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

TUTOR

EFRAÍN ALEJANDRO PÉREZ

DIRECTOR

JUAN CARLOS VEGA

PRESENTADO POR:

WILMAR CHACON GONZALEZ

1033703941

GRUPO

203092_33

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

CEAD JOSÉ ACEVEDO Y GÓMEZ

BOGOTA

MAYO 27, 2018

INTRODUCCIÓN

Durante la prueba de habilidades con Packet Tracer en la versión 7.1 afianzamos nuestros conocimientos prácticos, con los laboratorios que se realizaron. Logramos diseñar y efectuar listas de acceso, trabajar con interfaces activas y pasivas, cambiamos asignaciones de ID de routers, armamos redes y verificamos las conectividades y asignamos puertos para VLANs.

Los laboratorios, el trabajo práctico y teórico fueron fundamentales para armar redes, comparar técnicas de seguridad y control, explicar funciones de las capas de enlace, probar cables y hacer diferentes tipos de pruebas de acuerdo a los parámetros básicos requeridos por los dispositivos.

OBJETIVOS

Armar la red y configurar los parámetros básicos de los dispositivos.

Armar la red y verificar la conectividad.

Asignar puertos a la VLAN 2.

Cambiar la preferencia de SDM.

Cambiar las asignaciones de ID del router.

Cambiar las métricas de OSPF.

Configurar DHCP para varias VLAN

Configurar DHCPv4.

Configurar DHCPv4 para la VLAN 1.

Configurar DHCPv4 para la VLAN 2.

Configurar interfaces OSPF pasivas.

Configurar IPv6 en los dispositivos.

Configurar la red para DHCPv6 con estado.

Configurar la red para DHCPv6 sin estado.

Configurar la red para SLAAC.

Configurar las ACL en R1 y R3 para mitigar los ataques.

Configurar una interfaz pasiva.

Configurar una ruta predeterminada.

Configurar y aplicar una ACL a líneas VTY.

Configurar y aplicar una ACL estándar designada.

Configurar y verificar el routing OSPF.

Configurar y verificar el routing OSPFv3.

Configurar y verificar el routing RIPng.

Configurar y verificar el routing RIPv2

Configurar y verificar la NAT dinámica.

Configurar y verificar la NAT estática.

Configurar y verificar PAT.

Configurar y verificar que se esté ejecutando RIPng en los routers.

Configurar y verificar que se esté ejecutando RIPv2 en los routers.

Configurar y verificar un conjunto de NAT con sobrecarga.

Configurar, aplicar y verificar una ACL de IPv6.

Configurar, aplicar y verificar una ACL estándar.

Configurar, aplicar y verificar una segunda ACL de IPv6.

Crear rutas estáticas.

Desactivar la sumarización automática.

Establecer la preferencia de SDM en lanbase-routing en el S1.

Examinar las tablas de routing.

Habilitar el routing IP.

Habilite el routing IP en el switch.

Planificar una implementación de ACL.

Utilizar las ACL para garantizar el acceso remoto a los enrutadores solo está disponible desde la estación de administración PC-C.

Verificar la conectividad de extremo a extremo.

Verificar la conectividad entre dispositivos antes de la configuración del firewall.

Verificar la conectividad y DHCPv4.

Verificar la funcionalidad de ACL.

Verificar la implementación de ACL.

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 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.

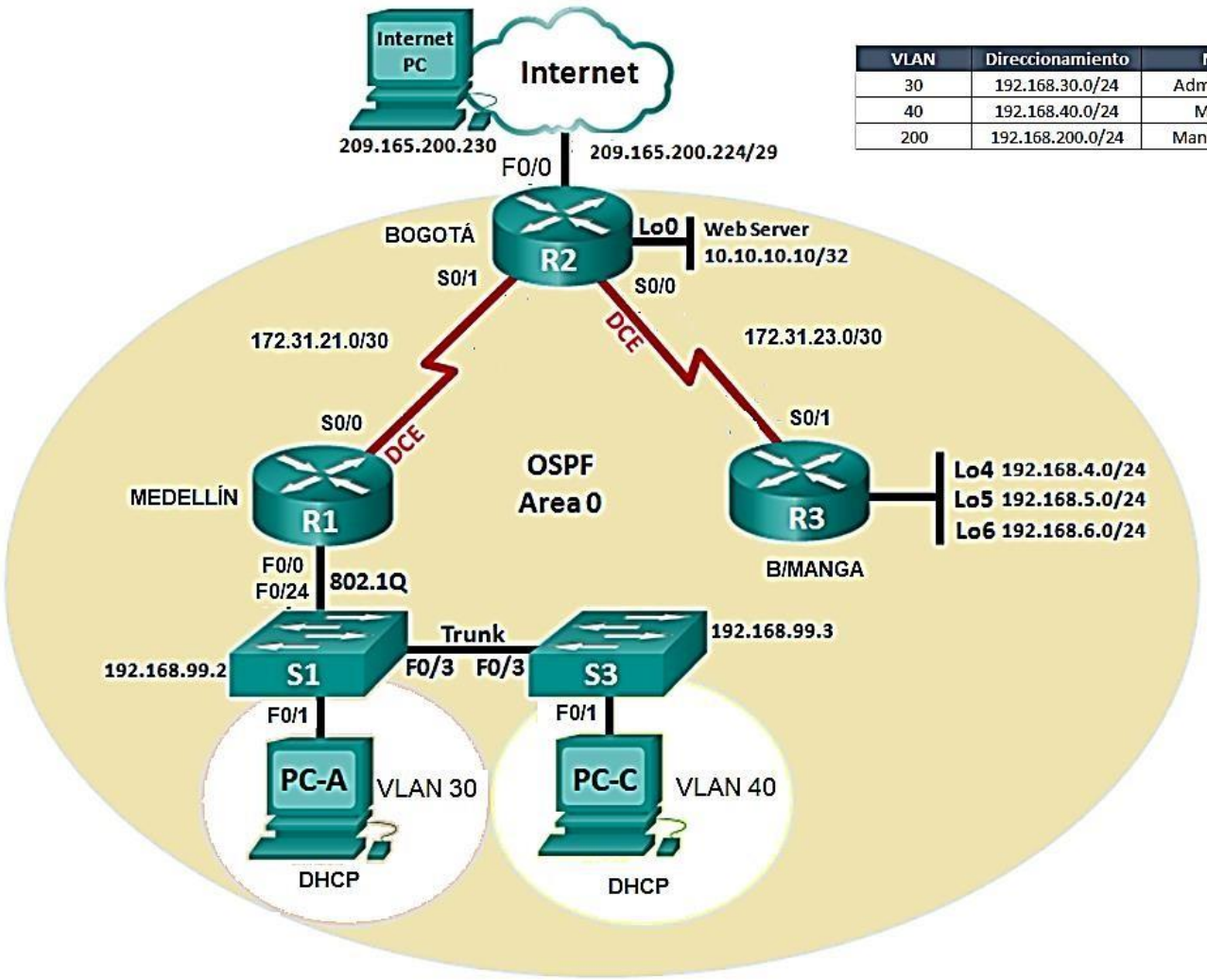
Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado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

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 DNSlookup
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.

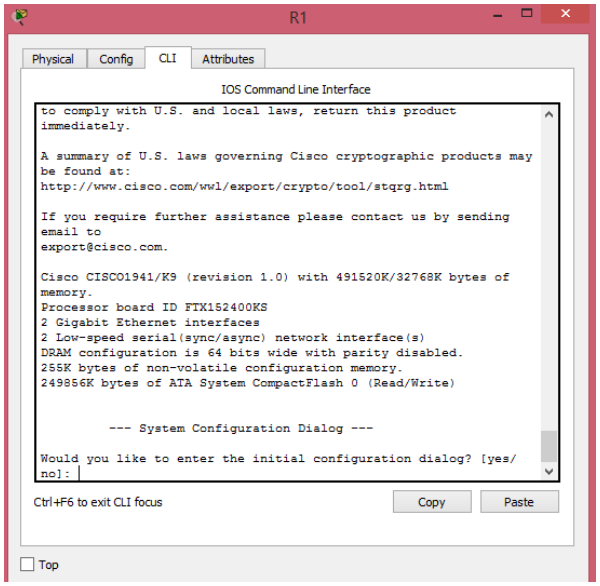
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

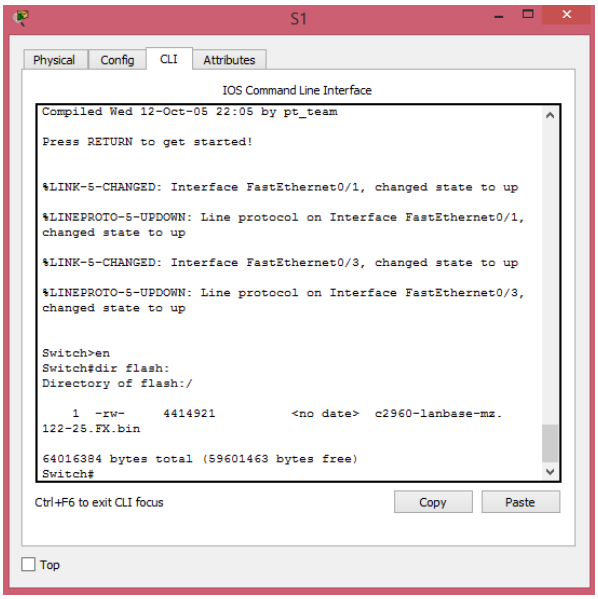
10. Configurar NAT en R2 para permitir que los host puedan salir a internet

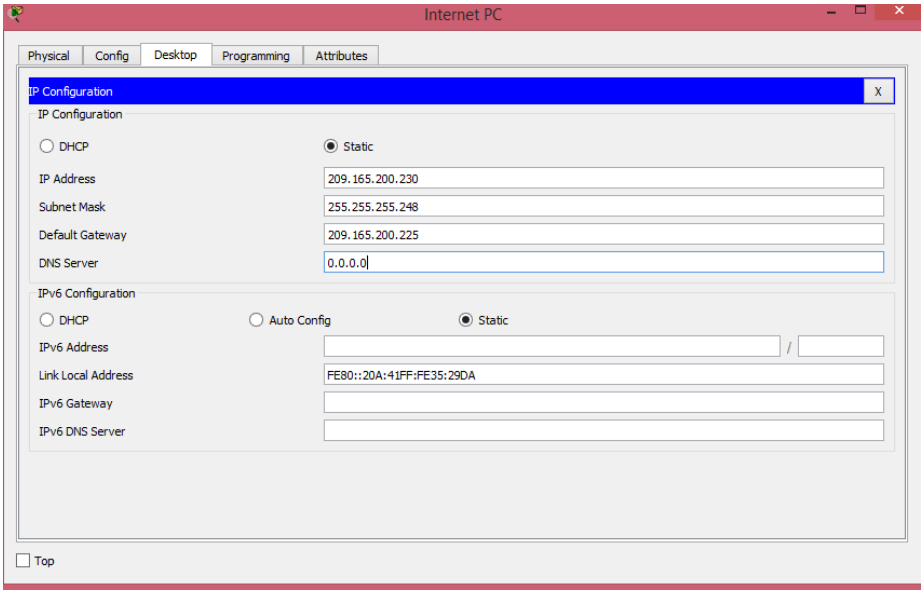
11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

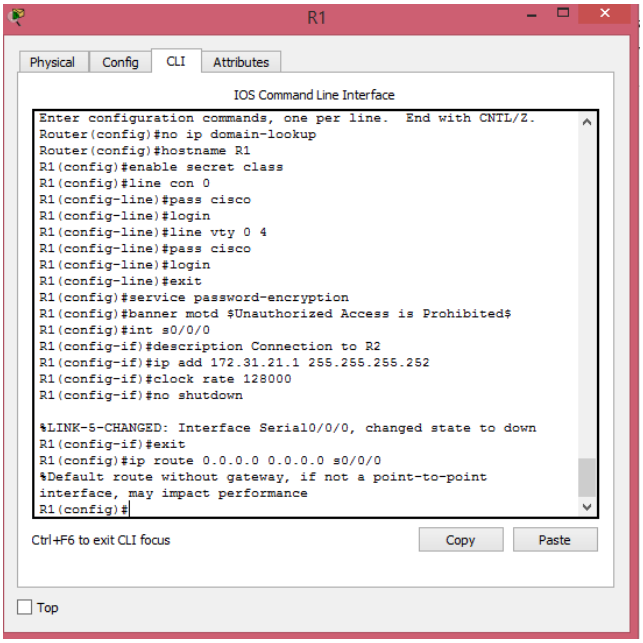
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

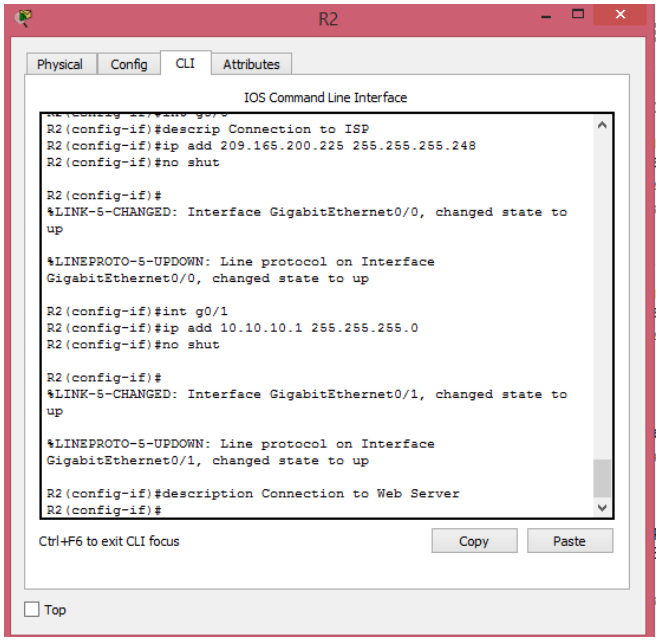
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

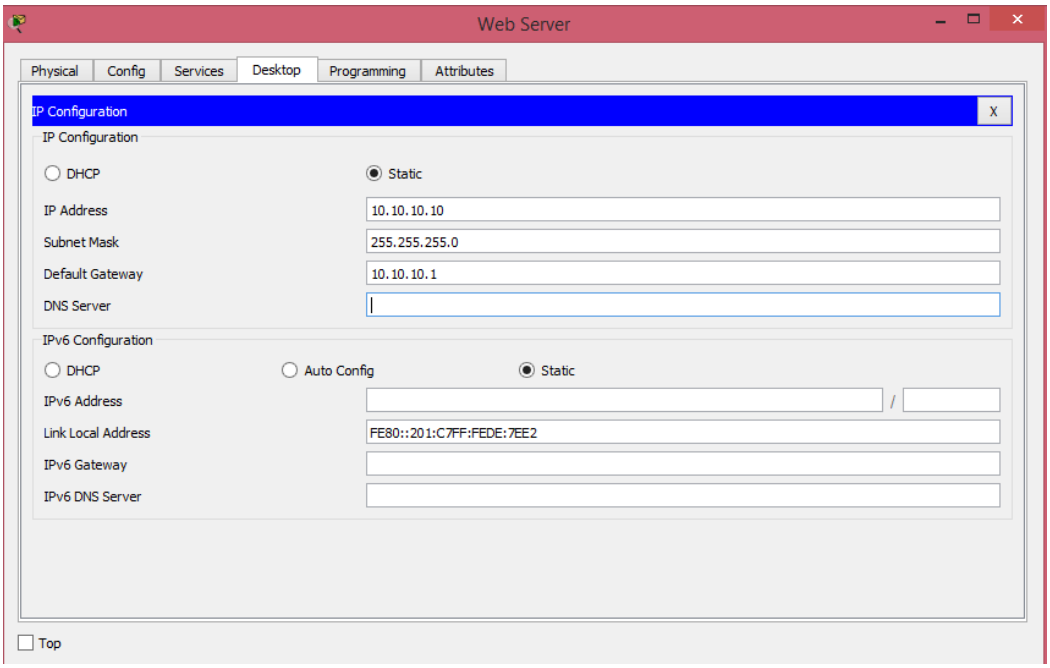


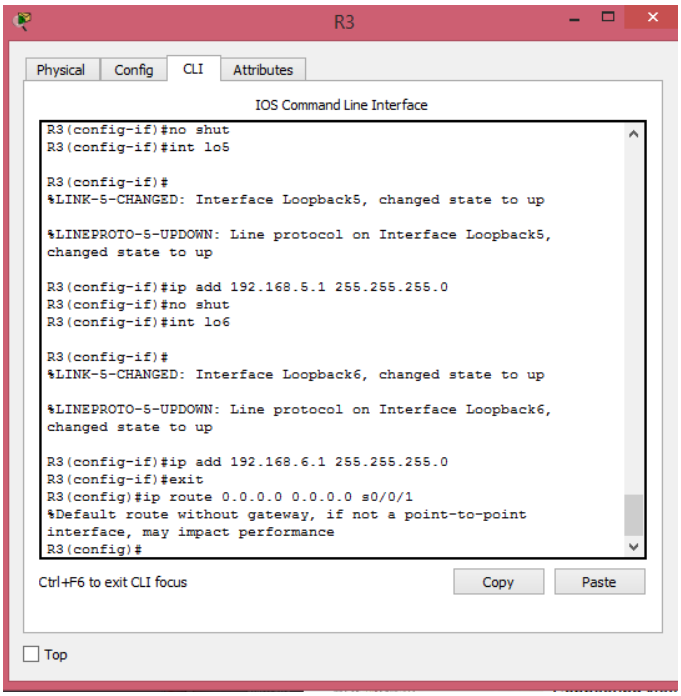


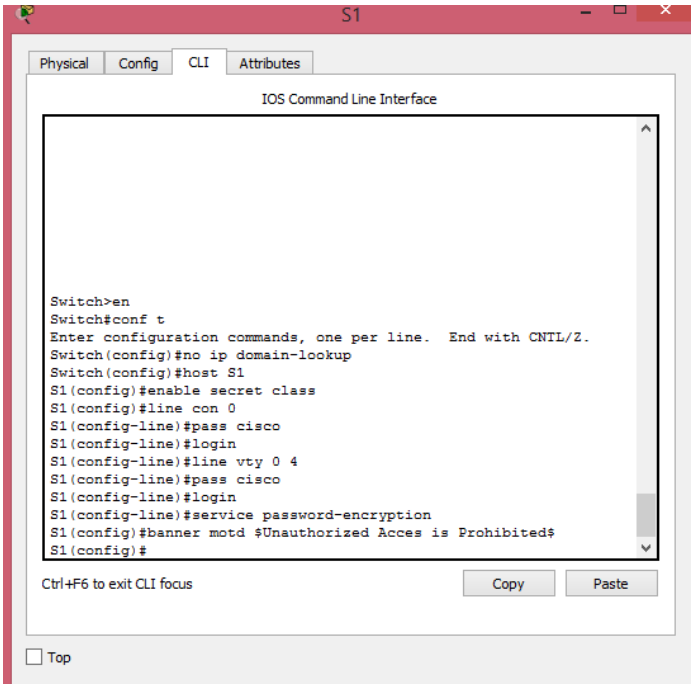


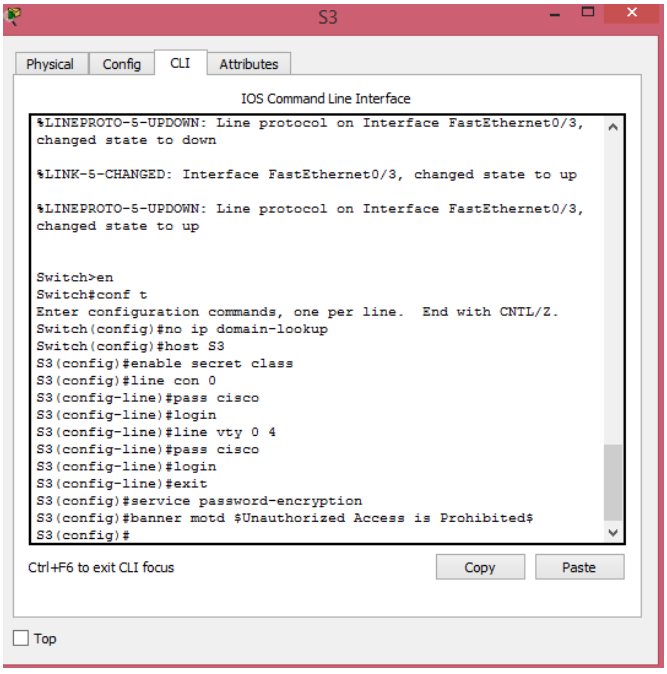

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd $Unauthorized Access is Prohibited$
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip add 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

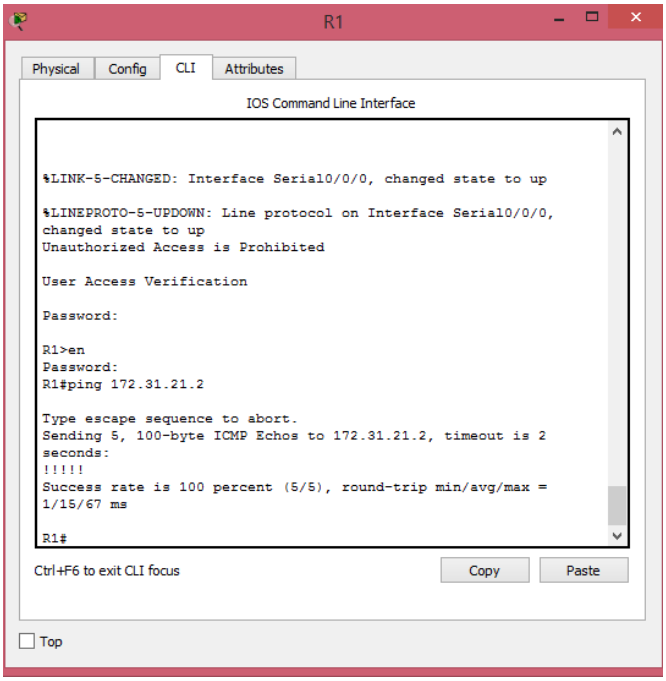

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2(config-if)#descrip Connection to ISP
R2(config-if)#ip add 209.165.200.225 255.255.255.248
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R2(config-if)#int g0/1
R2(config-if)#ip add 10.10.10.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R2(config-if)#description Connection to Web Server
R2(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

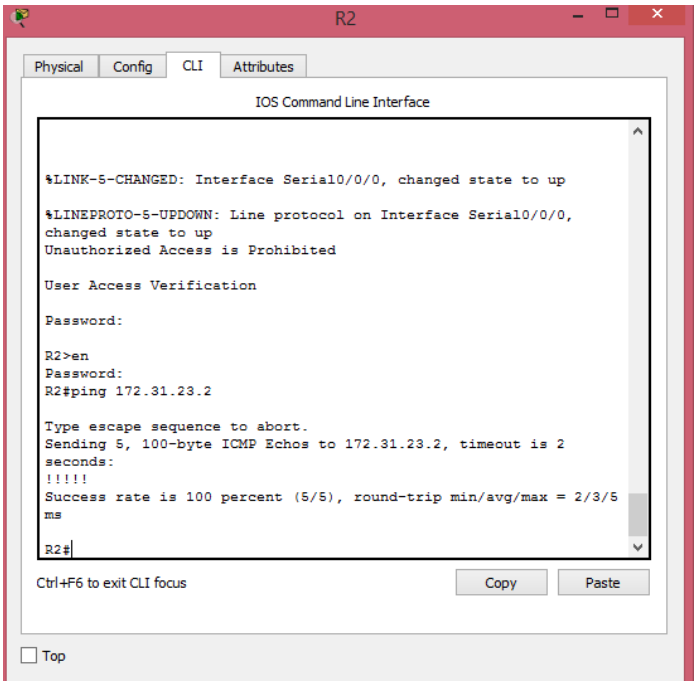

Web Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.10.10.10
Subnet Mask
255.255.255.0
Default Gateway
10.10.10.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:C7FF:FEDE:7EE2
IPv6 Gateway
IPv6 DNS Server
Top

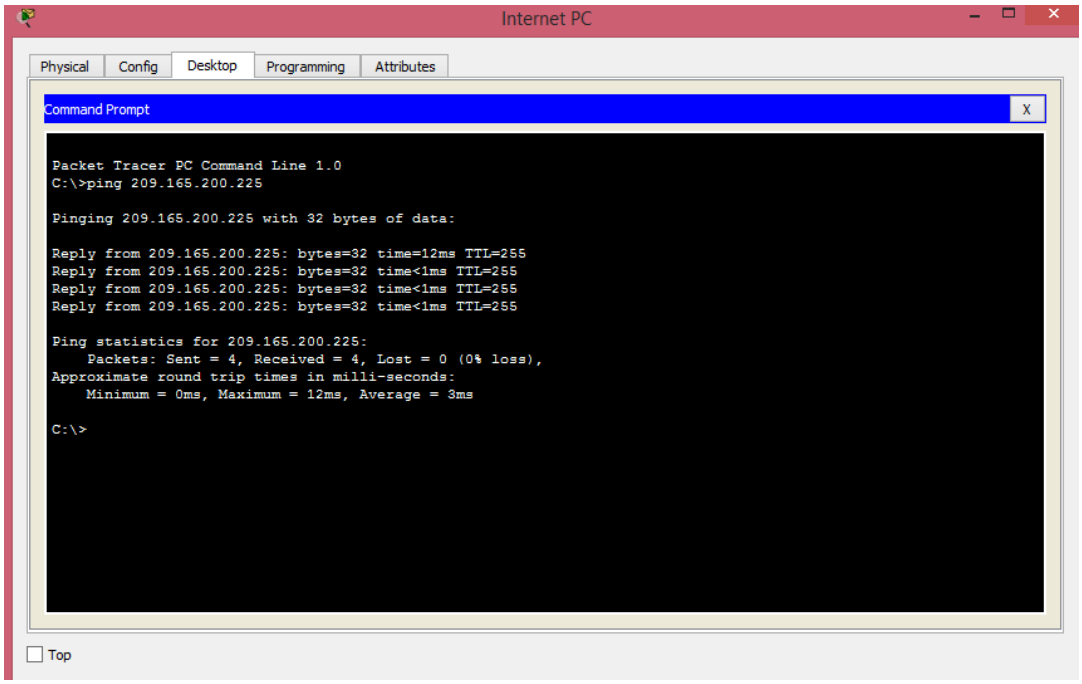

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3(config-if)#no shut
R3(config-if)#int lo5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo6
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 add 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

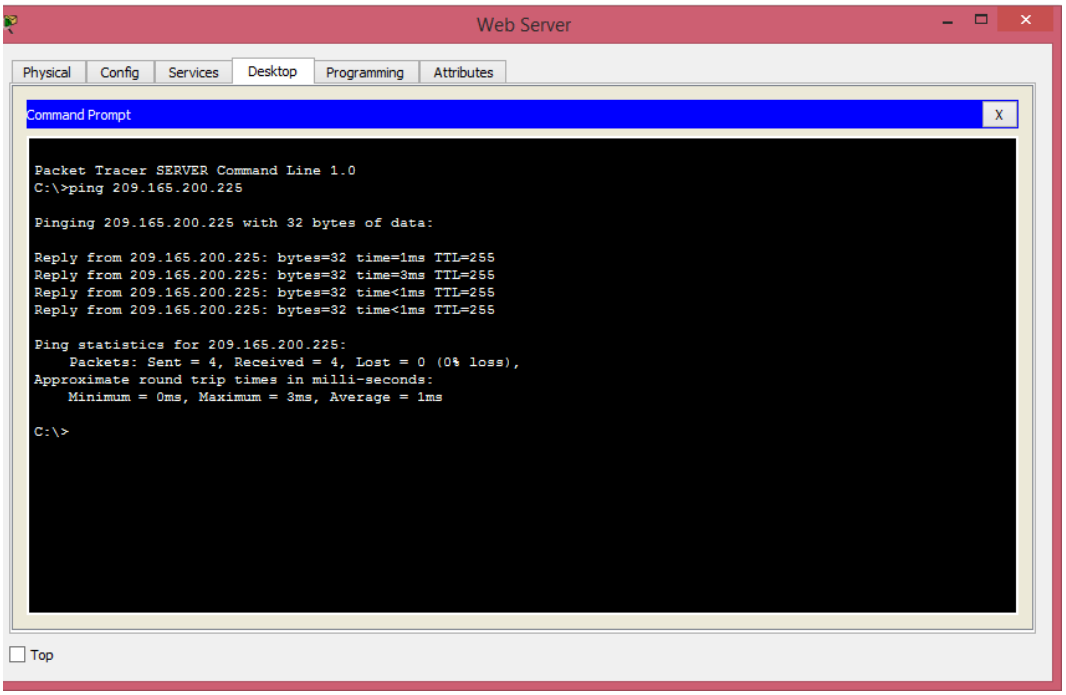

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host S1
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd $Unauthorized Acces is Prohibited$
S1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

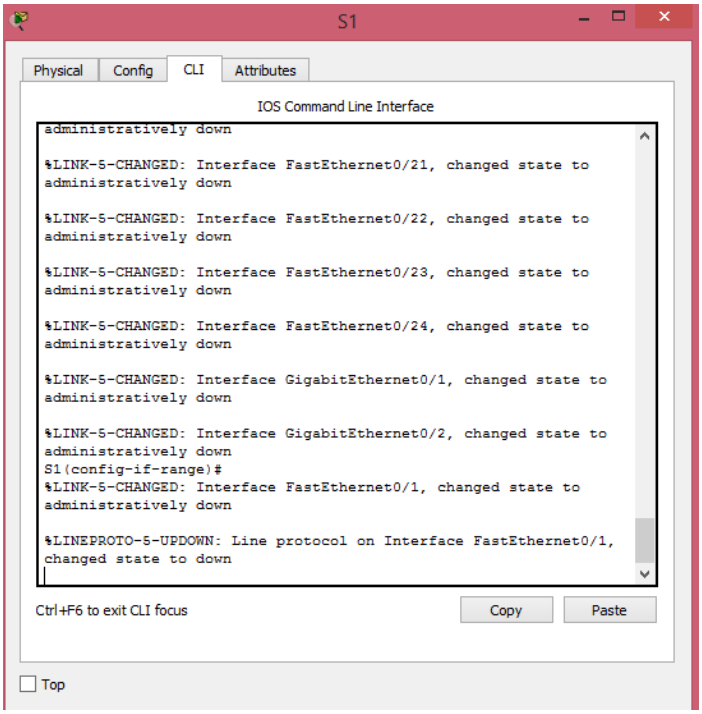

S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd $Unauthorized Access is Prohibited$
S3(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

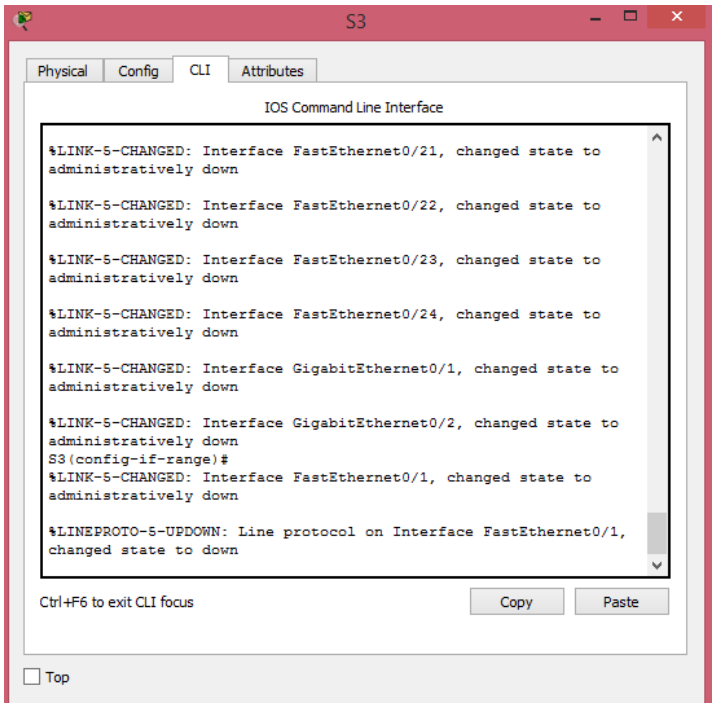

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Unauthorized Access is Prohibited
User Access Verification
Password:
R1>en
Password:
R1#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/67 ms
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

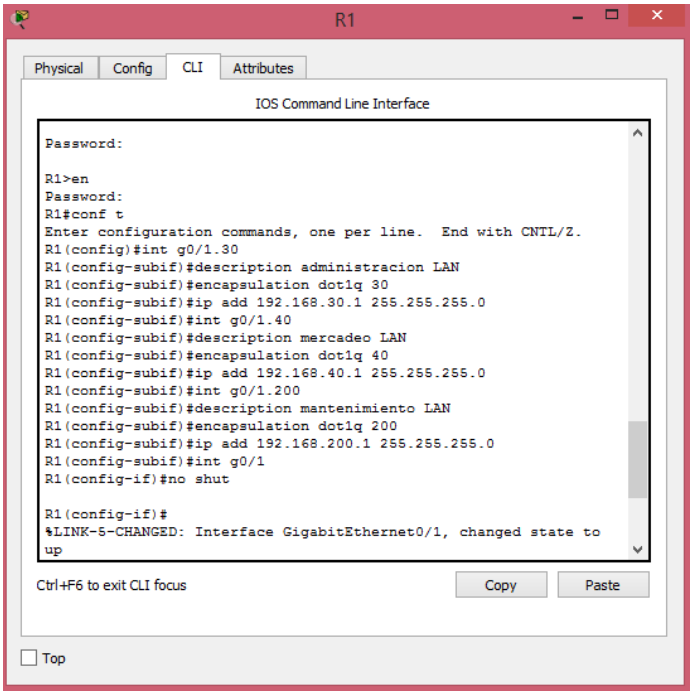

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Unauthorized Access is Prohibited
User Access Verification
Password:
R2>en
Password:
R2#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
R2#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

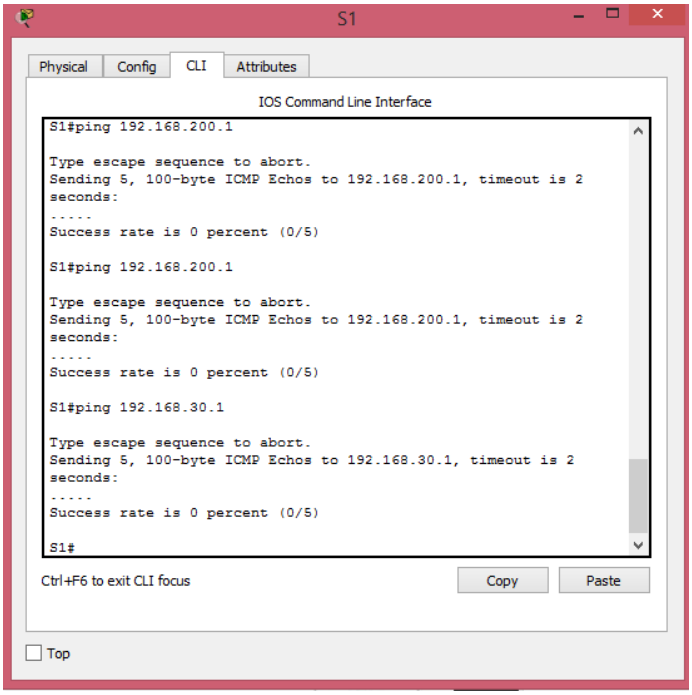

Internet PC
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=12ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
C:\>
Top

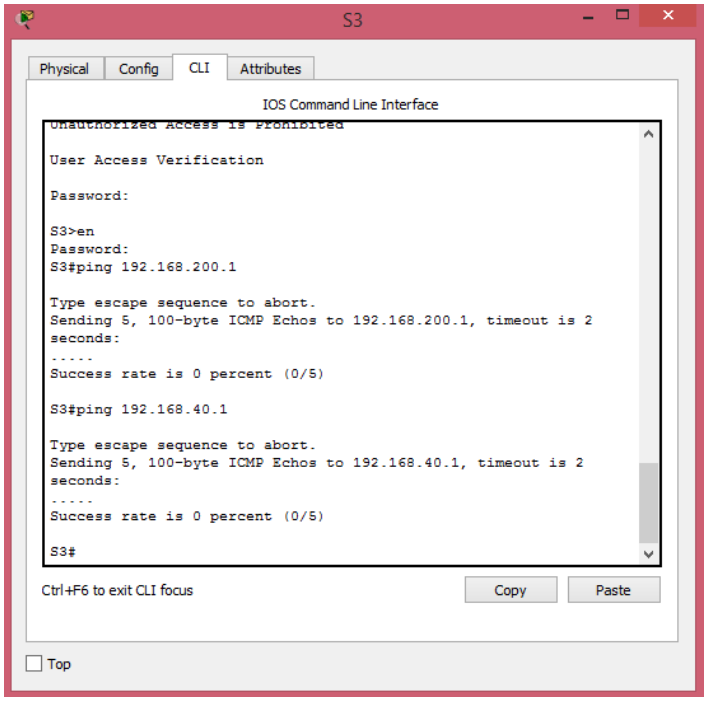

Web Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time=3ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms
C:\>
Top

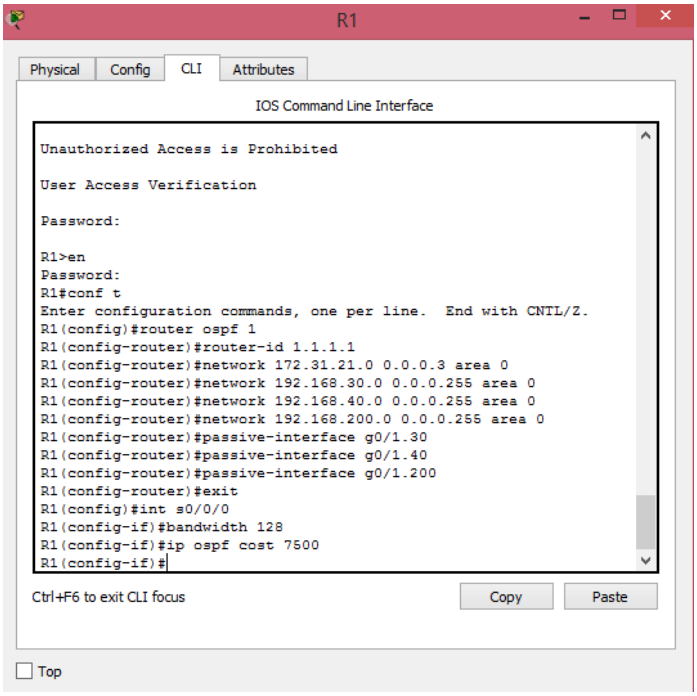

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed 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)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

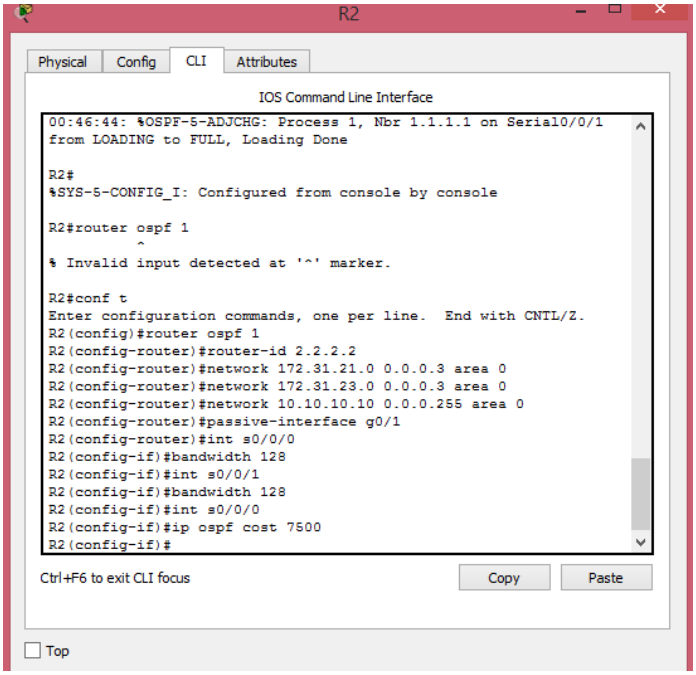

S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively 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
S3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

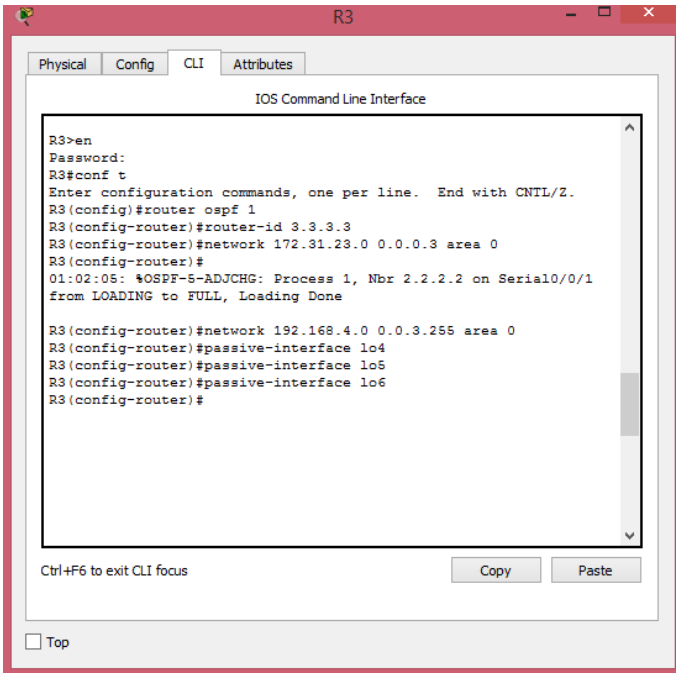

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.30
R1(config-subif)#description administracion LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/1.40
R1(config-subif)#description mercadeo LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/1.200
R1(config-subif)#description mantenimiento LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

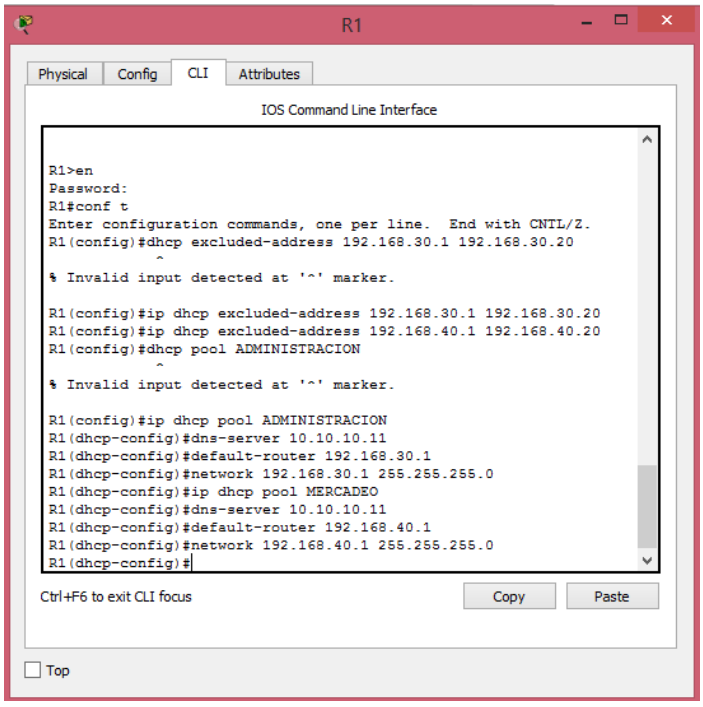

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S1#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S1#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

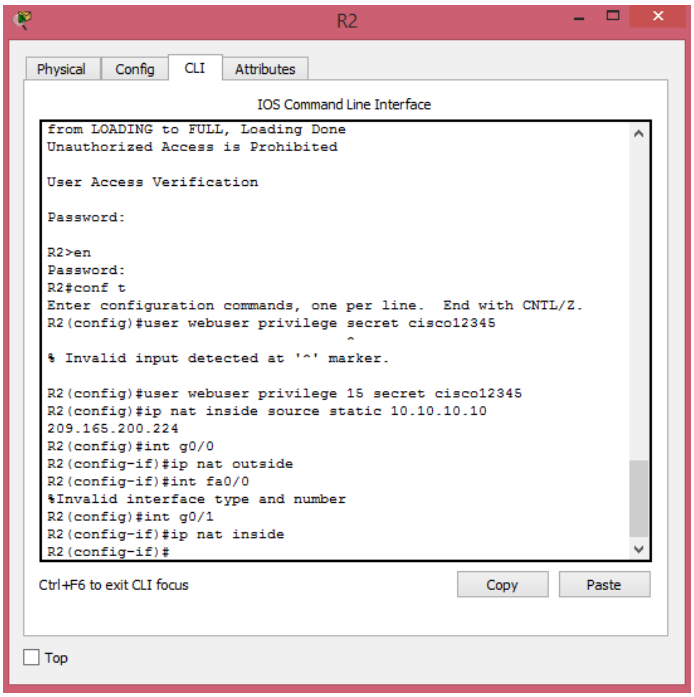

S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Unauthorized Access is Prohibited
User Access Verification
Password:
S3>en
Password:
S3#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
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 0 percent (0/5)
S3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

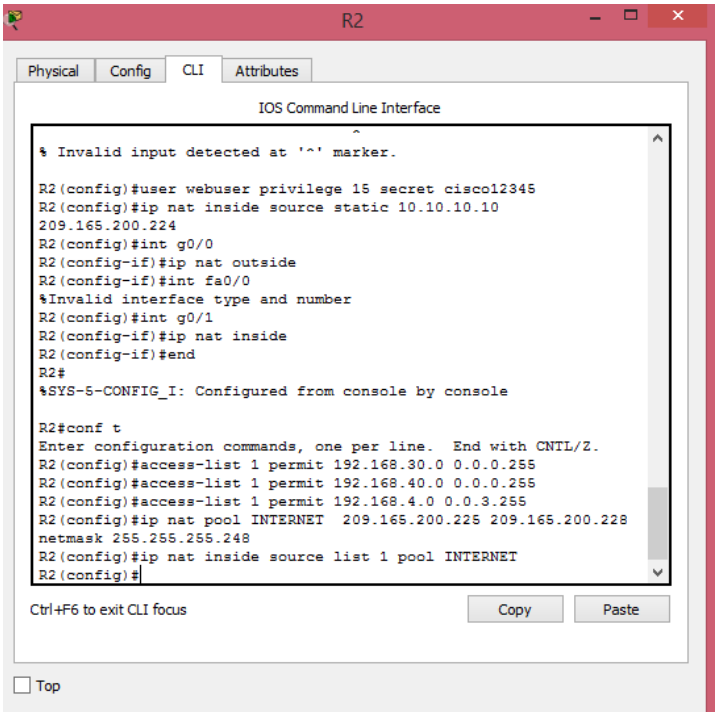

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Unauthorized Access is Prohibited
User Access Verification
Password:
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 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)#exit
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

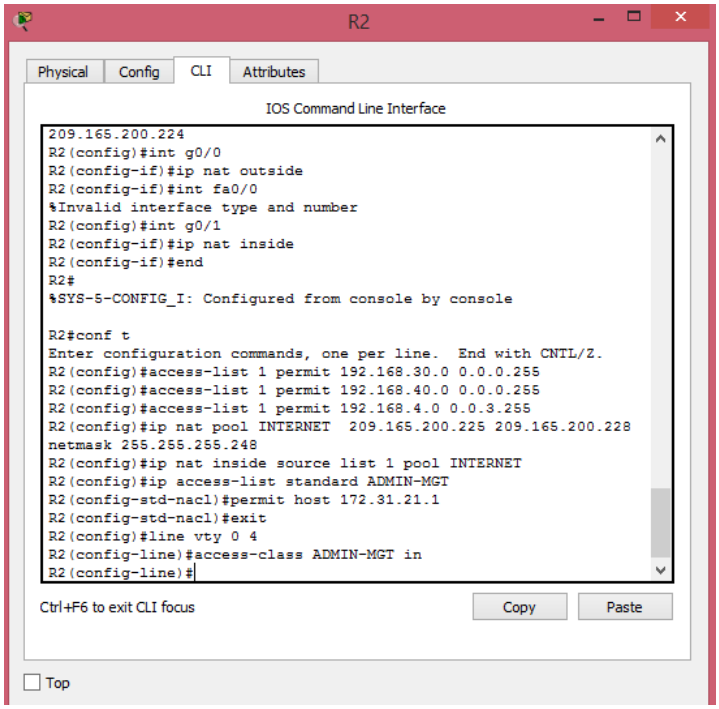

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
00:46:44: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1
from LOADING to FULL, Loading Done
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#router ospf 1
^
% Invalid input detected at '^' marker.
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#passive-interface g0/1
R2(config-router)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/0
R2(config-if)#ip ospf cost 7500
R2(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

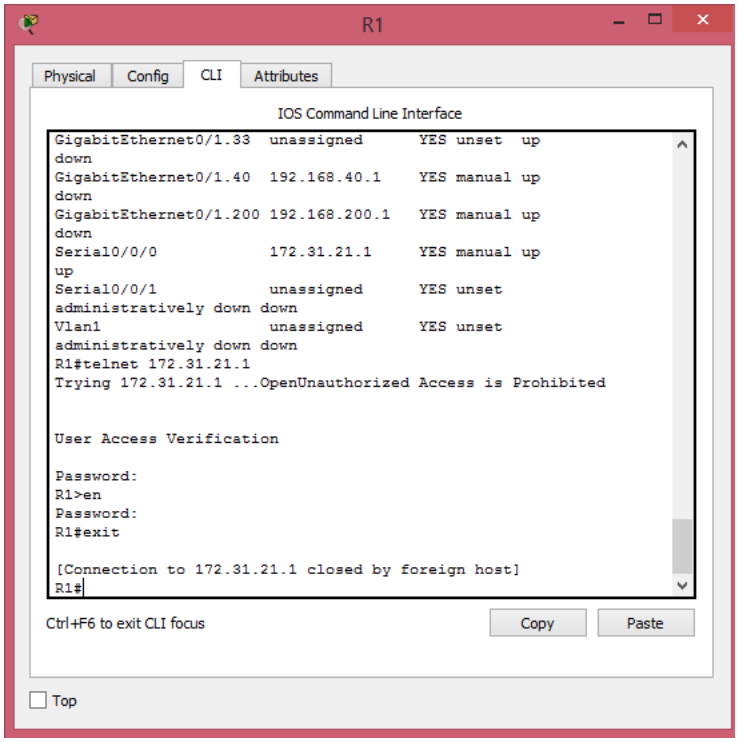

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#
01:02:05: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

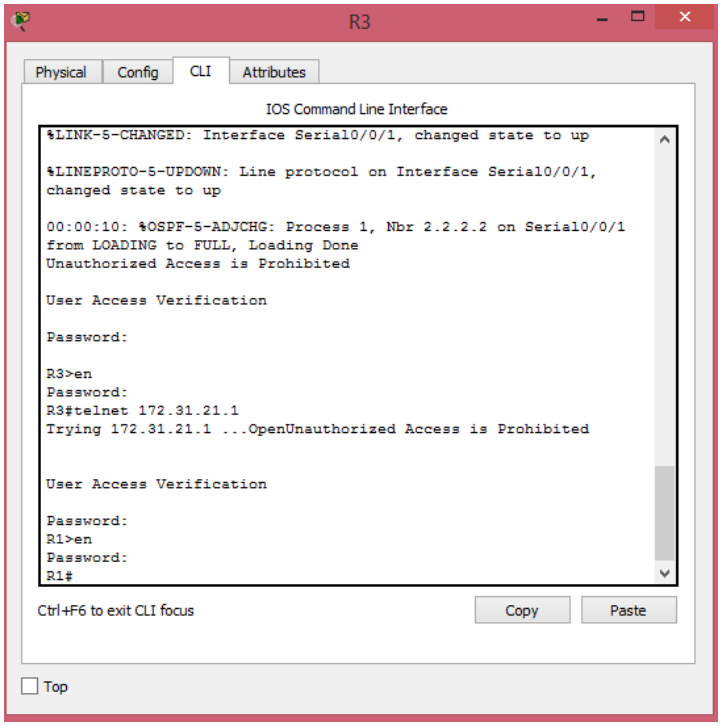

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#dhcp excluded-address 192.168.30.1 192.168.30.20
^
% Invalid input detected at '^' marker.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.20
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.20
R1(config)#dhcp pool ADMINISTRACION
^
% Invalid input detected at '^' marker.
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.1 255.255.255.0
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.1 255.255.255.0
R1(dhcp-config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

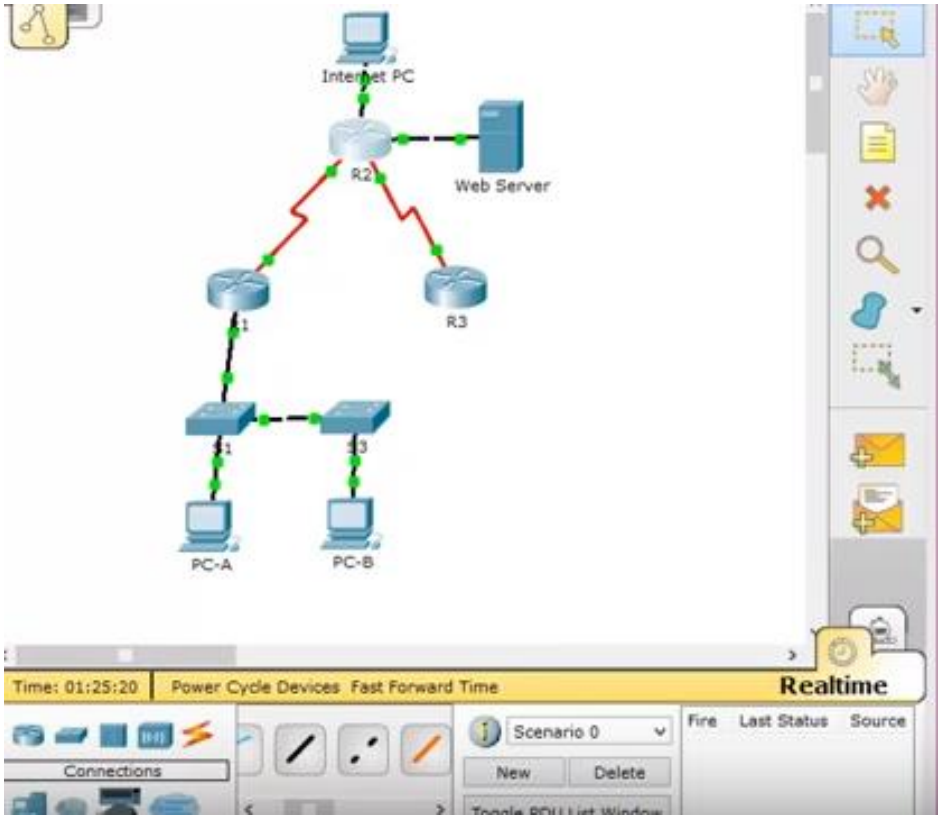

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
from LOADING to FULL, Loading Done
Unauthorized Access is Prohibited
User Access Verification
Password:
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege secret cisco12345
^
% Invalid input detected at '^' marker.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10
209.165.200.224
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int fa0/0
%Invalid interface type and number
R2(config)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#
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)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10
209.165.200.224
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int fa0/0
%Invalid interface type and number
R2(config)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
209.165.200.224
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int fa0/0
%Invalid interface type and number
R2(config)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
GigabitEthernet0/1.33 unassigned YES unset up
down
GigabitEthernet0/1.40 192.168.40.1 YES manual up
down
GigabitEthernet0/1.200 192.168.200.1 YES manual up
down
Serial0/0/0 172.31.21.1 YES manual up
up
Serial0/0/1 unassigned YES unset
administratively down down
Vlan1 unassigned YES unset
administratively down down
R1#telnet 172.31.21.1
Trying 172.31.21.1 ...OpenUnauthorized Access is Prohibited
User Access Verification
Password:
R1>en
Password:
R1#exit
[Connection to 172.31.21.1 closed by foreign host]
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%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
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done
Unauthorized Access is Prohibited
User Access Verification
Password:
R3>en
Password:
R3#telnet 172.31.21.1
Trying 172.31.21.1 ...OpenUnauthorized Access is Prohibited
User Access Verification
Password:
R1>en
Password:
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Internet PC
R2
Web Server
R3
PC-A
PC-B
Time: 01:25:20
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Scenario 0
New
Delete
Fire
Last Status
Source

CONCLUSIONES

- La Lista de control de acceso de Cisco (ACL) se usa para filtrar el tráfico según un criterio de filtrado determinado en un enrutador o interfaz de conmutador. En función de las condiciones proporcionadas por la ACL, un paquete está permitido o bloqueado para un mayor movimiento.
- La NAT dinámica es útil cuando hay menos direcciones disponibles que la cantidad real de hosts que se traducirán. Crea una entrada en la tabla NAT cuando el host inicia una conexión y establece una correspondencia de uno a uno entre las direcciones. Sin embargo, el mapeo puede variar dependiendo de la dirección registrada disponible en el grupo en el momento de la comunicación. Dynamic NAT permite que las sesiones se inicien solo desde redes internas o externas para las que está configurado. Las entradas NAT dinámicas se eliminan de la tabla de traducción si el host no se comunica durante un período específico configurable. La dirección se devuelve al grupo para que la use otro host.
- La NAT estática y dinámica también se puede configurar simultáneamente en el mismo dispositivo. Esto es necesario cuando los hosts brindan servicios de aplicaciones y cuando los hosts que necesitan conectarse a Internet comparten menos direcciones IP válidas.
- La Traducción de direcciones de red (NAT) reemplaza las direcciones IP dentro de un paquete con diferentes direcciones IP. Es útil para conservar la dirección IP y conectar una red privada usando una dirección no registrada a una red pública como Internet. Los dos tipos principales de configuraciones NAT son estáticas y dinámicas.
- Las ACL para el filtrado de tráfico TCP/IP se dividen principalmente en dos tipos que son las listas de acceso estándar, y las listas de acceso extendidas

REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module 7/index.html#7.0.1.1

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

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/ index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/ index.html#11.0.1.1

Onedrive
https://onedrive.live.com/?id=5740FF51A2590A8B%211008&cid=5740FF51A2590A8B