál es su aplicación con relación a VLANs?

R// Las siglas VTP significan VLAN Trunking Protocol, el cual es un protocolo de Cisco para reducir la administración en una red de switches. Su aplicación con relación a VLANs es la de permitir que cuando se cree una nueva en un servidor VTP, la VLAN se distribuya automáticamente a través de todos los switches del dominio. De este modo, se reduce la necesidad de configurar la misma VLAN en todas partes. Suele estar disponible en la mayoría de los productos de la serie Cisco Catalyst.

2. ¿Cuántas VLANs soporta un switch? Seleccionar un fabricante, luego un par de modelos de dicho fabricante y mostrar un recorte del datasheet del equipo en donde se encuentre dicha información.

R// El Cisco Catalyst 2960-S soporta un máximo de 64 VLANs, tal como se evidencia en la siguiente datasheet del equipo:

Table 3. Hardware Features for Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software

Performance and Scalability Numbers for All Switch Models	
Forwarding bandwidth	16 Gbps (2960), 50 Gbps (2960-S)
Flash memory	32 MB (2960), 64 MB (2960-S)
Memory DRAM	64 MB (2960), 128 MB (2960-S)
Max VLANs	64
VLAN IDs	4000
Maximum transmission unit (MTU)	Up to 9198 bytes
Jumbo frames	9016 bytes (2960), 9216 bytes (2960-S)
Forwarding Rate	
2960S-48TS-S	74.4 mpps
2960S-24TS-S	38.7 mpps
2960-8TC-S	2.7 mpps
2960-24-S	3.6 mpps
2960-24TC-S	6.5 mpps
2960-24PC-S	6.5 mpps
2960-24LC-S	6.5 mpps
2960-48TT-S	10.1 mpps
2960-48TC-S	10.1 mpps
2960-48PST-S	13.3 mpps

Por otro lado, los Cisco Catalyst 3560-CX y 2960-CK soportan un máximo de 1023 VLANs como se evidencia en la siguiente datasheet:

Product Specifications

Table 5 provides hardware specifications for the Cisco Catalyst 3560-CX and 2960-CX compact switches.

Table 5. Cisco Catalyst 3560-CX and 2960-CX Series Compact Switch Hardware

Description	Specification		
Performance		**Cisco Catalyst 3560-CX**	**Cisco Catalyst 2960-CX**
	Forwarding Bandwidth	46 Gbps (with C3560CX-8XPD-S) 34 Gbps (with C3560CX-12PD-S) 16 Gbps (with 1 G uplinks)	12 Gbps
	Switching Bandwidth (full-duplex capacity)	92 Gbps (with C3560CX-8XPD-S) 68 Gbps (with C3560CX-12PD-S) 32 Gbps (with 1 G uplinks)	24 Gbps
	Flash memory	128 MB	128 MB
	Memory DRAM	512 MB	512 MB
	Max VLANs	1023	255
	VLAN IDs	4000	4000

Por último, los Cisco Catalyst 4500-X soportan un máximo de 4094 VLANs como se evidencia en la siguiente datasheet:

Table 1. Cisco Catalyst 4500-X Switch Series Performance and Scalability Features

Product Number	Description
System	
Base System	Front to Back Airflow: • 32x10 GE SFP+/SFP - WS-C4500X-32SFP+ • 16x10 GE SFP+/SFP - WS-C4500X-16SFP+ Back to Front Airflow: • 32x10 GE SFP+/SFP - WS-C4500X-F-32SFP+ • 16x10 GE SFP+/SFP - WS-C4500X-F-16SFP+
Expansion Module (Optional)	8x10 GE SFP+/SFP - C4KX-NM-8SFP+
Management Port	10/100/1000 Base-T
USB Port	Type A (storage and boot) up-to 4 GB
Dual Power Supply	Yes
Field Replaceable Fans	Yes (5 fans)
Fan Redundancy	No performance impact with single fan failure
Scalability	
System Throughput	Up to 800 Gbps
IPv4 Routing in Hardware	Up to 250 Mpps

Product Number	Description
IPv6 Routing in Hardware	Up to 125 Mpps
L2 Bridging in Hardware	Up to 250 Mpps
Media Access Control (MAC) Entries	55K
Forwarding Entries	32x10 GE Port Base SKU: IPv4: 256K, IPv6: 128K 16x10 GE Port Base SKU: IPv4: 64K, IPv6: 32K
Flexible Netflow Entries	128K
Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN)	8 line rate bidirectional sessions (ingress and egress)
Total VLANs	4094

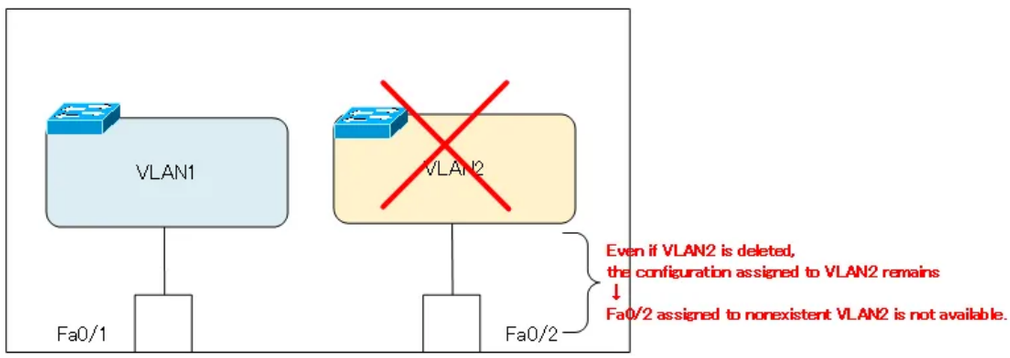
Nota: En los switches Catalyst la cantidad máxima de VLAN disponibles es de 4096, ya que le campo de ID de VLAN tiene 12 bits en el encabezado.

3. ¿Le recomendaría el uso de VLANs a un administrador inexperto de una red de un campus universitario? ¿En qué se basa para brindar la recomendación? Explique.

R// Sí recomendaríamos el uso de VLANs, esto se debe a que ellas permiten segmentar una red muy grande, como la de un campus universitario en fragmentos más pequeños que son más fáciles de manejar. Adicionalmente, al crear diferentes VLANs el tráfico pasa de estar en una sola red compartida a estar distribuido entre cada subred. Un ejemplo de esto es que se puede separar el tráfico de dispositivos invitados de las demás secciones de la red, esto permite a dichos dispositivos el acceso a internet sin tener que disminuir el ancho de banda del resto de dispositivos del campus. No obstante, esto también trae otros beneficios para la empresa que vaya a utilizar VLANs, como por ejemplo seguridad (se previene el acceso a ciertas partes de la red a dispositivos no autorizados), costos (se reduce la necesidad de realizar mejoras dentro de la red, pues las VLANs usan el ancho de banda y sus terminales de una manera más eficiente) y flexibilidad. Además, su configuración no es muy compleja dependiendo del fabricante de los dispositivos de red del campus.

4. ¿Qué ocurre con un puerto asociado a la VLAN 20 cuando el administrador de la red elimina la VLAN 20 del switch?

R// Cuando se elimina una VLAN y hay un puerto asociado a este, prácticamente sucede que dicho puerto queda no disponible. Esto sucede pues el puerto está asignado exclusivamente a una sola VLAN. Si la VLAN es eliminada, entonces estará asignado a una VLAN que no existe y por tanto será inutilizable. Esto se puede ver en la siguiente imagen:



5. ¿Cómo se puede manejar seguridad en una red inalámbrica? Explique.

R// Una red inalámbrica se puede proteger mediante varias prácticas como las siguientes:

- Evitar utilizar la contraseña predeterminada, ya que los atacantes suelen probar el acceso de acuerdo al fabricante del router para obtener acceso y ejercer fines dañinos.

- Desactivar que los dispositivos inalámbricos indiquen su presencia, al inutilizar la difusión del identificador de red SSID para evitar que se anuncie de su presencia al mundo que lo rodea y dificultar aún más la identificación de un objetivo de ataque.
- Cambiar el nombre SSID del dispositivo, ya que si se deja el nombre por defecto facilita la localización de la red para un atacante.
- En la configuración de conexión se debe asegurar de activar el cifrado, preferiblemente WPA si está disponible, de lo contrario con cifrado WEP.
- Utilizar filtrado MAC, para bloquear dispositivos indeseados.

6. ¿Qué es un filtrado MAC en una red inalámbrica? ¿En qué casos sería útil?

R// Un filtrado MAC en una red inalámbrica es un mecanismo de protección por el cuál configuramos exactamente qué dispositivos se conectarán a nuestra red, evitando que terceros lo hagan sin nuestra autorización y mejorando la seguridad de la red. Todo esto es puede actuar mediante listas blancas y negras de los dispositivos a partir de su dirección MAC. Es útil para evitar que extraños se conecten a nuestra red o incluso tras de que hayan obtenido sistemáticamente el acceso con la intención de generar ataques informáticos a los dispositivos de la red.

Listado de referencias

- https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf
- https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd806b0bd8.html
- https://internetfuture.net/pdf/cisco/Cisco-Catalyst-4500-X-Series-Fixed-10-Gigabit-Ethernet-Aggregation-Switch-Data-Sheet.pdf
- https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.2.1.1/3.2.1.1.html#:~:text=Nota%3A%20la%20cantidad%20m%C3%A1xima%20de,el%20encabezado%20IEEE%20802.1Q
- https://internetfuture.net/pdf/cisco/Cisco-Catalyst-3560-CX-and-2960-CX-Series-Compact-Switches-Data-Sheet.pdf
- https://www.bloglenovo.es/filtrado-mac-convertir-wifi-seguro/
- https://www.muycomputer.com/2017/11/26/filtrado-mac-debes-utilizarlo/
- https://www.kaspersky.es/resource-center/preemptive-safety/protecting-wireless-networks
- https://www.n-study.com/en/vlan-detail/notes-on-deleting-vlans/
- https://www.linkedin.com/pulse/importance-using-vlans-segment-network-traffic-mike