PRUEBA DE HABILIDADES PRÁCTICAS

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRESENTADO POR:

MABIL JULIETH MARTÍNEZ

Tutor:

Giovanni Alberto Bracho

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

SANTA MARTA

2018

Tabla de contenido

INTRODUCCIÓN

En este documento se expone los resultados de construir una solución de red, que permite la comunicación en internet de los hosts conectados a una red de comunicación entre 3 ciudades, usando el concepto de VLANs, servidores DHCP, entre otros.

OBJETIVOS

Objetivo general

Construir una solución de red para la comunicación en internet de los hosts ubicados en 3 ciudades capitales de Colombia

Objetivos específicos

1. Configurar un servidor DHCP
2. Configurar los parámetros de seguridad
3. Bloquear el acceso por telnet
4. Configurar un usuario y contraseña para cada router

DESARROLLO DE LA ACTIVIDAD

Evaluación –Prueba de habilidades prácticas CCNA

Descripción general de la prueba de habilidades

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

La prueba de habilidades podrá ser desarrollada en el **Laboratorio SmartLab** o mediante el uso de **herramientas de Simulación (Puede ser Packet Tracer o GNS3)**. El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario. No obstante, es importante mencionar que **aquellos estudiantes que hagan uso del laboratorio SmartLab se les considerarán un estímulo adicional a la hora de evaluar el informe, teniendo en cuenta que su trabajo fue realizado sobre equipos reales y con ello será la oportunidad poner a prueba las habilidades y competencias adquiridas durante el diplomado.** Adicionalmente, es importante considerar, que esta actividad puede ser realizada en varias sesiones sobre este entorno, teniendo en cuenta que disponen de casi 15 días para su desarrollo.

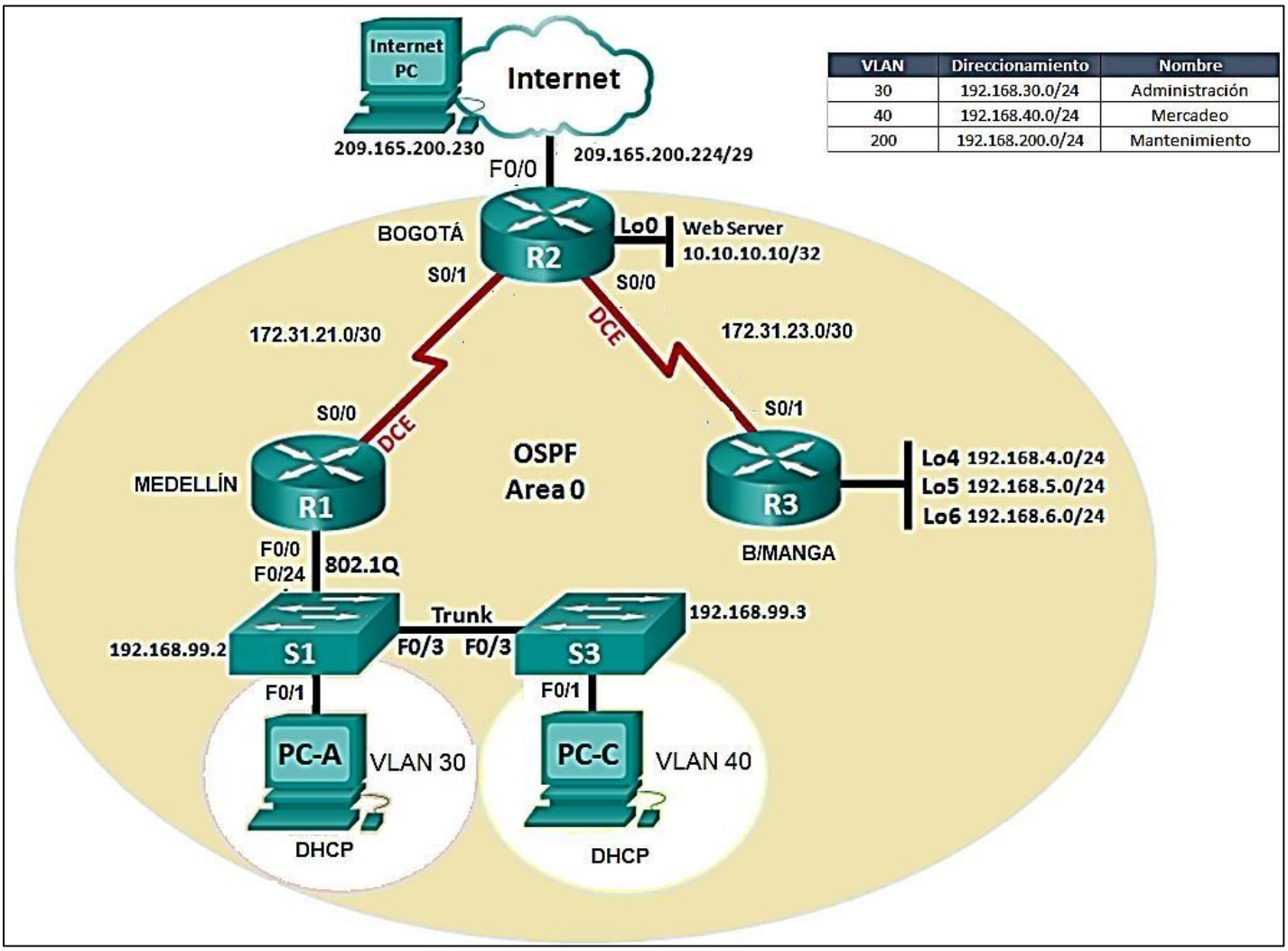
Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado al finalizar el curso.

Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos, las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD**.

Descripción del escenario propuesto para la prueba de habilidades

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología de red



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
4. En el Switch 3 deshabilitar DNS lookup
5. Asignar direcciones IP a los Switches acorde a los lineamientos.
6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com

	Establecer default gateway.

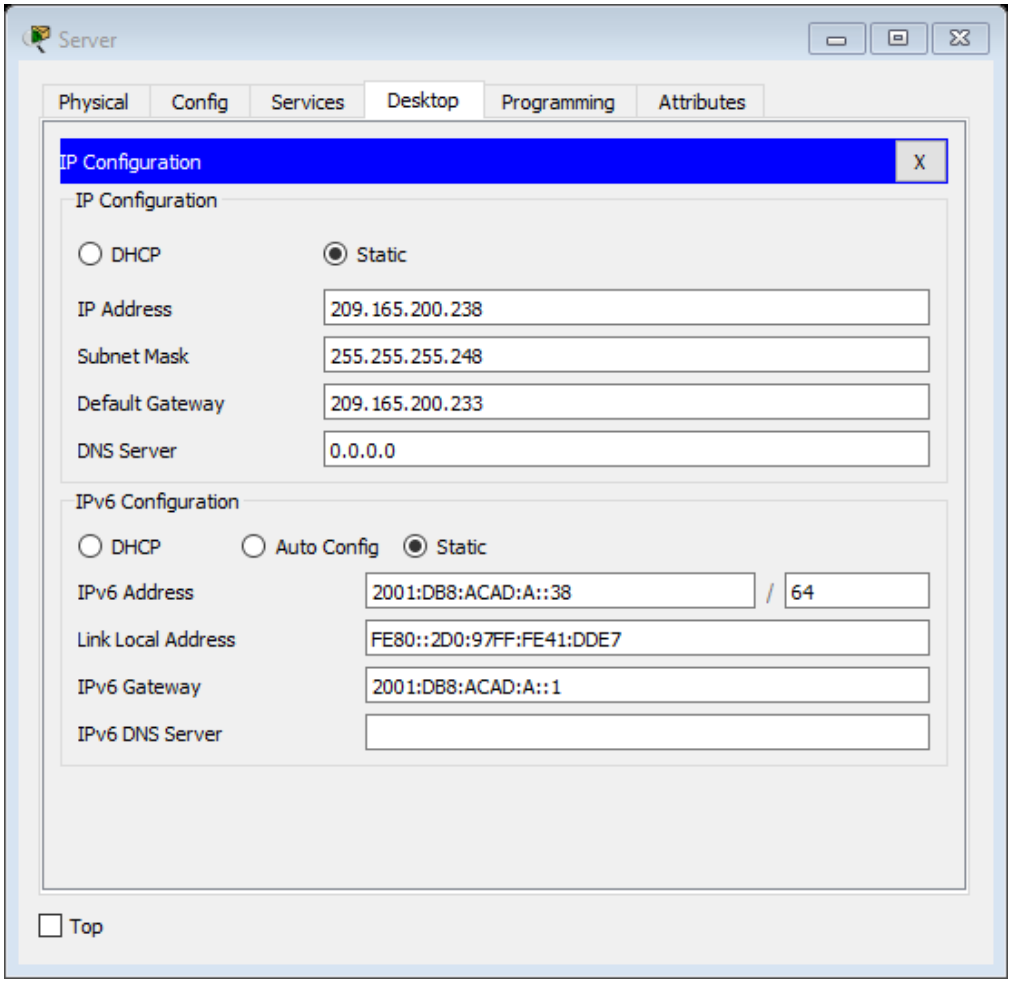
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

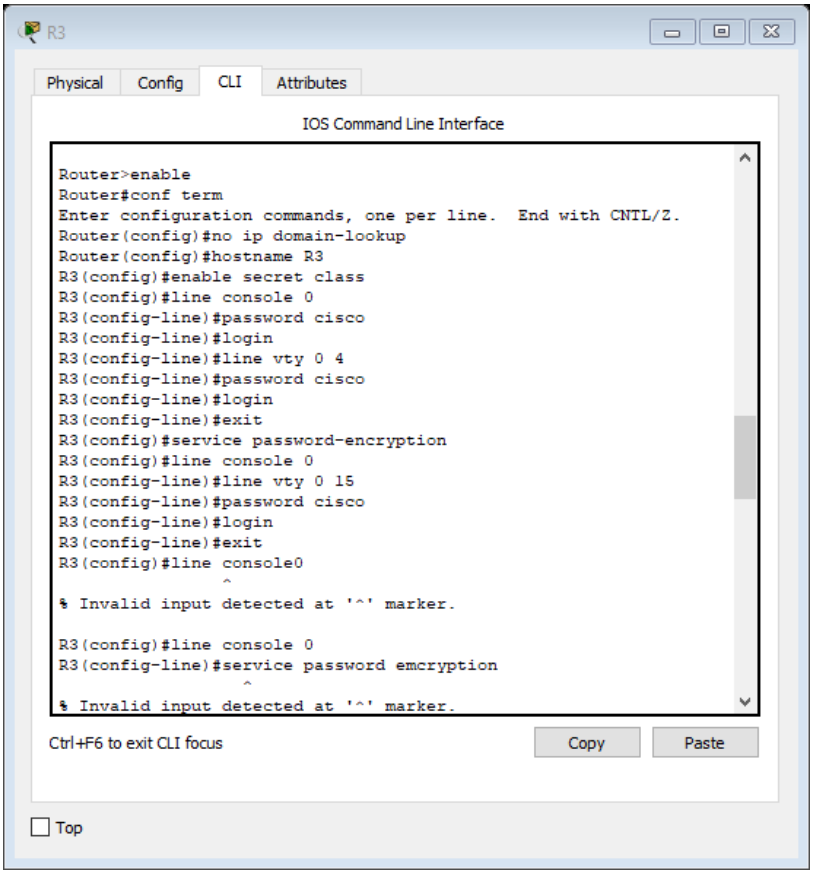
10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet

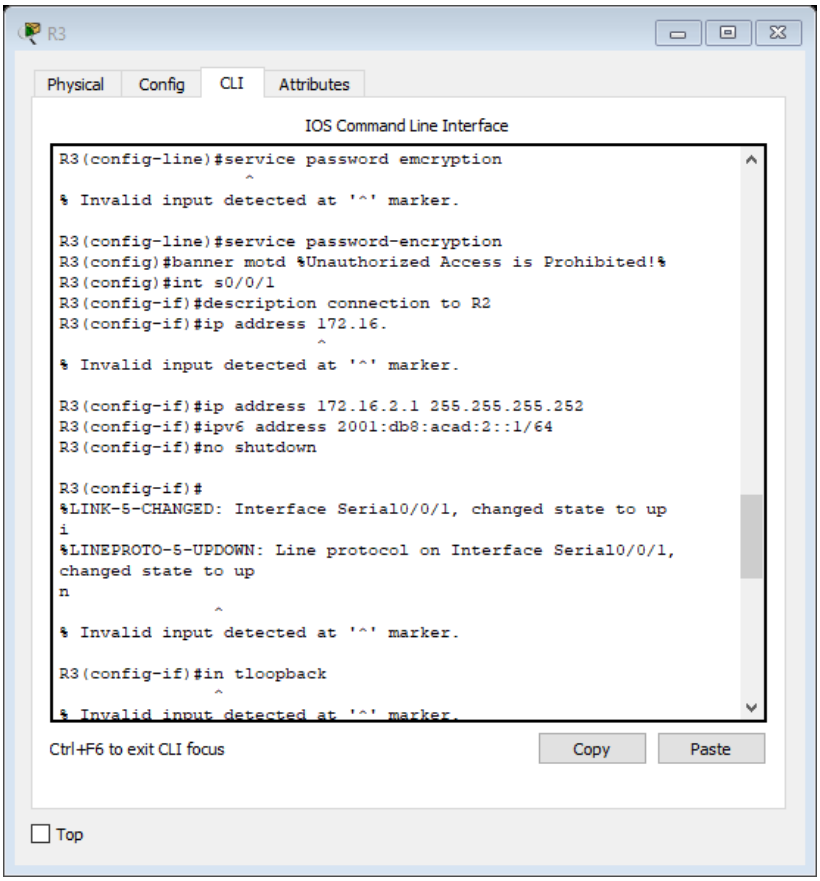
11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

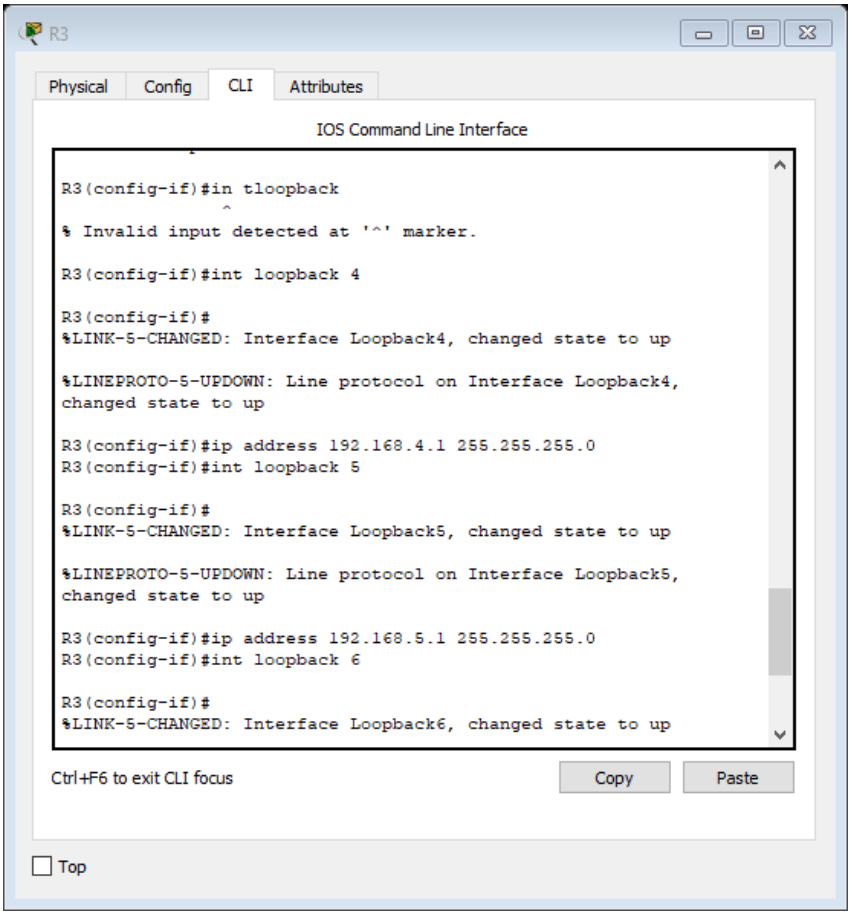
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

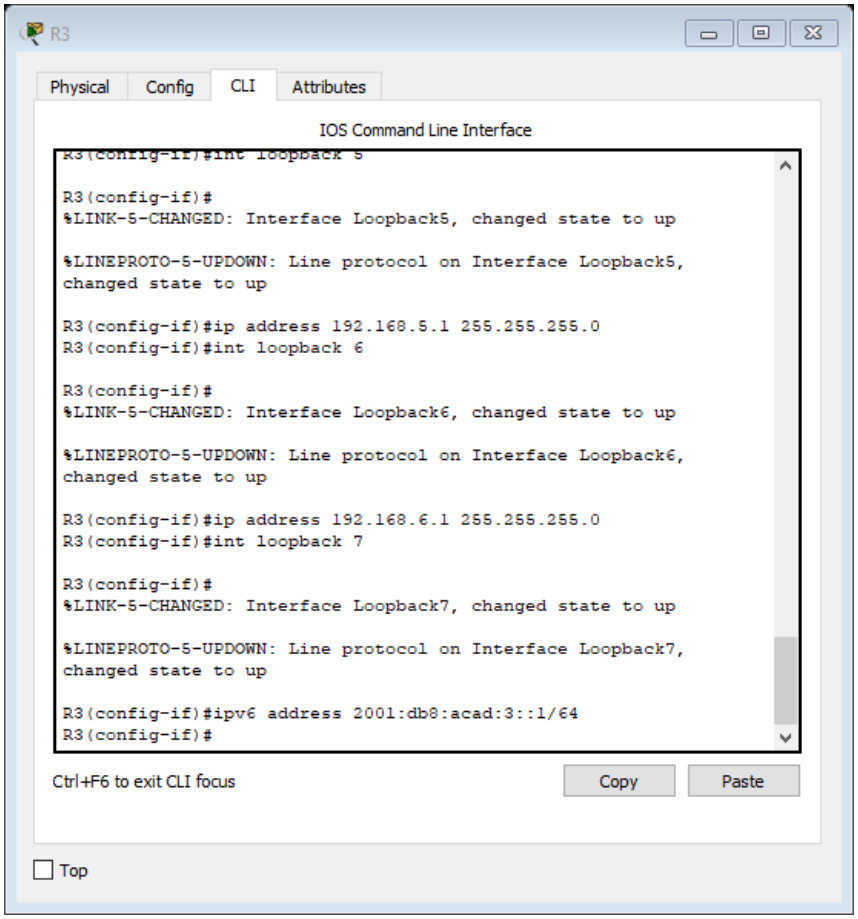
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

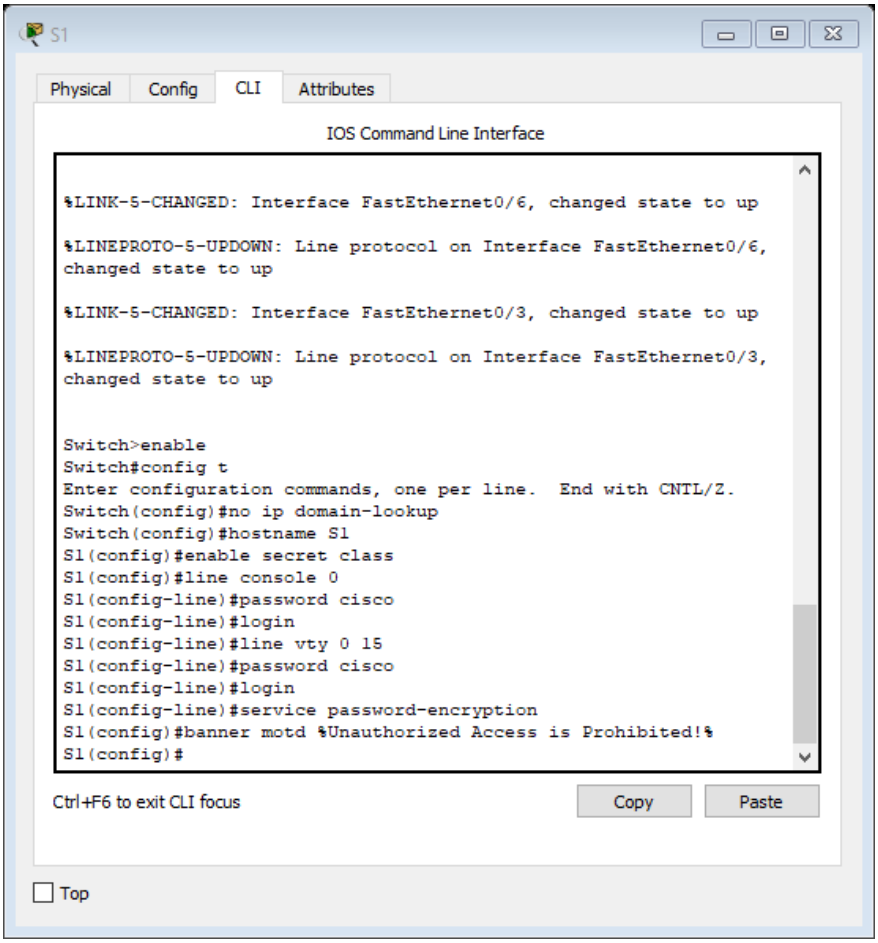


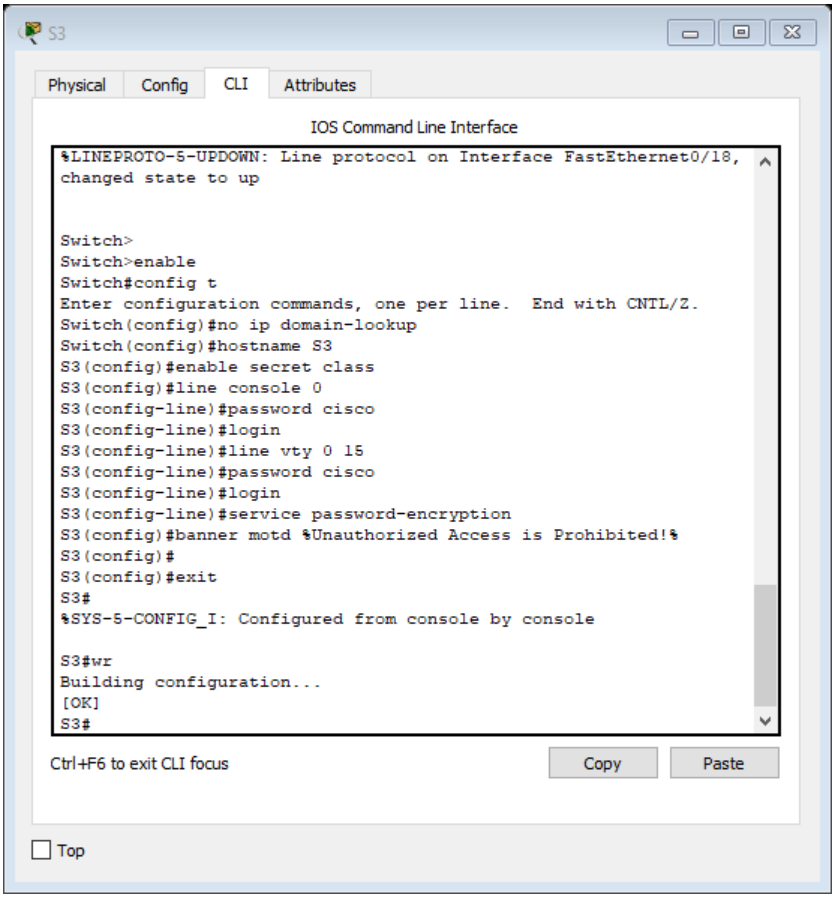

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#line console 0
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line console0
                 ^
% Invalid input detected at '^' marker.
R3(config)#line console 0
R3(config-line)#service password emcryption
                       ^
% Invalid input detected at '^' marker.
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3(config-line)#service password emcryption
                       ^
% Invalid input detected at '^' marker.
R3(config-line)#service password-encryption
R3(config)#banner motd %Unauthorized Access is Prohibited!%
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.
                          ^
% Invalid input detected at '^' marker.
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
i
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
n
                ^
% Invalid input detected at '^' marker.
R3(config-if)#in tloopback
                ^
% Invalid input detected at '^' marker.
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

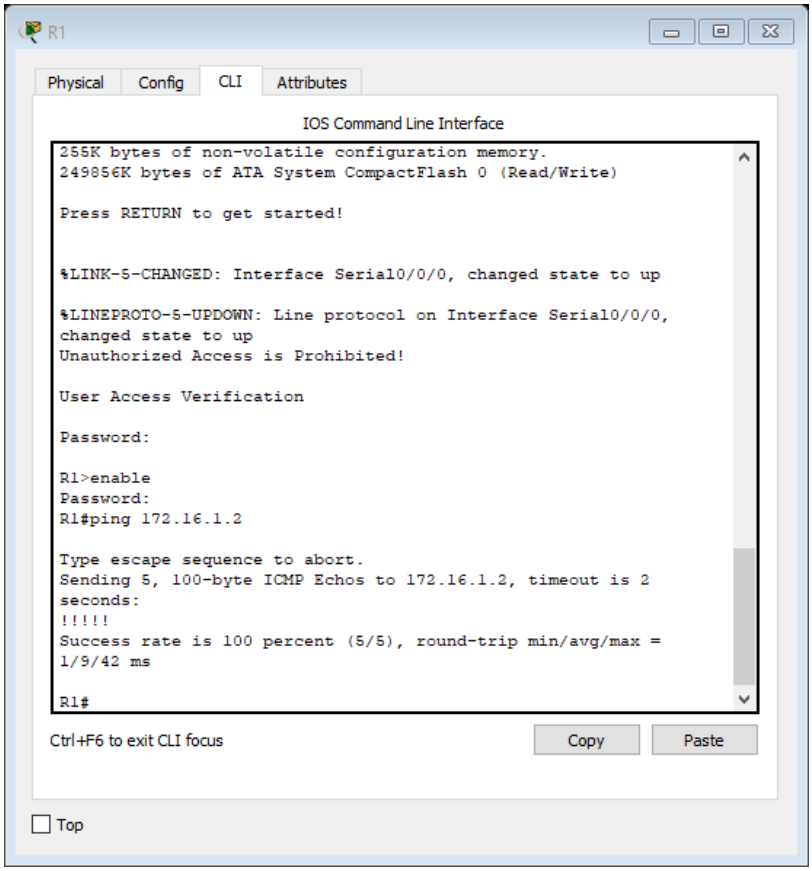

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3(config-if)#in tloopback
^
% Invalid input detected at '^' marker.
R3(config-if)#int loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4,
changed state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

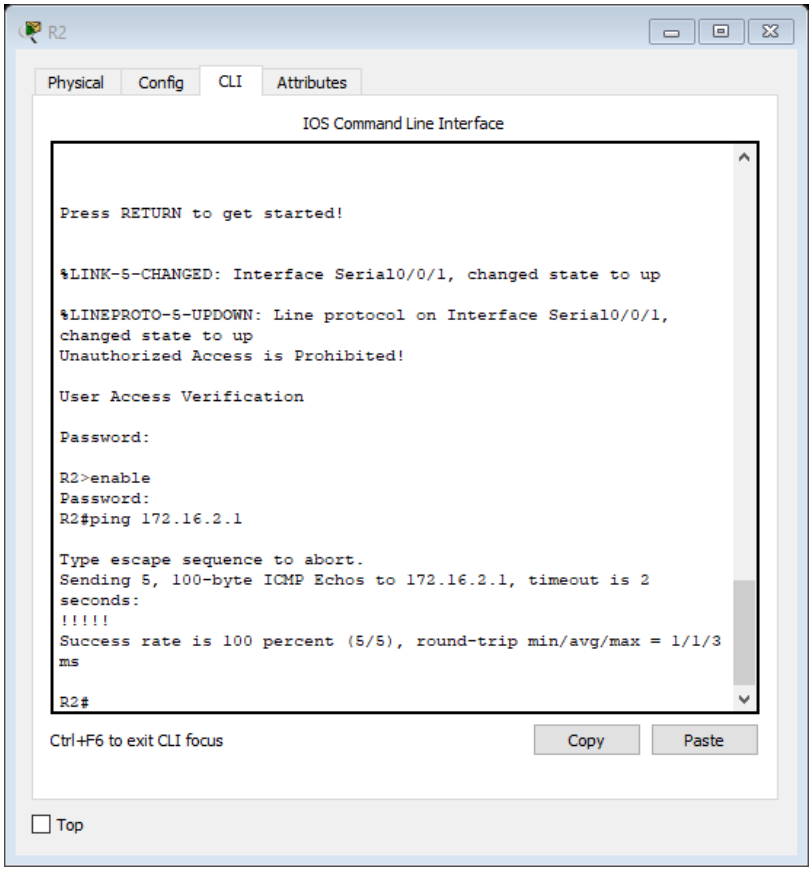

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6,
changed state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7,
changed state to up
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

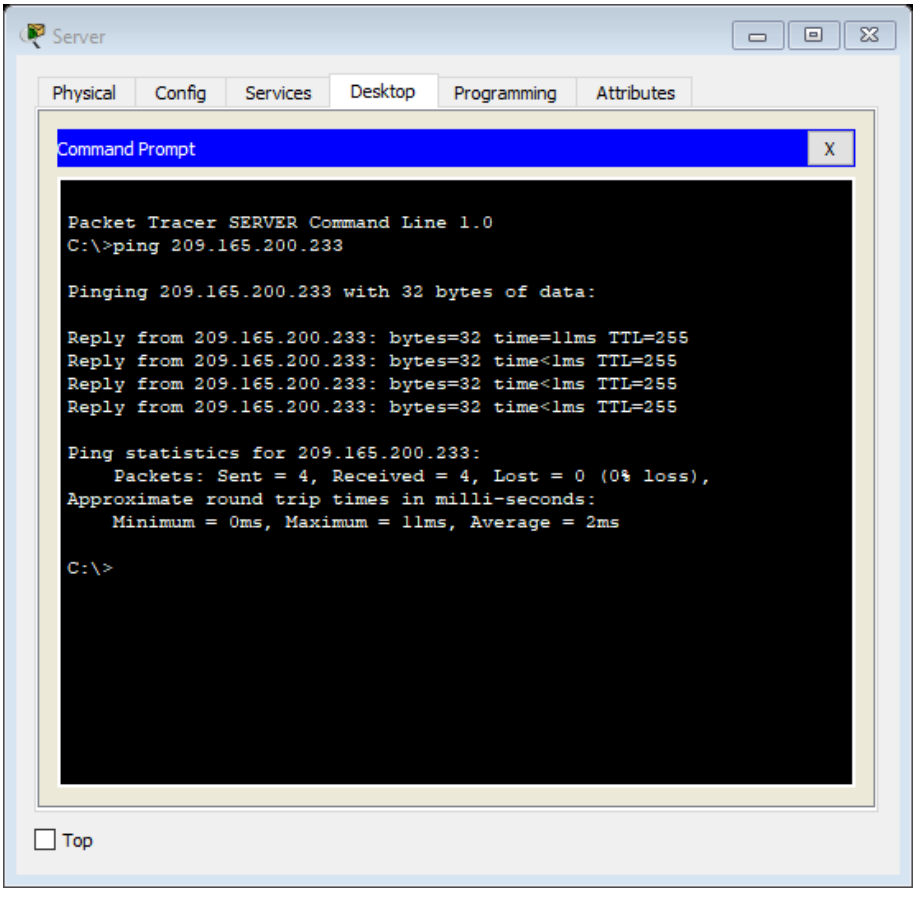

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Unauthorized Access is Prohibited!%
S1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

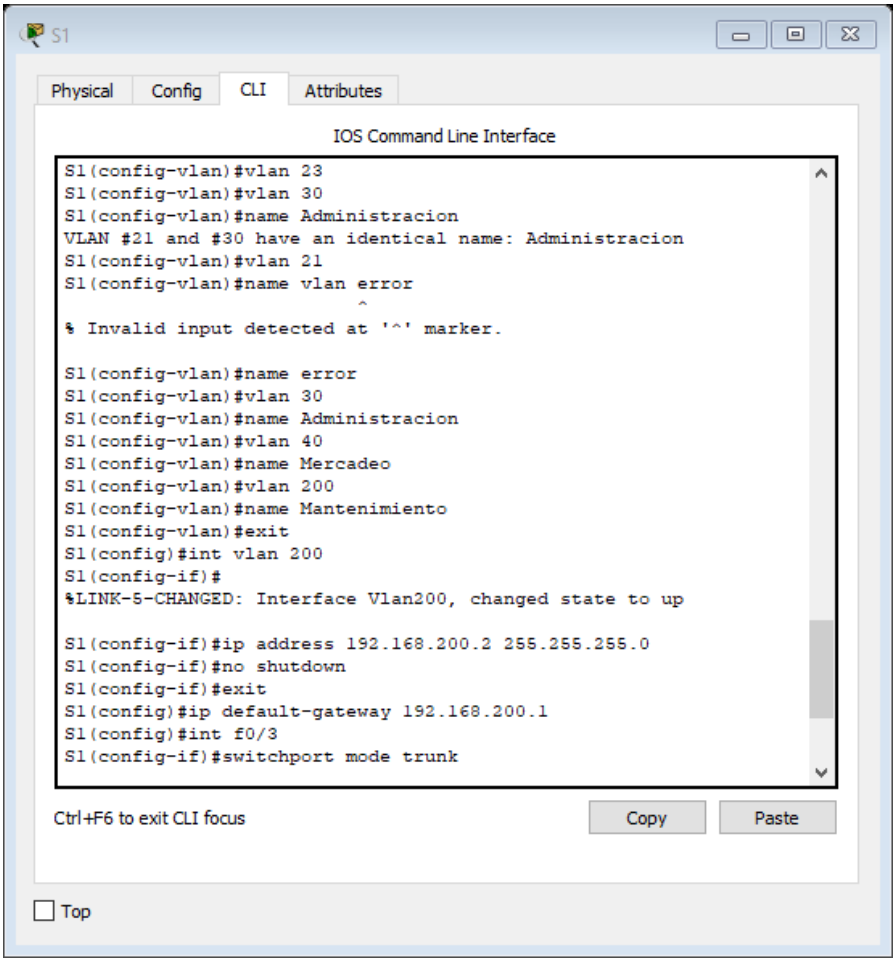

S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd %Unauthorized Access is Prohibited!%
S3(config)#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#wr
Building configuration...
[OK]
S3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

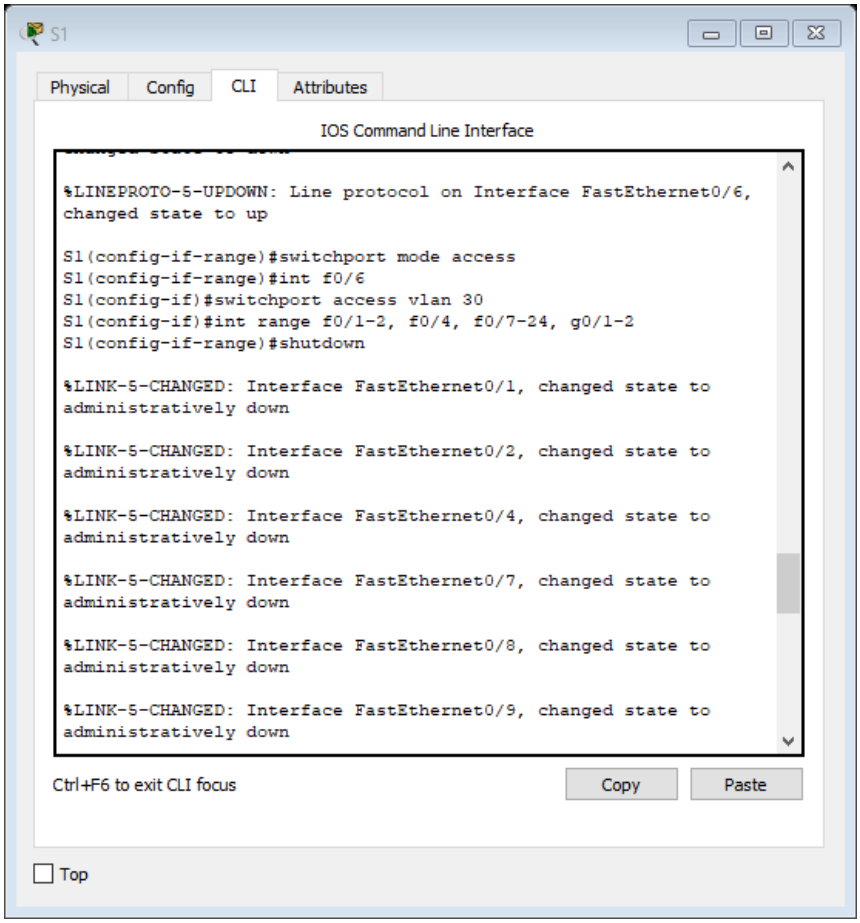
RESULTADOS

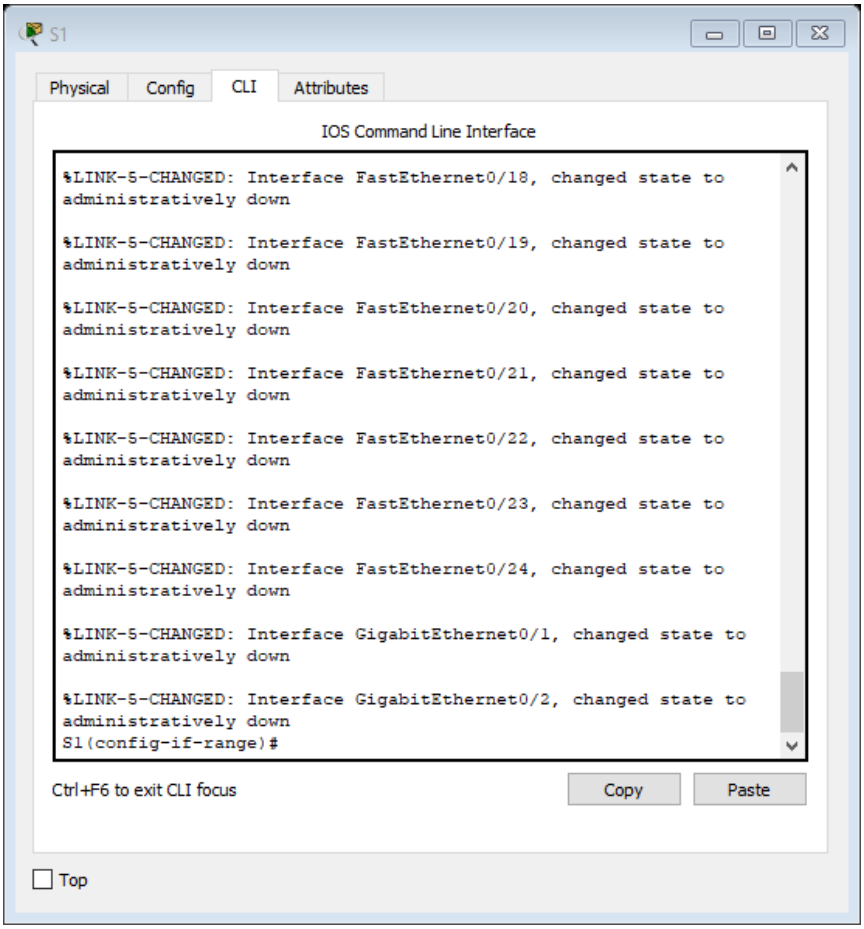

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
Unauthorized Access is Prohibited!
User Access Verification
Password:
R1>enable
Password:
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/9/42 ms
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

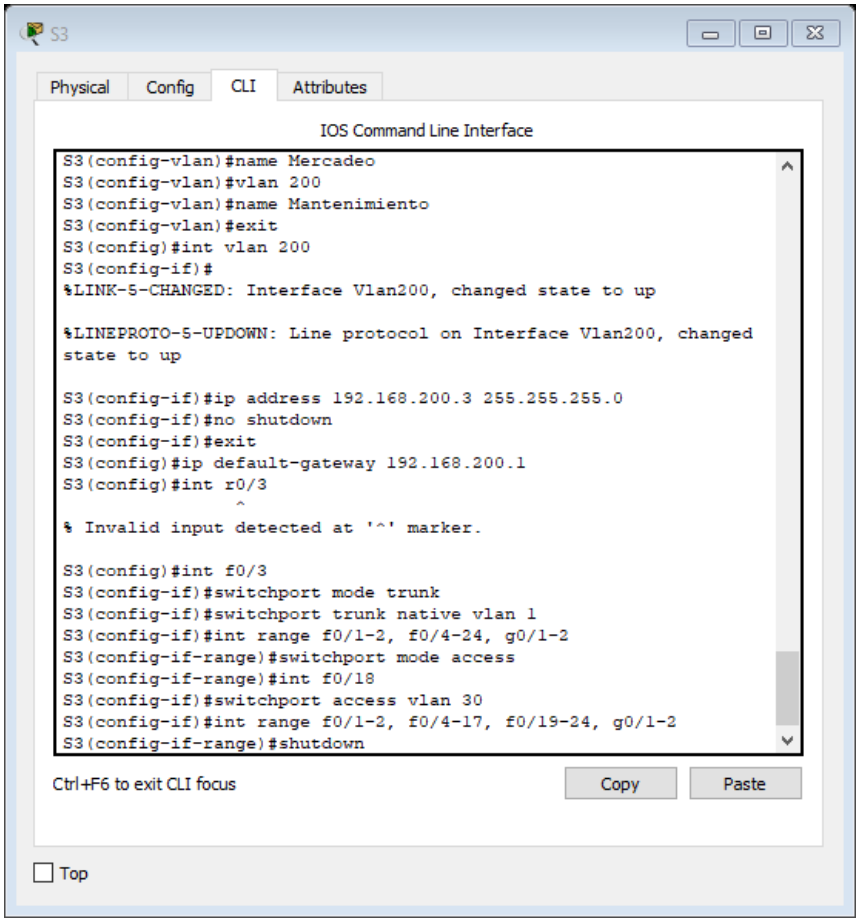

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Unauthorized Access is Prohibited!
User Access Verification
Password:
R2>enable
Password:
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
R2#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

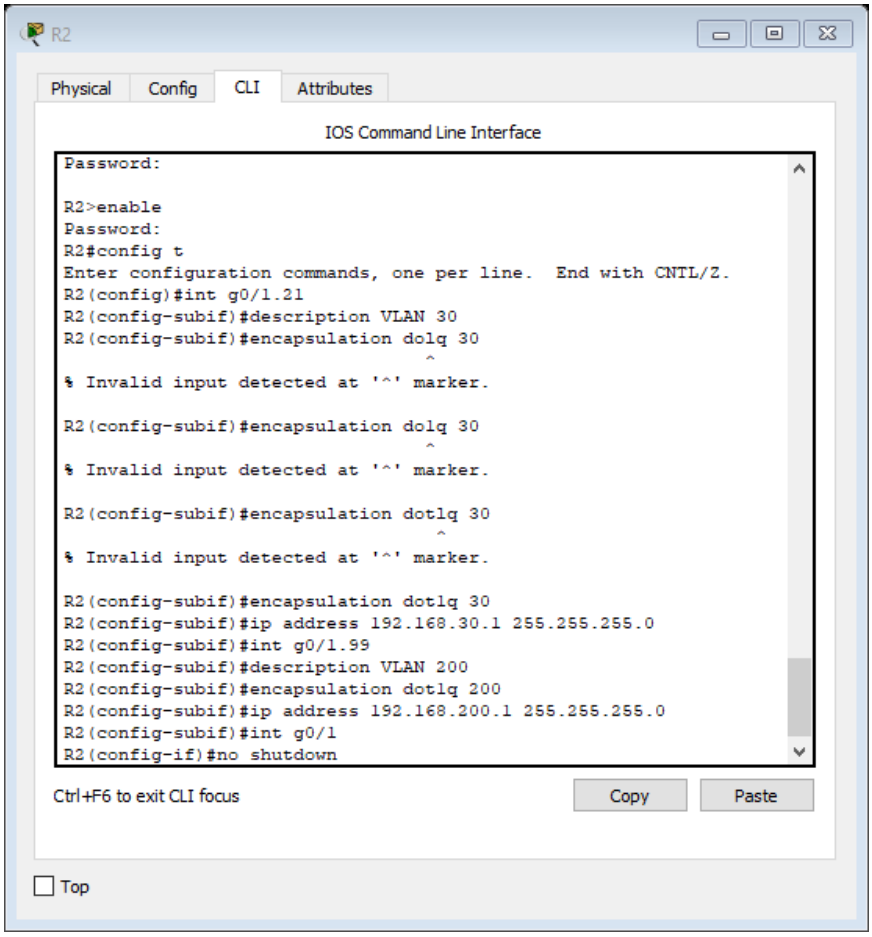

Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233
Pinging 209.165.200.233 with 32 bytes of data:
Reply from 209.165.200.233: bytes=32 time=11ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Ping statistics for 209.165.200.233:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 2ms
C:\>
Top

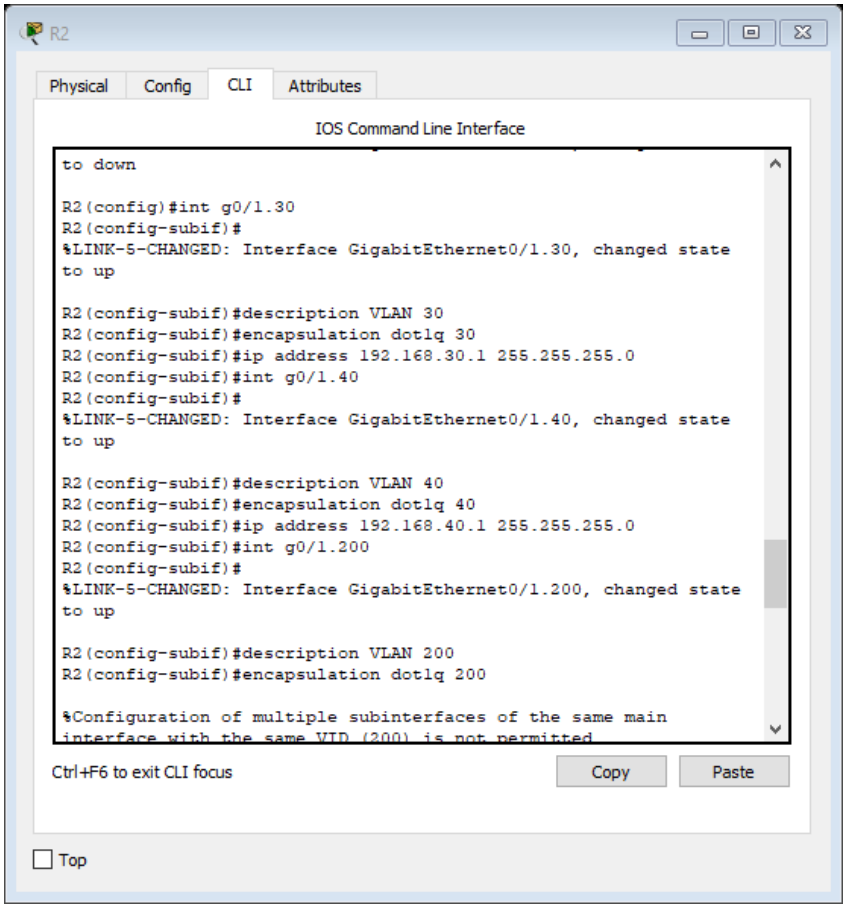

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1(config-vlan)#vlan 23
S1(config-vlan)#vlan 30
S1(config-vlan)#name Administracion
VLAN #21 and #30 have an identical name: Administracion
S1(config-vlan)#vlan 21
S1(config-vlan)#name vlan error
^
% Invalid input detected at '^' marker.
S1(config-vlan)#name error
S1(config-vlan)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

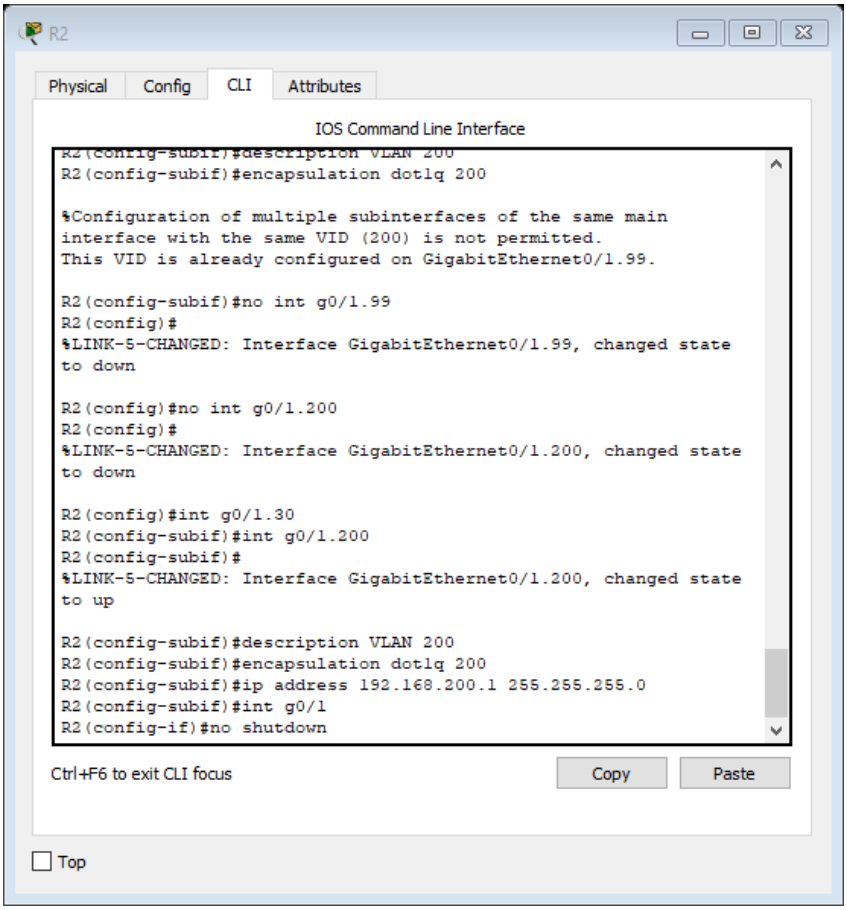

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to up
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 30
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, 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
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

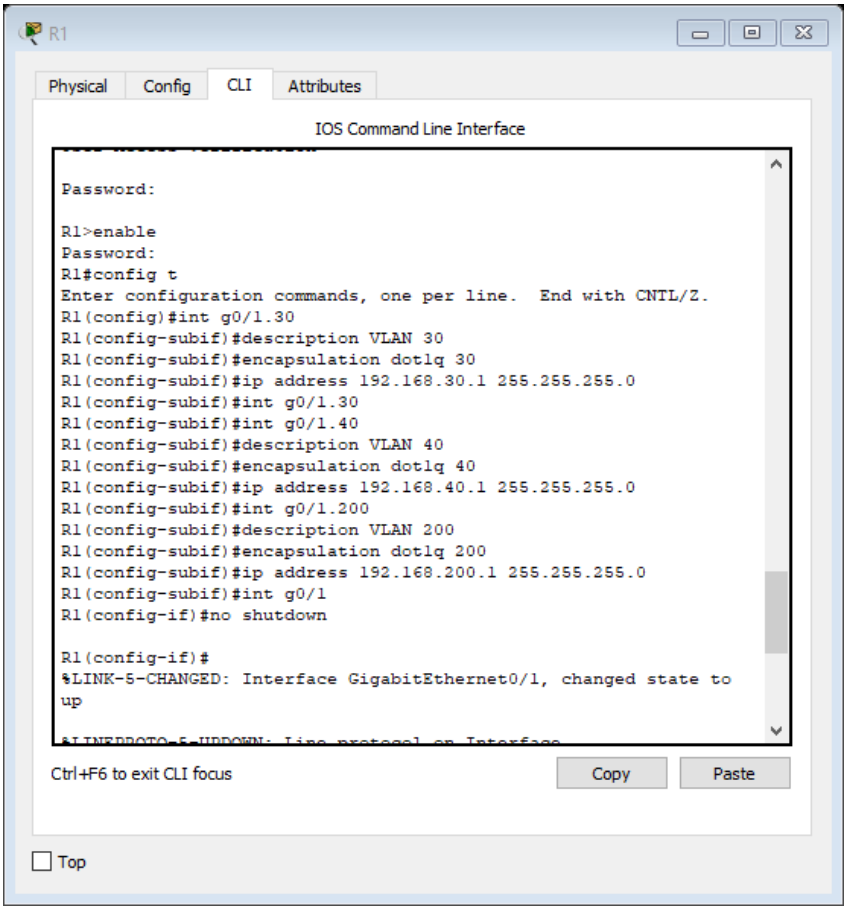

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

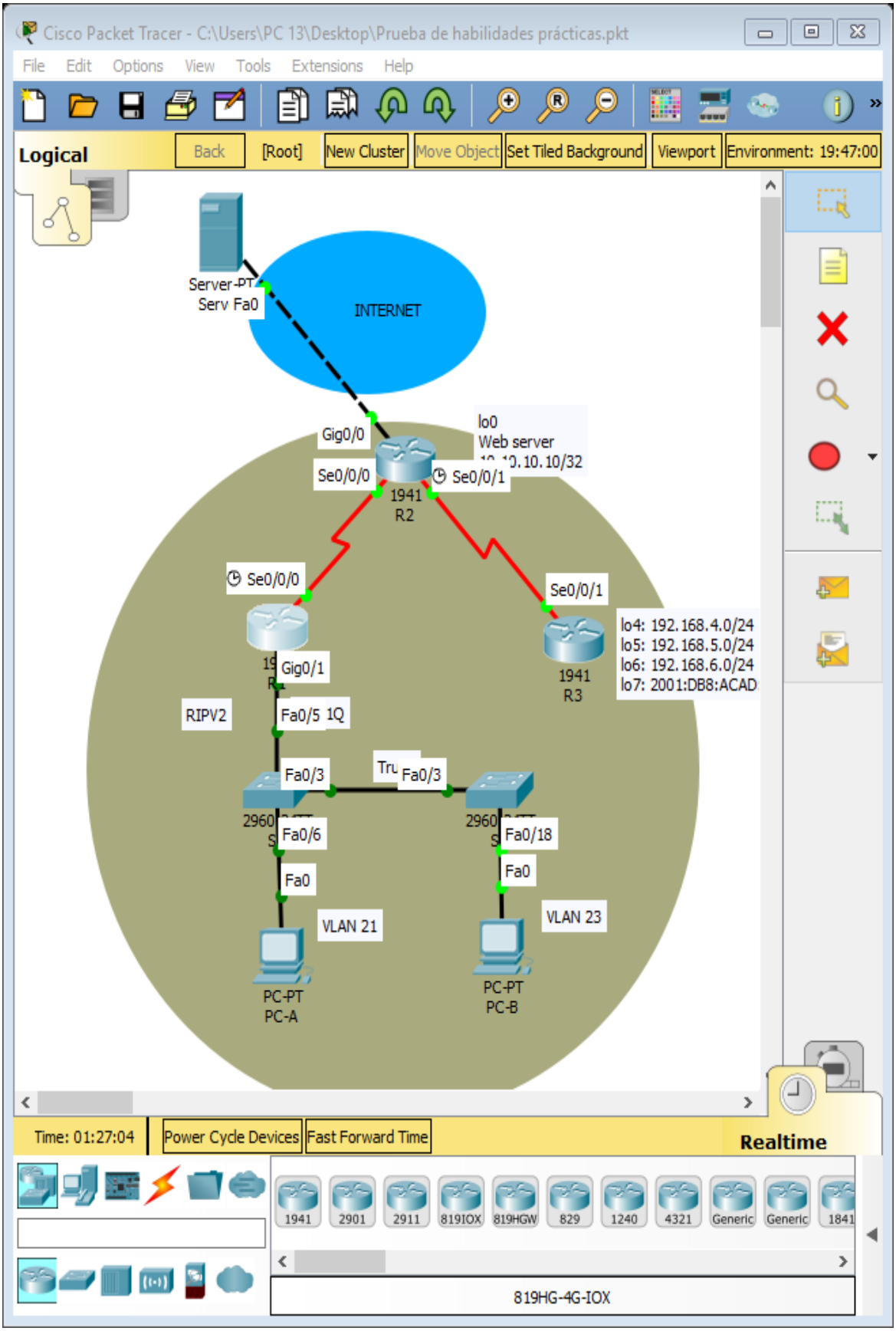

S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.200.1
S3(config)#int r0/3
^
% Invalid input detected at '^' marker.
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 30
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
R2>enable
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/1.21
R2(config-subif)#description VLAN 30
R2(config-subif)#encapsulation dolq 30
^
% Invalid input detected at '^' marker.
R2(config-subif)#encapsulation dolq 30
^
% Invalid input detected at '^' marker.
R2(config-subif)#encapsulation dotlq 30
^
% Invalid input detected at '^' marker.
R2(config-subif)#encapsulation dotlq 30
R2(config-subif)#ip address 192.168.30.1 255.255.255.0
R2(config-subif)#int g0/1.99
R2(config-subif)#description VLAN 200
R2(config-subif)#encapsulation dotlq 200
R2(config-subif)#ip address 192.168.200.1 255.255.255.0
R2(config-subif)#int g0/1
R2(config-if)#no shutdown
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

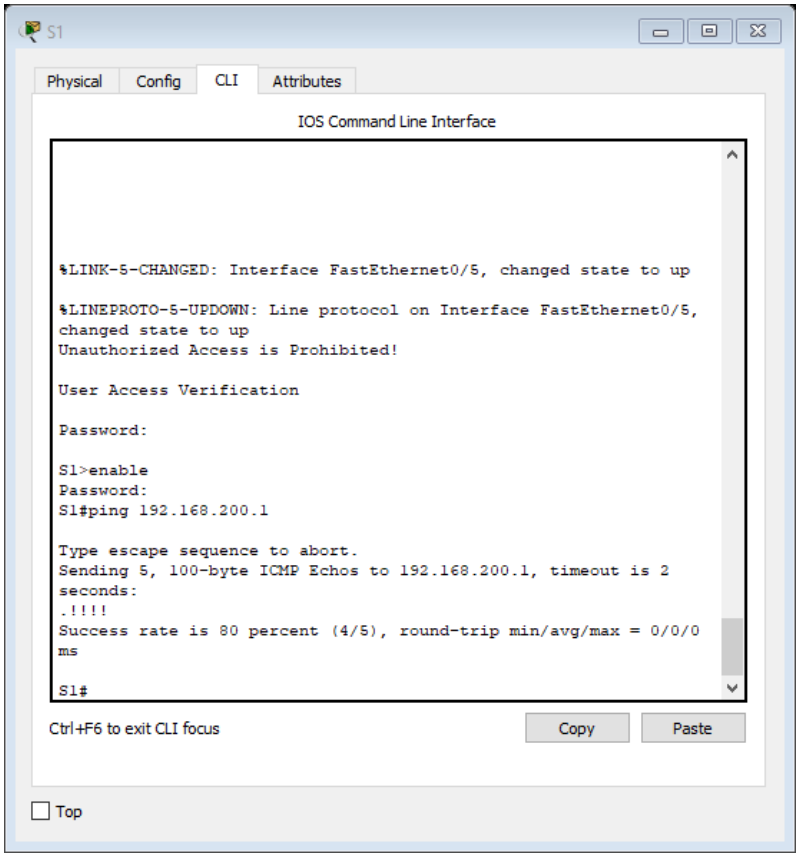

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
to down
R2(config)#int g0/1.30
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state
to up
R2(config-subif)#description VLAN 30
R2(config-subif)#encapsulation dot1q 30
R2(config-subif)#ip address 192.168.30.1 255.255.255.0
R2(config-subif)#int g0/1.40
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.40, changed state
to up
R2(config-subif)#description VLAN 40
R2(config-subif)#encapsulation dot1q 40
R2(config-subif)#ip address 192.168.40.1 255.255.255.0
R2(config-subif)#int g0/1.200
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.200, changed state
to up
R2(config-subif)#description VLAN 200
R2(config-subif)#encapsulation dot1q 200
%Configuration of multiple subinterfaces of the same main
interface with the same VID (200) is not permitted
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

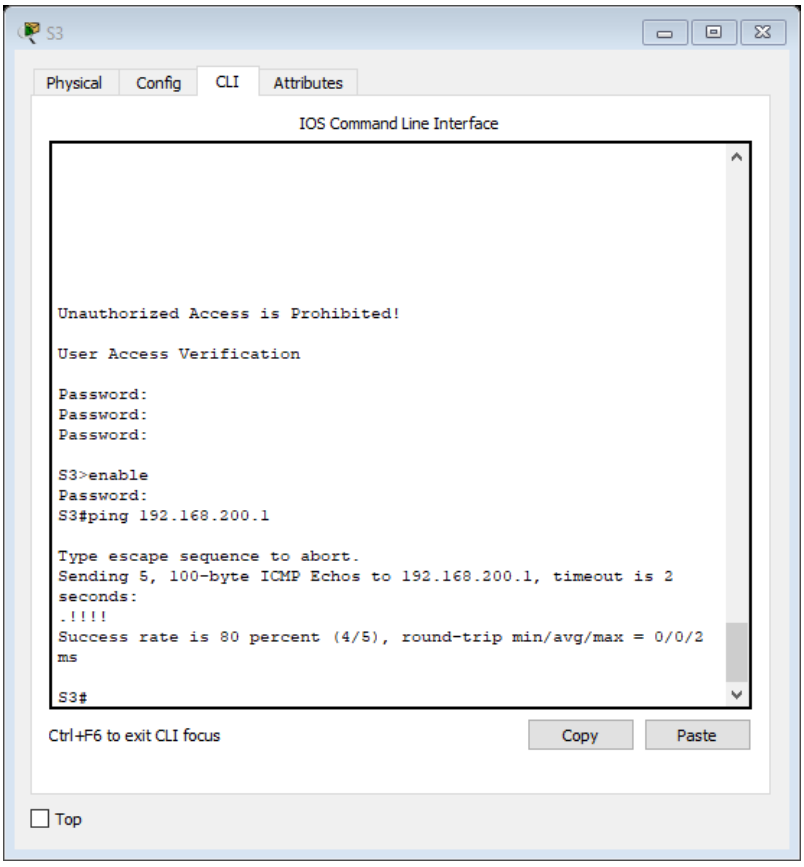

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2(config-subif)#description VLAN 200
R2(config-subif)#encapsulation dot1q 200
%Configuration of multiple subinterfaces of the same main
interface with the same VID (200) is not permitted.
This VID is already configured on GigabitEthernet0/1.99.
R2(config-subif)#no int g0/1.99
R2(config)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state
to down
R2(config)#no int g0/1.200
R2(config)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.200, changed state
to down
R2(config)#int g0/1.30
R2(config-subif)#int g0/1.200
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.200, changed state
to up
R2(config-subif)#description VLAN 200
R2(config-subif)#encapsulation dot1q 200
R2(config-subif)#ip address 192.168.200.1 255.255.255.0
R2(config-subif)#int g0/1
R2(config-if)#no shutdown
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

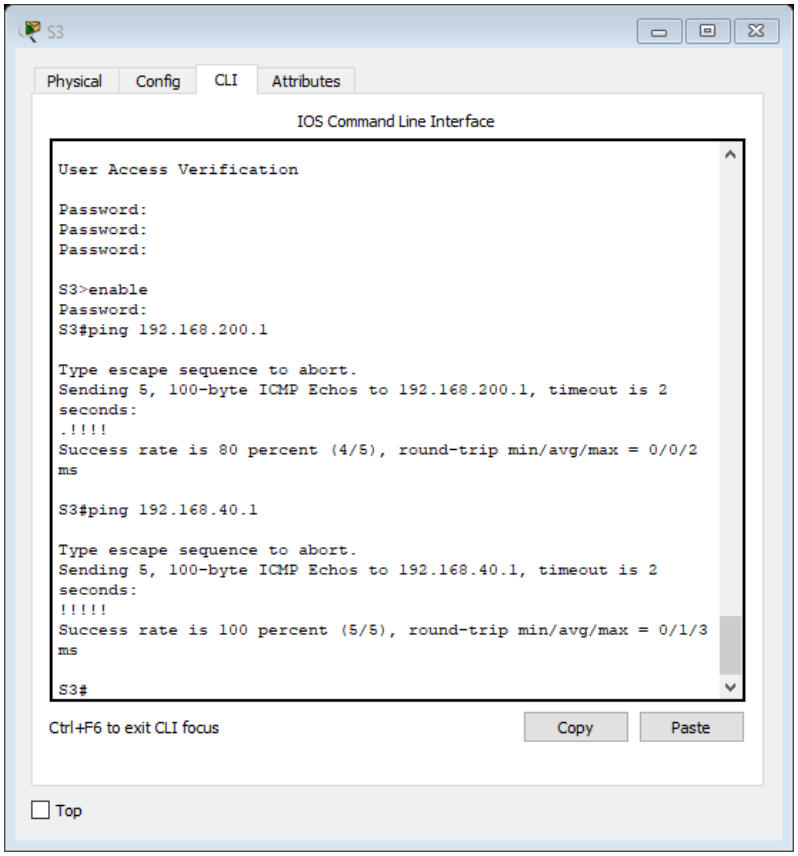

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.30
R1(config-subif)#description VLAN 30
R1(config-subif)#encapsulation dotlq 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/1.30
R1(config-subif)#int g0/1.40
R1(config-subif)#description VLAN 40
R1(config-subif)#encapsulation dotlq 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/1.200
R1(config-subif)#description VLAN 200
R1(config-subif)#encapsulation dotlq 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Cisco Packet Tracer - C:\Users\PC 13\Desktop\Prueba de habilidades prácticas.pkt
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 19:47:00
Server-PT
Serv Fa0
INTERNET
Gig0/0
lo0
Web server
Se0/0/0
Se0/0/1
1941
R2
Se0/0/0
Se0/0/1
Gig0/1
1941
R3
lo4: 192.168.4.0/24
lo5: 192.168.5.0/24
lo6: 192.168.6.0/24
lo7: 2001:DB8:ACAD
RIPV2
Fa0/5
1Q
Fa0/3
Fa0/3
Fa0/6
Fa0/18
Fa0
Fa0
VLAN 21
VLAN 23
PC-PT
PC-A
PC-PT
PC-B
Time: 01:27:04
Power Cycle Devices
Fast Forward Time
Realtime
1941
2901
2911
819IOX
819HGW
829
1240
4321
Generic
Generic
1841
819HG-4G-IOX

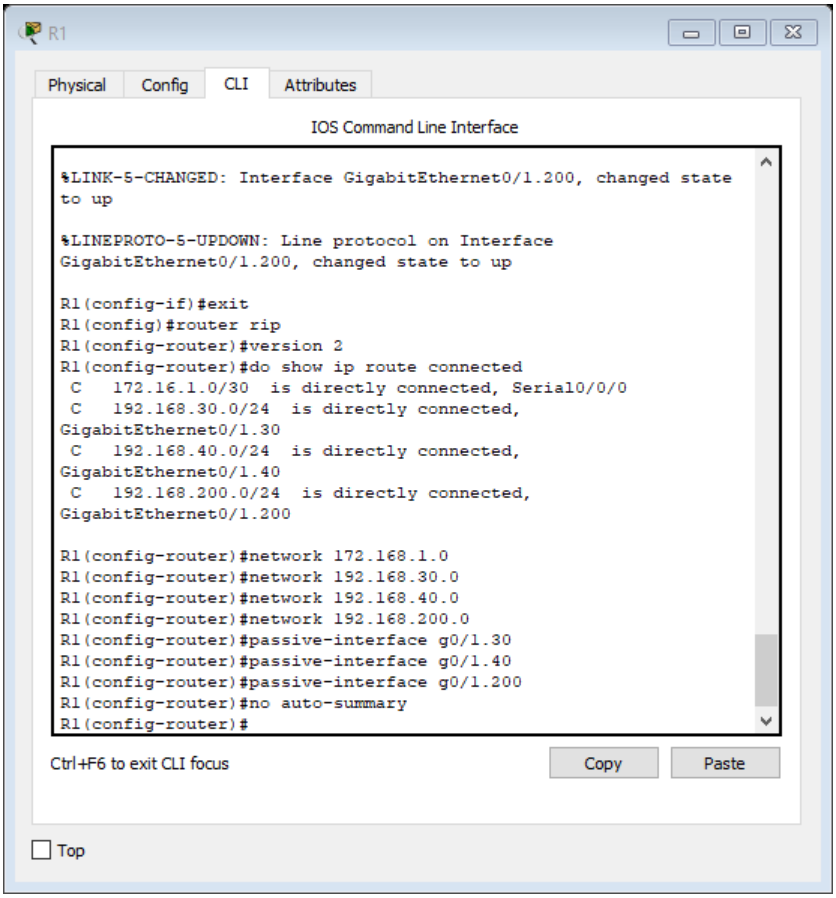
PINGS DE VERIFICACIÓN

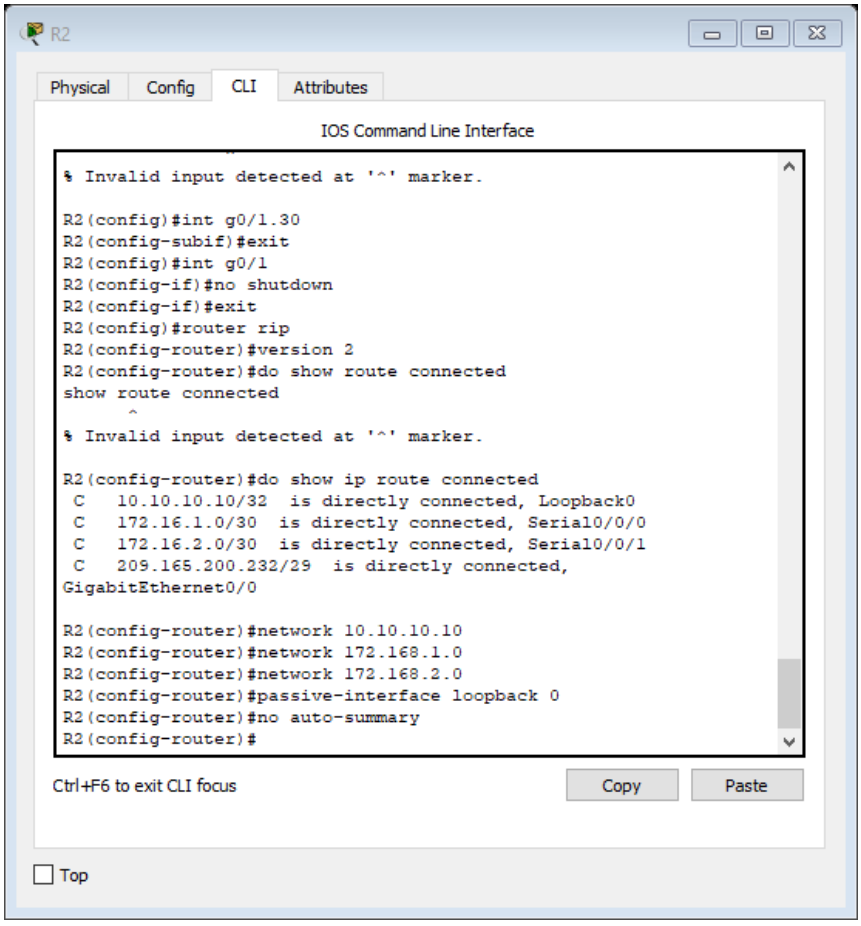


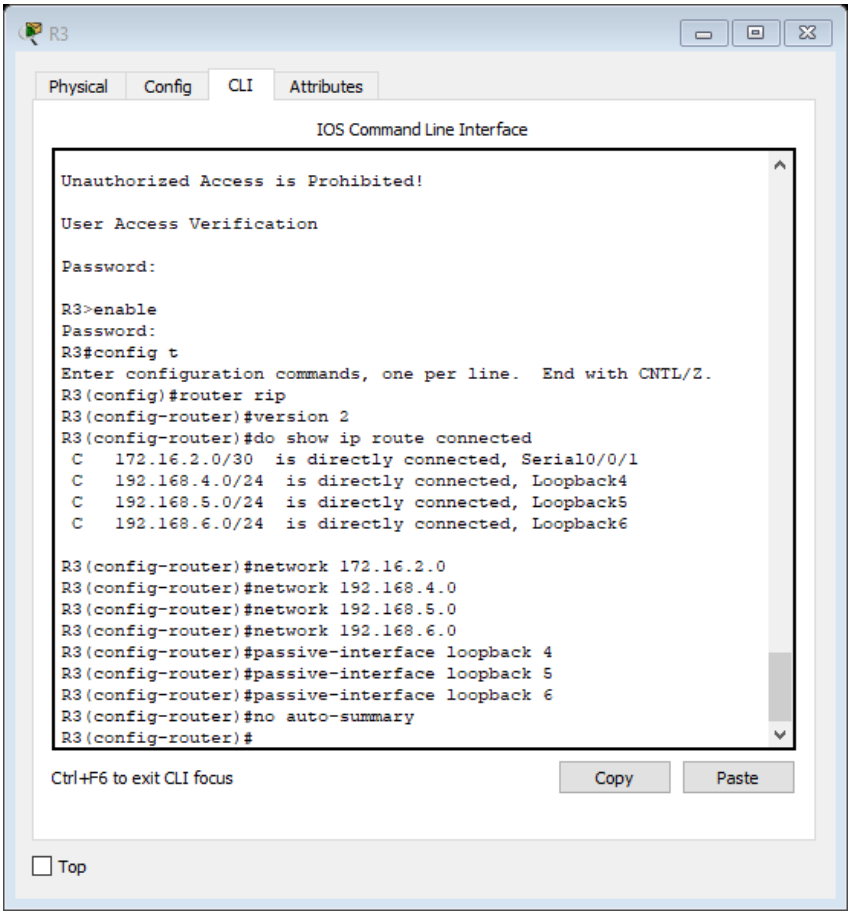



S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
Password:
Password:
S3>enable
Password:
S3#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2
ms
S3#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3
ms
S3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

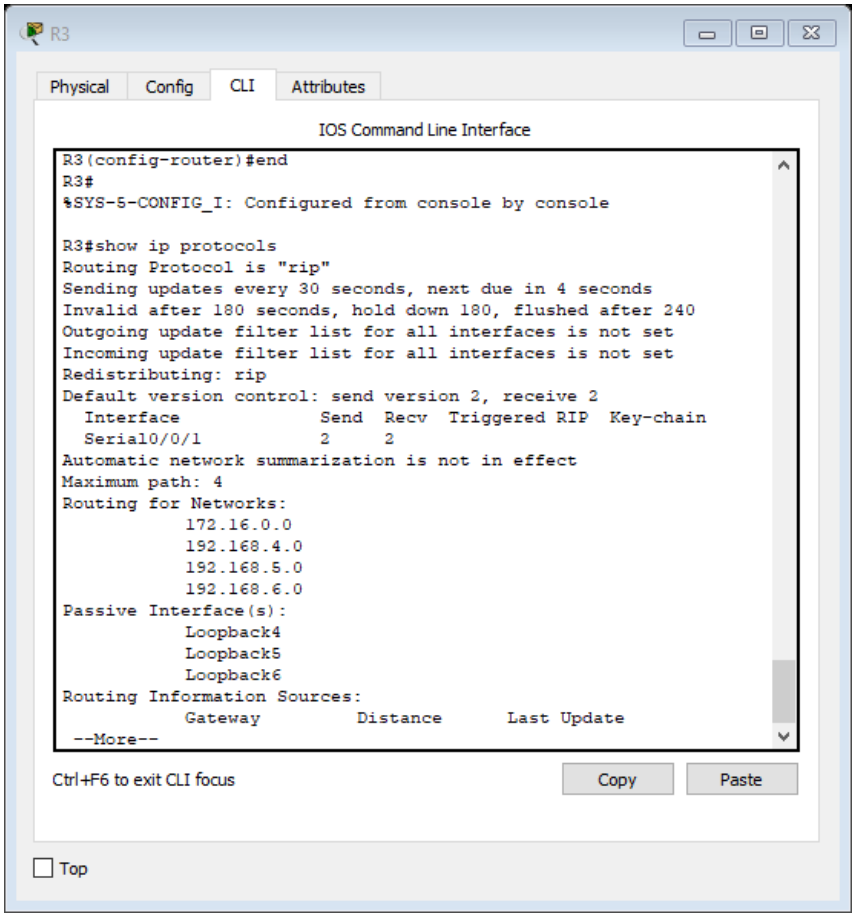
CONFIGURACIÓN DEL DHCP

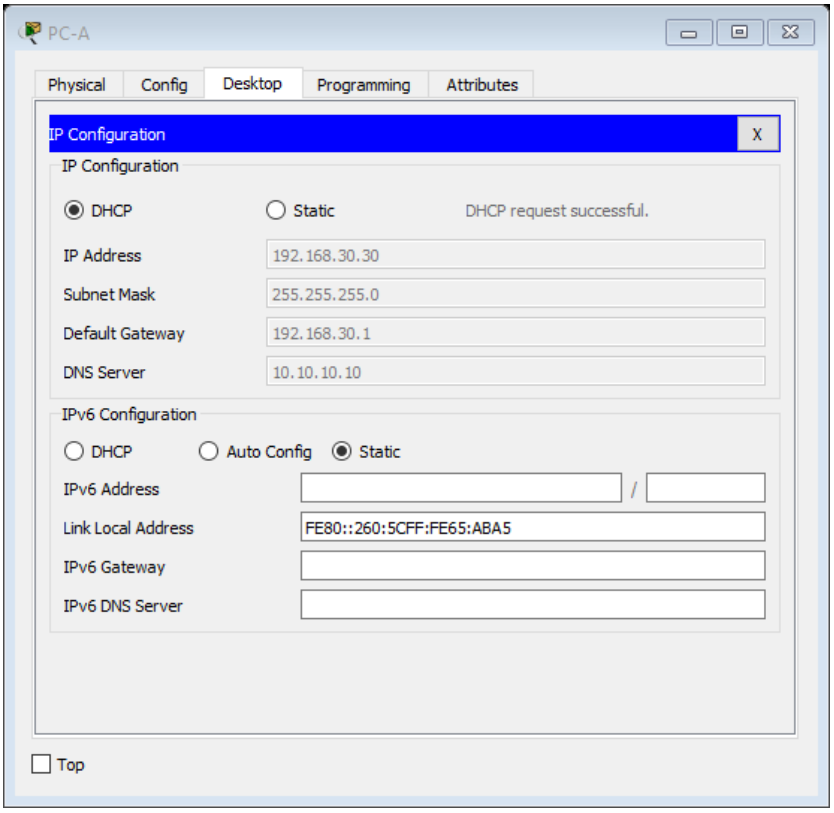


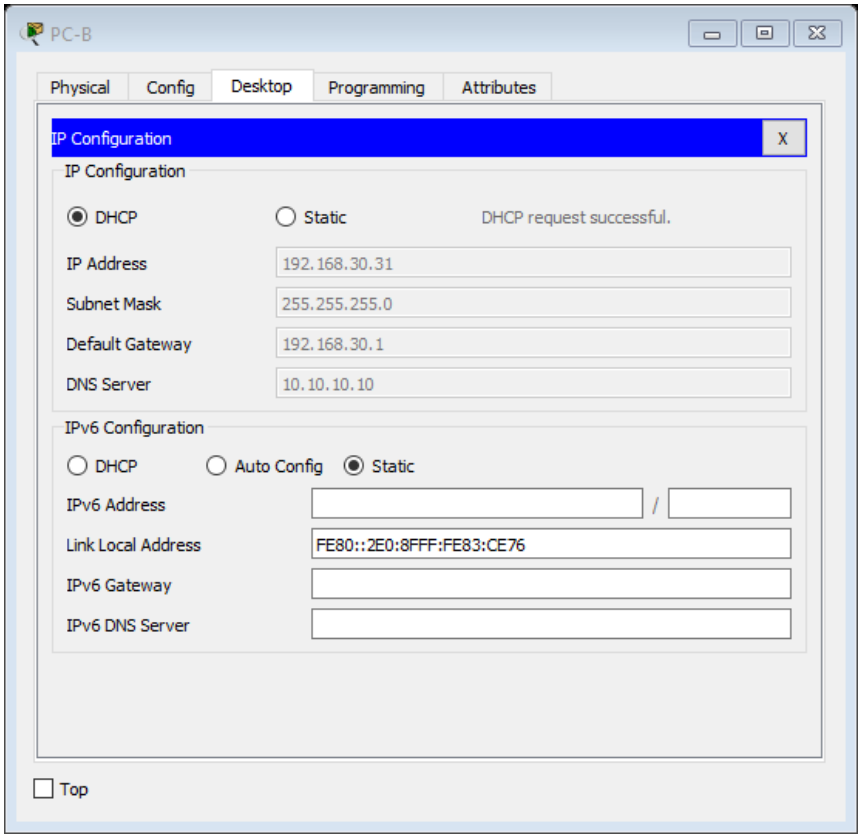

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
R2(config)#int g0/1.30
R2(config-subif)#exit
R2(config)#int g0/1
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show route connected
show route connected
^
% Invalid input detected at '^' marker.
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected,
GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.168.1.0
R2(config-router)#network 172.168.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
R2(config-router)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

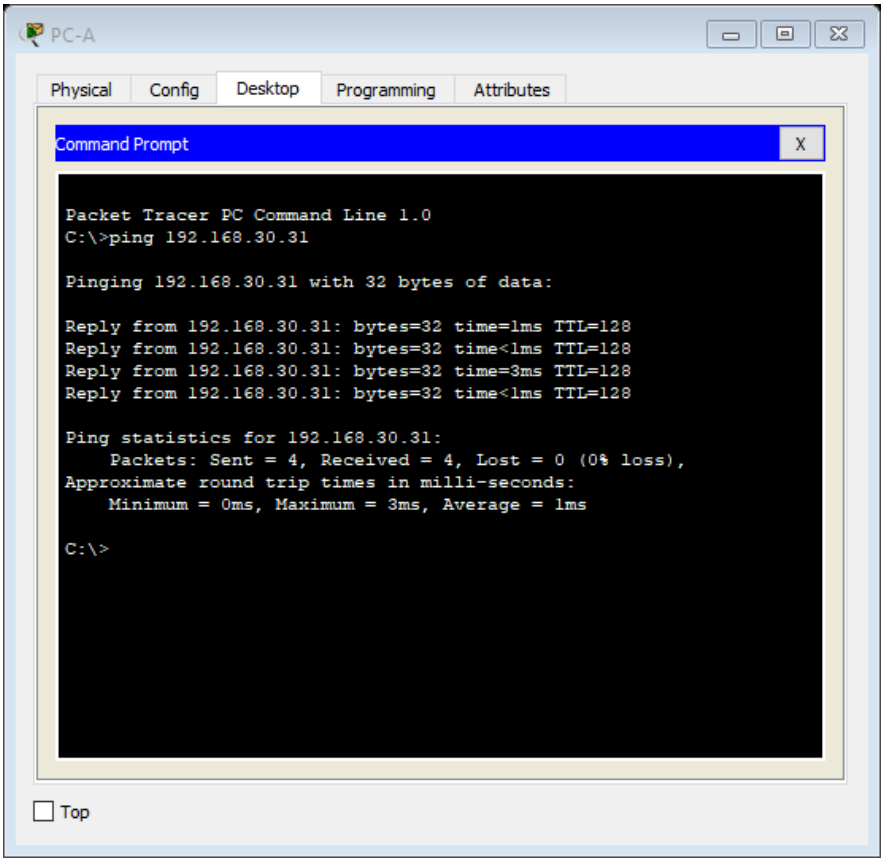

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Unauthorized Access is Prohibited!
User Access Verification
Password:
R3>enable
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
R3(config-router)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

PROTOCOLOS CONFIGURADOS

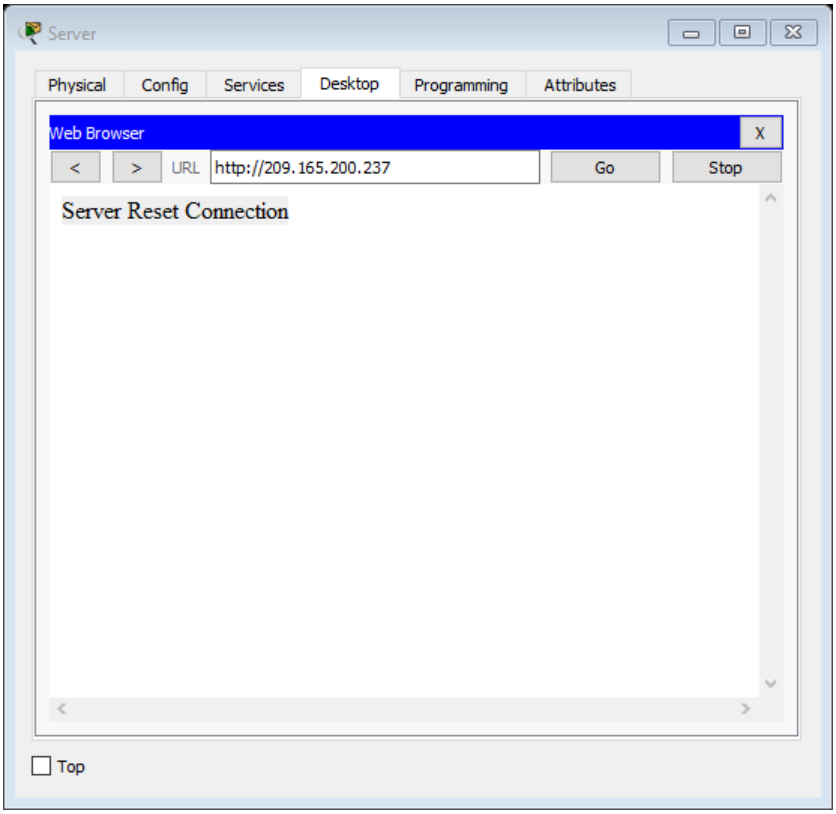




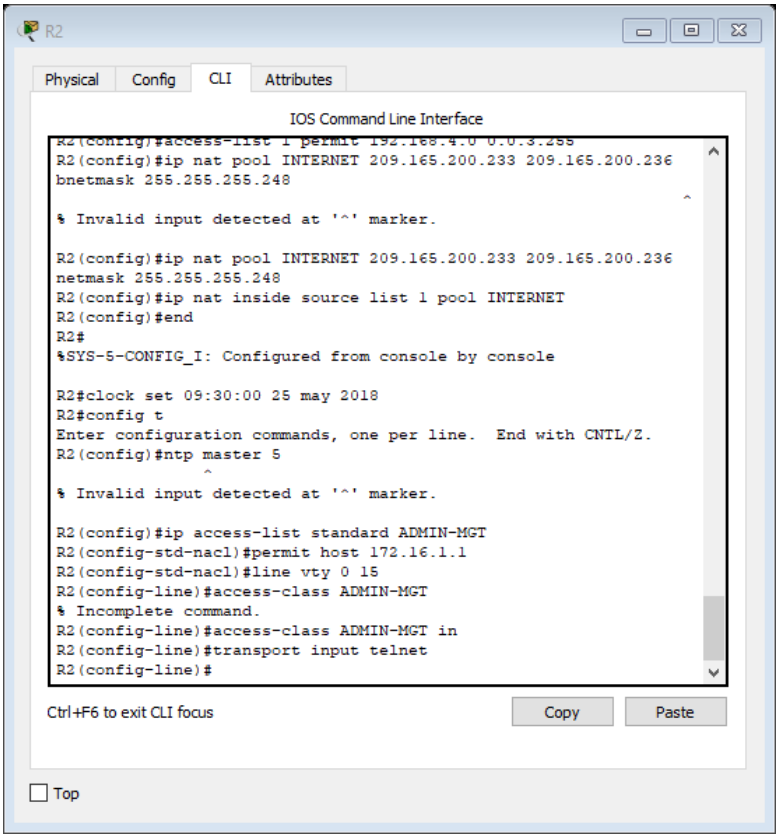

PC-B
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.30.31
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
10.10.10.10
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2E0:8FFF:FE83:CE76
IPv6 Gateway
IPv6 DNS Server
Top

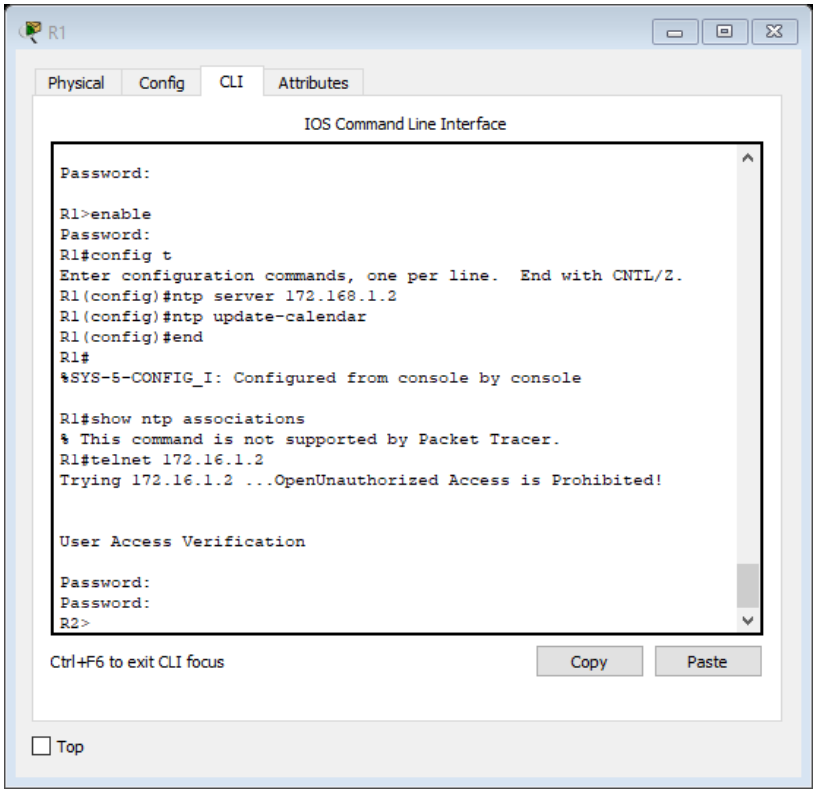

PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.31
Pinging 192.168.30.31 with 32 bytes of data:
Reply from 192.168.30.31: bytes=32 time=1ms TTL=128
Reply from 192.168.30.31: bytes=32 time<1ms TTL=128
Reply from 192.168.30.31: bytes=32 time=3ms TTL=128
Reply from 192.168.30.31: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.30.31:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms
C:\>
Top

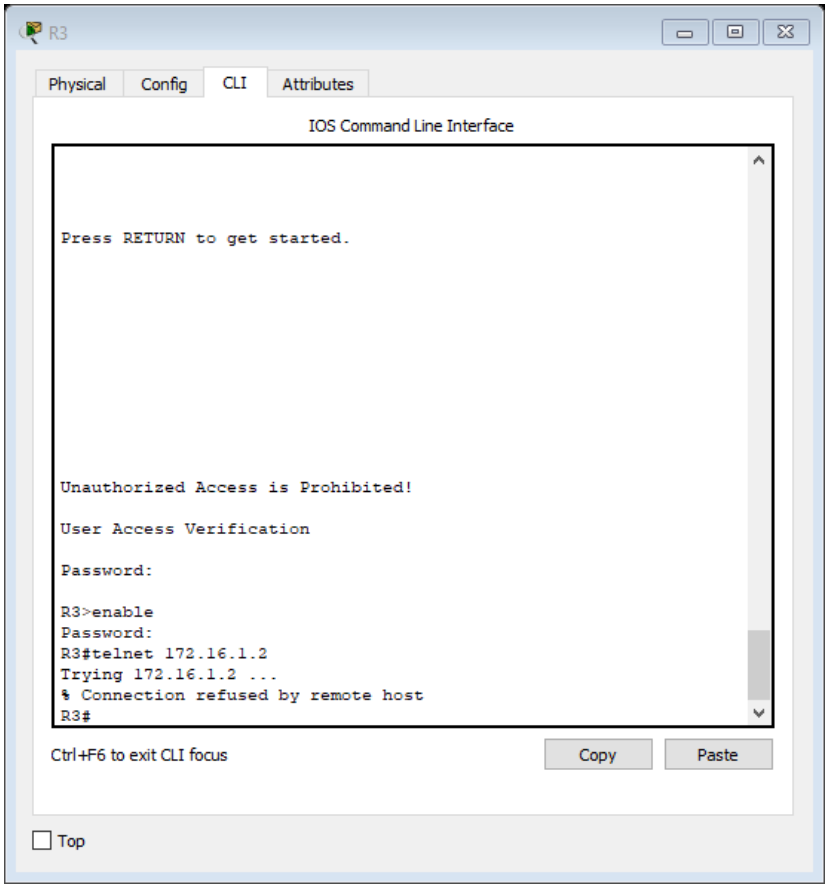
Server Reset Connection

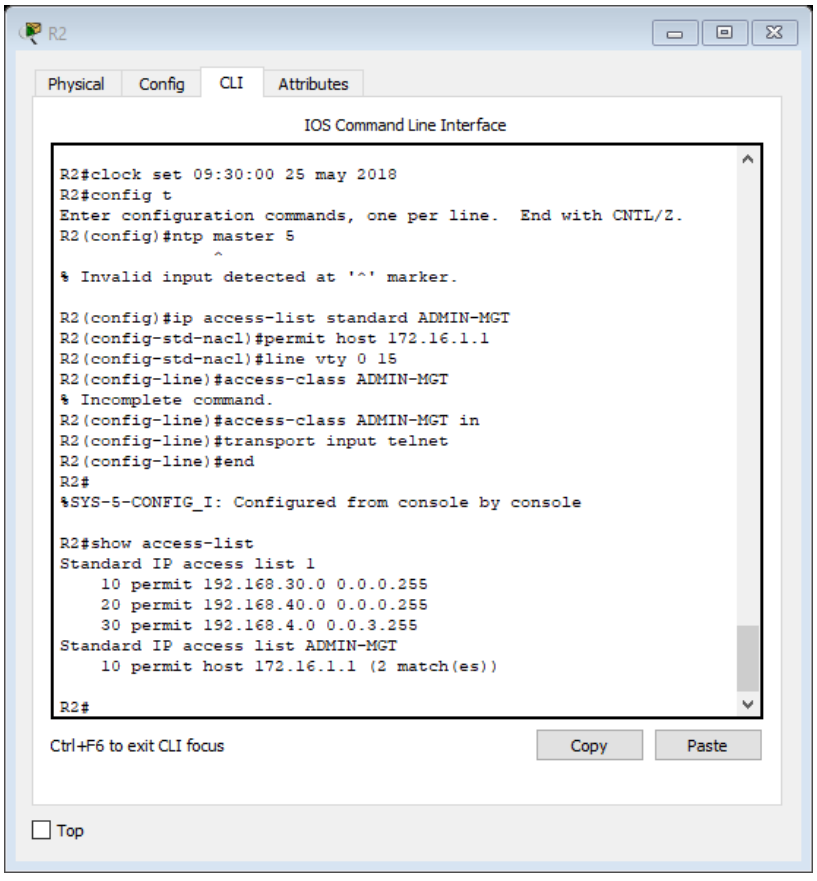


Configuración de seguridad anti telnet






R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
Unauthorized Access is Prohibited!
User Access Verification
Password:
R3>enable
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2#clock set 09:30:00 25 may 2018
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
^
% Invalid input detected at '^' marker.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT
% Incomplete command.
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show access-list
Standard IP access list 1
10 permit 192.168.30.0 0.0.0.255
20 permit 192.168.40.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

CONCLUSIONES

Gracias a DHCP no tendrá que dedicar gran parte de su tiempo a configurar una red TCP/IP ni a la administración diaria de dicha red. Tenga en cuenta que, en la implementación de Oracle Solaris, DHCP sólo funciona con IPv4.

DHCP ofrece las ventajas siguientes:

- Administración de direcciones IP: una de las principales ventajas de DHCP es que facilita la administración de las direcciones IP. En una red sin DHCP, debe asignar manualmente las direcciones IP. Debe asignar una dirección IP exclusiva a cada cliente y configurar cada uno de los clientes de modo individual. Si un cliente se pasa a una red distinta, debe realizar modificaciones manuales para dicho cliente. Si DHCP está activo, el servidor DHCP administra y asigna las direcciones IP sin necesidad de que intervenga el administrador. Los clientes pueden moverse a otras subredes sin necesidad de reconfiguración manual, ya que obtienen del servidor DHCP la nueva información de cliente necesaria para la nueva red.
- Configuración de cliente de red centralizada: Puede crear una configuración a medida para determinados clientes o para determinados tipos de clientes. La información de configuración se almacena en un lugar, el almacén de datos de DHCP. No es necesario iniciar sesión en un cliente para cambiar su configuración. Puede realizar modificaciones en múltiples clientes cambiando la información del almacén de datos.
- Compatibilidad con clientes BOOTP: Tanto los servidores BOOTP como los servidores DHCP escuchan y responden las emisiones de los clientes. El servidor DHCP puede responder a las solicitudes de clientes BOOTP y de clientes DHCP. Los clientes BOOTP reciben una dirección IP y la información que necesitan para iniciar desde un servidor.
- Compatibilidad con clientes locales y remotos: BOOTP permite reenviar mensajes de una red a otra. DHCP aprovecha la función de reenvío de BOOTP de distintos modos. La mayoría de los enrutadores de red se pueden configurar como agentes de reenvío de BOOTP para transferir solicitudes BOOTP a servidores que no se encuentren en la red del cliente. Las solicitudes DHCP se pueden reenviar del mismo modo, ya que el enrutador no distingue las solicitudes DHCP de las solicitudes BOOTP. El servidor DHCP también se puede configurar como agente de reenvío de BOOTP, si no hay disponible ningún enrutador que admita el reenvío de BOOTP.
- Inicio de red: los clientes pueden utilizar DHCP para obtener la información necesaria para iniciar desde un servidor de la red, en lugar de utilizar RARP (Reverse Address Resolution Protocol) y el archivo bootparams. El servidor DHCP puede facilitar a un cliente toda la información que necesita para funcionar, incluida la dirección IP, el servidor de inicio y la información de configuración de red. Dado que las solicitudes DHCP se pueden reenviar por subredes, es posible usar menos servidores de inicio en la red cuando se utiliza el inicio de red DHCP. El inicio RARP requiere que cada subred tenga un servidor de inicio.

- Amplia compatibilidad de red: las redes con millones de clientes DHCP pueden utilizar DHCP. El servidor DHCP utiliza varios subprocesos para procesar a la vez múltiples solicitudes de clientes. El servidor también admite almacenes de datos optimizados para administrar grandes cantidades de datos. El acceso de los almacenes de datos se administra mediante módulos de procesamiento independientes.

Bibliografía

MACFARLANE, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

LUCAS, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

ODOM, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1