

DISEÑO E IMPLEMENTACIÓN DE REDES DE TELECOMUNICACIONES

VIVIANA MAGALLY MEJIA OSPINA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E
IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)**

Grupo: 203092_17

IBAGUE

2018



DISEÑO E IMPLEMENTACIÓN DE REDES DE TELECOMUNICACIONES

VIVIANA MAGALLY MEJIA OSPINA

**MONOGRAFIA PARA OPTAR POR EL TÍTULO DE INGENIERO EN
SISTEMAS**

DIRECTOR DE CURSO

JUAN CARLOS VESGA

TUTOR

GIOVANNI ALBERTO BRACHO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E
IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)**

Grupo: 203092_17

IBAGUE

2018

TABLA DE CONTENIDO

INTRODUCCIÓN.....	4
OBJETIVOS.....	5
Objetivo general.....	5
Objetivos específicos.....	5
1. DESARROLLO DE LA ACTIVIDAD.....	6
1.1. METODOLOGÍA.....	6
1.2. EVALUACIÓN –PRUEBA DE HABILIDADES PRÁCTICAS CCNA.....	6
1.2.1 Descripción general de la prueba de habilidades.....	6
1.2.2. Descripción del escenario propuesto para la prueba de habilidades.....	7
1.2.2.1. Escenario.....	7
1.2.2.2. Topología de red.....	7
1.2.2.3. OSPFv2 área 0.....	8
1.2.2.4. Verificar información de OSPF.....	8
2. RESULTADOS.....	14
3. PINGS DE VERIFICACIÓN.....	21
4. CONFIGURACIÓN DEL DHCP.....	23
5. PROTOCOLOS CONFIGURADOS.....	25
6. SERVER RESET CONNECTION.....	28
7. CONFIGURACIÓN DE SEGURIDAD ANTI TELNET.....	29
8. CONCLUSIONES.....	31
BIBLIOGRAFIA.....	32

INTRODUCCIÓN

En este documento se expone la configuración implementada para usar el método de VLANs para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa OSI 3 y 4).

Más adelante, 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. El presente curso cubre la arquitectura, componentes y operaciones de enrutadores y conmutadores en una red pequeña. Los estudiantes aprenden a configurar un enrutador y un conmutador para la funcionalidad básica.

OBJETIVOS

Objetivo general

Construir una solución de red que permita la comunicación entre las sucursales de una empresa ubicadas en ciudades lejanas, configurando e interconectando entre sí cada uno de los dispositivos que forman parte del escenario.

Objetivos específicos

1. Describir la arquitectura, los componentes y las operaciones de los enrutadores y los switches en redes más grandes y más complejas.
2. Aprender a configurar enrutadores y conmutadores para que tengan una realidad avanzada en entornos requeridos de DHCP, NAT, VLAN, Enrutamiento estático y Dinámico.
3. Configurar y solucionar problemas de enrutadores y conmutadores en una LAN.

1. DESARROLLO DE LA ACTIVIDAD

1.1.METODOLOGÍA

- Clases teóricas, donde se presentan los contenidos desarrollados por Cisco y disponibles en la plataforma [NETACAD](#).
- E-learning, el estudiante debe dedicar tiempo extra clase para reforzar los conocimientos en la plataforma [NETACAD](#).
- Prácticas de laboratorio para el desarrollo de las prácticas correspondientes a cada capítulo.
- Prácticas en simulador, uso de packet tracer para reforzar conocimientos y habilidades.

1.2.EVALUACIÓN –PRUEBA DE HABILIDADES PRÁCTICAS

CCNA

1.2.1. 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 le considerará 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.

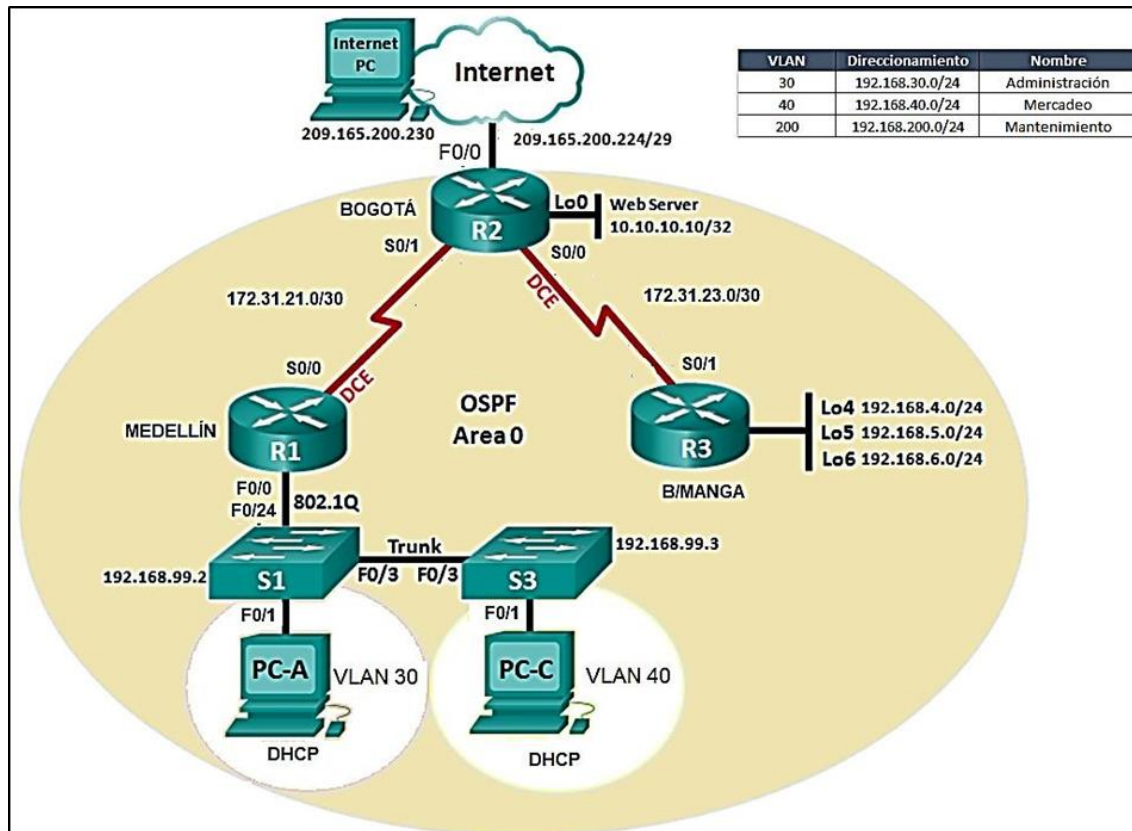
Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos, las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en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

1.2.2. Descripción del escenario propuesto para la prueba de habilidades

1.2.2.1 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.

1.2.2.2. Topología de red



Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

1. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

1.2.2.3. OSPFv2 área 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

1.2.2.4. 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.
2. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
 3. En el Switch 3 deshabilitar DNSlookup
 4. Asignar direcciones IP a los Switches acorde a los lineamientos.
 5. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
 6. Implement DHCP and NAT for IPv4
 7. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
 8. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Configurar DHCP pool para VLAN 30	Name: ADMINI STRACI ON 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.

9. Configurar NAT en R2 para permitir que los hosts puedan salir a internet
10. 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.
11. 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.
12. Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

The screenshot shows a configuration window titled 'Server' with tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The 'Config' tab is active, displaying the 'IP Configuration' section. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IP Address: 209.165.200.238, Subnet Mask: 255.255.255.248, Default Gateway: 209.165.200.233, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section has the 'Static' radio button selected, with fields for IPv6 Address (2001:DB8:ACAD:A::38 / 64), Link Local Address (FE80::2D0:97FF:FE41:DDE7), IPv6 Gateway (2001:DB8:ACAD:A::1), and IPv6 DNS Server (empty). A 'Top' checkbox is at the bottom left.

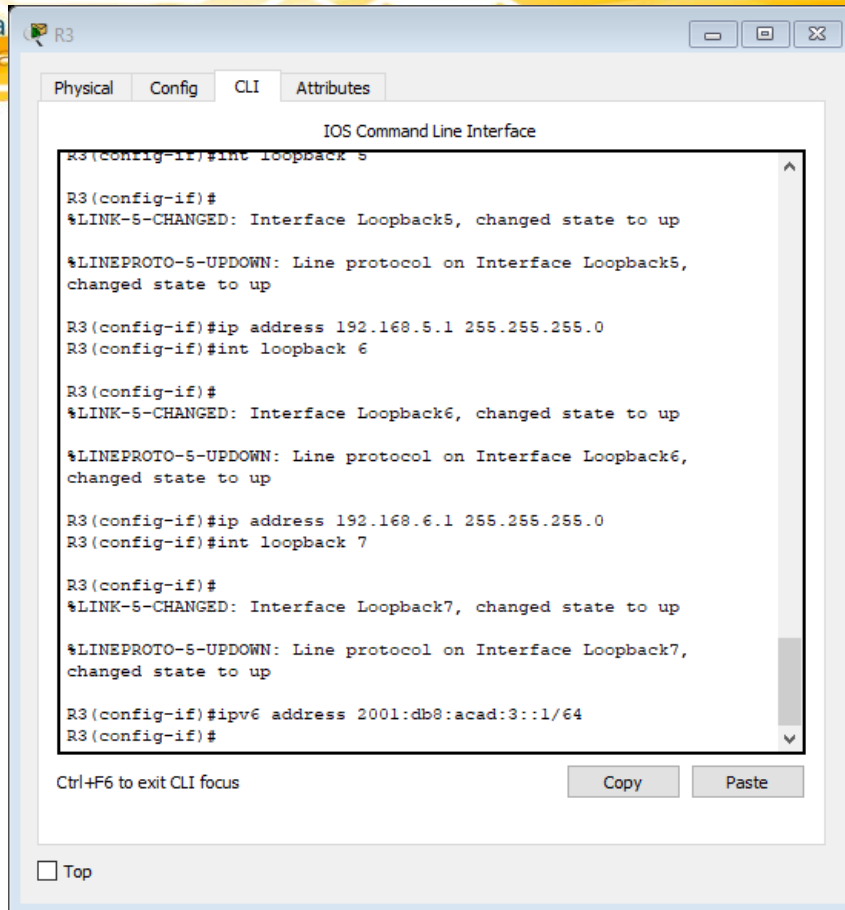
The screenshot shows a configuration window titled 'R3' with tabs for Physical, Config, CLI, and Attributes. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal text is as follows:

```
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 emryption
^
% Invalid input detected at '^' marker.
```

At the bottom, there is a 'Ctrl+F6 to exit CLI focus' instruction and 'Copy' and 'Paste' buttons. A 'Top' checkbox is at the bottom left.

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config-line)#service password emryption
^
% 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
```



The screenshot shows a window titled "R3" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
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)#
```

At the bottom of the CLI window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "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

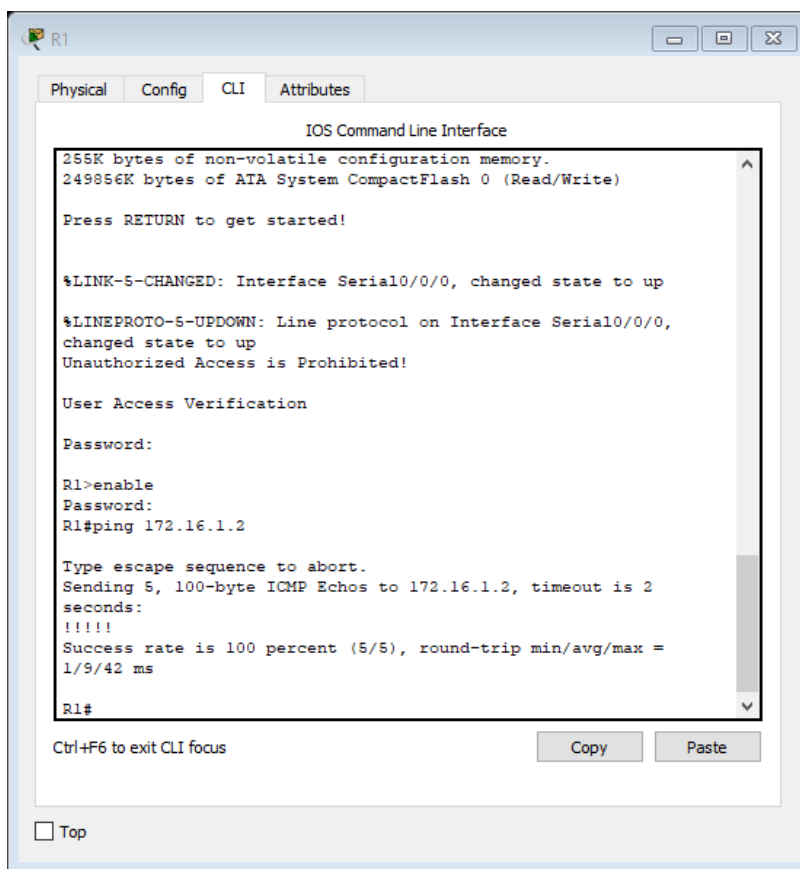
S3#wr
Building configuration...
[OK]
S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

2. RESULTADOS



The screenshot shows a Cisco IOS Command Line Interface window titled "R1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main text area displays the following output:

```
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

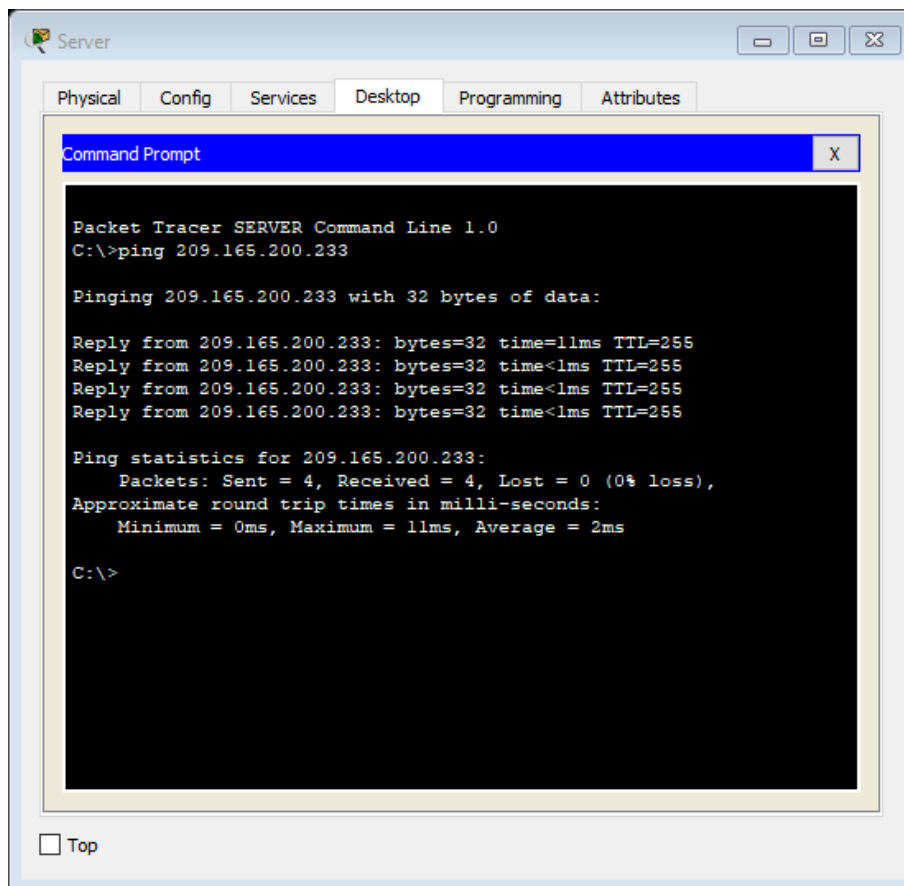
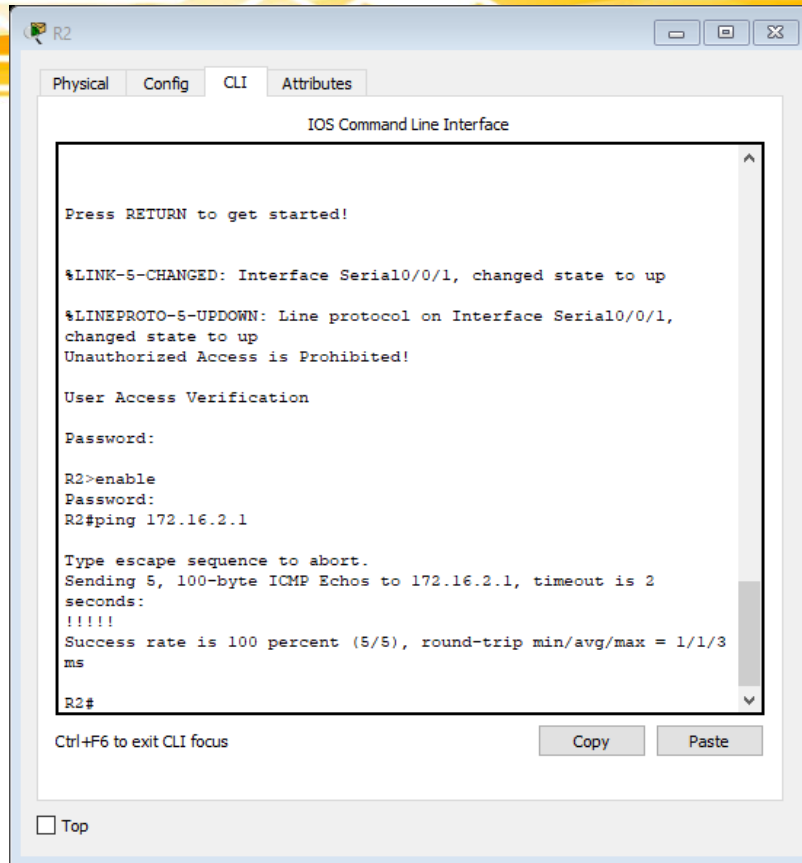
Password:

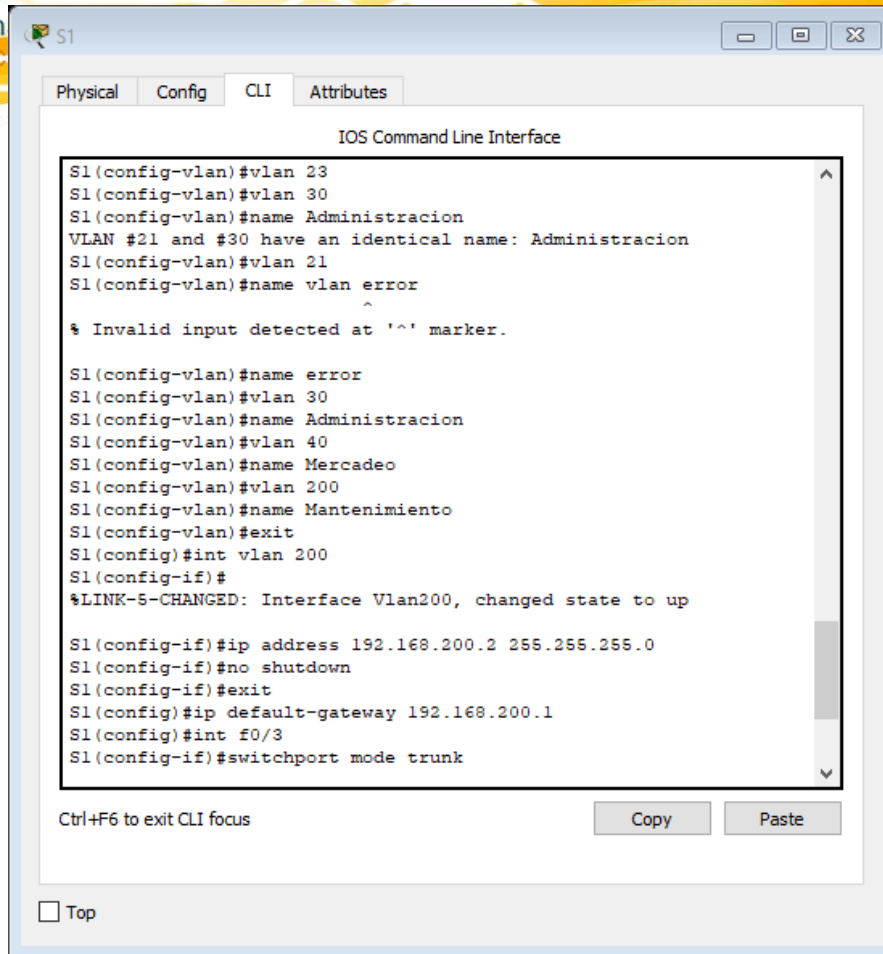
R1>enable
Password:
R1#ping 172.16.1.2

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#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" label, "Copy" and "Paste" buttons, and a "Top" button with an unchecked checkbox.





The screenshot shows a web-based interface for configuring a network device (S1). The interface has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following commands and their outputs:

```
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
```

At the bottom of the CLI window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "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

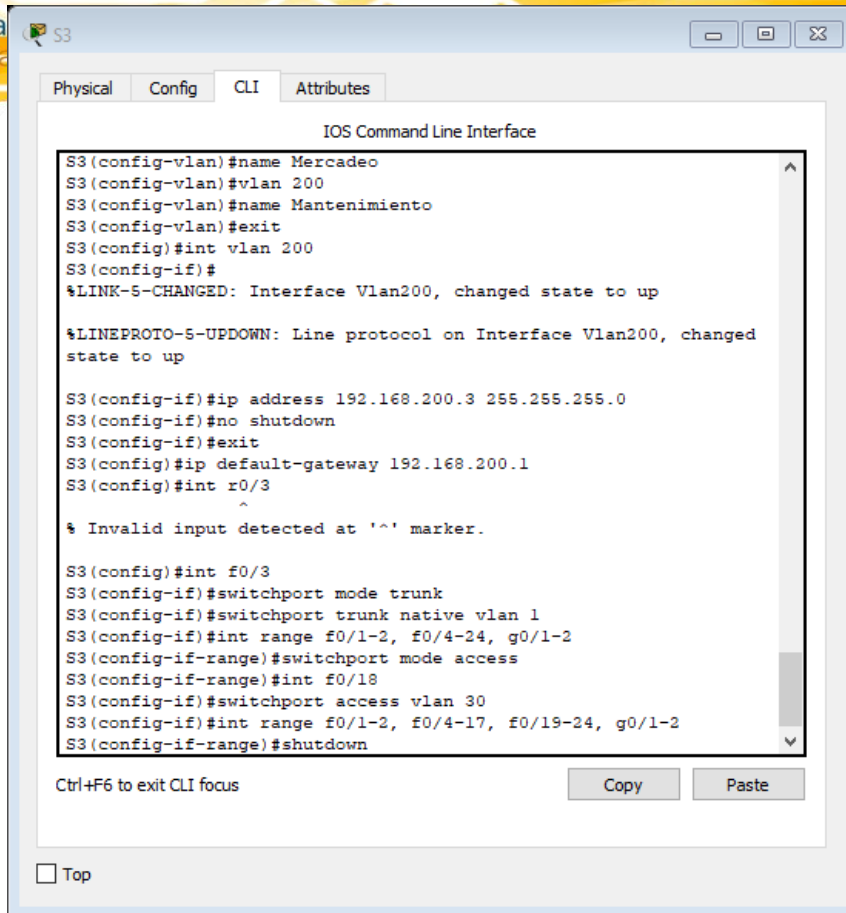
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down

%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

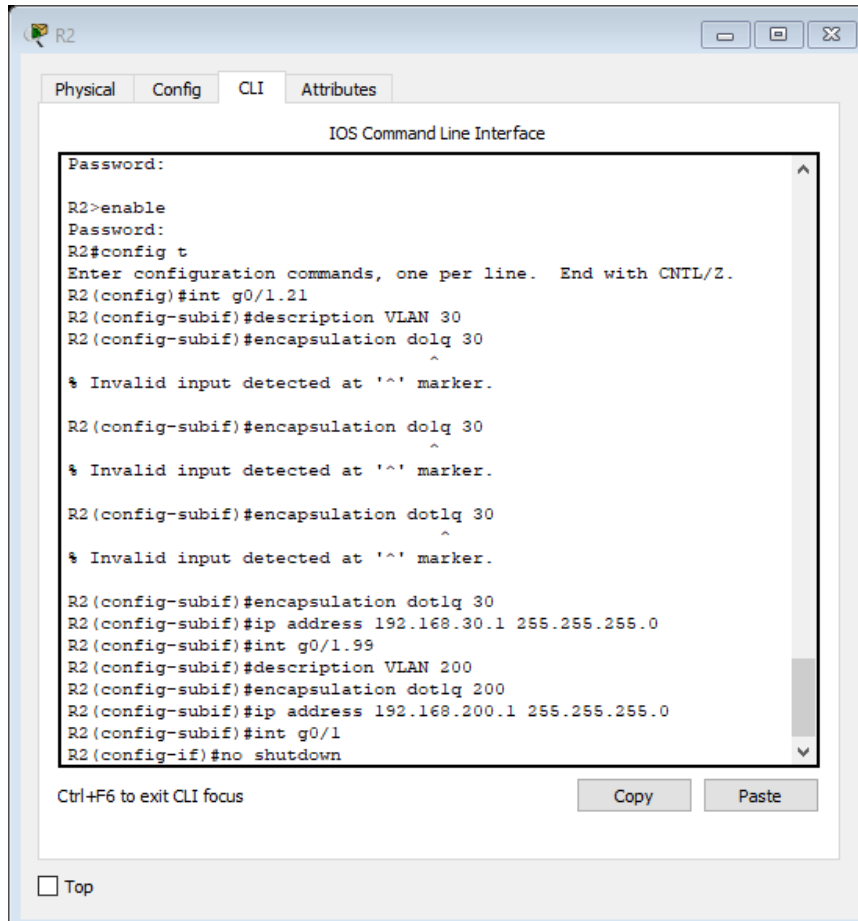
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.200.1
S3(config)#int r0/3
^
% Invalid input detected at '^' marker.

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 dotq 30
^
% Invalid input detected at '^' marker.

R2(config-subif)#encapsulation dotq 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

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

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 dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/1.40
R1(config-subif)#description VLAN 40
R1(config-subif)#encapsulation dot1q 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 dot1q 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

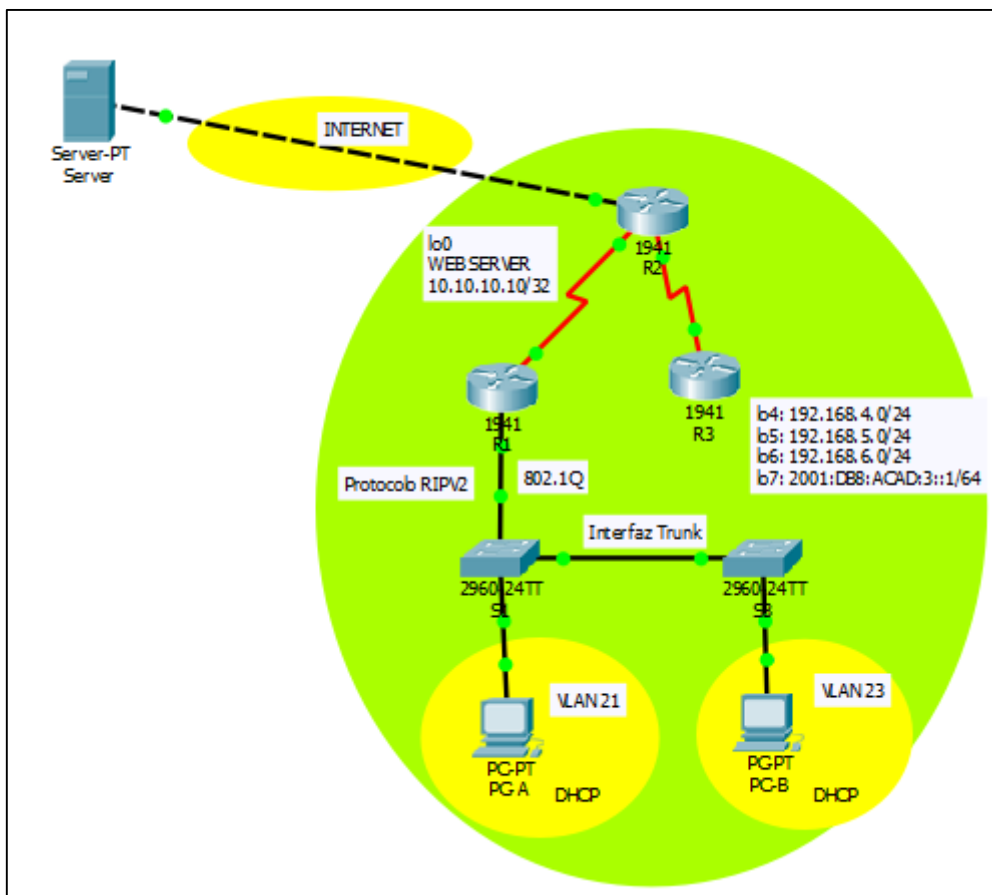
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface

```

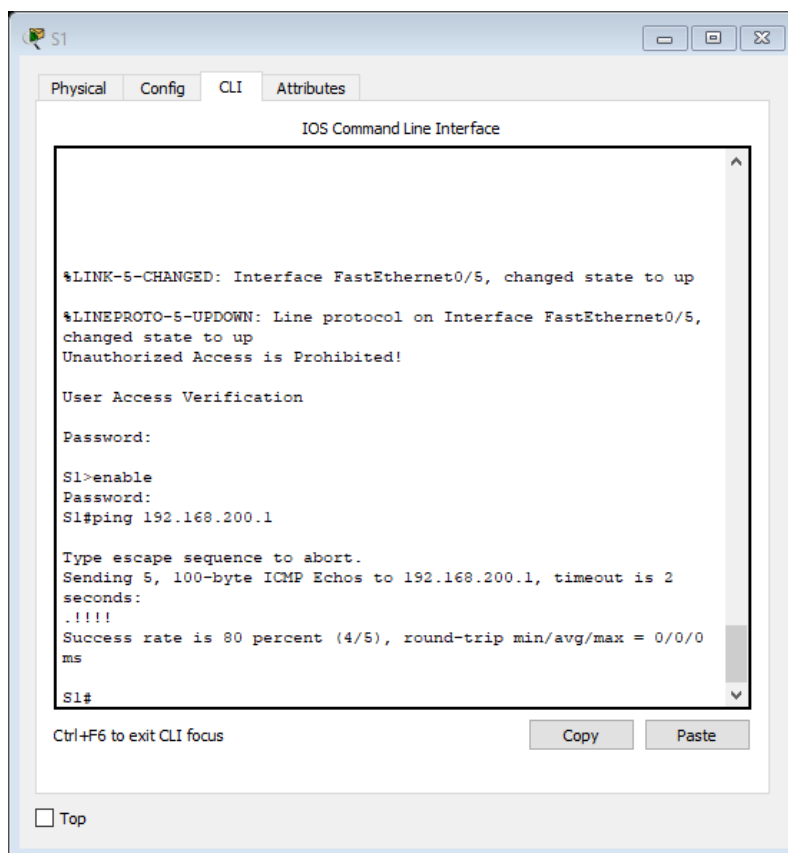
Ctrl+F6 to exit CLI focus

Copy Paste

Top



3. PINGS DE VERIFICACIÓN



The screenshot shows a network device CLI window titled 'S1'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area displays the following text:

```
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state to up
Unauthorized Access is Prohibited!

User Access Verification

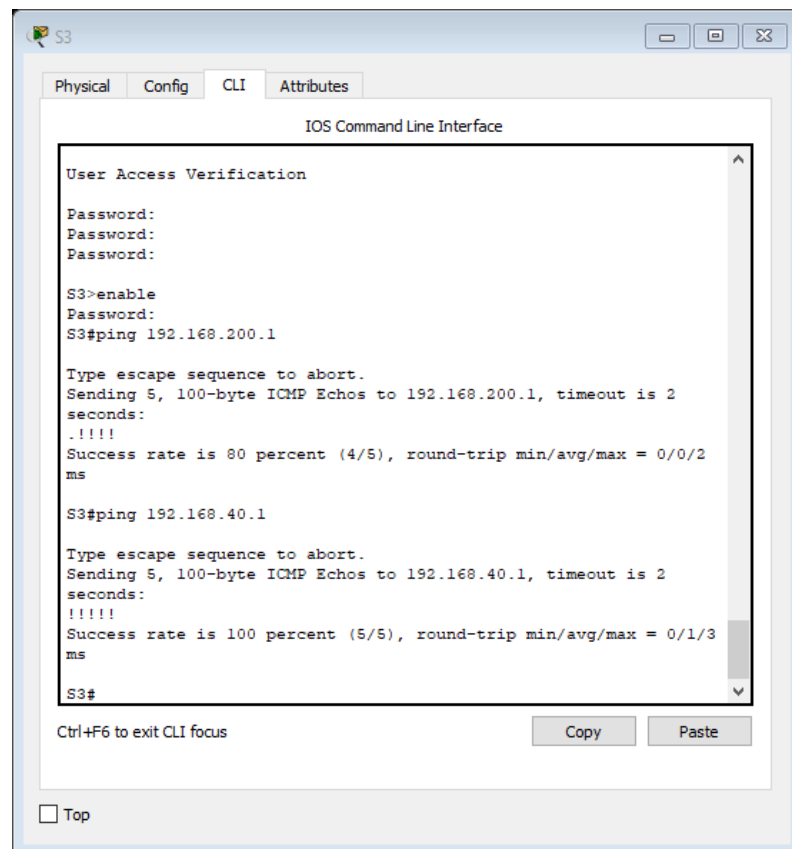
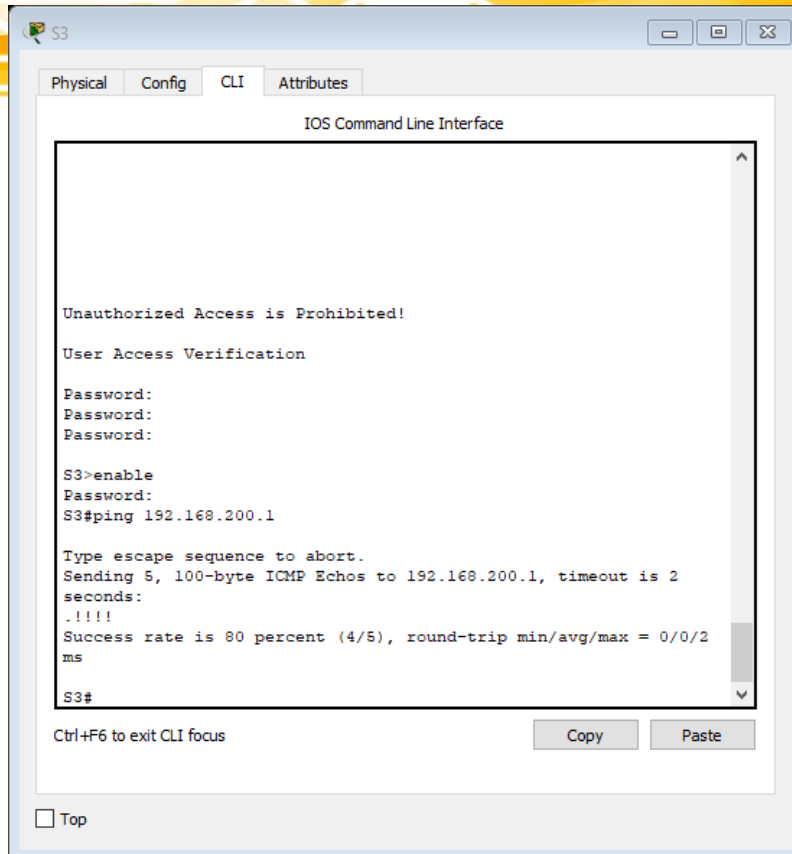
Password:

S1>enable
Password:
S1#ping 192.168.200.1

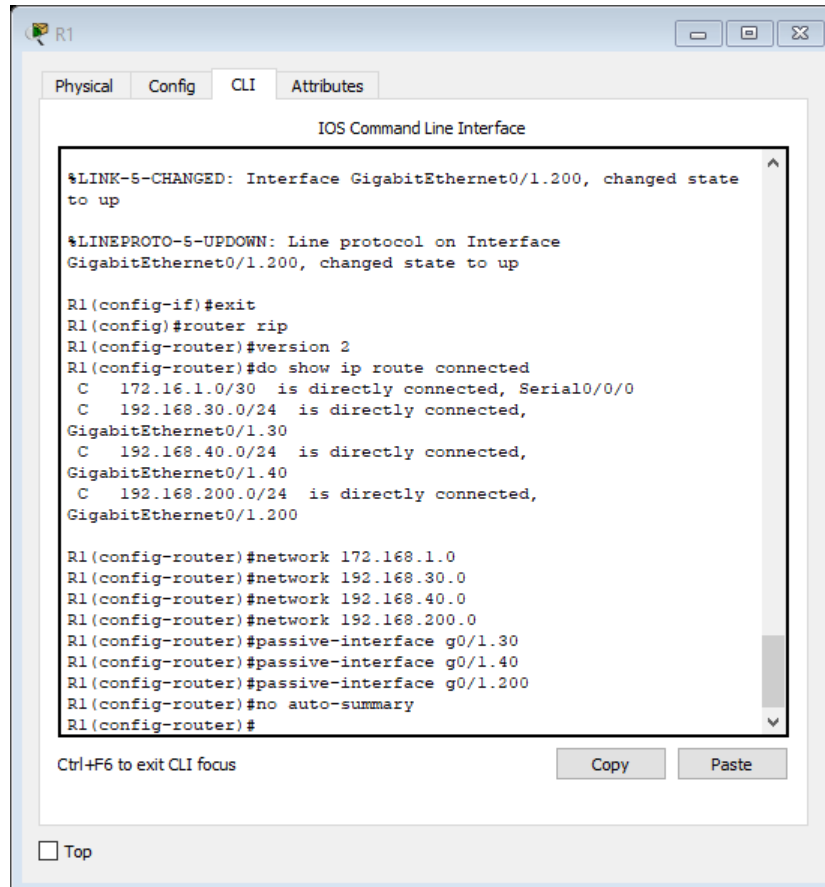
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0
ms

S1#
```

At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a checkbox labeled 'Top'.



4. CONFIGURACIÓN DEL DHCP



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet0/1.200, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.200, changed state to up

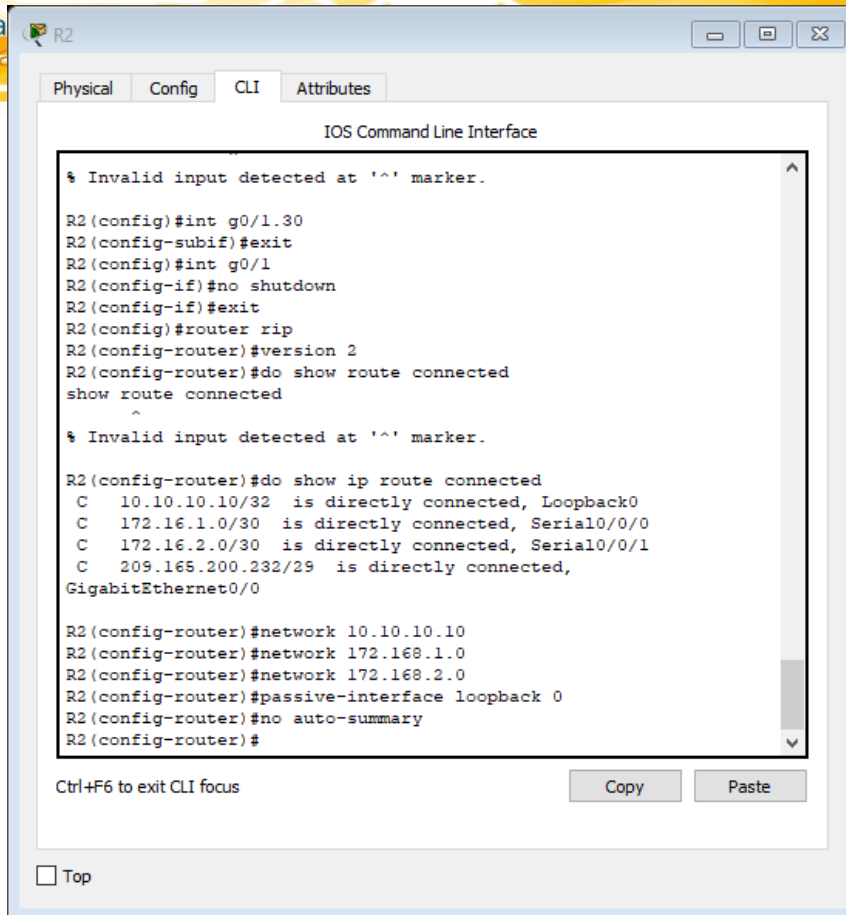
R1(config-if)#exit
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.30.0/24 is directly connected,
GigabitEthernet0/1.30
C 192.168.40.0/24 is directly connected,
GigabitEthernet0/1.40
C 192.168.200.0/24 is directly connected,
GigabitEthernet0/1.200

R1(config-router)#network 172.168.1.0
R1(config-router)#network 192.168.30.0
R1(config-router)#network 192.168.40.0
R1(config-router)#network 192.168.200.0
R1(config-router)#passive-interface g0/1.30
R1(config-router)#passive-interface g0/1.40
R1(config-router)#passive-interface g0/1.200
R1(config-router)#no auto-summary
R1(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top



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.

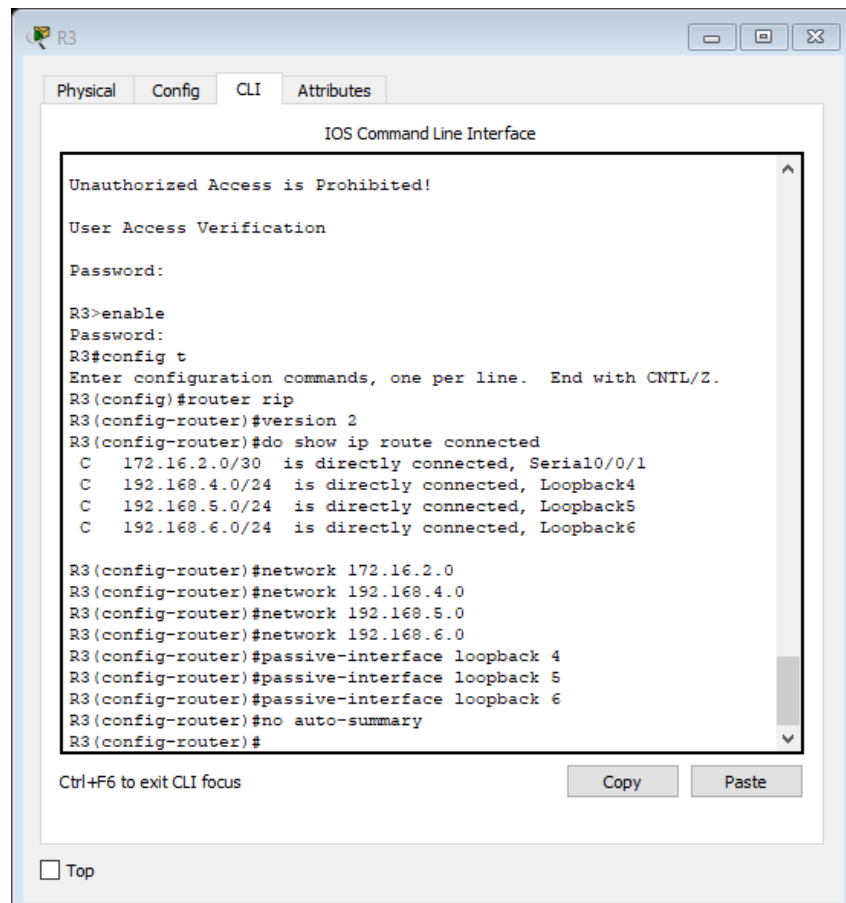
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected,
GigabitEthernet0/0

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

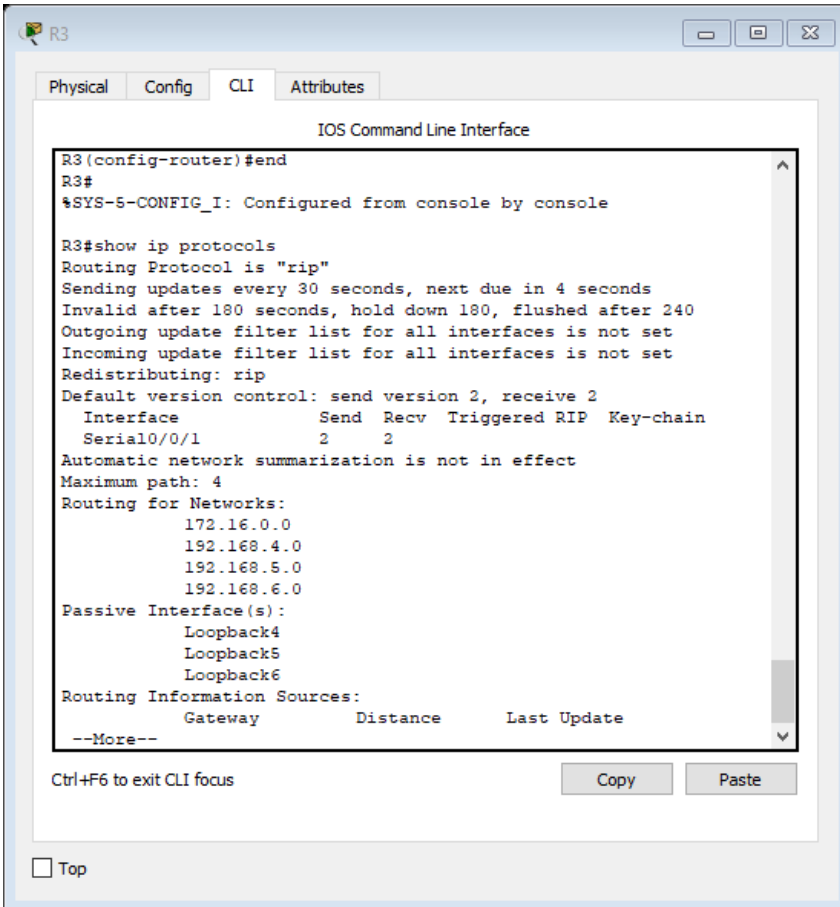
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
R3(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

5. PROTOCOLOS CONFIGURADOS

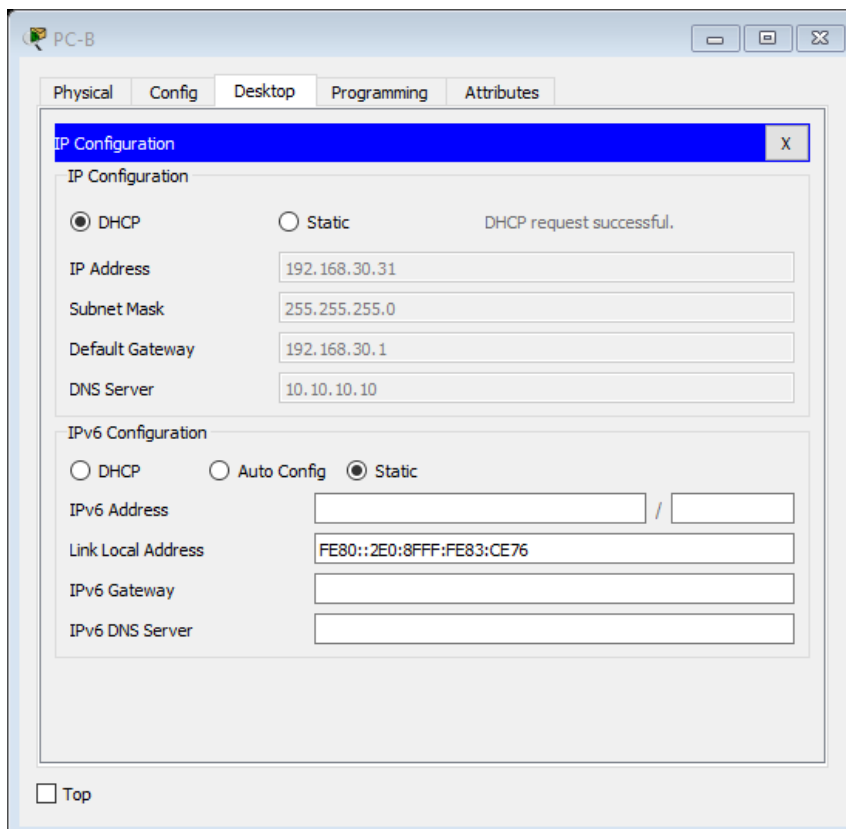
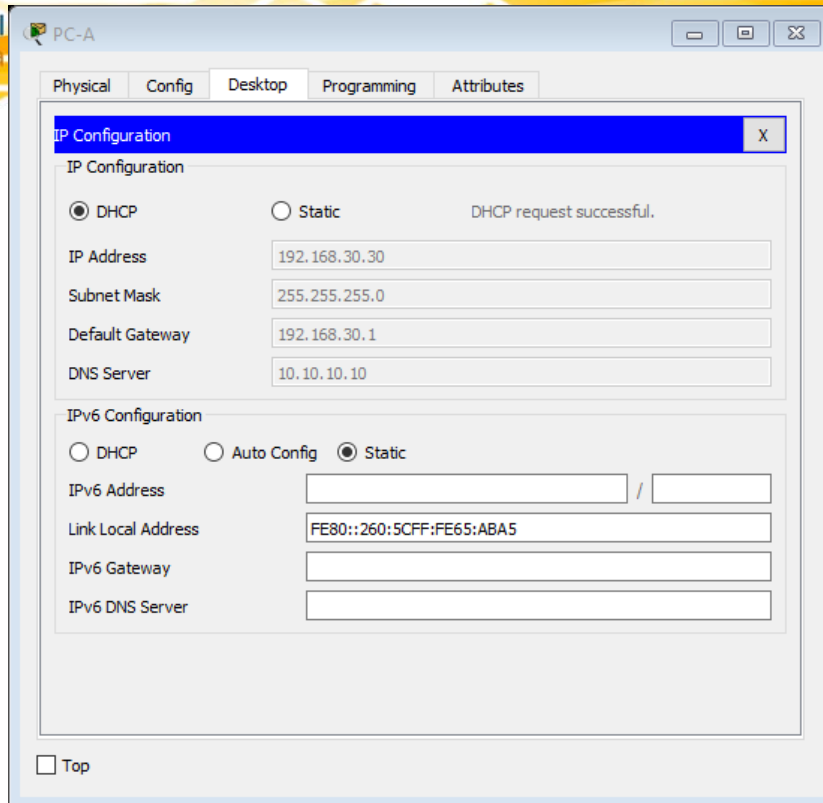


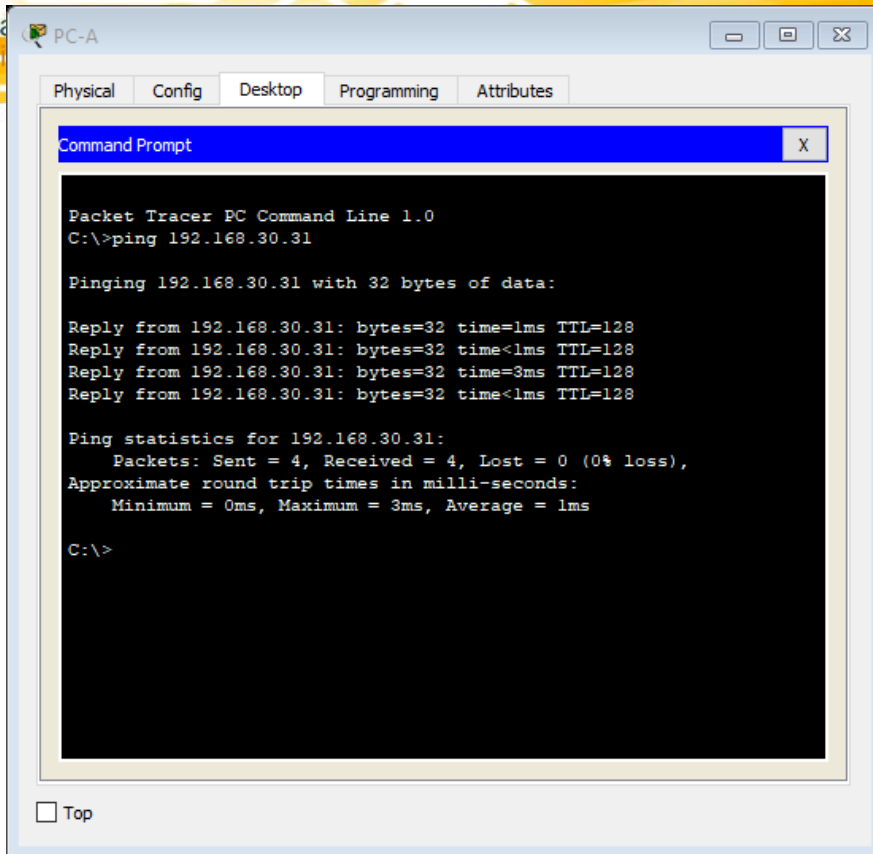
The screenshot shows a Cisco IOS CLI window for router R3. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```
R3 (config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
    Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/1          2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.4.0
    192.168.5.0
    192.168.6.0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
  --More--
```

At the bottom of the CLI window, there are buttons for "Copy" and "Paste", and a "Top" button with a checkbox.





The image shows a screenshot of a Packet Tracer PC Command Line window. The window title is "PC-A" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, showing a "Command Prompt" window. The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.31

Pinging 192.168.30.31 with 32 bytes of data:

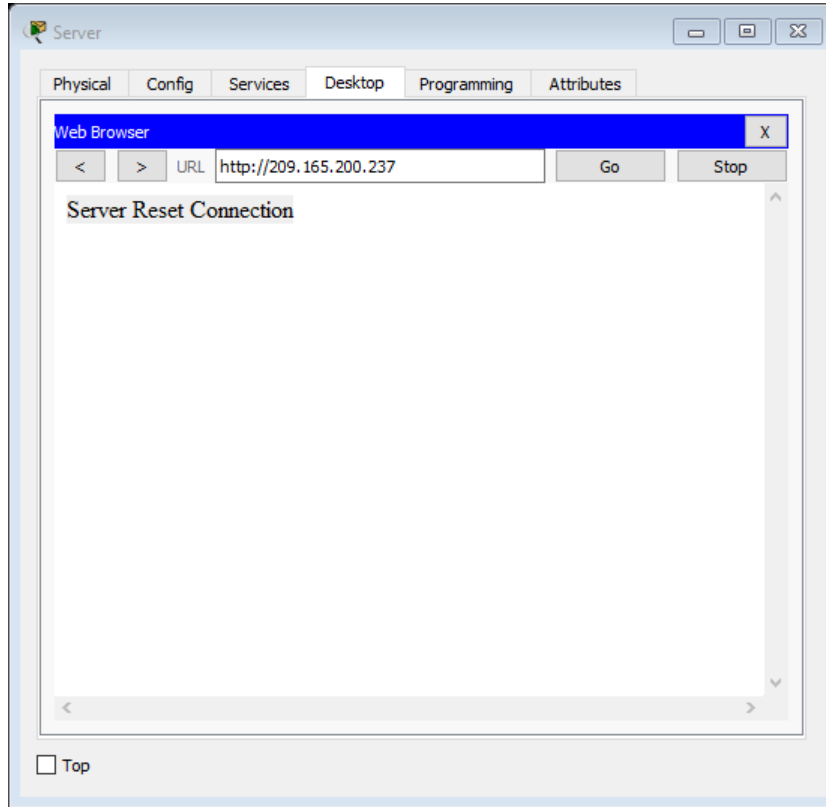
Reply from 192.168.30.31: bytes=32 time<1ms TTL=128
Reply from 192.168.30.31: bytes=32 time<1ms TTL=128
Reply from 192.168.30.31: bytes=32 time=3ms TTL=128
Reply from 192.168.30.31: bytes=32 time<1ms TTL=128

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

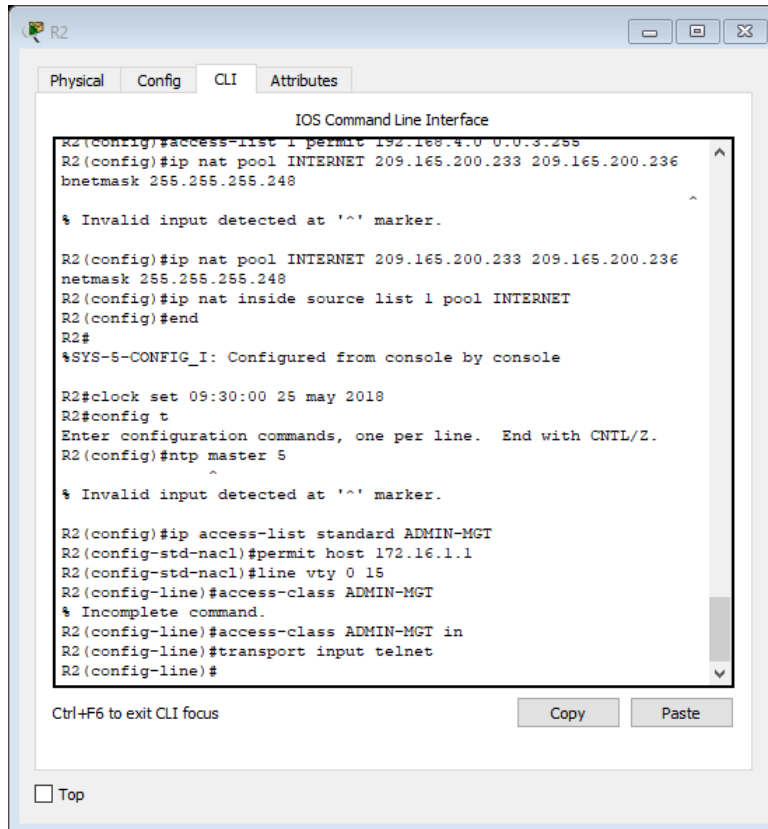
C:\>
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top" which is currently unchecked.

6. SERVER RESET CONNECTION



7. CONFIGURACIÓN DE SEGURIDAD ANTI TELNET



The screenshot shows the CLI window for router R2. The window title is 'R2' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, showing the 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

```
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236
bnetworkmask 255.255.255.248

% Invalid input detected at '^' marker.

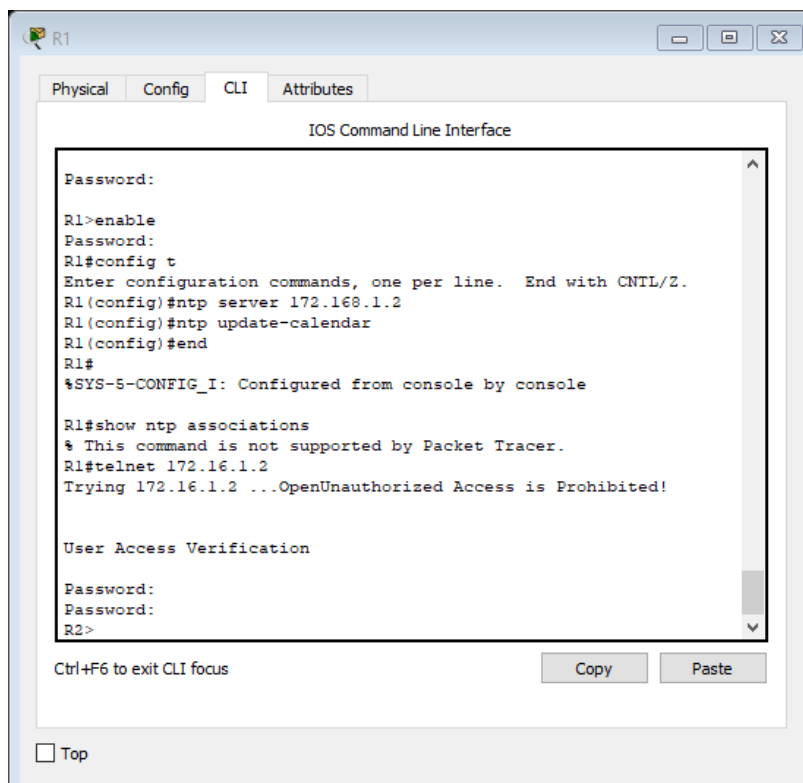
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236
networkmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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)#
```

At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a checkbox for 'Top'.



The screenshot shows the CLI window for router R1. The window title is 'R1' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, showing the 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

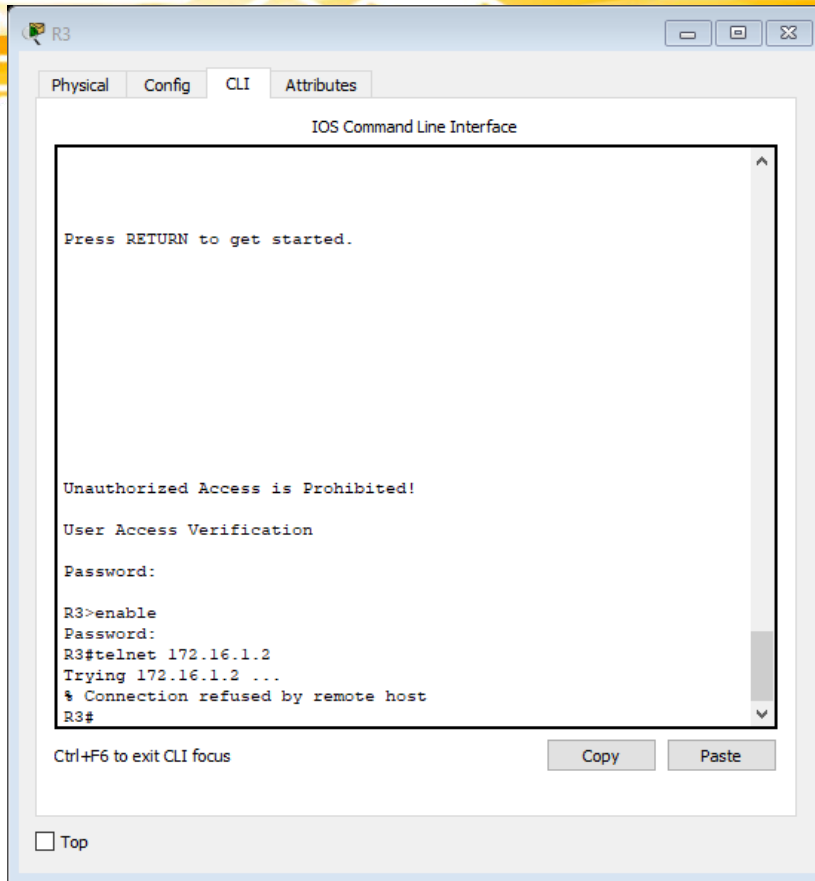
```
Password:
R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.168.1.2
R1(config)#ntp update-calendar
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp associations
% This command is not supported by Packet Tracer.
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!

User Access Verification

Password:
Password:
R2>
```

At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a checkbox for 'Top'.

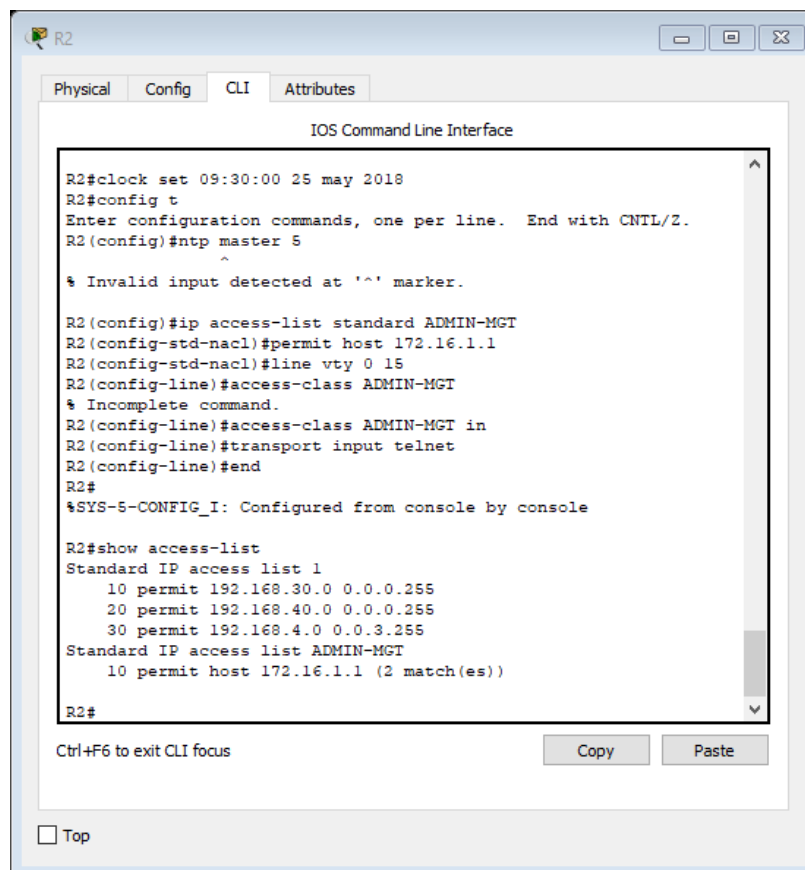


The screenshot shows the CLI interface for router R3. The window title is 'R3'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The text in the terminal window is as follows:

```
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#
```

At the bottom of the terminal window, there are two buttons: 'Copy' and 'Paste'. Below the terminal window, there is a 'Top' button with a checkbox.



The screenshot shows the CLI interface for router R2. The window title is 'R2'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The text in the terminal window is as follows:

```
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#
```

At the bottom of the terminal window, there are two buttons: 'Copy' and 'Paste'. Below the terminal window, there is a 'Top' button with a checkbox.

8. CONCLUSIONES

Los servidores DHCP usan un protocolo de configuración automatizado de redes IP, lo cual elimina la intervención humana en las máquinas clientes.

Ventajas

- Únicamente se configura el servidor que entregara un rango de direcciones, una IP a cada cliente.
- Facilidad de configuración.
- Las direcciones son controladas por el servidor, lo cual logra su fácil seguimiento y supervisión.
- En una red de varios usuarios, el servidor DHCP es necesario para asignación de IP de forma automática.

Desventajas

- En caso de que se requiera un DNS, es necesario configurarlo manualmente para indicar las direcciones IP correspondientes.
- En caso de que el servidor DHCP falle, todas las máquinas clientes renovaran su IP, al no obtener respuesta alguna provocara que toda la red se detenga.

Direcciones IP estáticas

Son direcciones de protocolo de internet, las direcciones estáticas son establecidas por el usuario asignadas a una computadora.

Ventajas

- Al tener una dirección estática son aptos para alojar servidores web indicados fácilmente por los DNS.
- Son aptas para el uso del internet dado que nunca cambian.
- Es fácil seguir el tráfico y supervisar a cada usuario.

Desventajas

- Asignar una IP a cada máquina cliente de la red es una tarea que requiere tiempo y coordinación.
- La actualización de la configuración de la red necesitara de nuevo la configuración de cada IP de la red.
- Las direcciones IP son asignadas a un solo equipo, y al momento que este apagado será una IP invalida.

BIBLIOGRAFIA

Montenegro Morales, L. A. (2008). Estudio e implementación de un servidor privado virtual (VPS), en el laboratorio de computación de la Facultad de Ingeniería, para Hosting Web, DNS, FTP, E-mail, Web mail, DHCP, ISP, Samba, Firewall y NTP bajo software libre (Bachelor's thesis, QUITO/PUCE/2008).

Cheza, C. (2013). Servicios en red (No. 004.7 004.6).

Haskins, R. (2007). ISPadmin: DHCP services. ; login:: the magazine of USENIX & SAGE, 32(1), 59-63.

Hall, E. A. (2000). De rienda suelta a la potencia del protocolo DHCP. Global communications, (42), 70-72.