Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN)

Actividad Colaborativa Unidad 4
Grupo 203092_25

Realizado por:

Edgar Jovanny Larrota
Daniel Eduardo Cáceres
Jullian Paola Villalobos
Rafael Antonio Quiroga García
Lady Alejandra Gómez Torres

Presentado a:
Martha Fabiola Contreras Higuera

Universidad Nacional Abierta y a Distancia (UNAD)
Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI
Junio, 2017

Contenido

Introducción

El presente trabajo pretende profundizar en aspectos de diseño e implementación de soluciones integradas LAN / WAN, orientándonos a realizar configuraciones, conocer e implementar protocolos y estándares de seguridad; acorde a las instalaciones de redes que se implementen y teniendo presente las normas establecidas que el Cisco exige, ya sea a nivel empresarial o personal. Lo anterior con el fin de obtener instalaciones seguras y adquirir conocimientos pertinentes para la protección de este tipo de redes.

De acuerdo al laboratorio propuesto se incorporó diversas etapas para alcanzar la solución de las actividades y los objetivos planteados, considerando básicamente:

1. Comprender el punto de partida; de cómo el grupo colaborativo visualizo e interpretó el problema, la necesidad o la motivación para la adquisición de los temas a desarrollar.

2. Búsqueda de recursos que nos diera una concepción adecuada de información previa a su desarrollo.

3. Realización de los procedimientos e implementación del software Packet Tracer

Entre los resultados que pretendemos conseguir con este Ejercicio y que aplican a la parte práctica, está en conocer la planificación y ejecución de proyectos similares en redes integradas LAN / WAN, que nos permita identificar las principales dificultades, sus ventajas, las posibles mejoras de elaboración, e impactos, establecer la utilidad, los costos y beneficios e identificar parámetros de diseño y optimización. Y a nivel personal en el mejoramiento de nuestro desarrollo personal y profesional, el cual consiste en brindar soluciones tecnológicas innovadoras para satisfacer las necesidades y problemáticas derivadas hacia este tipo de alternativas.

En esta unidad se abarcan varias temáticas que aplican al desarrollo de las actividades propuestas para este, continuando con la herramienta PacketTracer.

Trataremos temas como la configuración del protocolo RIP que es poco utilizado en las redes modernas pero muy útil en las redes pequeñas pero si se requiere para redes de gran tamaño también veremos el protocolo OSPF el cual nos ayudara a detectar fallas de enlace y poder realizar actualizaciones.

Objetivos

Objetivo General

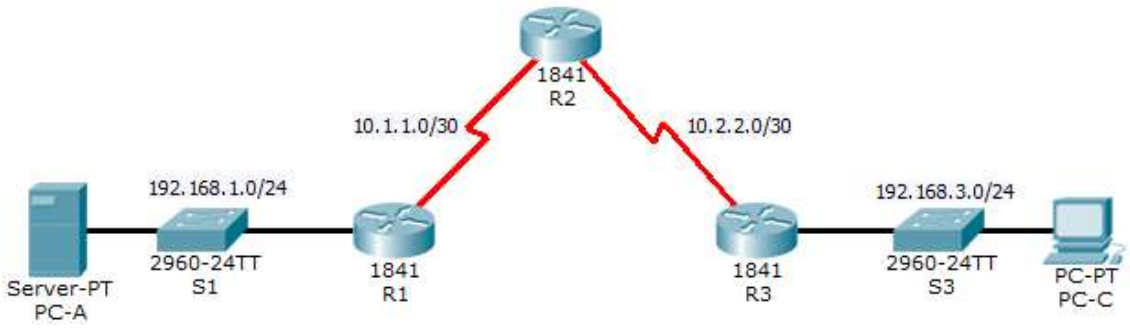
Desarrollar destreza y conocimientos relacionados a la construcción y protección de la Redes LAN / WAN.

Objetivos Específicos

- Adquirir conceptos básicos para implementar configuraciones en una red
- Conocer los componentes necesarios para instalar redes sencillas inicialmente
- Conceptualizar sobre los diferentes protocolos y estándares de seguridad

Ejercicio 4.4.1.2

Packet Tracer - Configure IP ACLs to Mitigate Attacks



Addressing Table

Device	Interface	IPAddress	Subnet Mask	DefaultGateway	SwitchPort
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objetives

Verify connectivity among devices before firewall configuration.

Use ACLs to ensure remote access to the routers is available only from management station PC-C.

Configure ACLs on R1 and R3 to mitigate attacks.

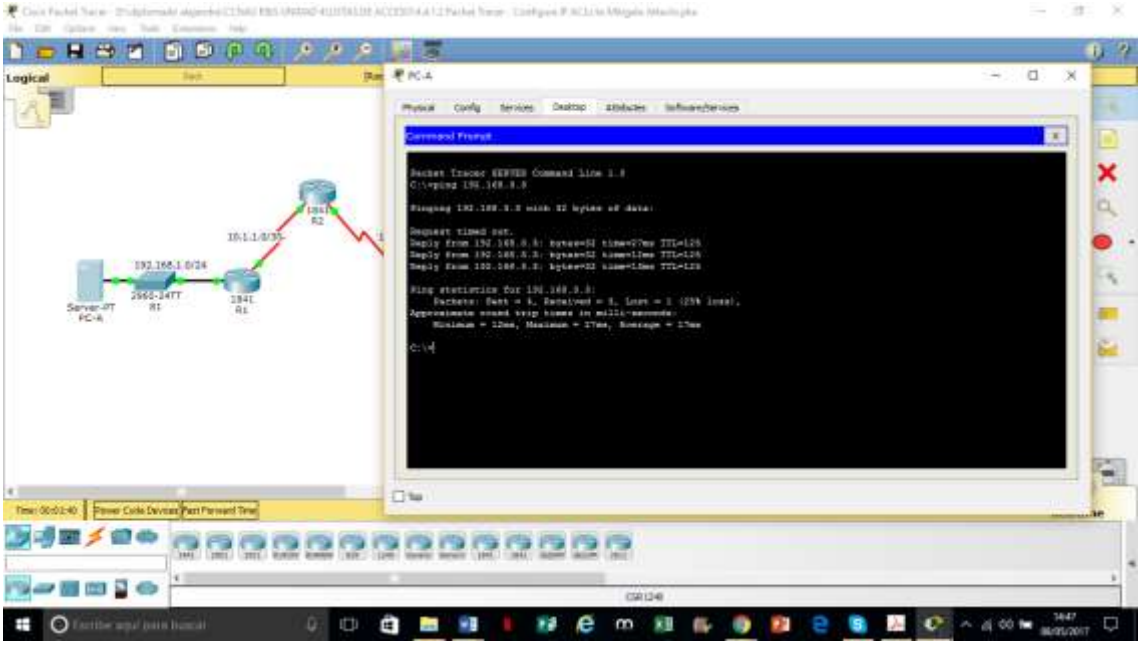
Verify ACL functionality.

Background / Scenario

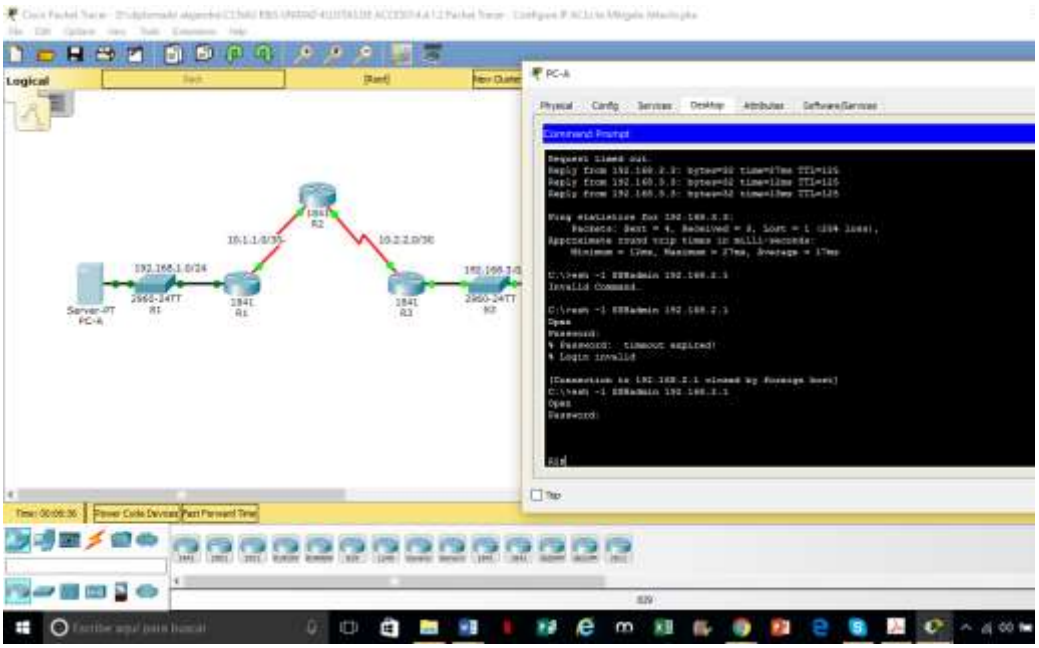
Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.
The routers have been pre-configured with the following:
Enable password: ciscoenpa55
Password for console: ciscoconpa55
Username for VTY lines: SSHadmin
Password for VTY lines: ciscosshpa55
IP addressing
Static routing
Part 1: Verify Basic Network Connectivity
Verify network connectivity prior to configuring the IP ACLs.

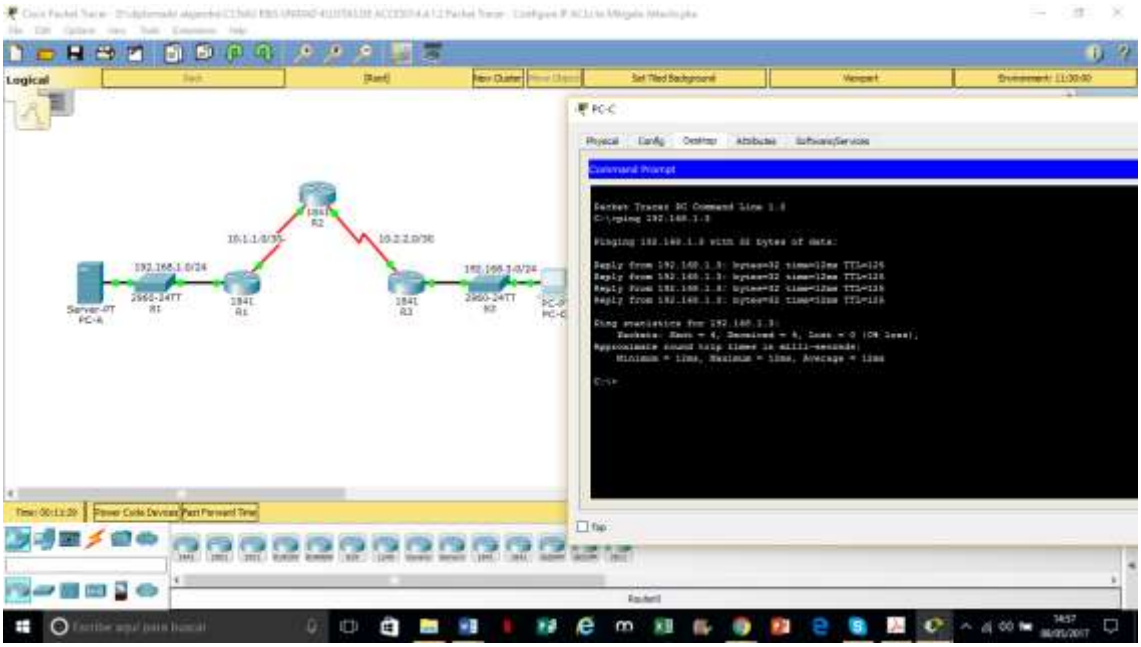
Step1:From PC-A, verify connectivity to PC-C andR2.
From the command prompt, ping PC-C(192.168.3.3).



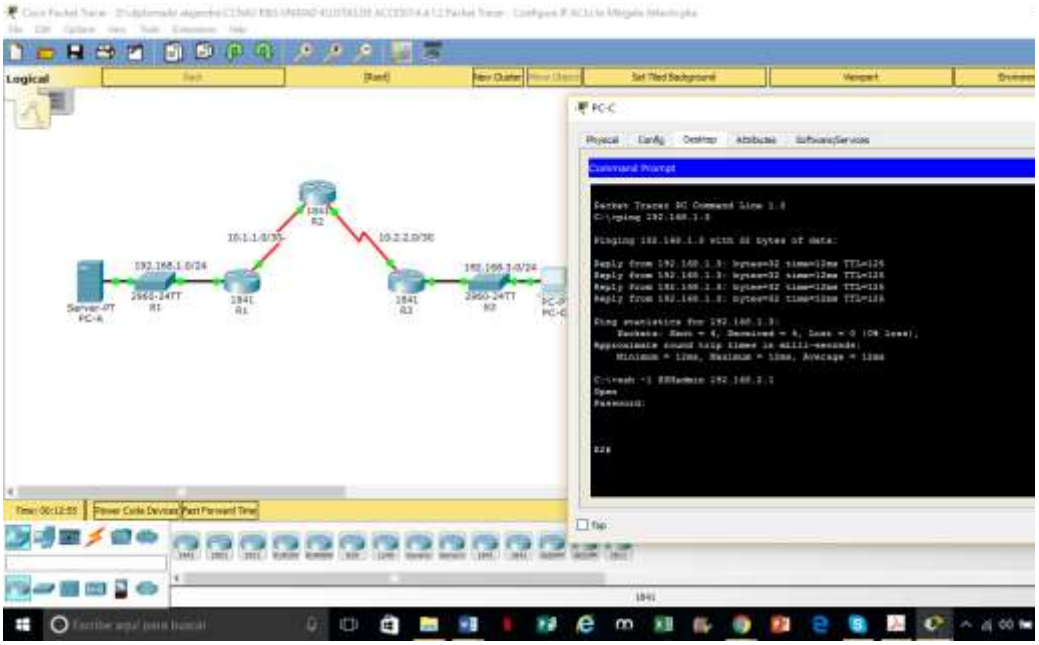
From the command prompt, establish a SSH session to R2 Lo0 interface (192.168.2.1) using username
SSHadmin and password ciscosshpa55. When finished, exit the SSH session.
PC> ssh -l SSHadmin 192.168.2.1



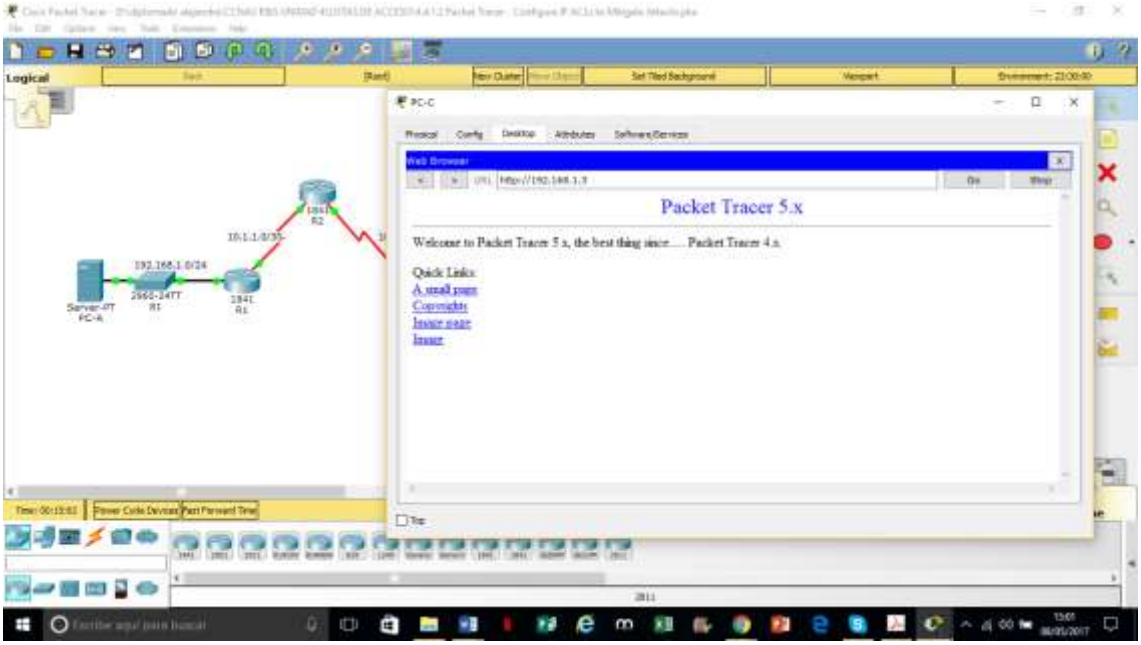
Step2:From PC-C, verify connectivity to PC-A andR2.
From the command prompt, ping PC-A(192.168.1.3).



From the command prompt, establish a SSH session to R2 Lo0 interface (192.168.2.1) using username
SSHadmin and password ciscosshpa55. Close the SSH session when finished.
PC> ssh -l SSHadmin 192.168.2.1



Open a web browser to the PC-A server (192.168.1.3) to display the web page. Close the browser when done.

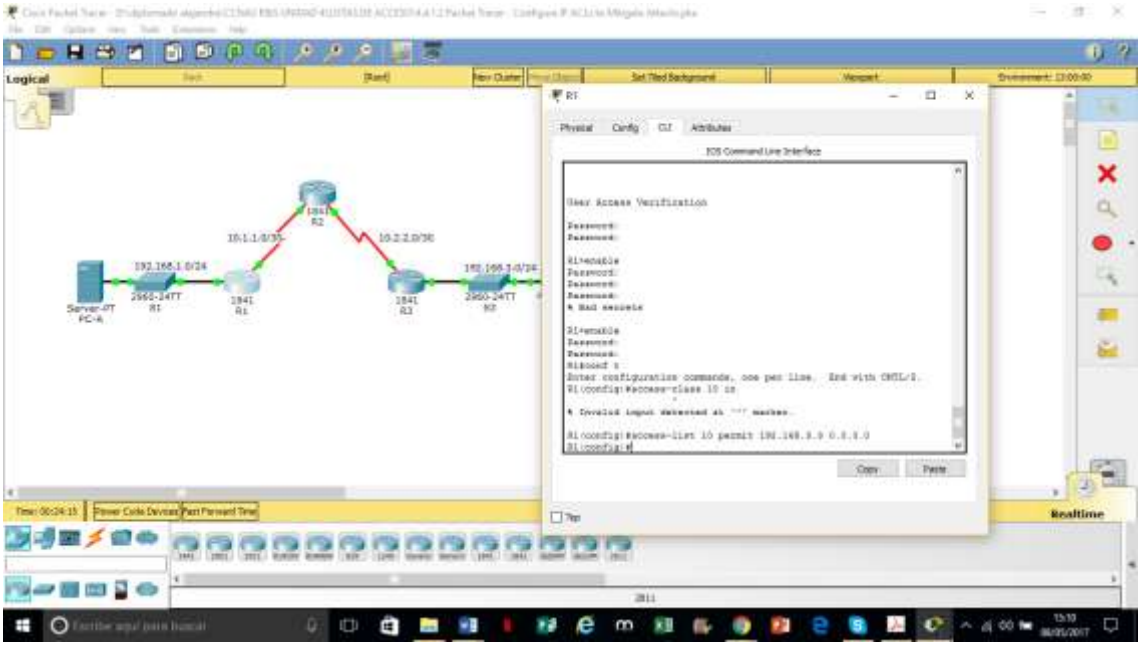


Part 2: Secure Access to Routers

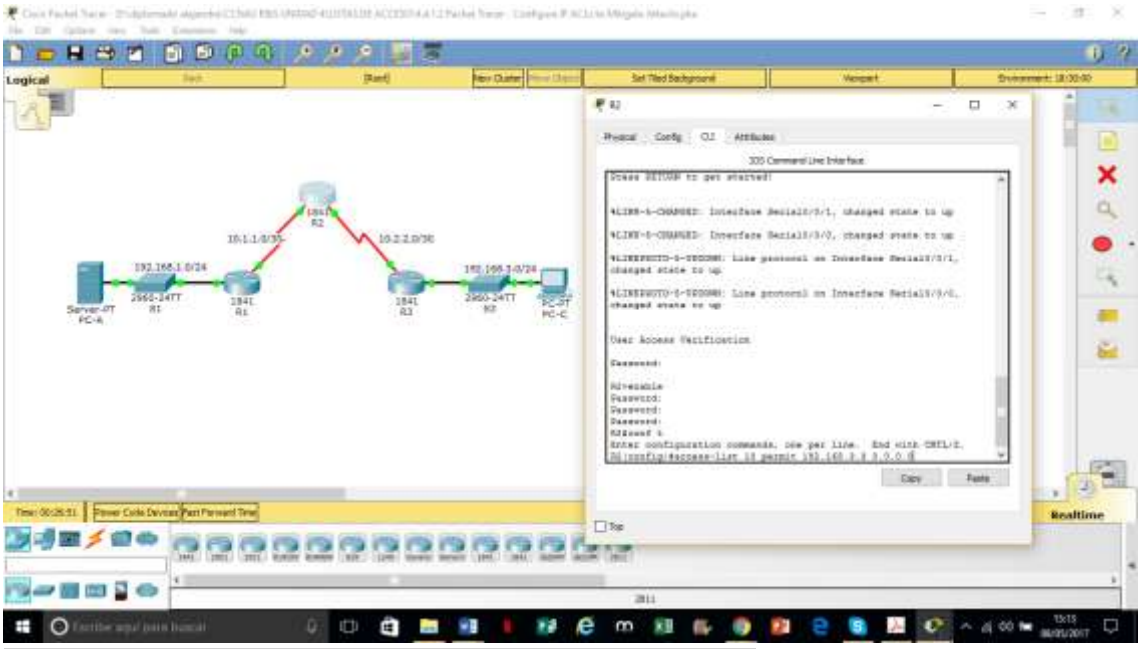
Step1:Configure ACL 10 to block all remote access to the routers except fromPC-C.

Use the access-list command to create a numbered IP ACL on R1, R2, and R3.

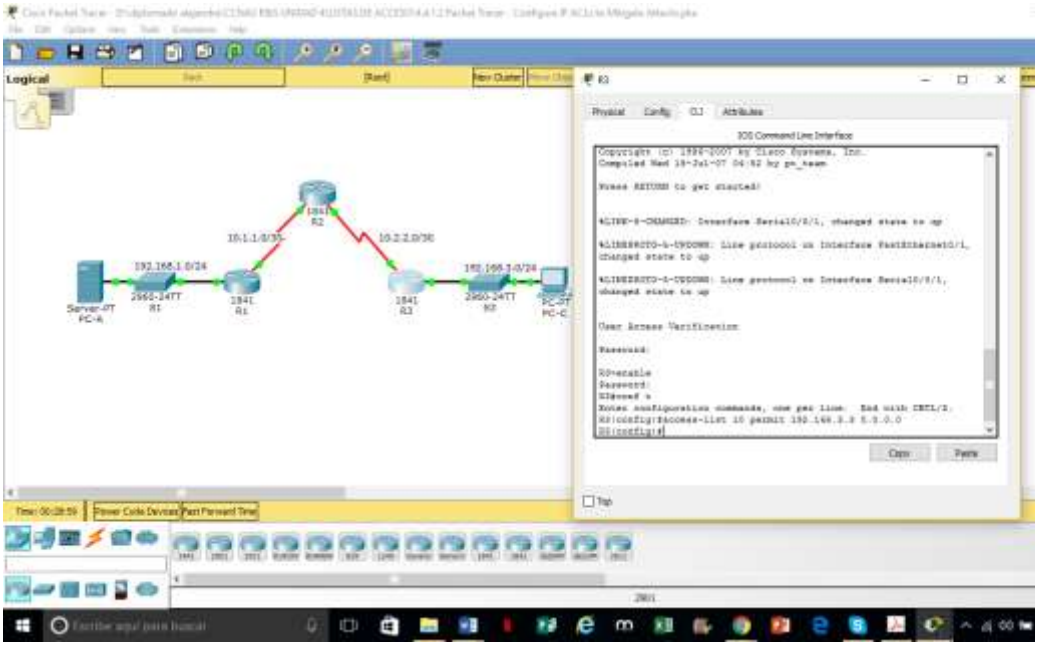
R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0



R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0



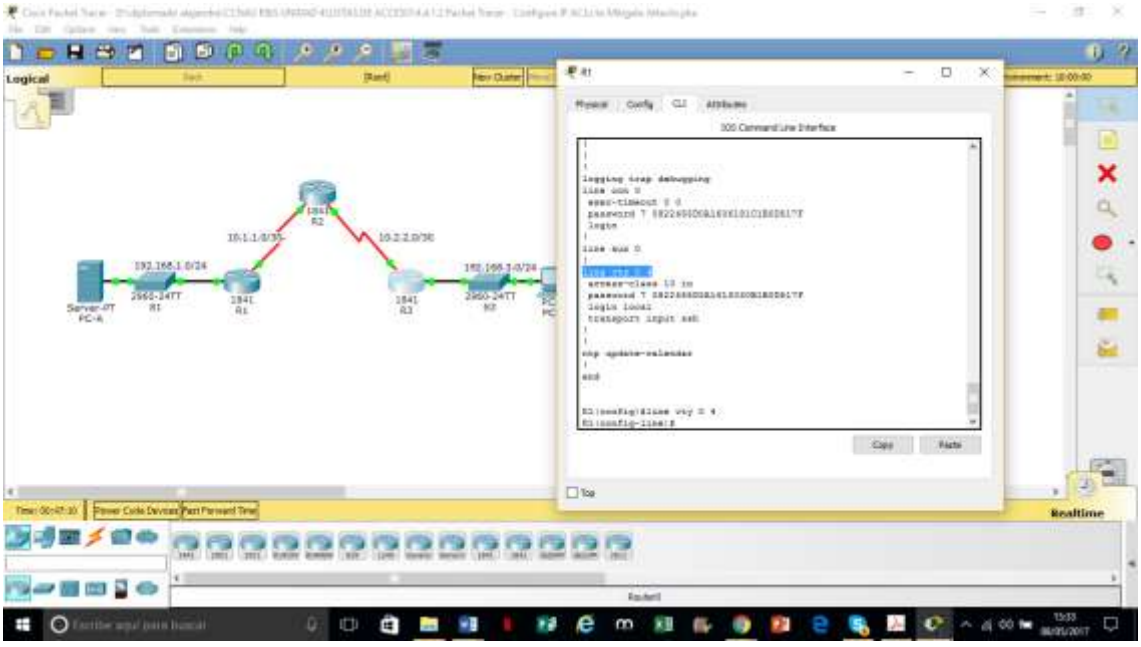
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0



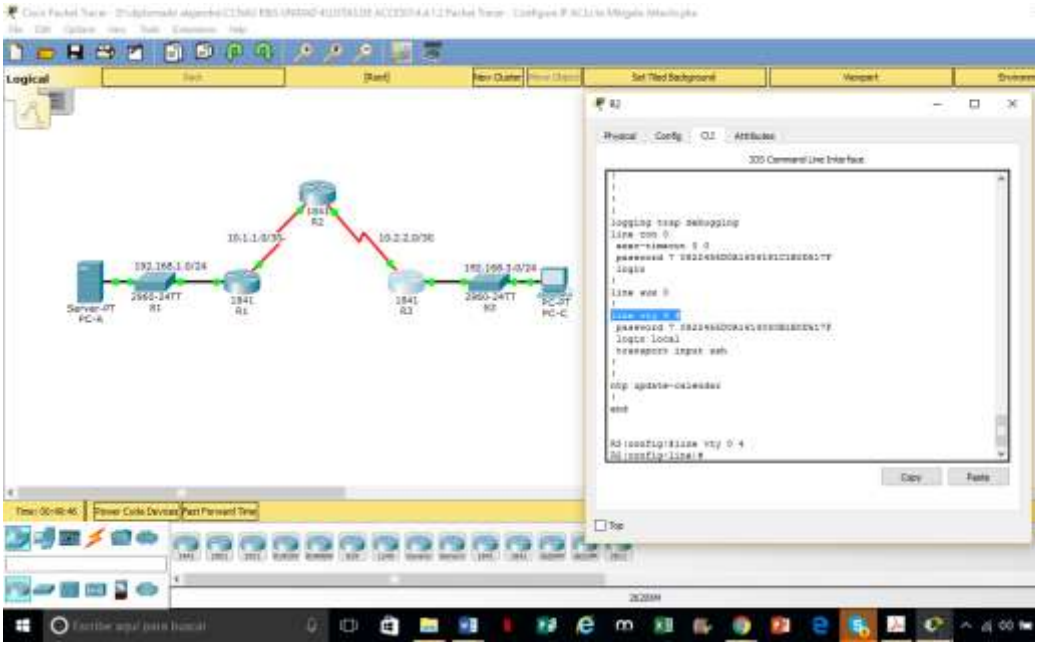
Step2:Apply ACL 10 to ingress traffic on the VTYlines.

Use the access-class command to apply the access list to incoming traffic on the VTY lines.

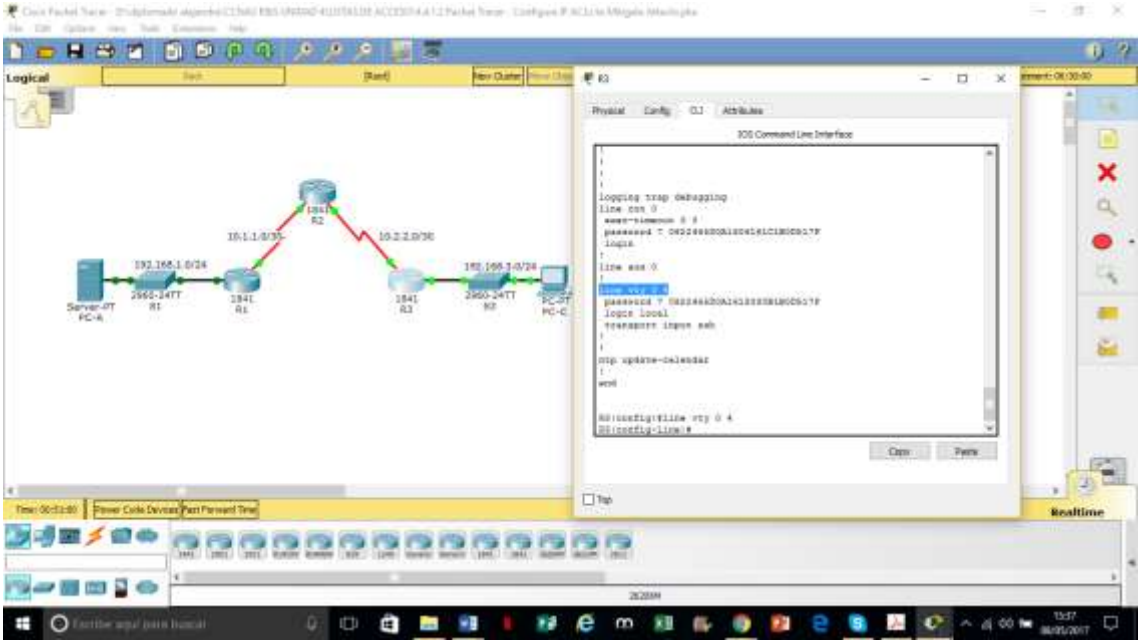
R1(config-line)# access-class 10 in



R2(config-line)# access-class 10 in



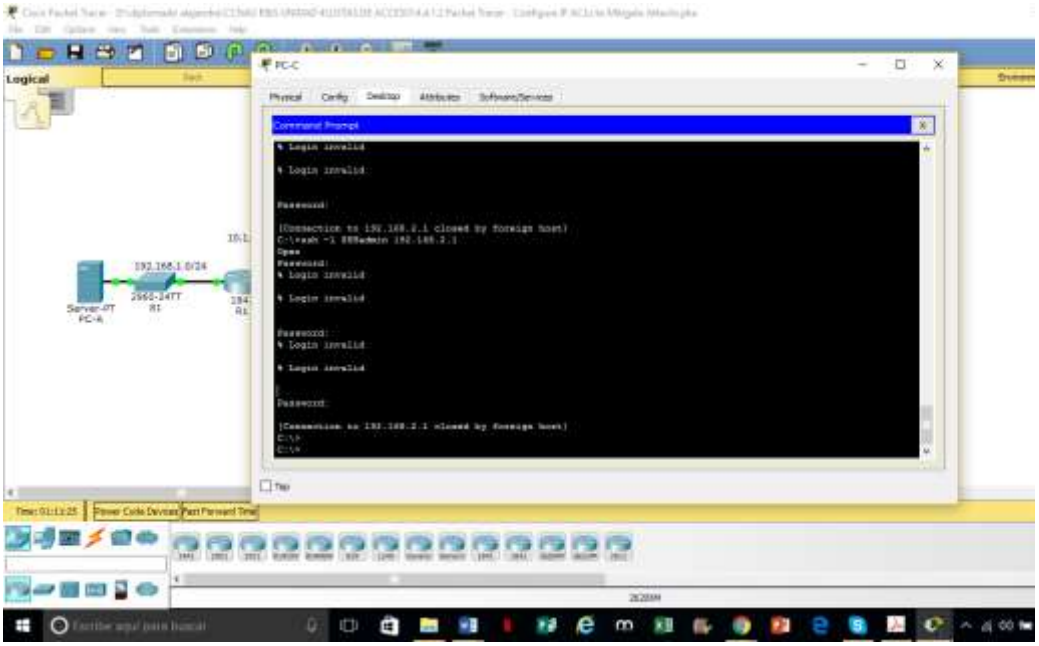
R3(config-line)# access-class 10 in



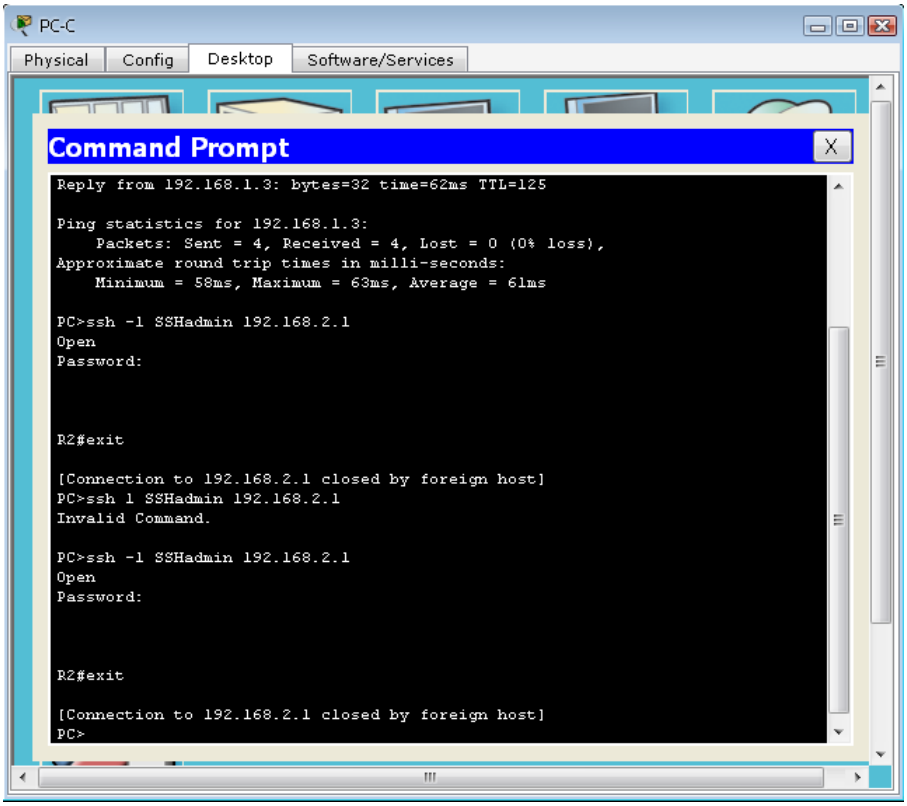
Step3:Verify exclusive access from management stationPC-C.

Establish a SSH session to 192.168.2.1 from PC-C (should besuccessful).

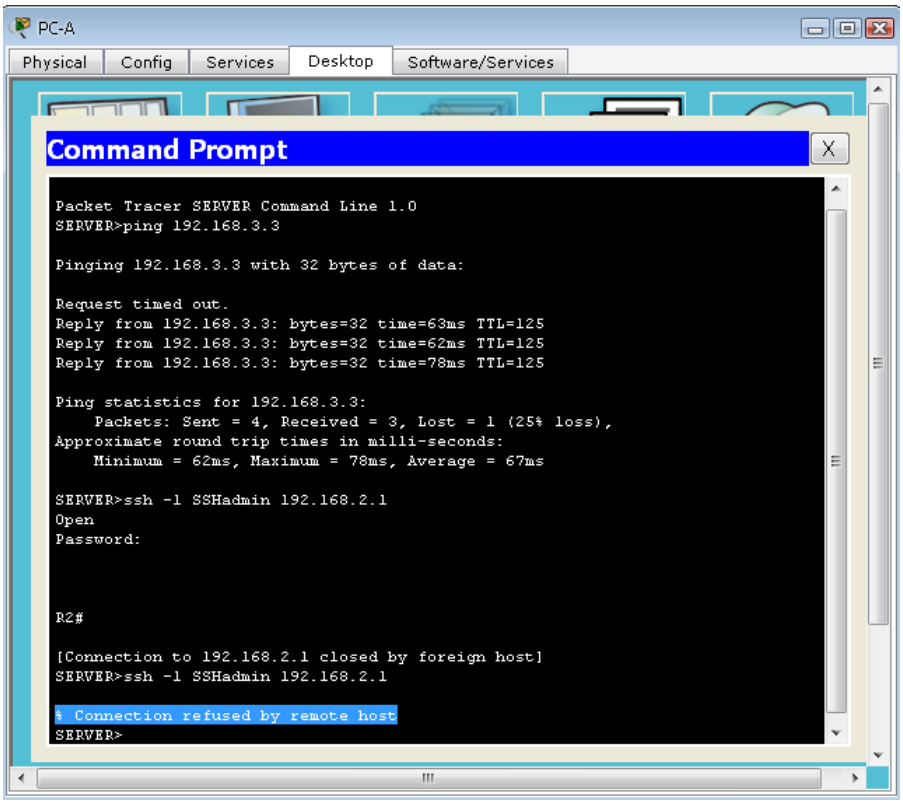
PC> ssh –l SSHadmin 192.168.2.1



Step3:Verify exclusive access from management stationPC-C.
Establish a SSH session to 192.168.2.1 from PC-C (should besuccessful).
PC> ssh –l SSHadmin 192.168.2.1



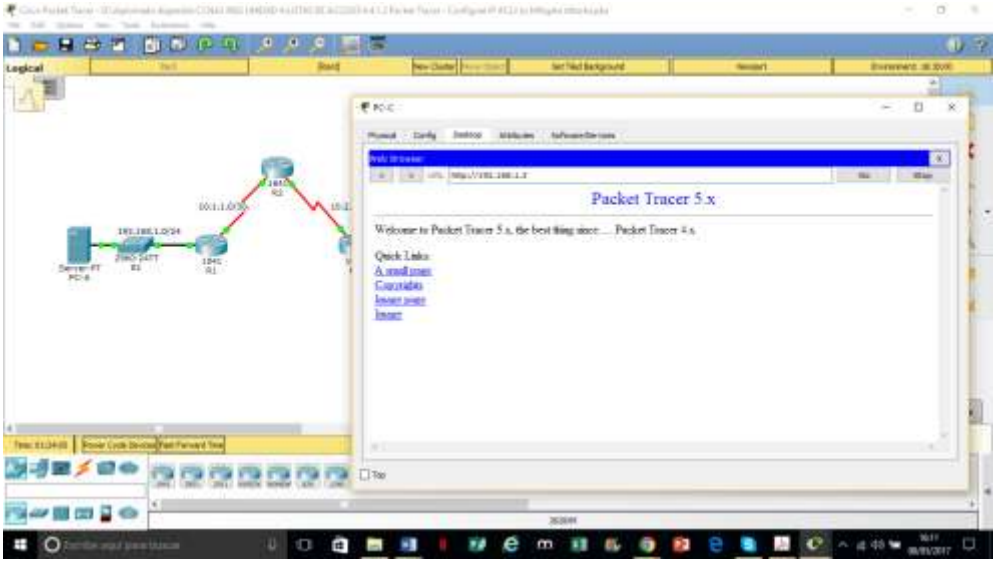
Establish a SSH session to 192.168.2.1 from PC-A (shouldfail). Rechazado



Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server PC-A, deny any outside host access to HTTPS services on PC-A, and permit PC-C to access R1 via SSH.

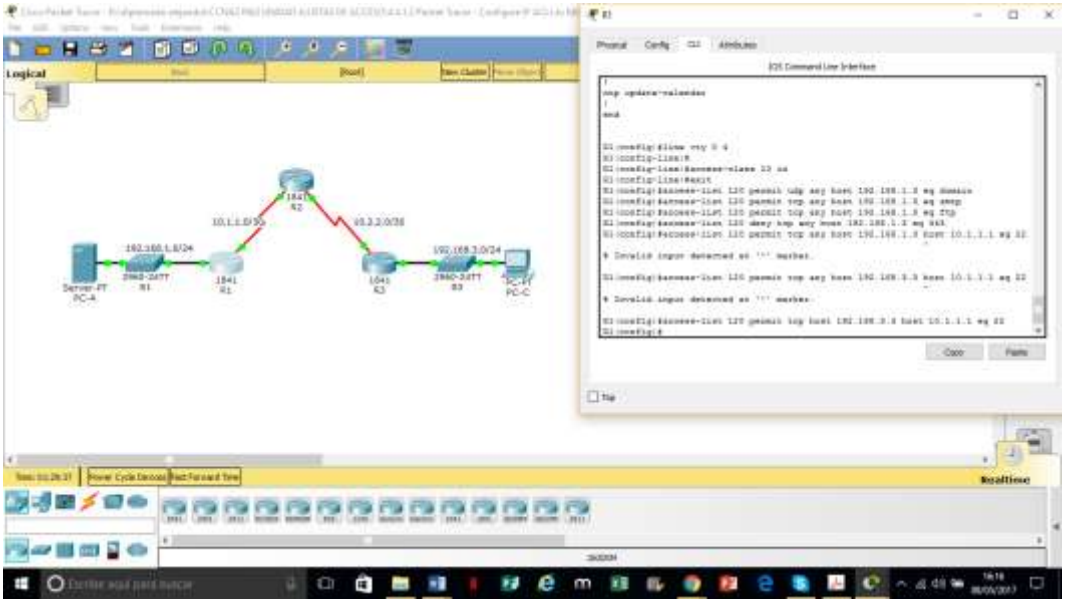
Step1:Verify that PC-C can access the PC-A via HTTPS using the webbrowser. Be sure to disable HTTP and enable HTTPS on server PC-A.



Step2:Configure ACL 120 to specifically permit and deny the specifiedtraffic.

Use the access-list command to create a numbered IP ACL.

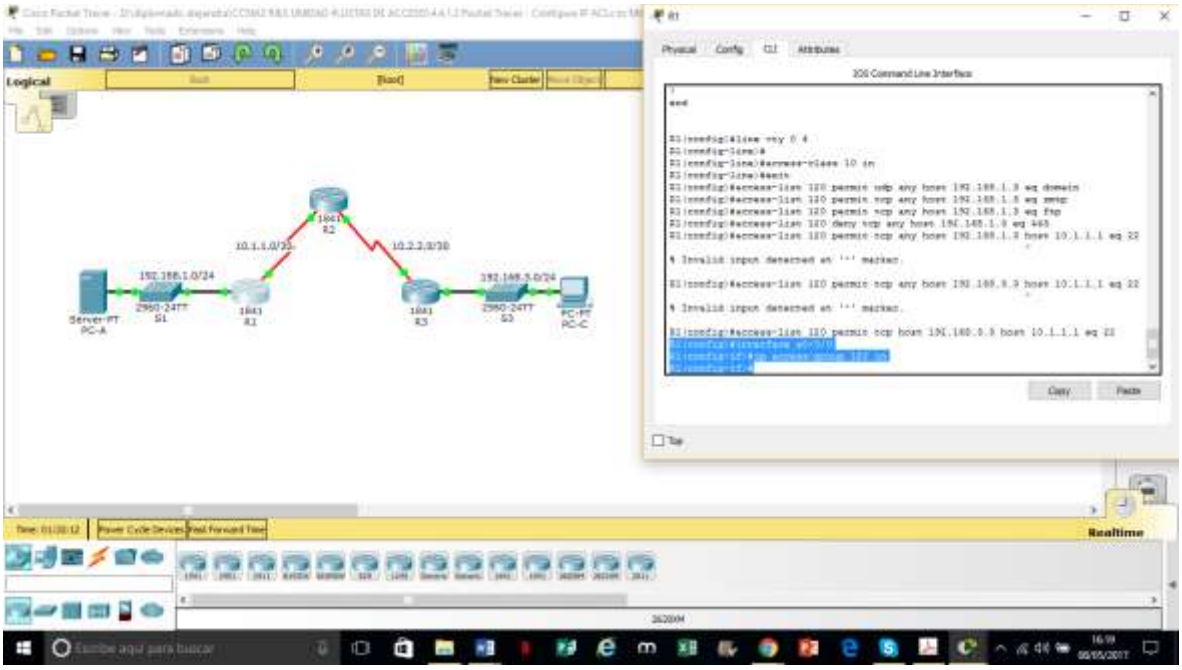
```
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq22
```



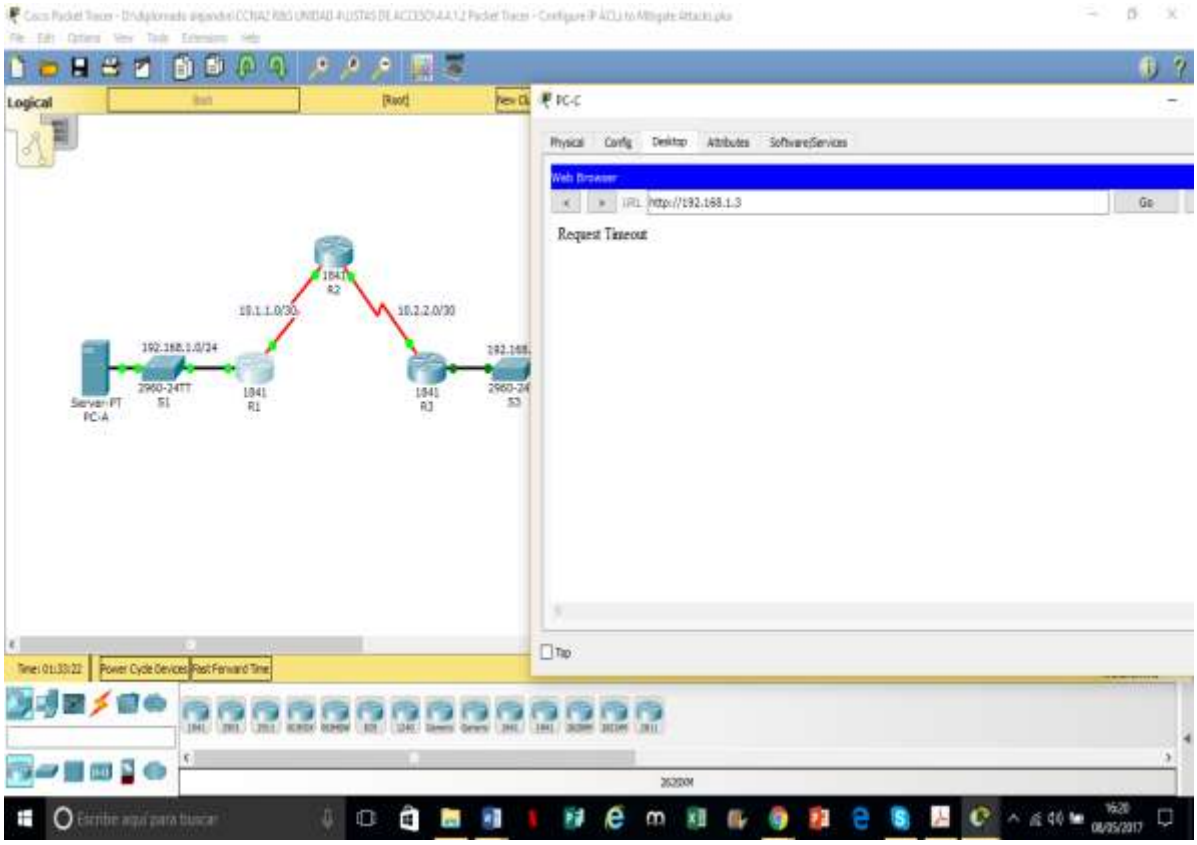
Step3:Apply the ACL to interfaceS0/0/0.

Use the ip access-group command to apply the access list to incoming traffic on interface S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 120 in
```



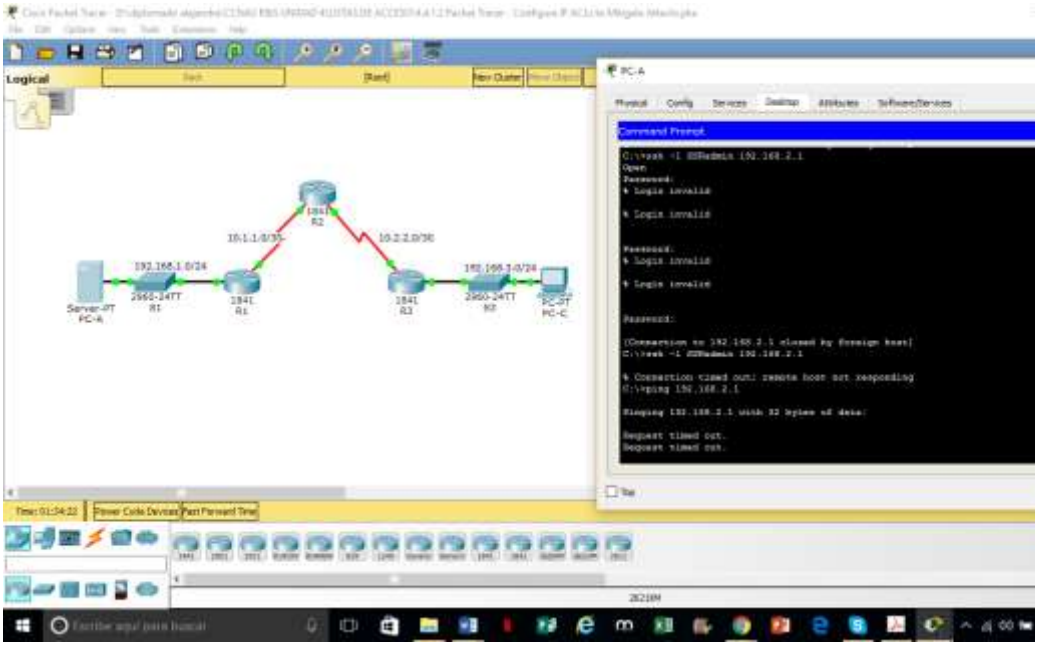
Step4:Verify that PC-C cannot access PC-A via HTTPS using the webbrowser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

Step1:Verify that PC-A cannot successfully ping the loopback interface onR2.



Step2:Make any necessary changes to ACL 120 to permit and deny the specified traffic.

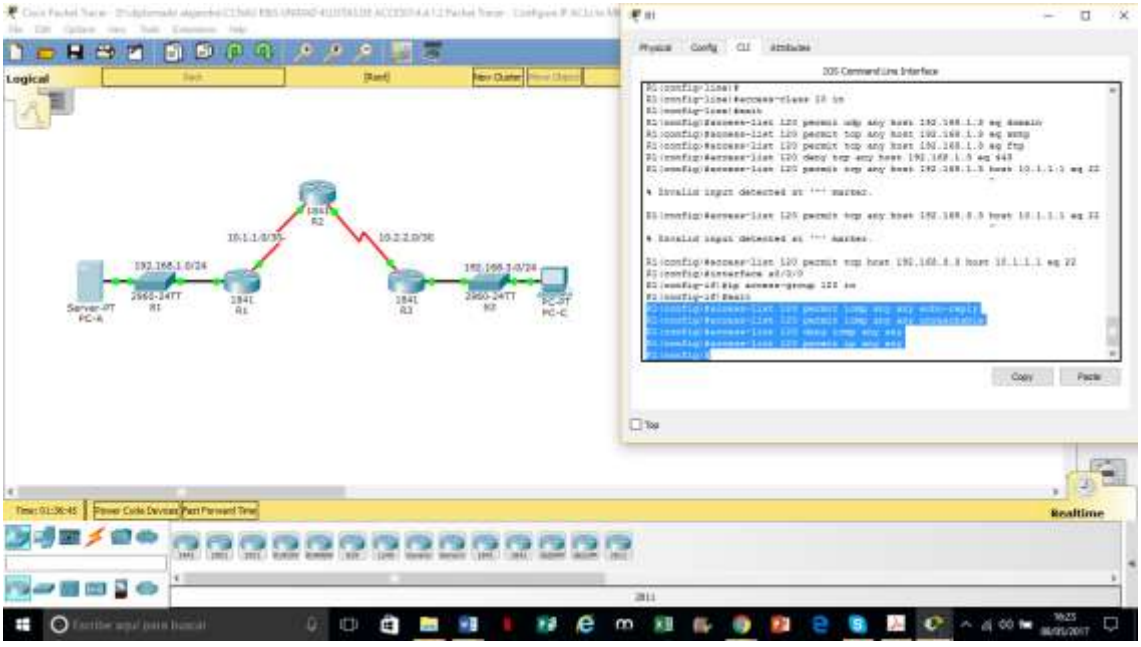
Use the access-list command to create a numbered IP ACL.

R1(config)# access-list 120 permit icmp any any echo-reply

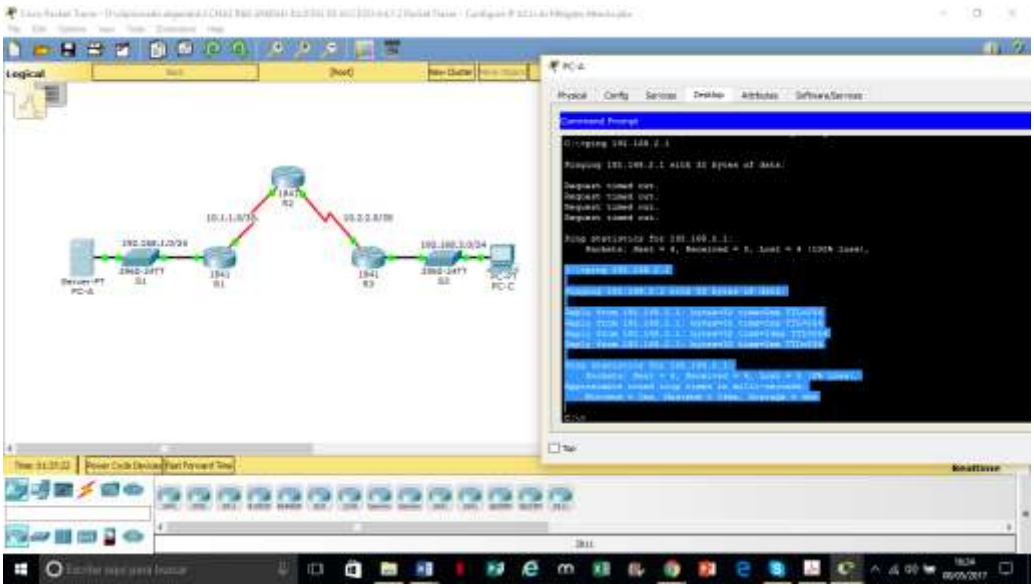
R1(config)# access-list 120 permit icmp any any unreachable

R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any



Step3:Verify that PC-A can successfully ping the loopback interface onR2.



Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on R3.

Step1:Configure ACL 110 to permit only traffic from the inside network.

Use the access-list command to create a numbered IP ACL.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Step2:Apply the ACL to interfaceF0/1.

Use the ip access-group command to apply the access list to incoming traffic on interface F0/1.

R3(config)# interface fa0/1

R3(config-if)# ip access-group 110 in

Part 6: Create a Numbered IP ACL 100 on R3

On R3, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

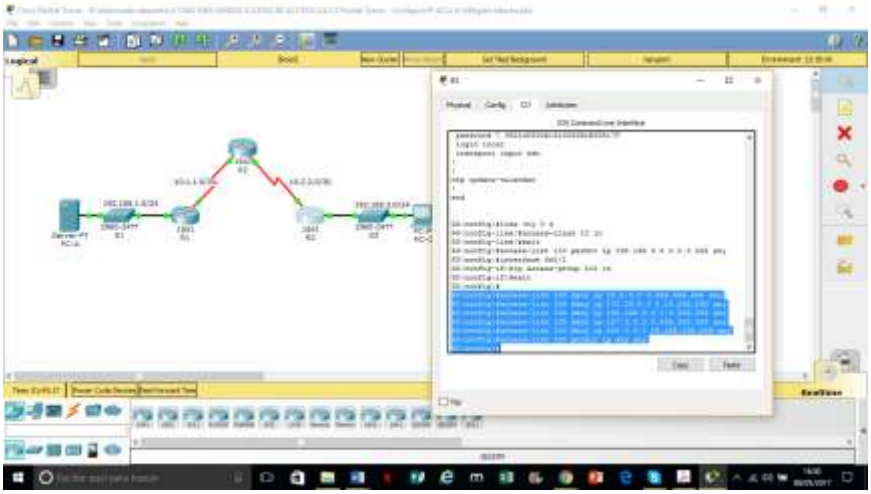
Step1:Configure ACL 100 to block all specified traffic from the outsidenetwork.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the access-list command to create a numbered IP ACL.

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

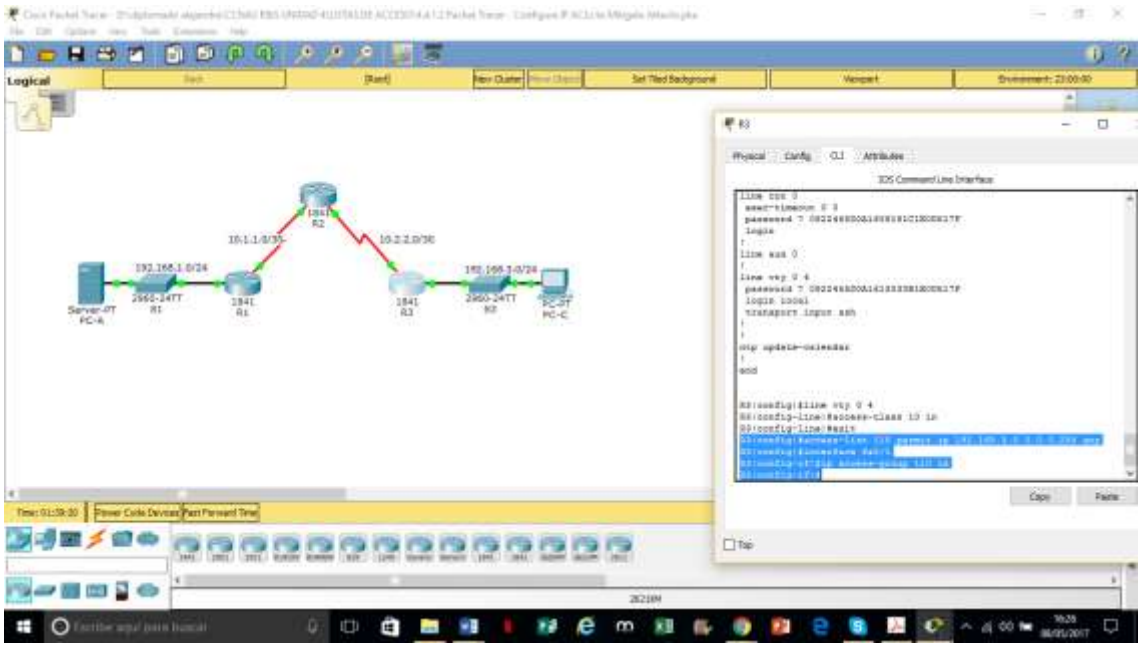
```
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any
```

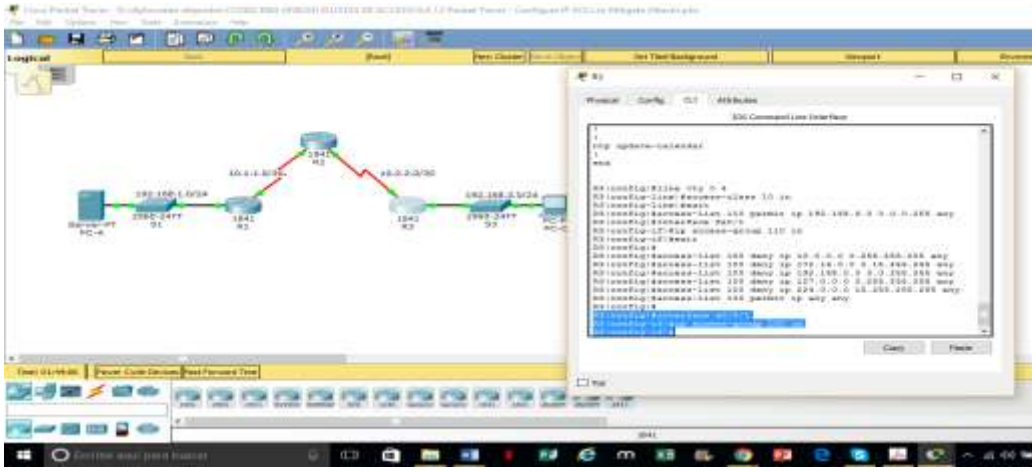


Step2:Apply the ACL to interface Serial0/0/1.

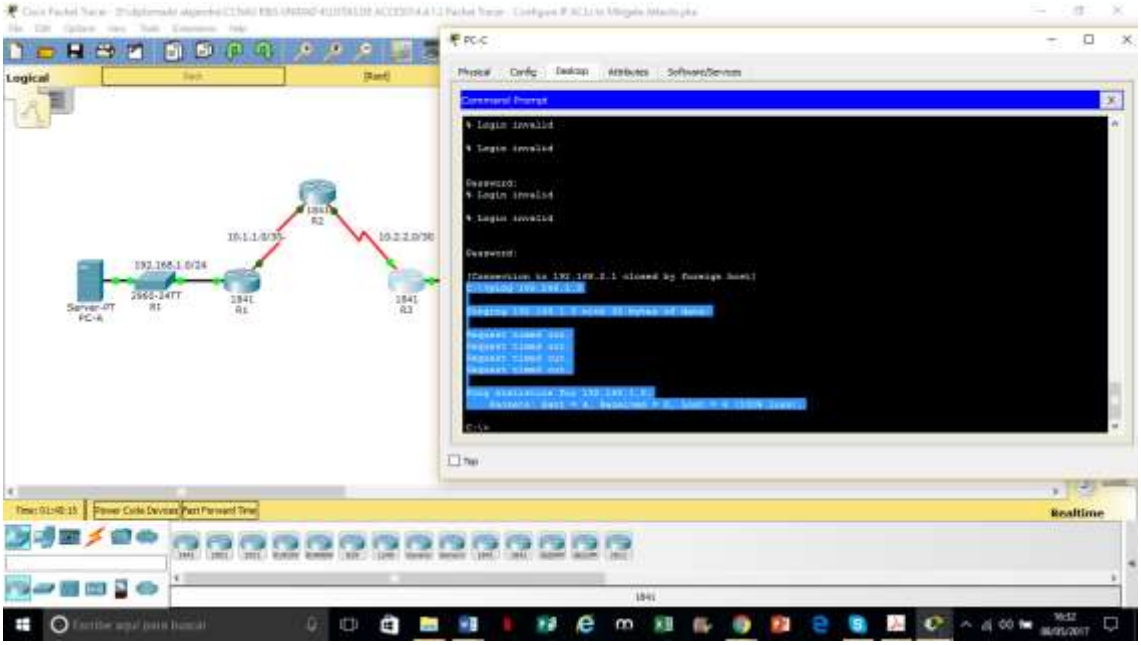
Use the ip access-group command to apply the access list to incoming traffic on interface Serial 0/0/1.

```
R3(config)# interface s0/0/1
R3(config-if)# ip access-group 100 in
```



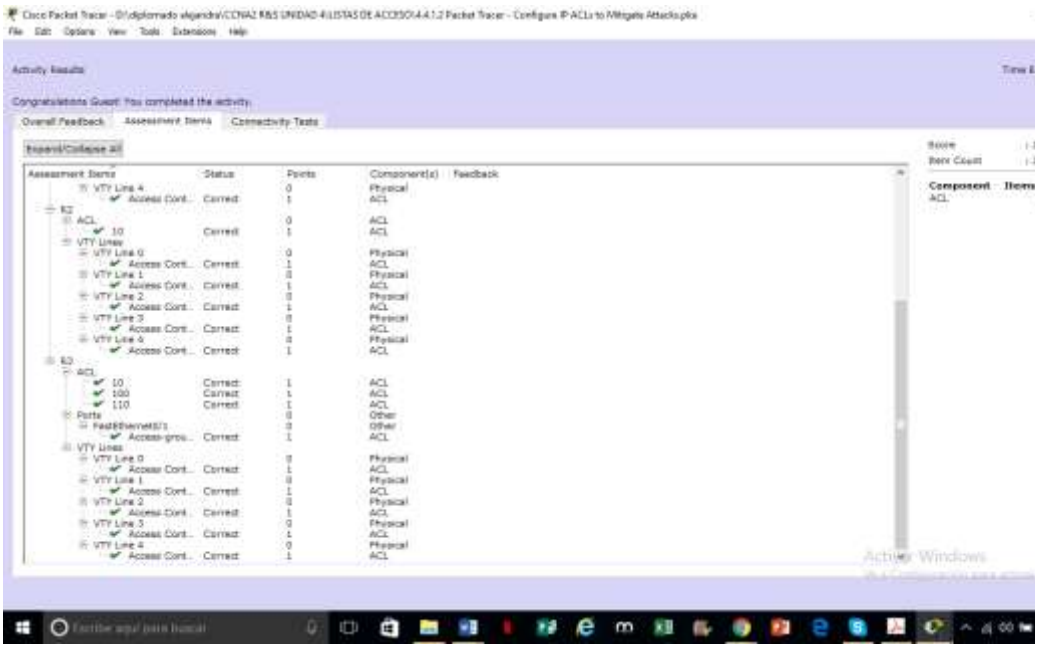


Step3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped. From the PC-C command prompt, ping the PC-A server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.



Step4: Check results.

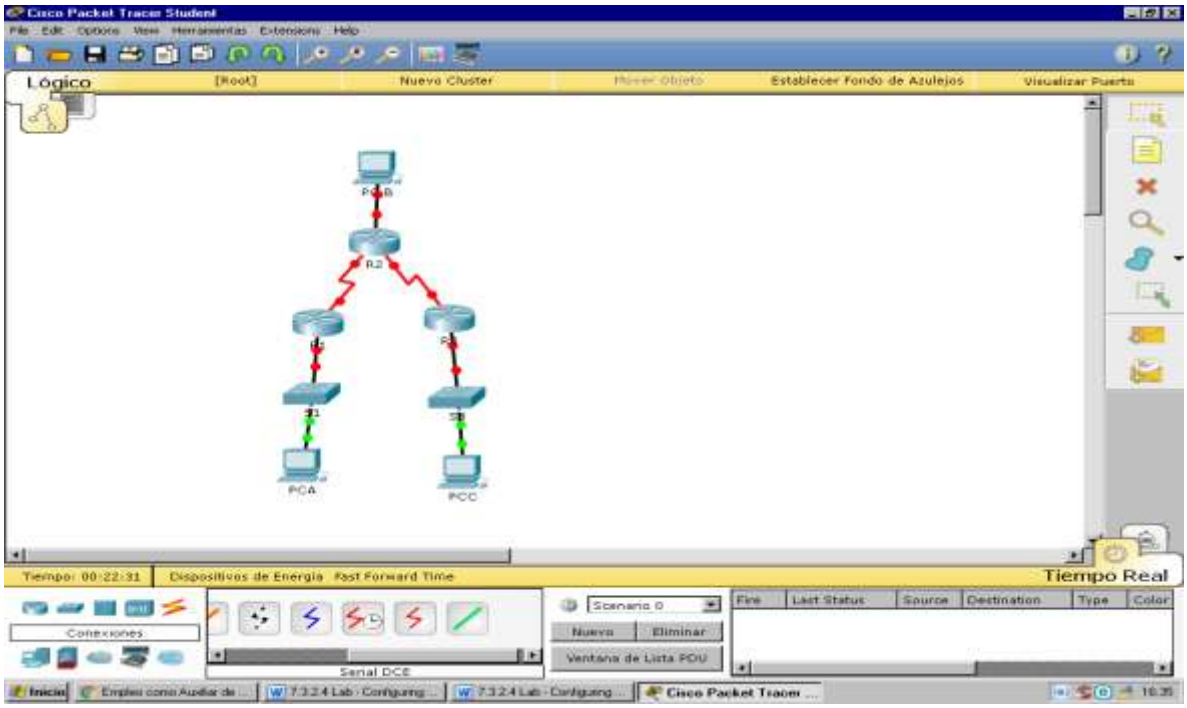
Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed



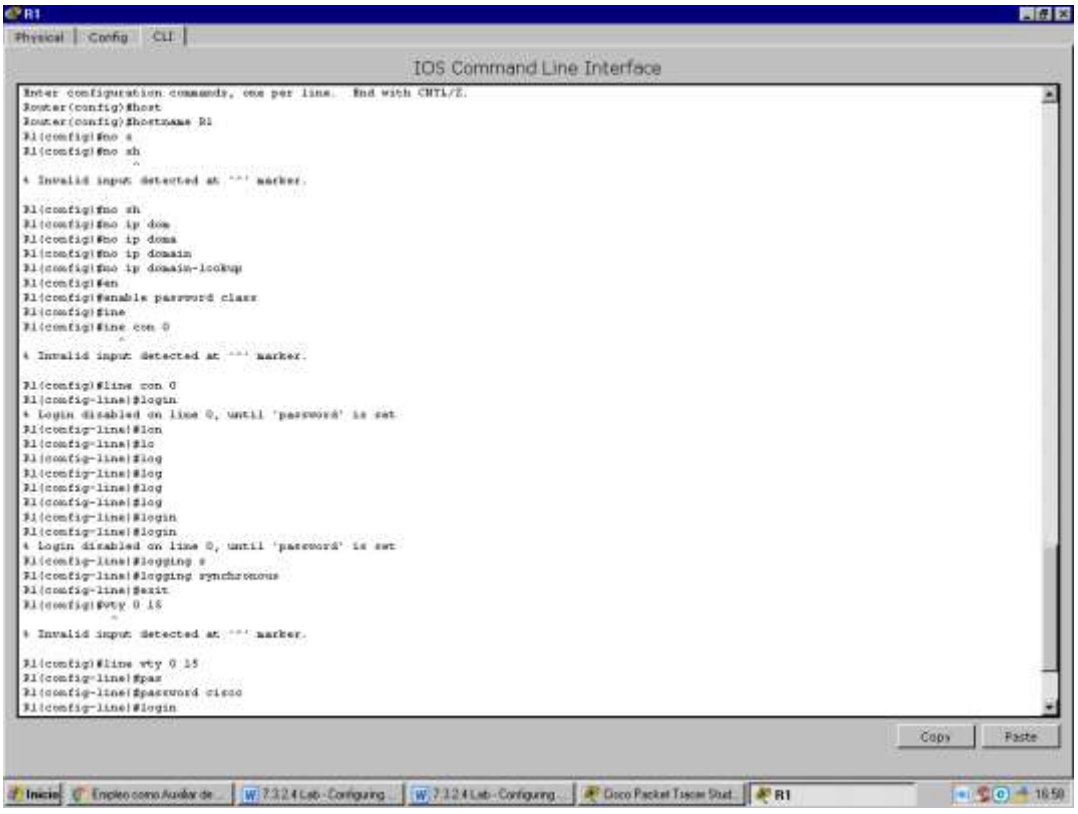
```
!!!Script for R1
access-list 10 permit 192.168.3.3 0.0.0.0 line vty 0 4
access-class 10 in
access-list 120 permit udp any host 192.168.1.3 eq domain access-list 120 permit
tcp any host 192.168.1.3 eq smtp access-list 120 permit tcp any host 192.168.1.3
eq ftp access-list 120 deny tcp any host 192.168.1.3 eq 443
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22 interface s0/0/0
 ip access-group 120 in
access-list 120 permit icmp any any echo-reply access-list 120 permit icmp any
any unreachable access-list 120 deny icmp any any
access-list 120 permit ip any any
!!!Script for R2
access-list 10 permit 192.168.3.3 0.0.0.0 line vty 0 4
 access-class 10 in
!!!Script for R3
access-list 10 permit 192.168.3.3 0.0.0.0 line vty 0 4
 access-class 10 in
access-list 100 deny ip 10.0.0.0 0.255.255.255 any access-list 100 deny ip
172.16.0.0 0.15.255.255 any access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any access-list 100 deny ip
224.0.0.0 15.255.255.255 any access-list 100 permit ip any any
interface s0/0/1
 ip access-group 100 in
access-list 110 permit ip 192.168.3.0 0.0.0.255 any interface fa0/1
 ip access-group 110 in
```

Ejercicio 7.3.2.1

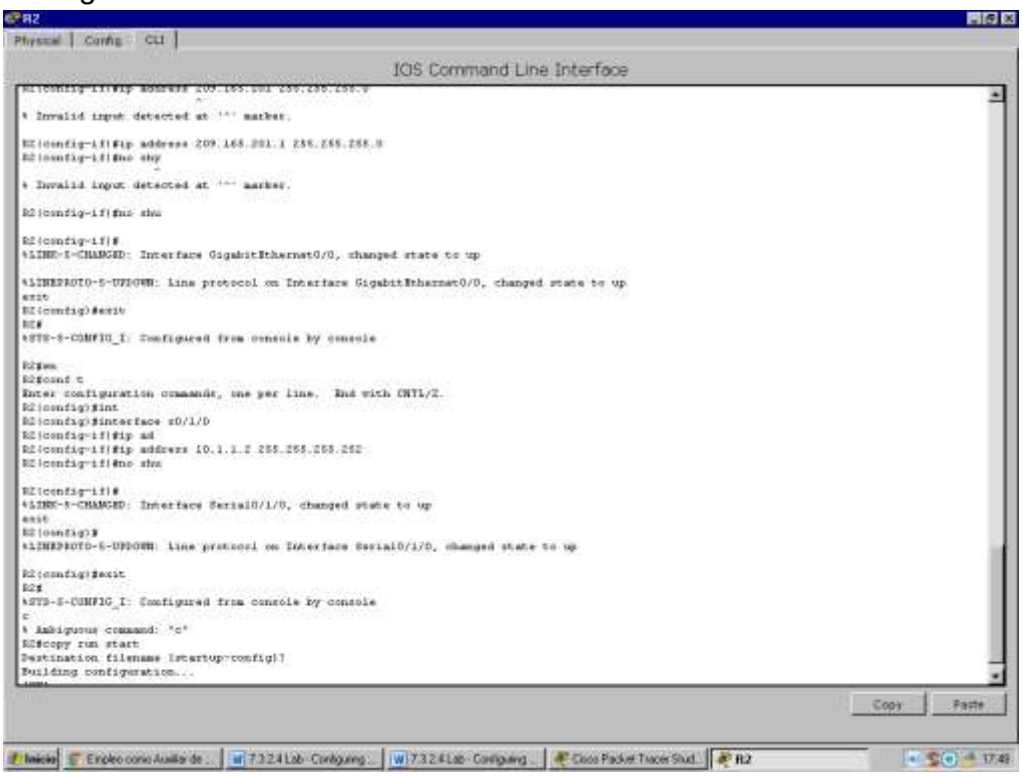
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

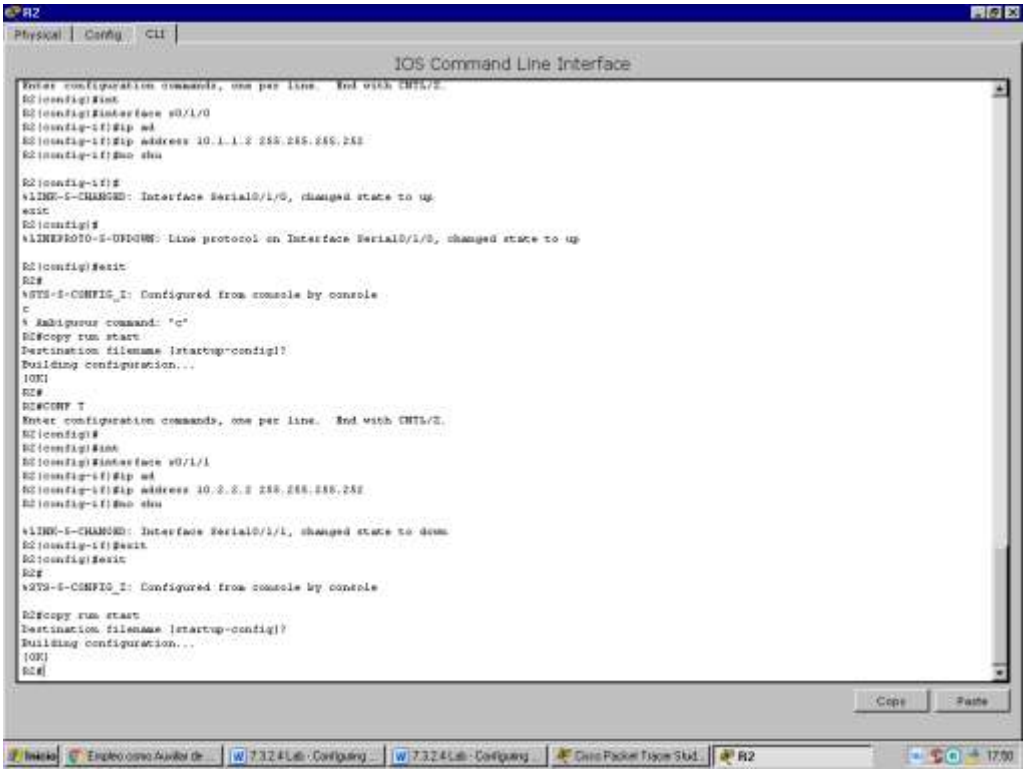


Configuración r1

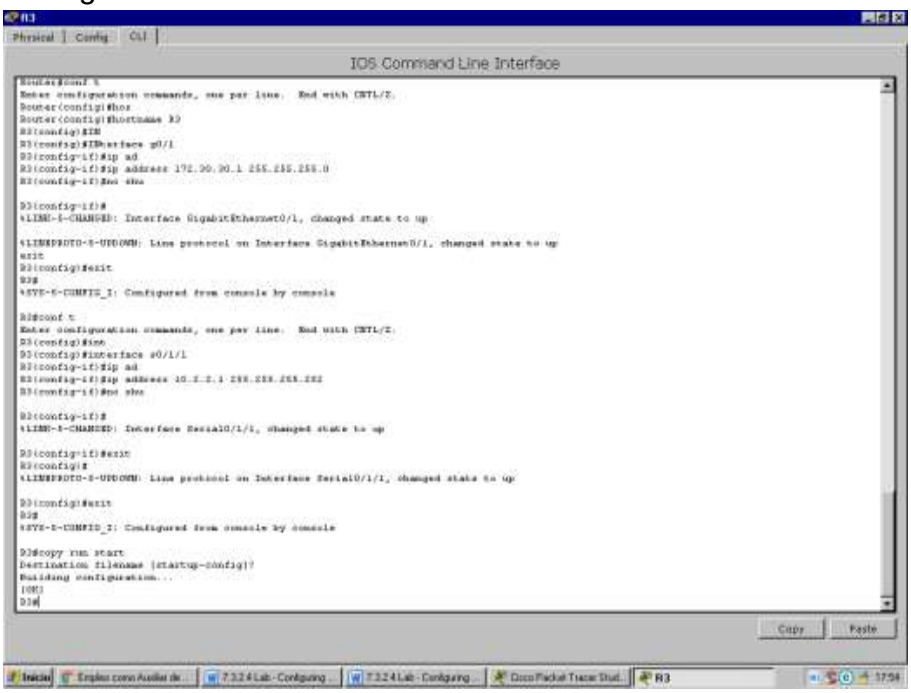


Configuración R2





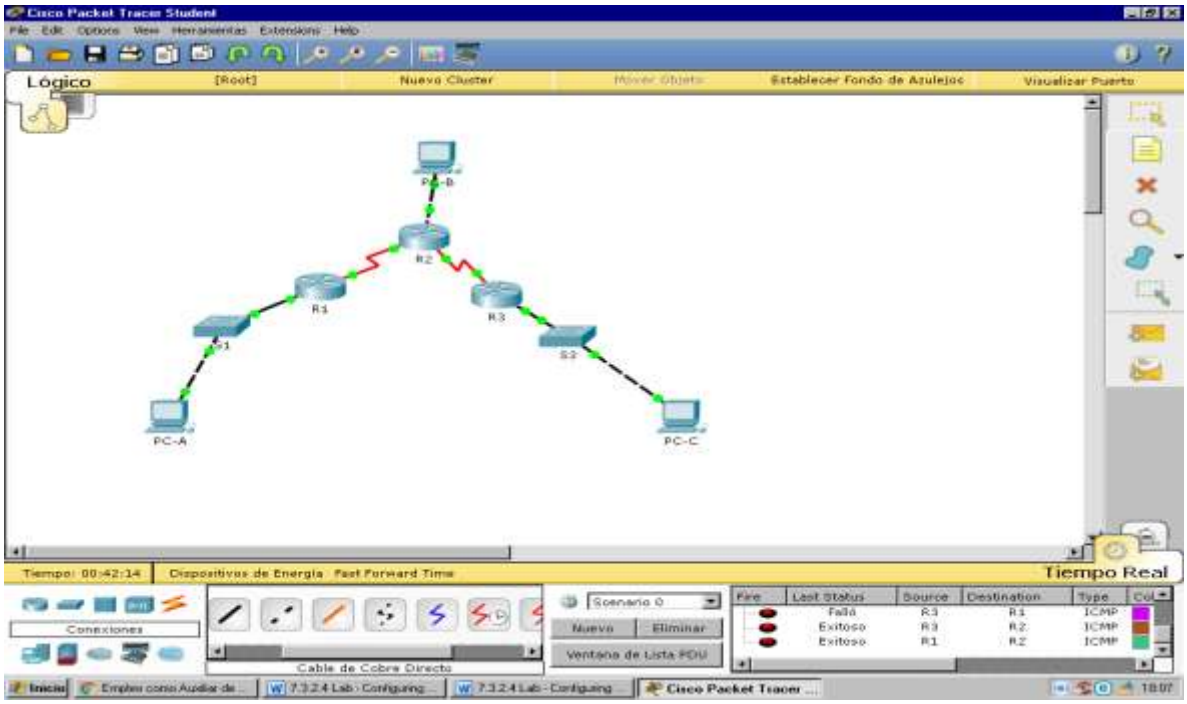
Configuración R3



Configurar los equipos host.

Se realiza la configuración de las computadoras realizando la destinación de las ips correspondientes según su tabla de enrutamiento

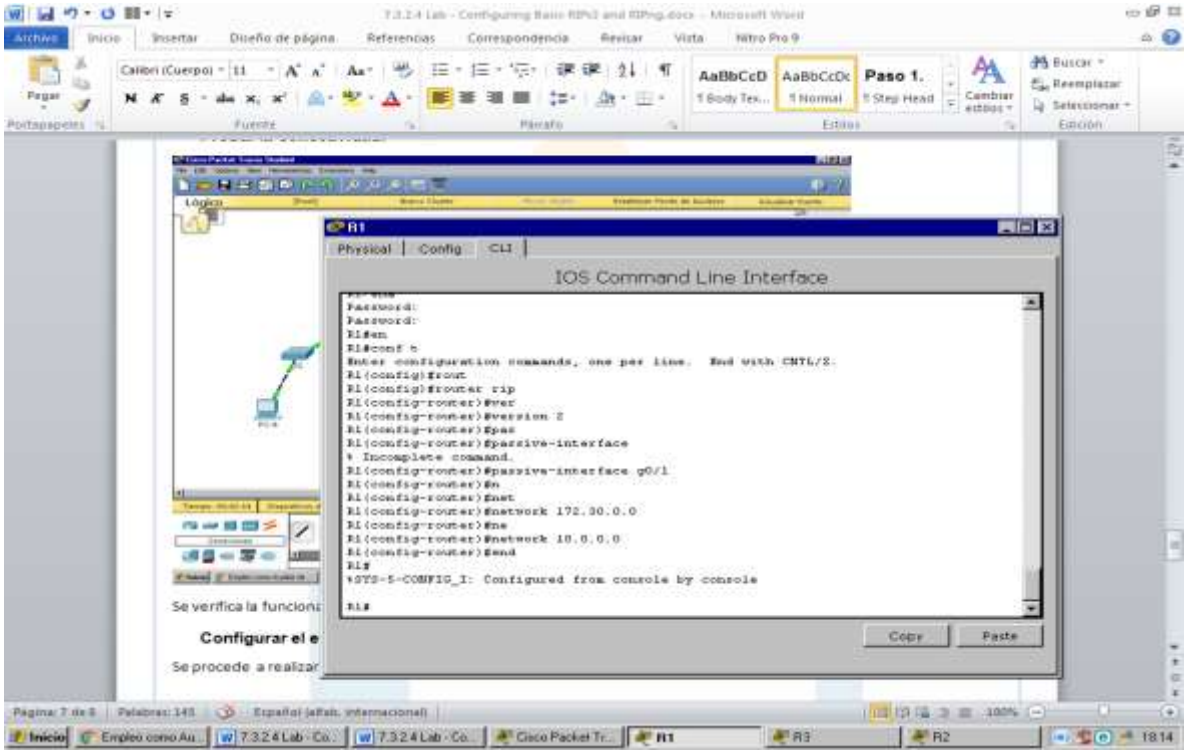
Probar la conectividad.

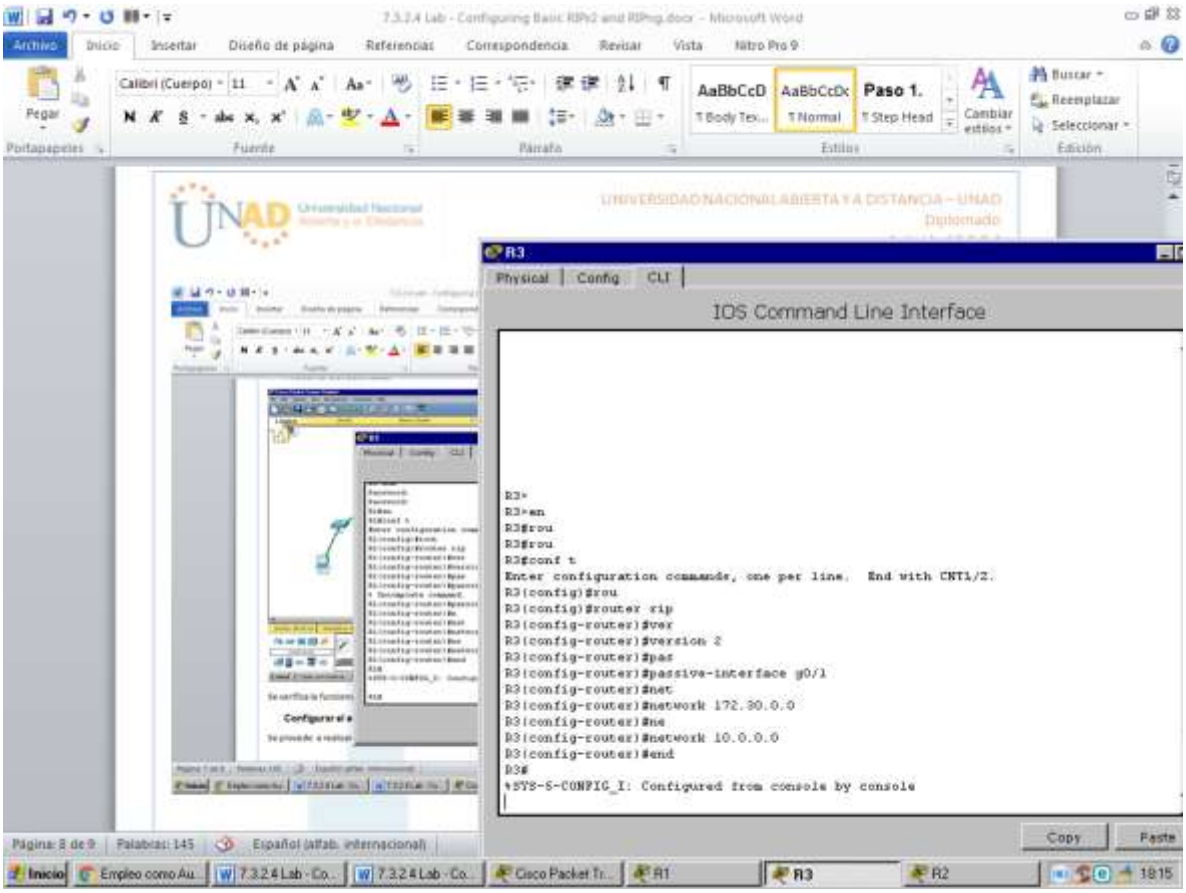


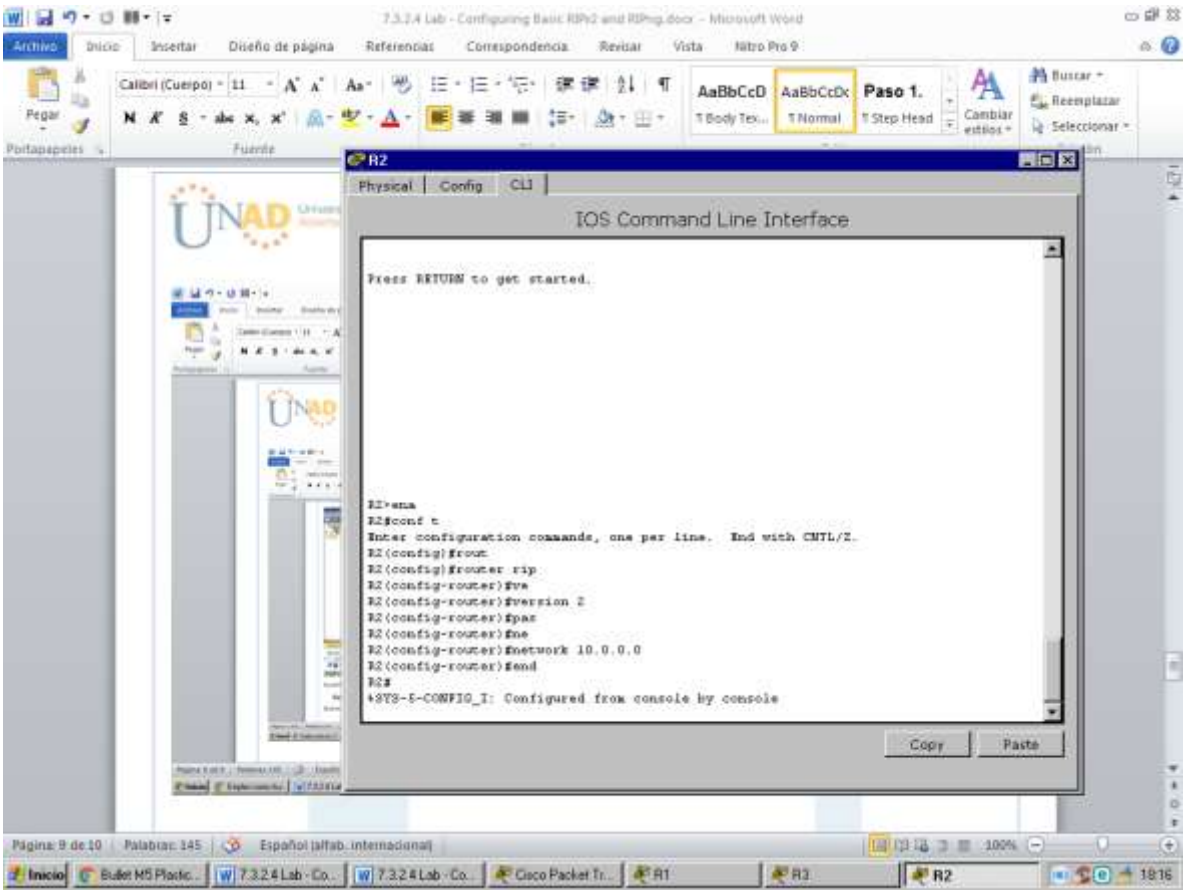
Se verifica la funcionalidad de la red y se determina que en varias partes no está pasando la comunicación

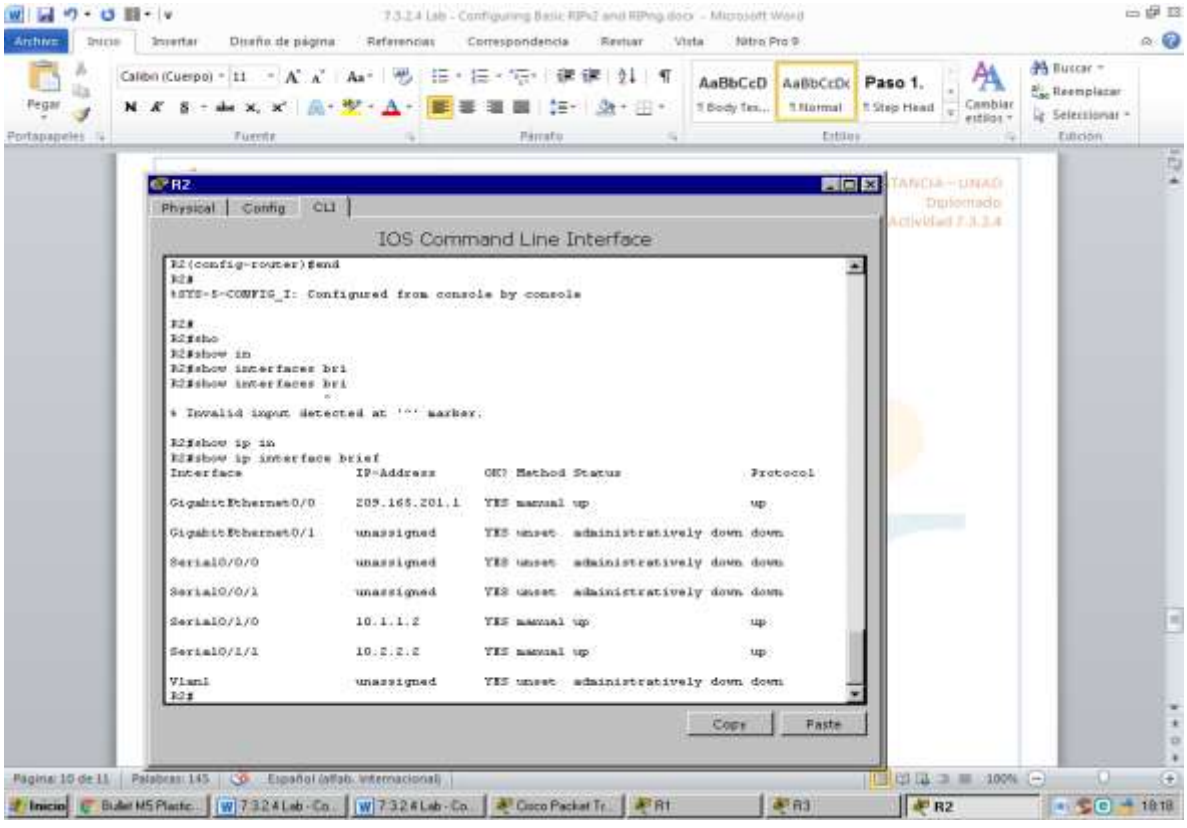
Configurar el enrutamiento RIPv2.

Se procede a realizar la configuración en cada uno de ellos

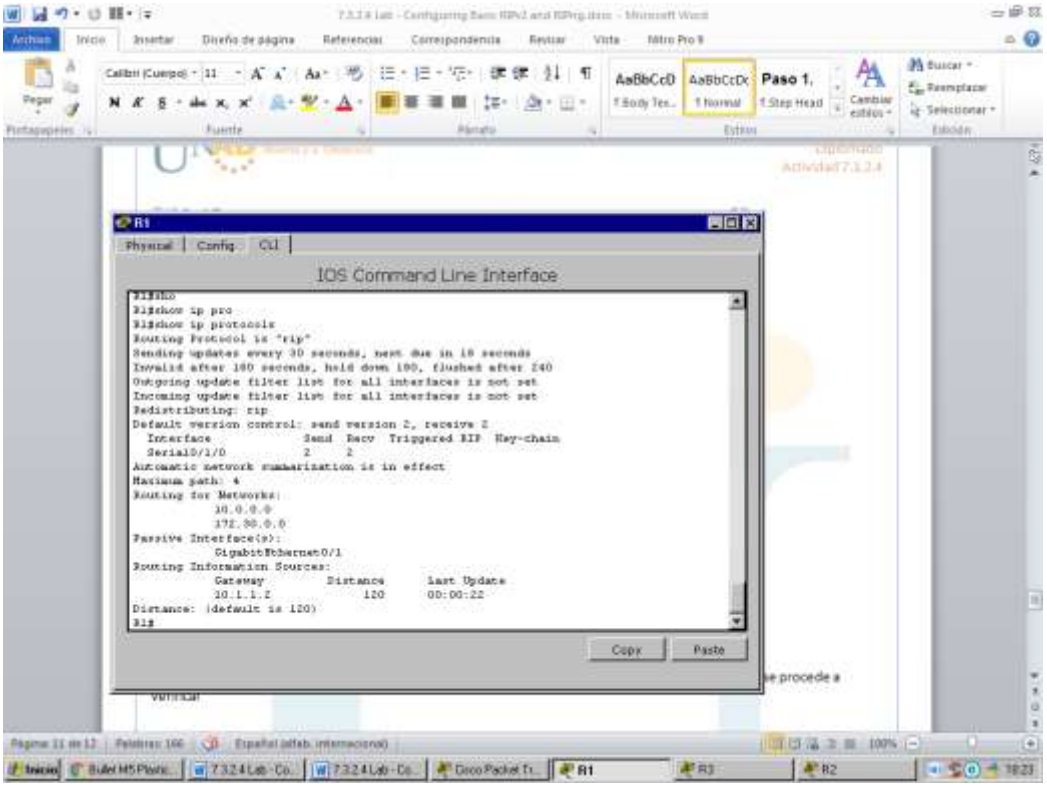


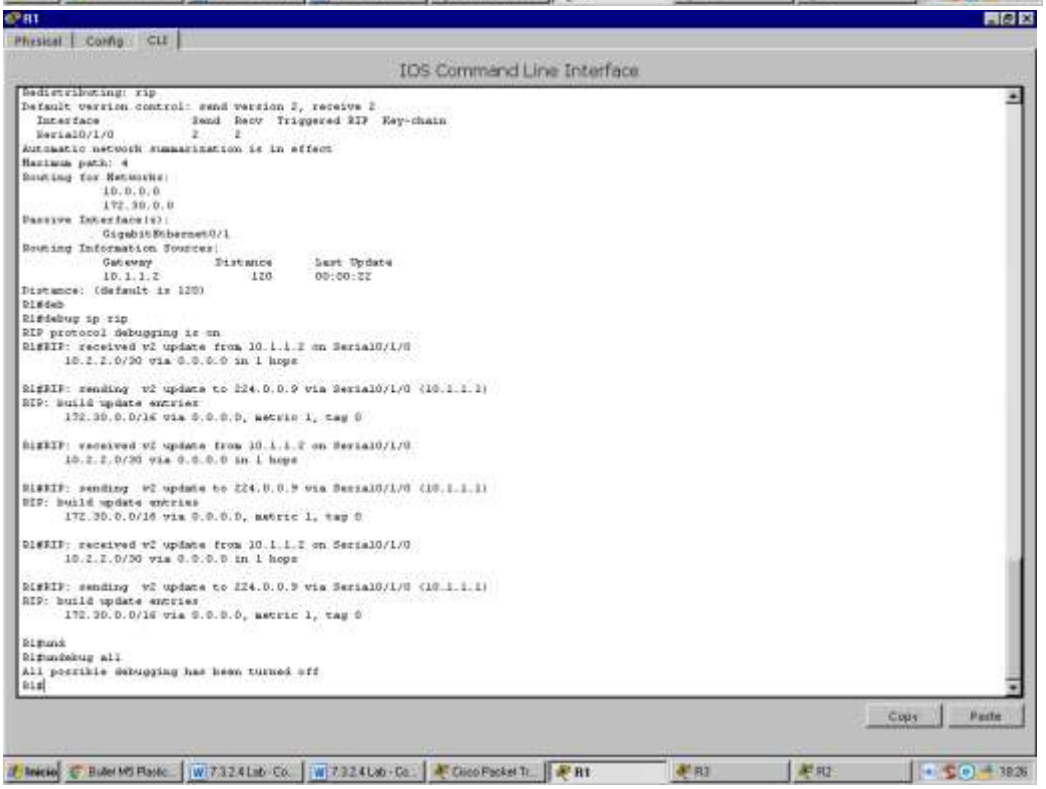


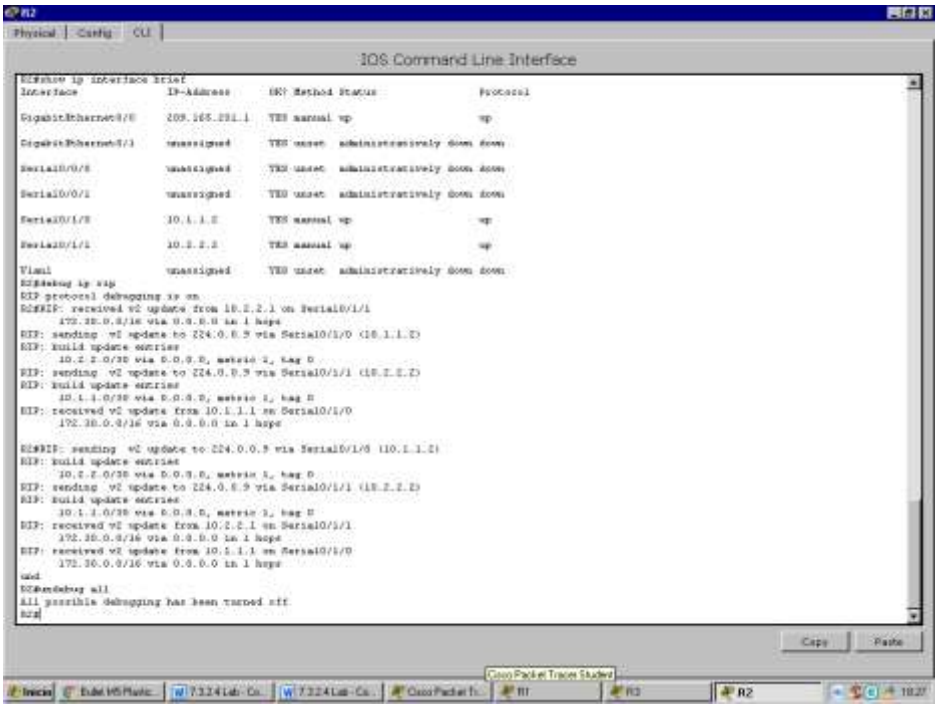

R2
Physical
Config
CLI
IOS Command Line Interface
Press RETURN to get started.
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#rout
R2(config)#router rip
R2(config-router)#ve
R2(config-router)#version 2
R2(config-router)#pas
R2(config-router)#ne
R2(config-router)#network 10.0.0.0
R2(config-router)#end
R2#
*SYS-5-CONFIG_I: Configured from console by console
Copy
Paste

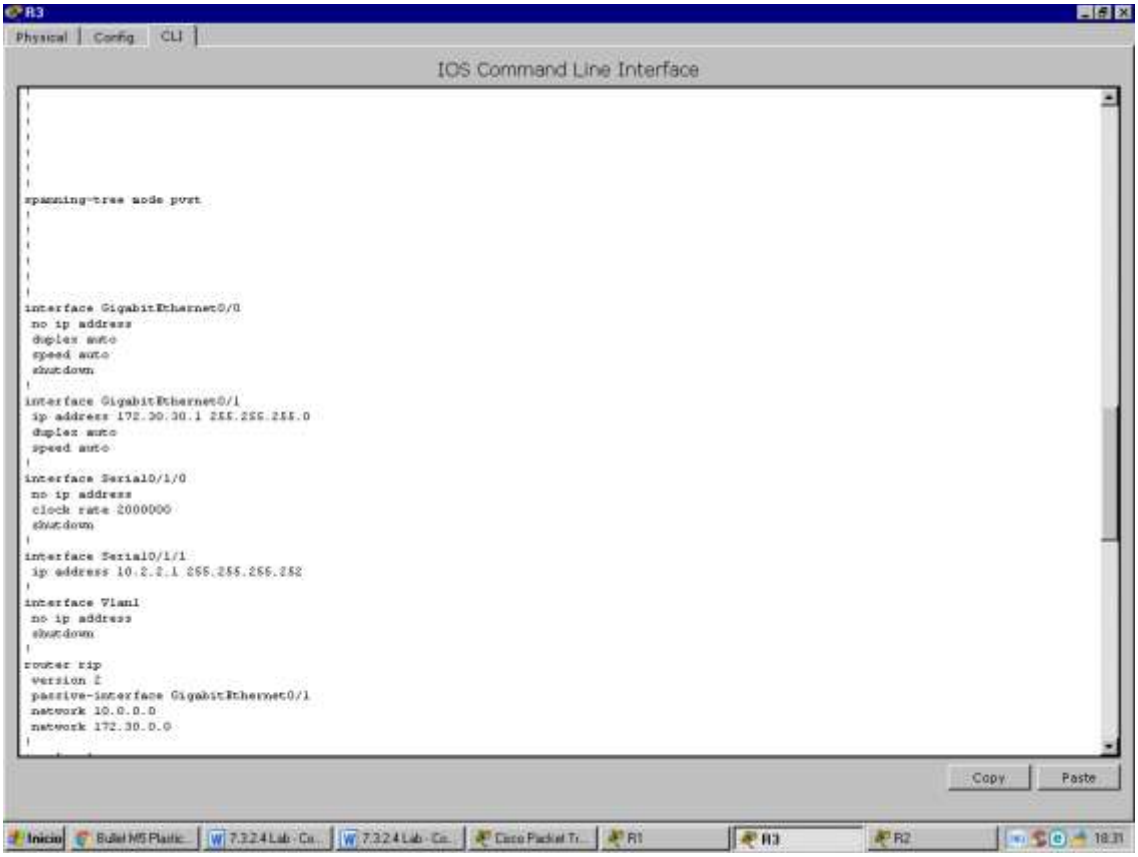

R2
Physical
Config
CLI
IOS Command Line Interface
R2(config-router)#end
R2#
*SYS-5-CONFIG_I: Configured from console by console
R2#
R2#sho
R2#show in
R2#show interfaces bri
R2#show interfaces bri
^
% Invalid input detected at '^' marker.
R2#show ip in
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 209.165.201.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 unassigned YES unset administratively down down
Serial0/1/0 10.1.1.2 YES manual up up
Serial0/1/1 10.2.2.2 YES manual up up
Vlan1 unassigned YES unset administratively down down
R2#
Copy
Paste

La mayoría de los paquetes pasan pero aun se presentan fallas en el transporte de algunos paquetes se procede a verificar y examinar el estado actual de la red

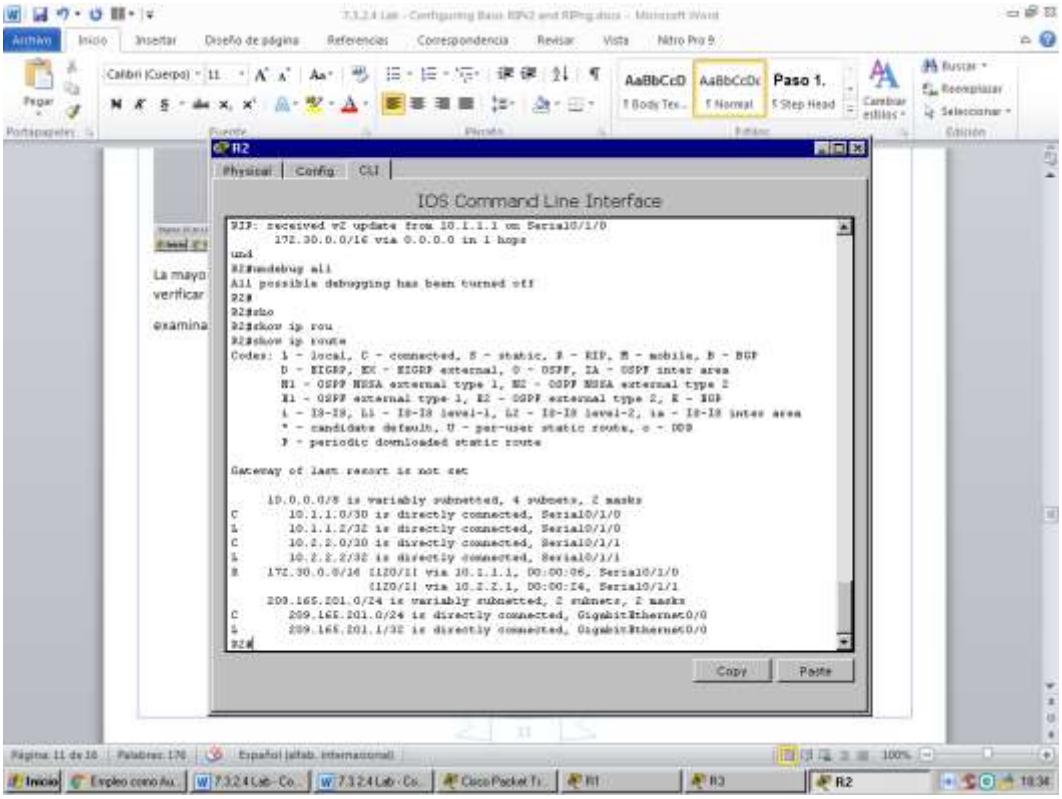


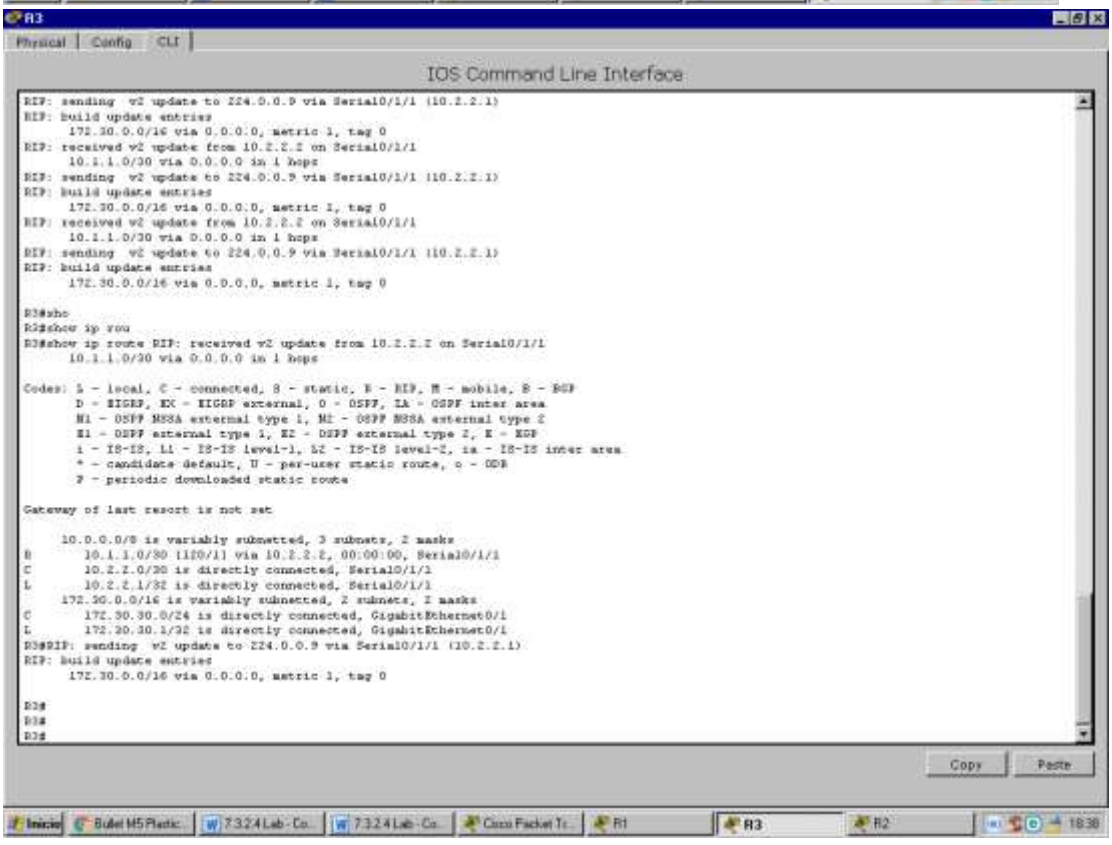


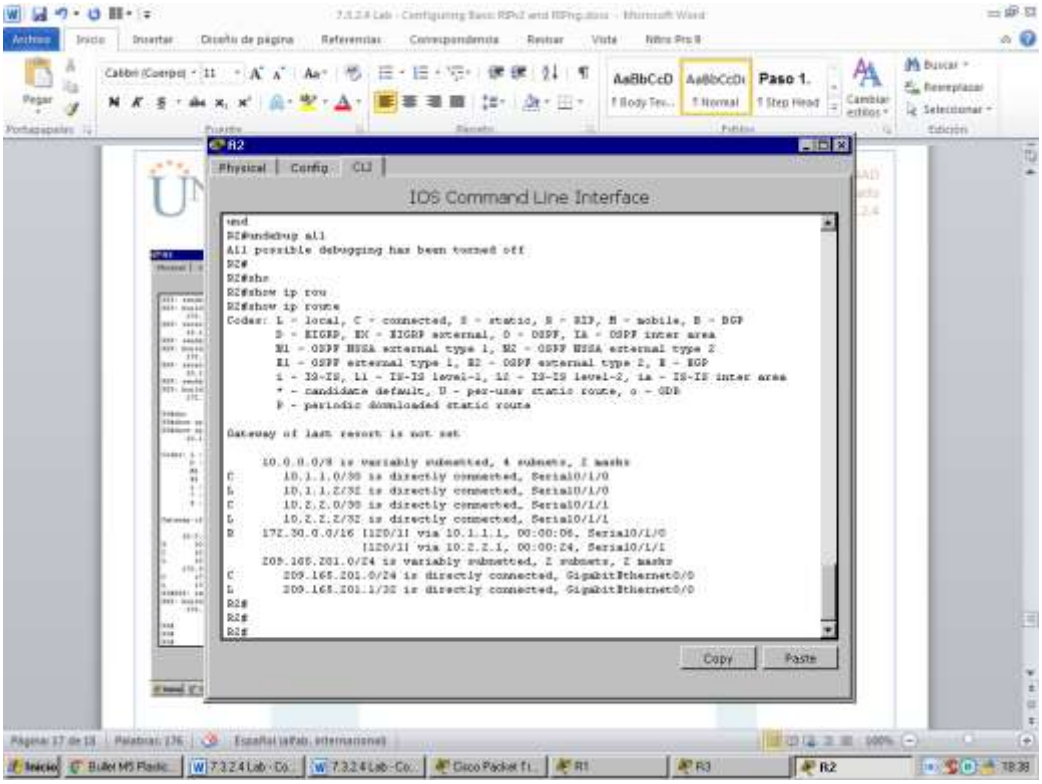

R2
Physical
Config
CLI
IOS Command Line Interface
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 209.165.201.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 unassigned YES unset administratively down down
Serial0/1/0 10.1.1.2 YES manual up up
Serial0/1/1 10.2.2.2 YES manual up up
Vlan1 unassigned YES unset administratively down down
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/1/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/1/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/1/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/1/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: sending v2 update to 224.0.0.9 via Serial0/1/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/1/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.2.2.1 on Serial0/1/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.1.1.1 on Serial0/1/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
end
R2#undebug all
All possible debugging has been turned off
R2#
Copy
Paste
Cisco Packet Tracer Student
Inicio
Bullet M5 Plastic
7.3.2.4 Lab - Co...
7.3.2.4 Lab - Co...
Cisco Packet Tr...
R1
R3
R2
10:27


R3
Physical
Config
CLI
IOS Command Line Interface
spanning-tree mode pvst
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface GigabitEthernet0/1
ip address 172.30.30.1 255.255.255.0
duplex auto
speed auto
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
interface Serial0/1/1
ip address 10.2.2.1 255.255.255.252
interface Vlan1
no ip address
shutdown
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
Copy
Paste
Inicio
Bullet M5 Plastic
7.3.2.4 Lab - Co...
7.3.2.4 Lab - Co...
Cisco Packet Tr...
R1
R3
R2
10:31

showiproute



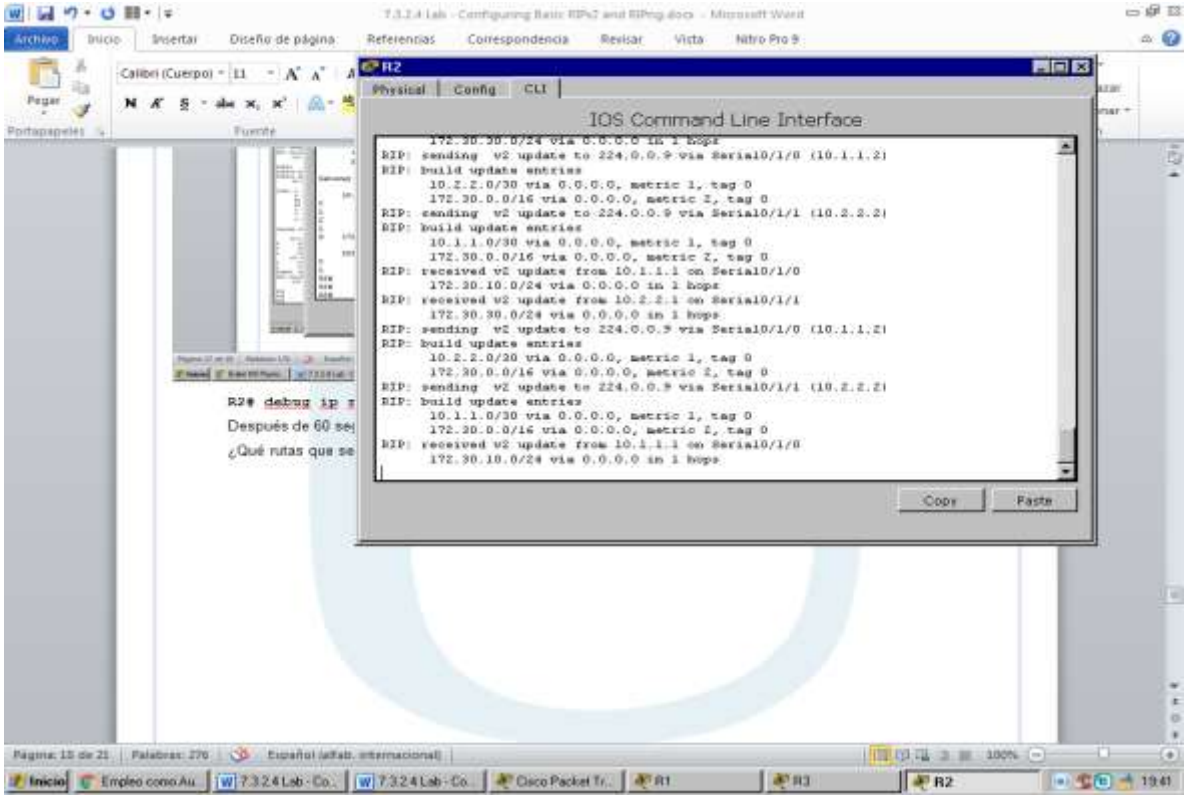


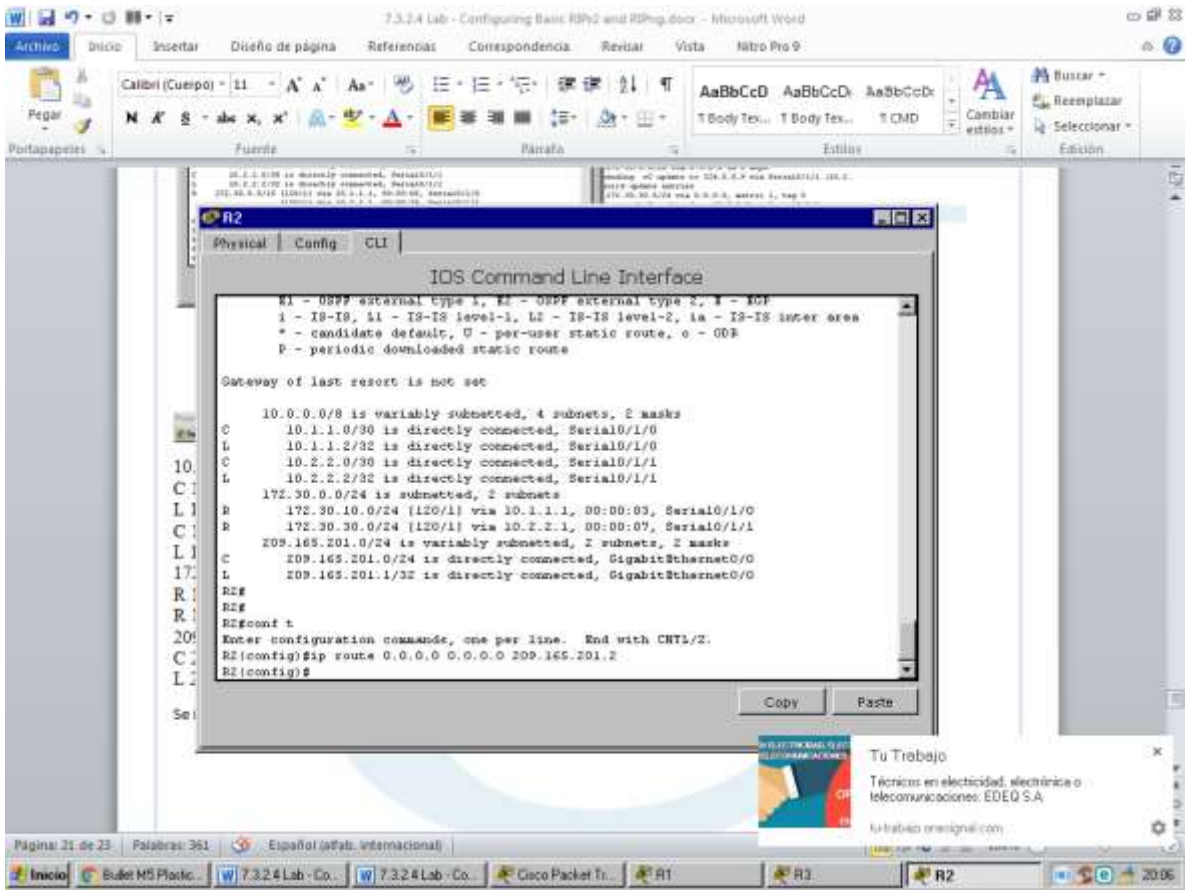


R2# debugiprip

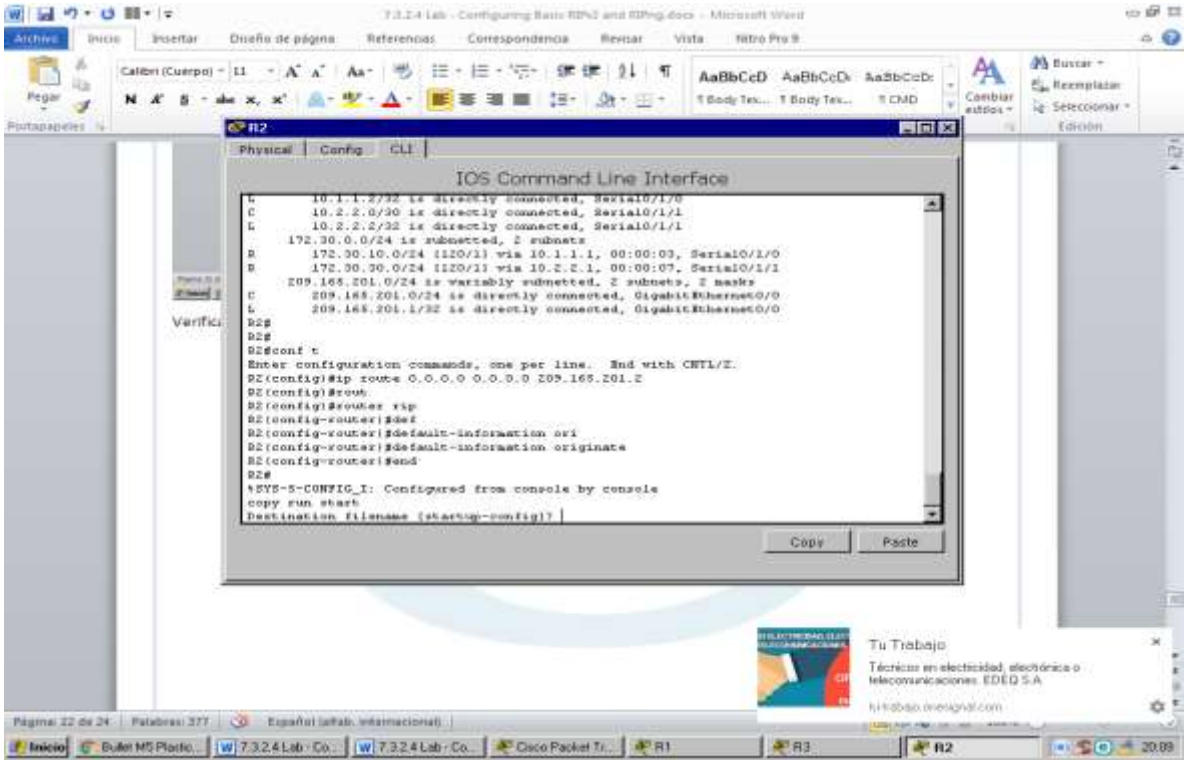
Después de 60 segundos, emita el comando no debugiprip.

¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?





Verificar la configuración de enrutamiento

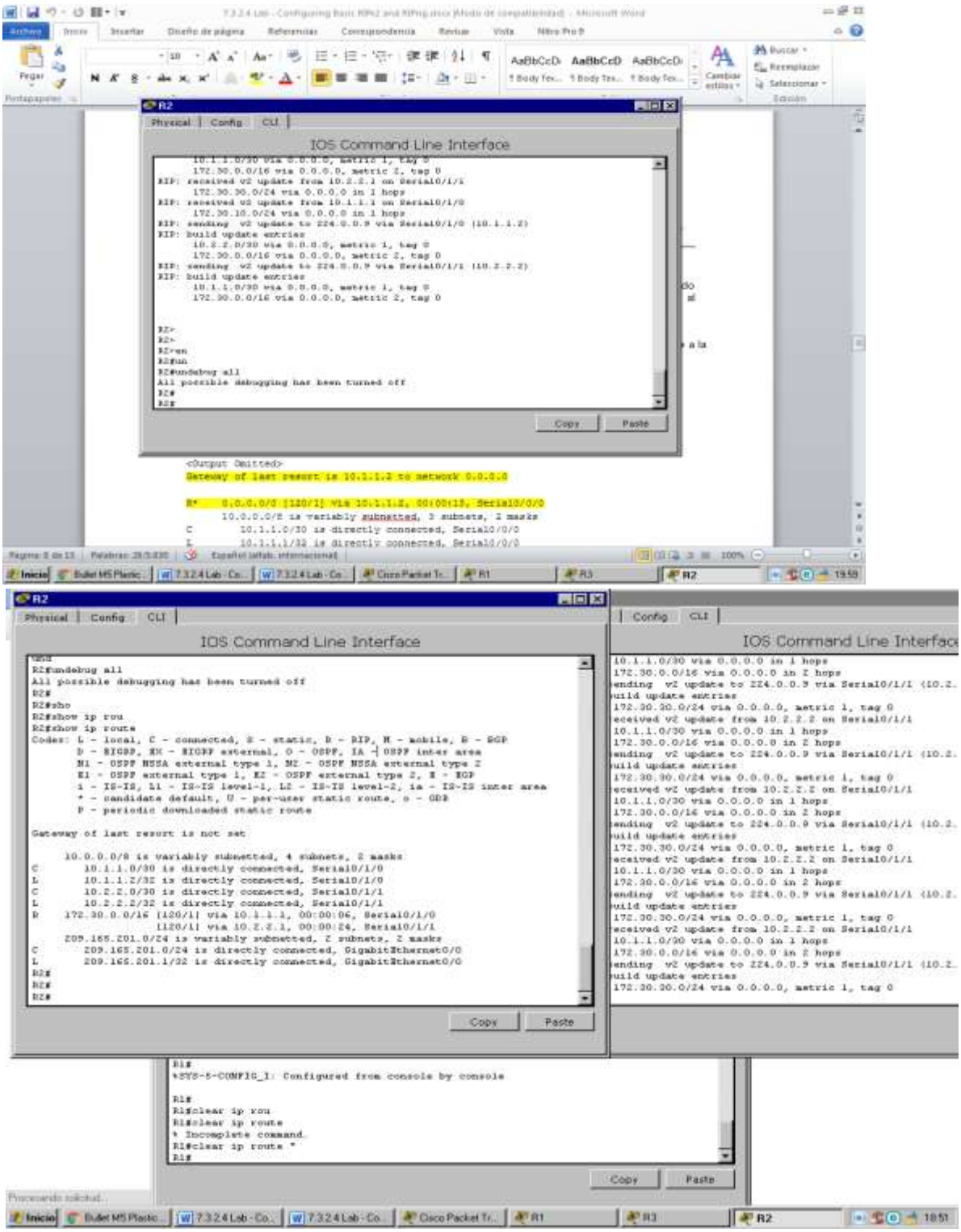


¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?

Es la 172.30.30.0/24

Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet?

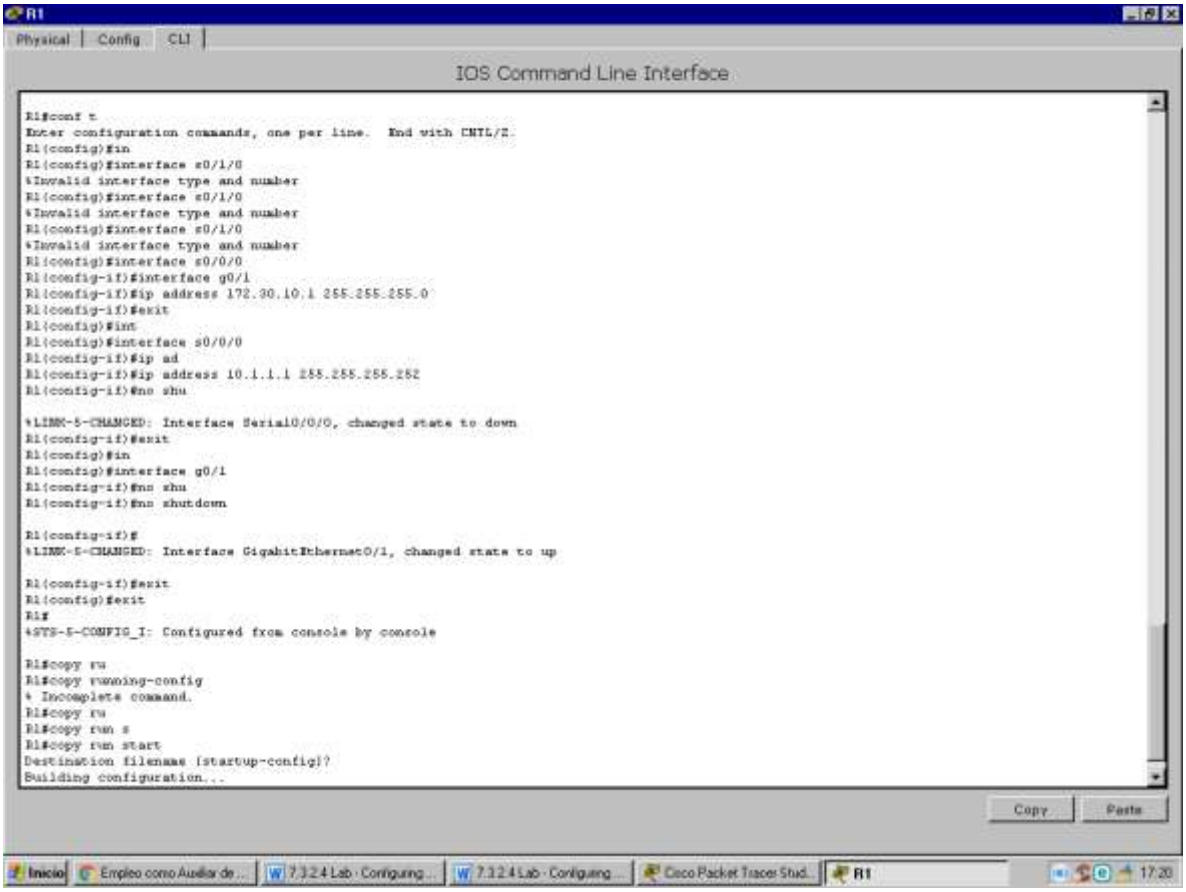
La puerta de enlace es distinta a la puerta de enlace por defaul en el router y según la tabla de direccionamiento está arriba



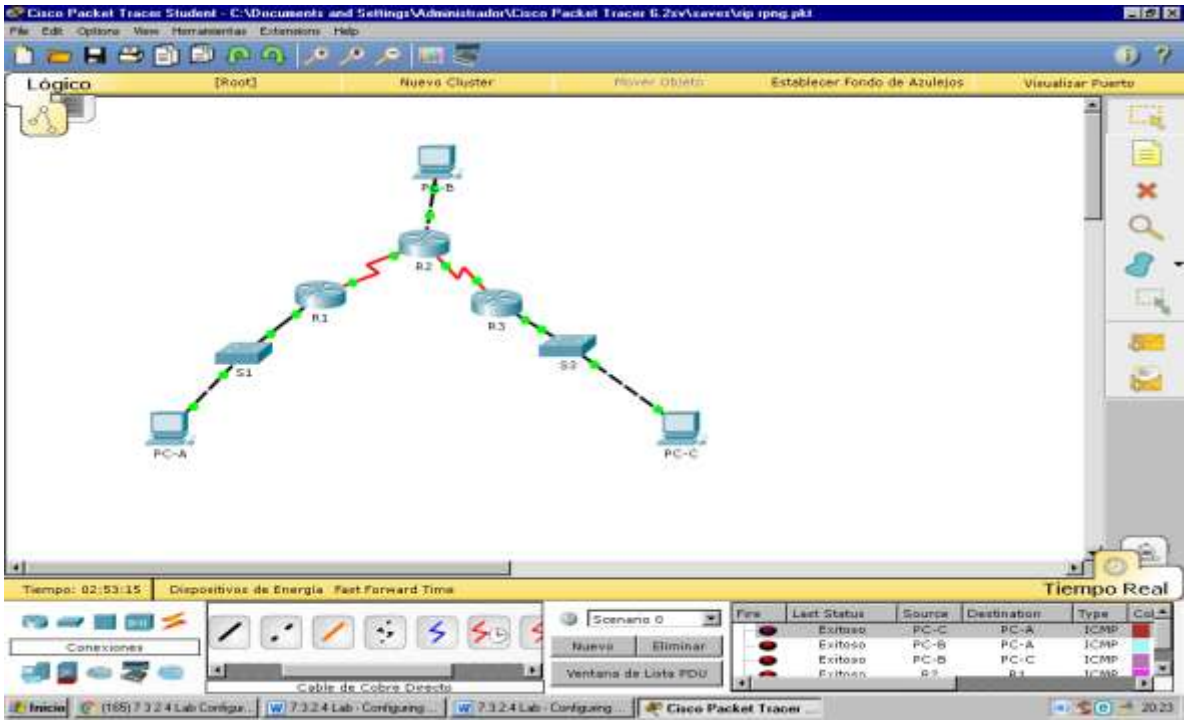
10.0.0.0/8 is variablysubnetted, 4 subnets, 2 masks
C 10.1.1.0/30 isdirectlyconnected, Serial0/1/0
L 10.1.1.2/32 isdirectlyconnected, Serial0/1/0
C 10.2.2.0/30 isdirectlyconnected, Serial0/1/1
L 10.2.2.2/32 isdirectlyconnected, Serial0/1/1

172.30.0.0/24 issubnetted, 2 subnets
R 172.30.10.0/24 [120/1] Vía 10.1.1.1, 00:00:03, Serial0/1/0
R 172.30.30.0/24 [120/1] Vía 10.2.2.1, 00:00:07, Serial0/1/1
209.165.201.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 209.165.201.0/24 isdirectlyconnected, GigabitEthernet0/0
L 209.165.201.1/32 isdirectlyconnected, GigabitEthernet0/0
Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento? Si

Configure y redistribuya una ruta predeterminada para el acceso a Internet

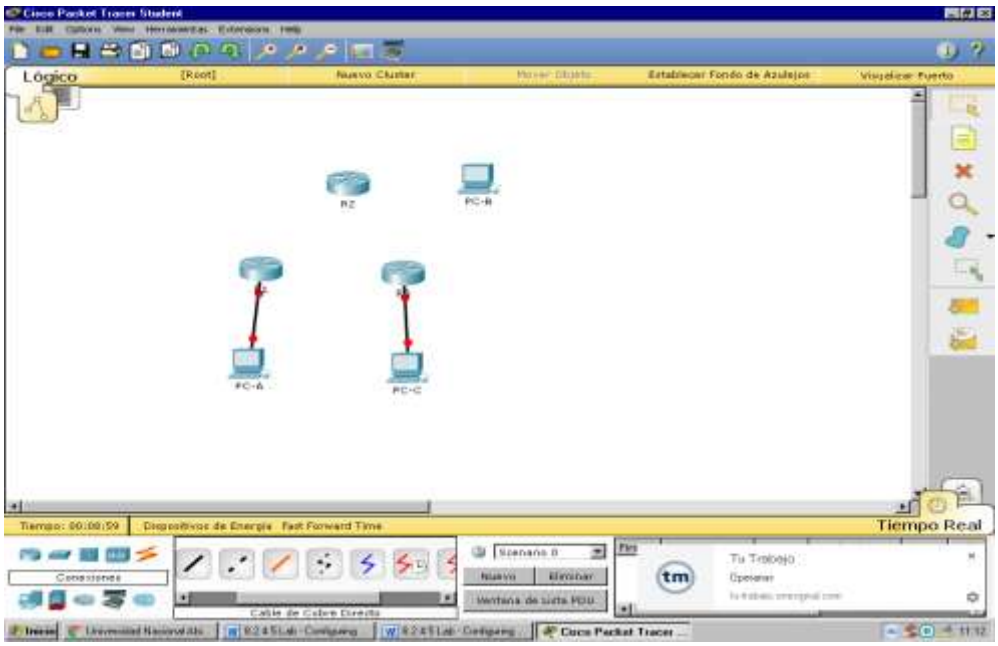


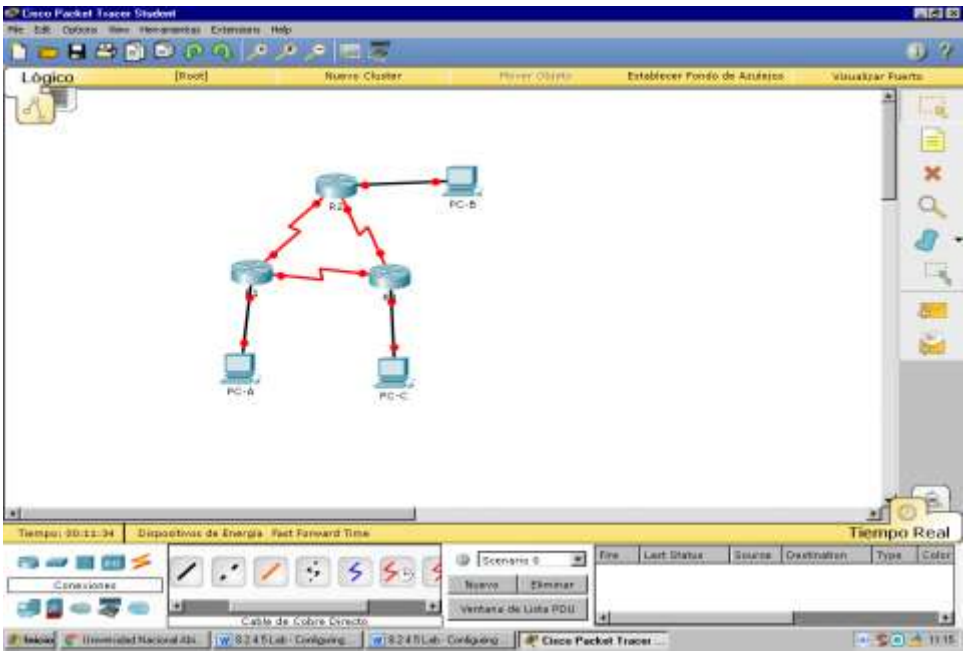
¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?
Para r2 siempre es estática y por defecto 0.0.0.0 209.165.201.2
Verifique la conectividad



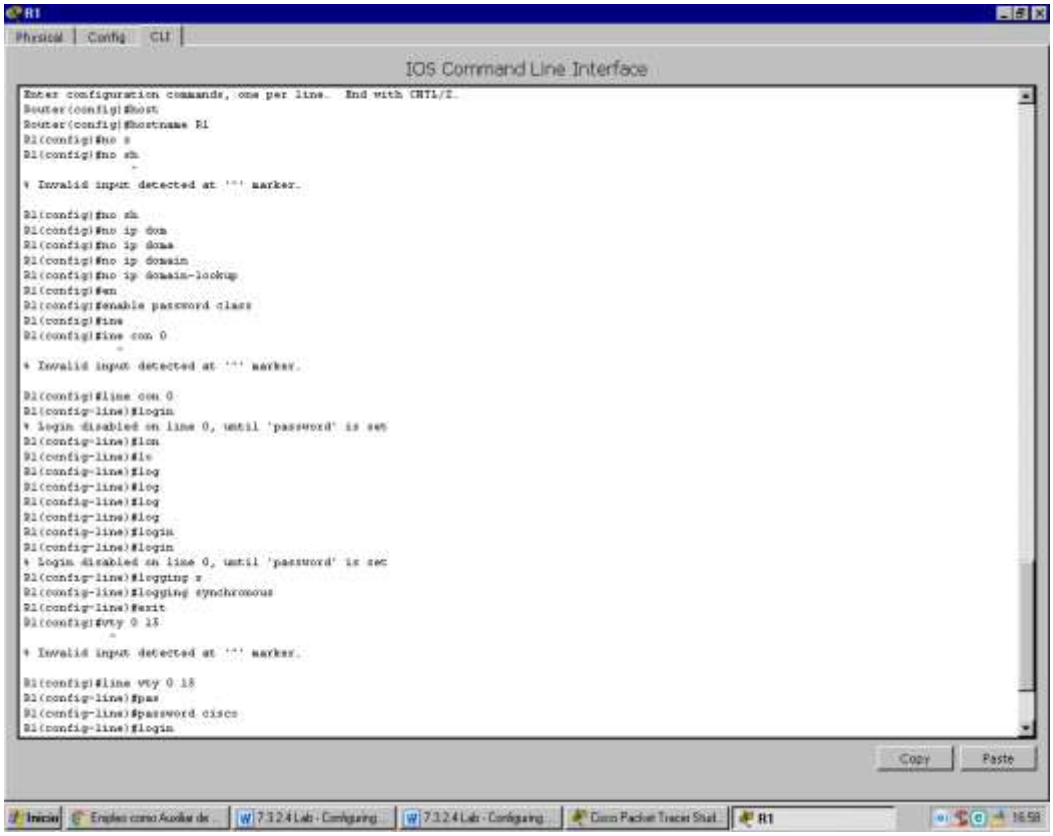
Ejercicio 8.2.4.5

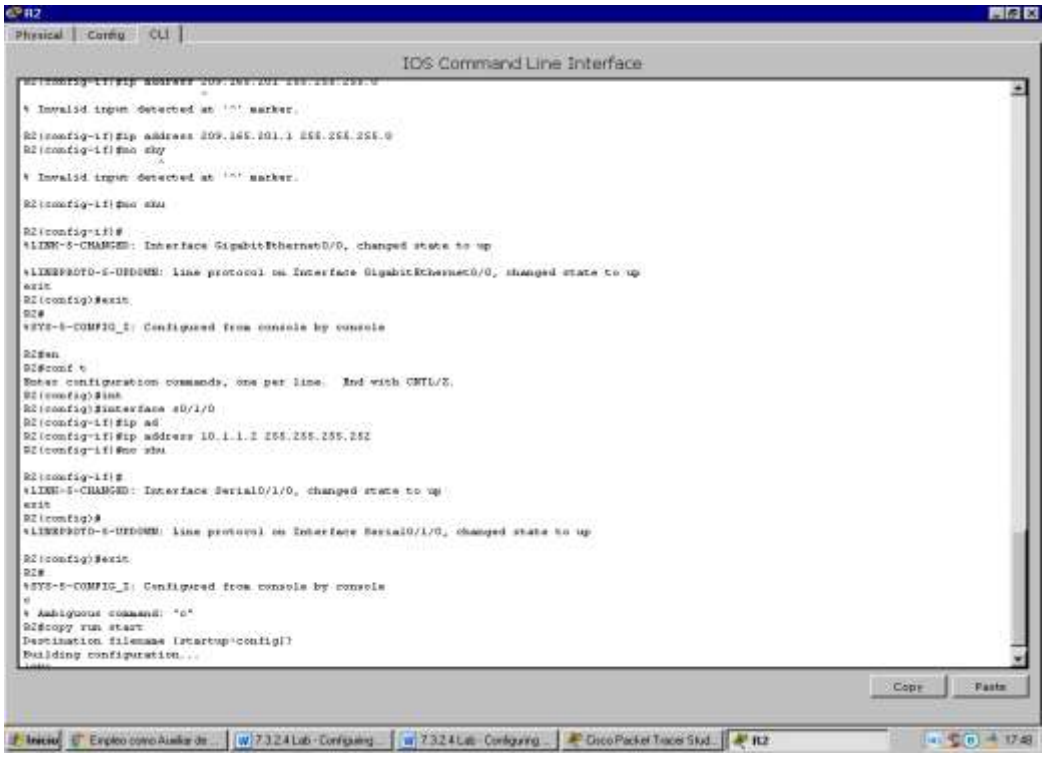
Armar la red y configurar los parámetros básicos de los dispositivos
Realizar el cableado de red tal como se muestra en la topología.
Inicializar y volver a cargar los routers según sea necesario.
Configurar los parámetros básicos para cada router.



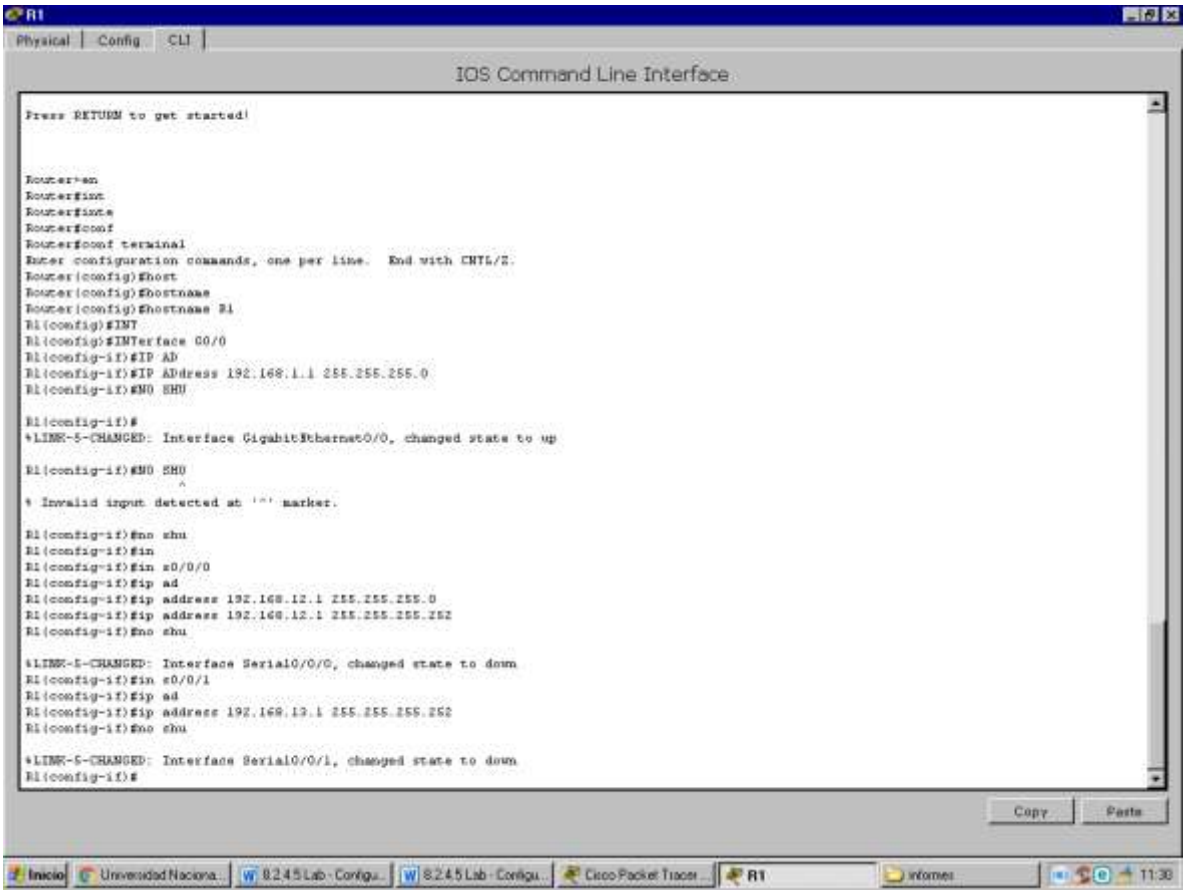


Configuración de R1 /R2 /R3

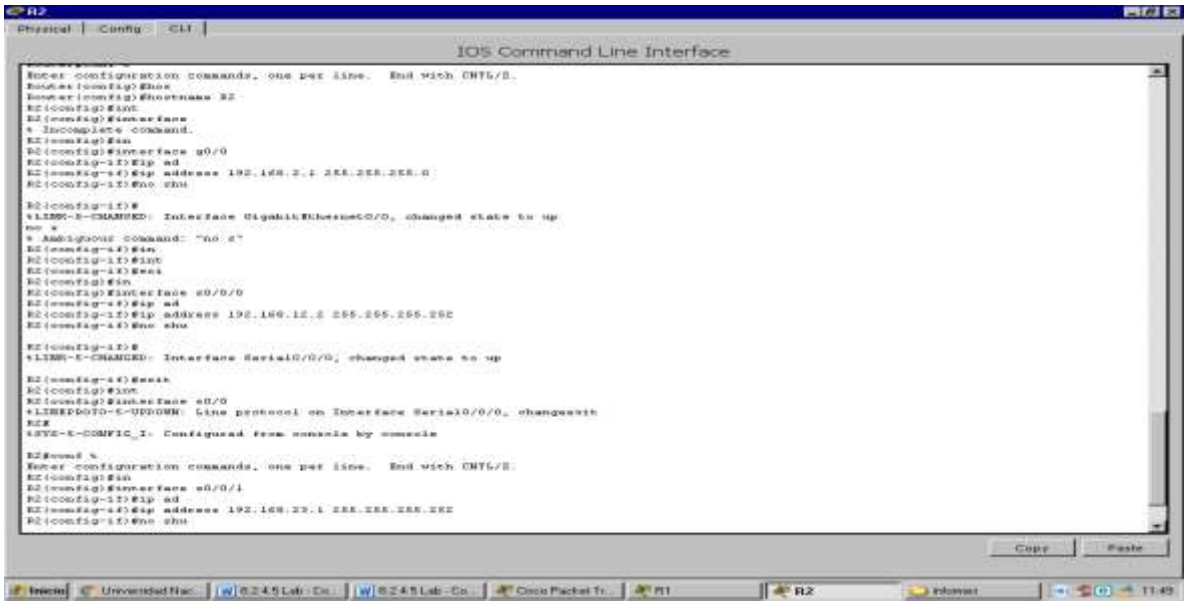




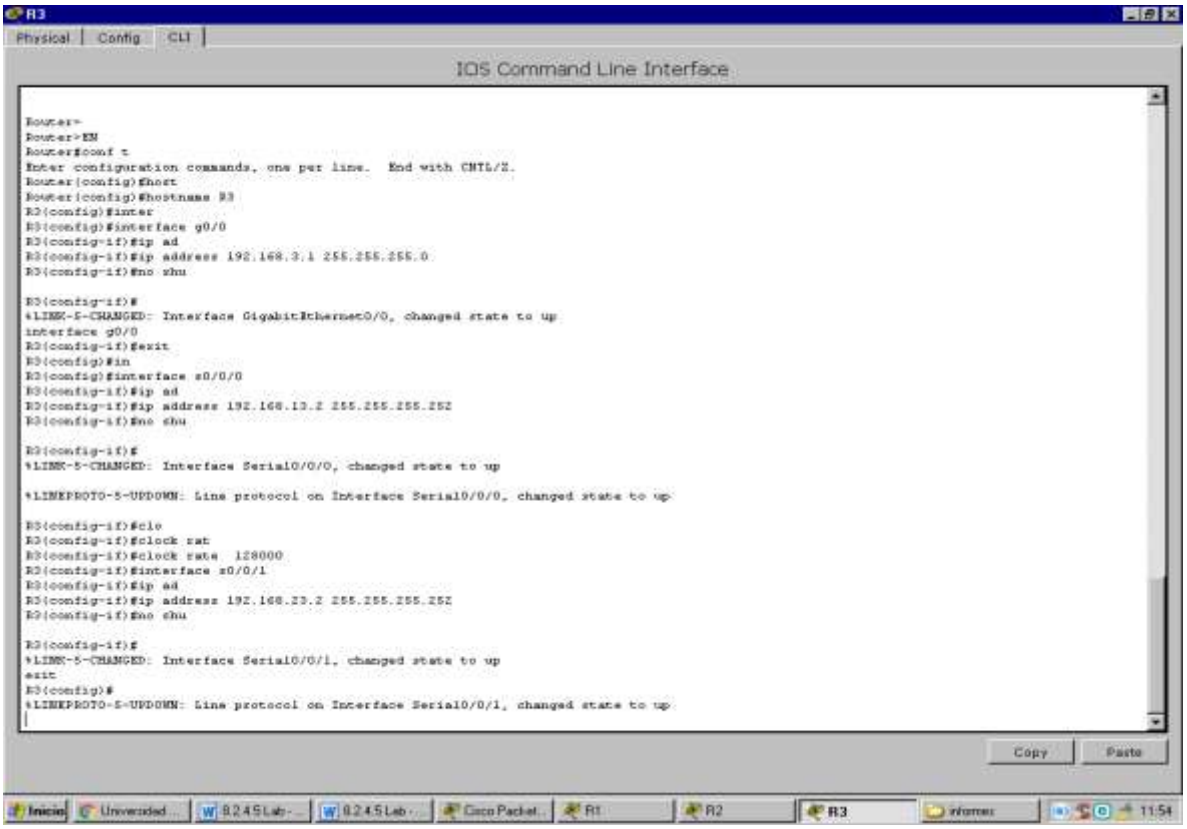
Configuración r1 ruteo

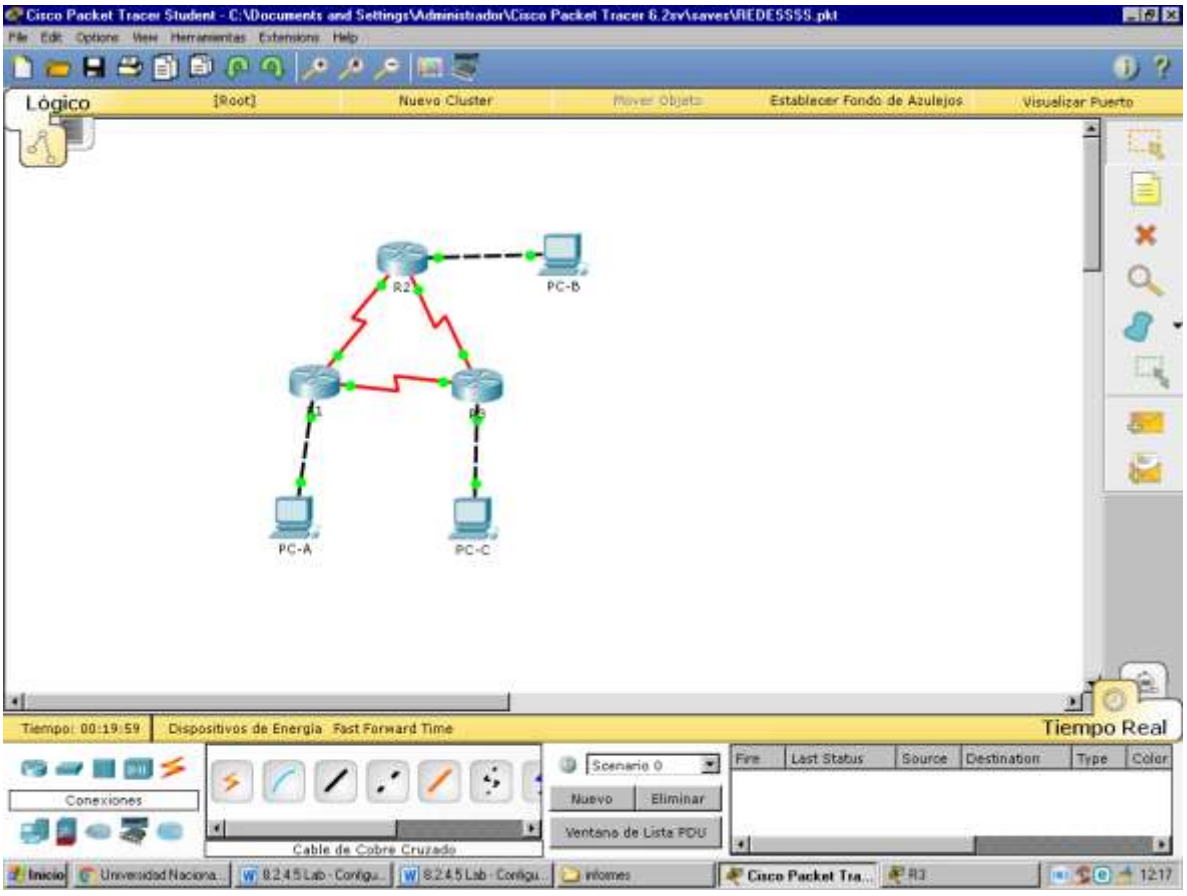

R1
Physical
Config
CLI
IOS Command Line Interface
Press RETURN to get started!
Router>en
Router#int
Router#inte
Router#conf
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname
Router(config)#hostname R1
R1(config)#INT
R1(config)#INTerface G0/0
R1(config-if)#IP AD
R1(config-if)#IP ADdress 192.168.1.1 255.255.255.0
R1(config-if)#NO SHU
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1(config-if)#NO SHU
^
% Invalid input detected at '^' marker.
R1(config-if)#no shu
R1(config-if)#in
R1(config-if)#in s0/0/0
R1(config-if)#ip ad
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#in s0/0/1
R1(config-if)#ip ad
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#
Copy
Paste
Inicio
Universidad Naciona...
8.2.4.5 Lab - Configu...
8.2.4.5 Lab - Configu...
Cisco Packet Tracer ...
R1
informes
11:38

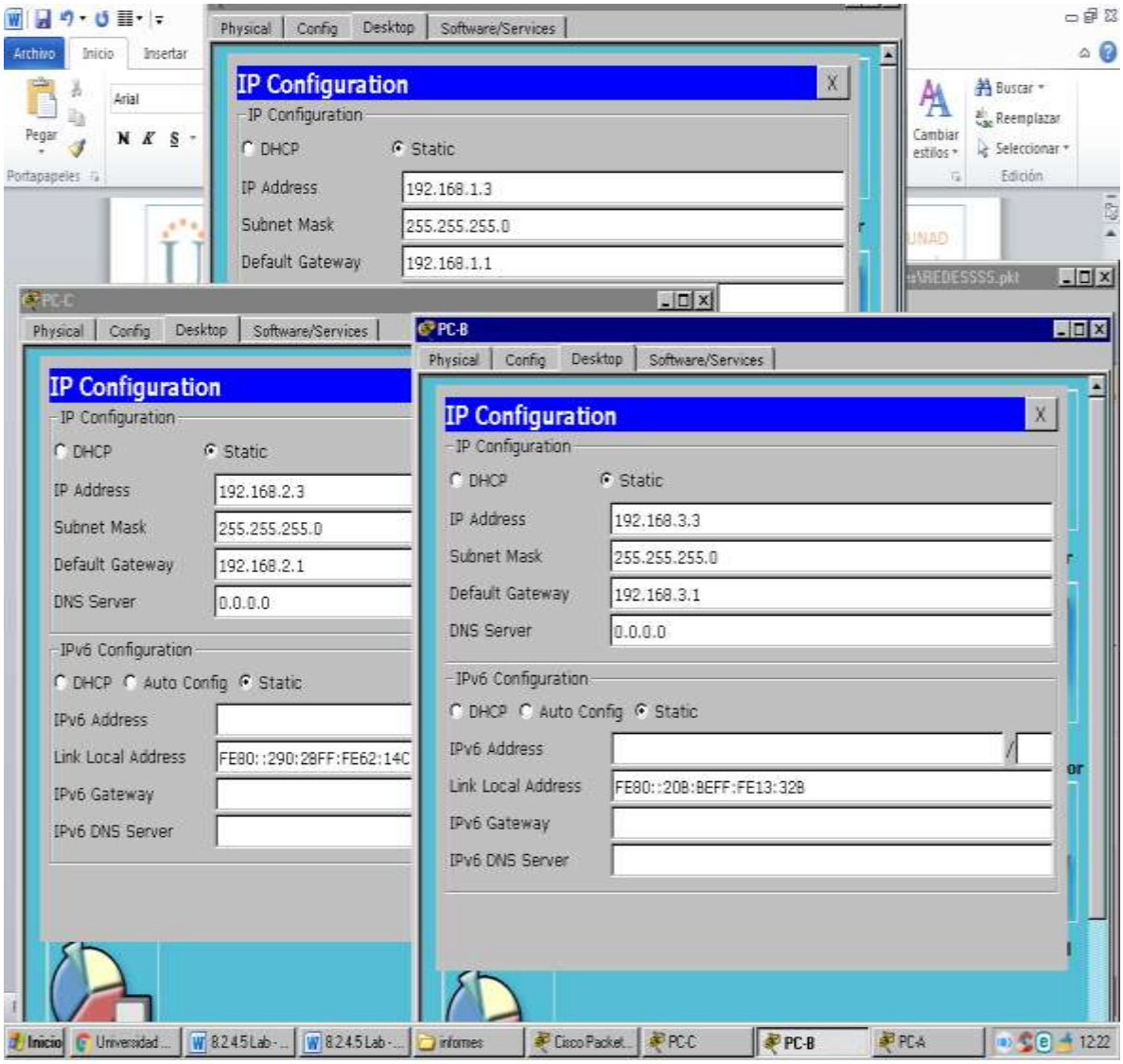
R2


R2
Physical
Config
CLI
IOS Command Line Interface
Copy
Paste
R2
informes

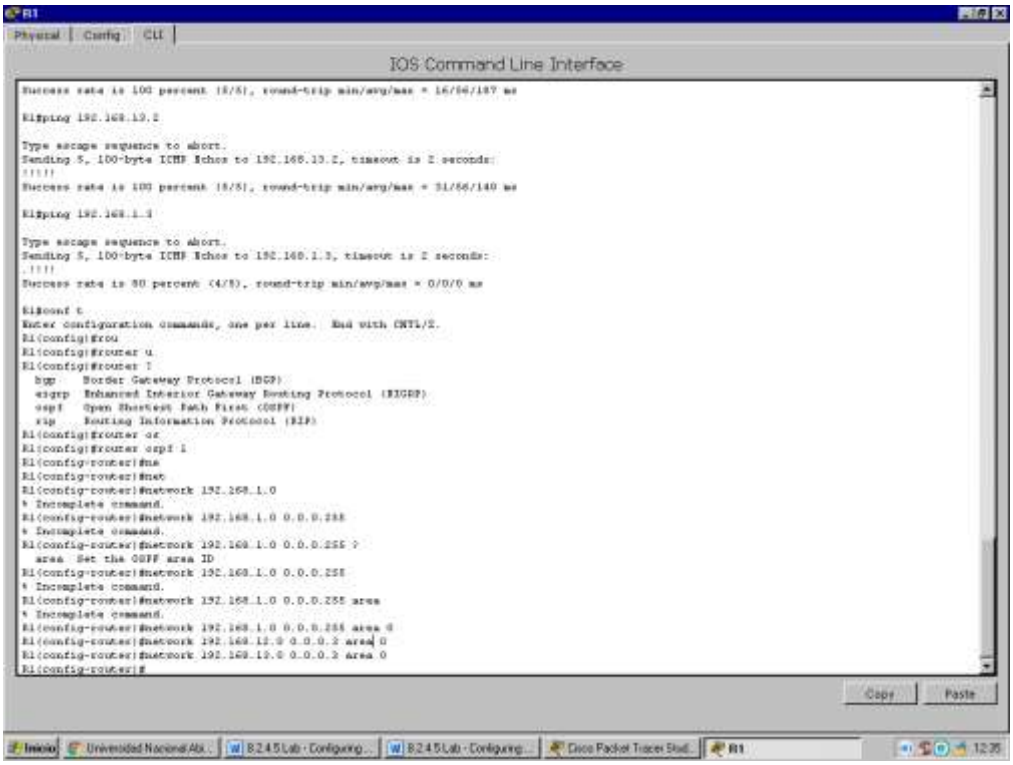
R3


R3
Physical
Config
CLI
IOS Command Line Interface
Router>
Router>EN
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname R3
R3(config)#inter
R3(config)#interface g0/0
R3(config-if)#ip ad
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shu
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
interface g0/0
R3(config-if)#exit
R3(config)#in
R3(config)#interface s0/0/0
R3(config-if)#ip ad
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config-if)#no shu
R3(config-if)#
%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
R3(config-if)#clo
R3(config-if)#clock rat
R3(config-if)#clock rate 128000
R3(config-if)#interface s0/0/1
R3(config-if)#ip ad
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no shu
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
exit
R3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Copy
Paste
Inicio
Universidad ...
8.2.4.5 Lab - ...
8.2.4.5 Lab - ...
Cisco Packet ...
R1
R2
R3
informes
11:54

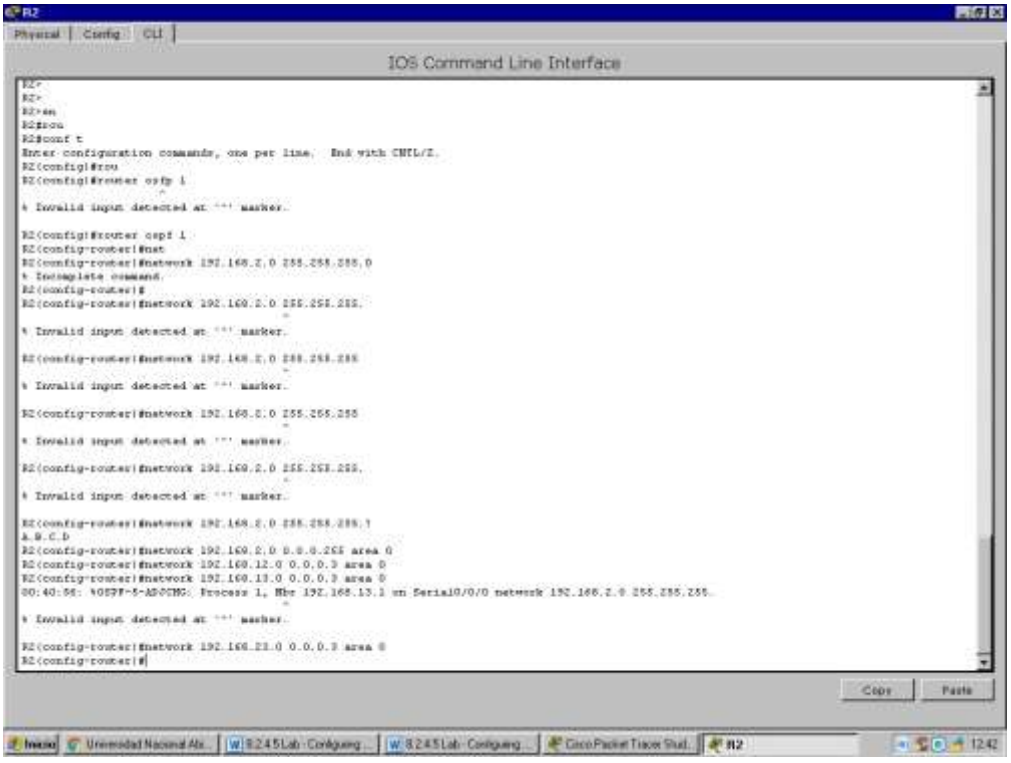

Cisco Packet Tracer Student - C:\Documents and Settings\Administrador\Cisco Packet Tracer 6.2sv\saves\REDE5SSS.pkt
File Edit Options View Herramientas Extensions Help
Lógico
[Root]
Nuevo Cluster
Mover Objeto
Establecer Fondo de Azulejos
Visualizar Puerto
R2
PC-B
R1
R3
PC-A
PC-C
Tiempo: 00:19:59
Dispositivos de Energía Fast Forward Time
Tiempo Real
Conexiones
Cable de Cobre Cruzado
Scenario 0
Nuevo
Eliminar
Ventana de Lista PDU
Fire
Last Status
Source
Destination
Type
Color
Inicio
Universidad Naciona...
8.2.4.5 Lab - Configu...
8.2.4.5 Lab - Configu...
informes
Cisco Packet Tra...
R3
12:17



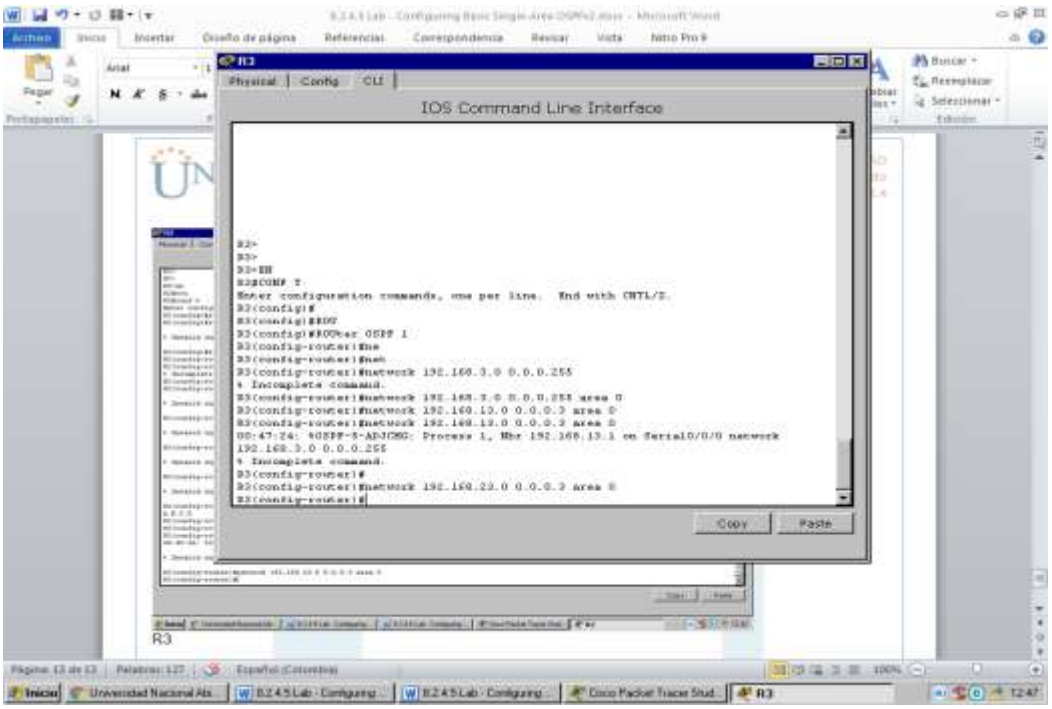
Configurar los equipos host.
Probar la conectividad


R1
Physical
Config
CLI
IOS Command Line Interface
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/56/187 ms
Sipping 192.168.13.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/140 ms
Sipping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#rou
R1(config)#router u
R1(config)#router ?
bgp Border Gateway Protocol (BGP)
eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)
ospf Open Shortest Path First (OSPF)
rip Routing Information Protocol (RIP)
R1(config)#router os
R1(config)#router ospf 1
R1(config-router)#ne
R1(config-router)#net
R1(config-router)#network 192.168.1.0
% Incomplete command.
R1(config-router)#network 192.168.1.0 0.0.0.255
% Incomplete command.
R1(config-router)#network 192.168.1.0 0.0.0.255 ?
area Set the OSPF area ID
R1(config-router)#network 192.168.1.0 0.0.0.255
% Incomplete command.
R1(config-router)#network 192.168.1.0 0.0.0.255 area
% Incomplete command.
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
Copy
Paste

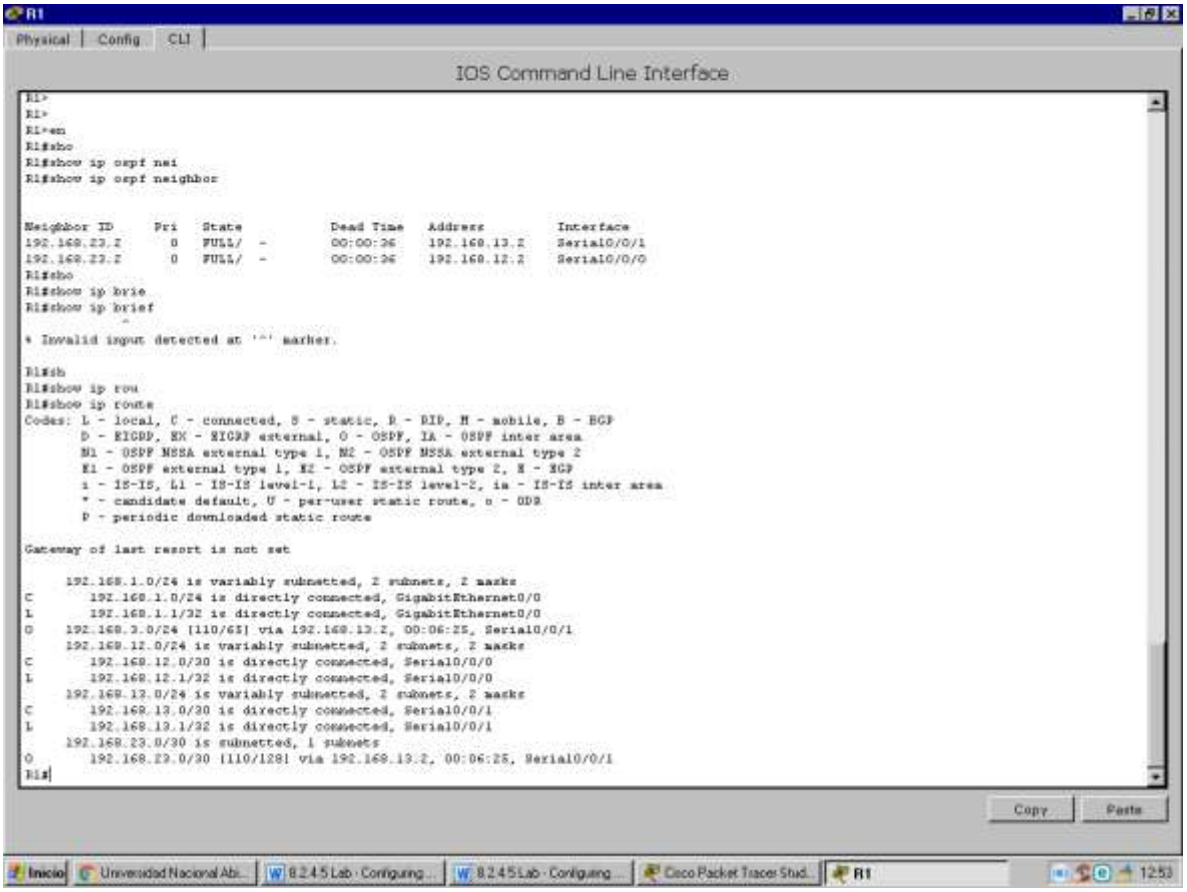
R2


R2
Physical
Config
CLI
IOS Command Line Interface
R2>
R2>
R2>en
R2#rou
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#rou
R2(config)#router ospf 1
% Invalid input detected at '^' marker.
R2(config)#router ospf 1
R2(config-router)#net
R2(config-router)#network 192.168.2.0 255.255.255.0
% Incomplete command.
R2(config-router)#
R2(config-router)#network 192.168.2.0 255.255.255.
% Invalid input detected at '^' marker.
R2(config-router)#network 192.168.2.0 255.255.255
% Invalid input detected at '^' marker.
R2(config-router)#network 192.168.2.0 255.255.255
% Invalid input detected at '^' marker.
R2(config-router)#network 192.168.2.0 255.255.255.
% Invalid input detected at '^' marker.
R2(config-router)#network 192.168.2.0 255.255.255.1
A.B.C.D
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.13.0 0.0.0.3 area 0
00:40:56: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 network 192.168.2.0 255.255.255.
% Invalid input detected at '^' marker.
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#
Copy
Paste

R3

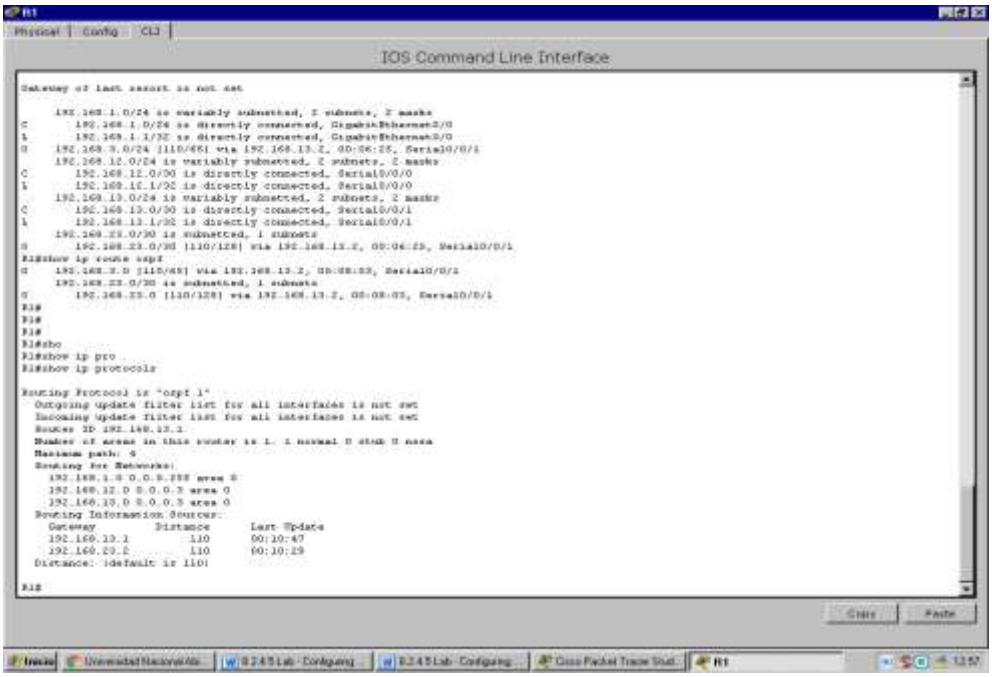


Verificar los vecinos OSPF y la información de routing

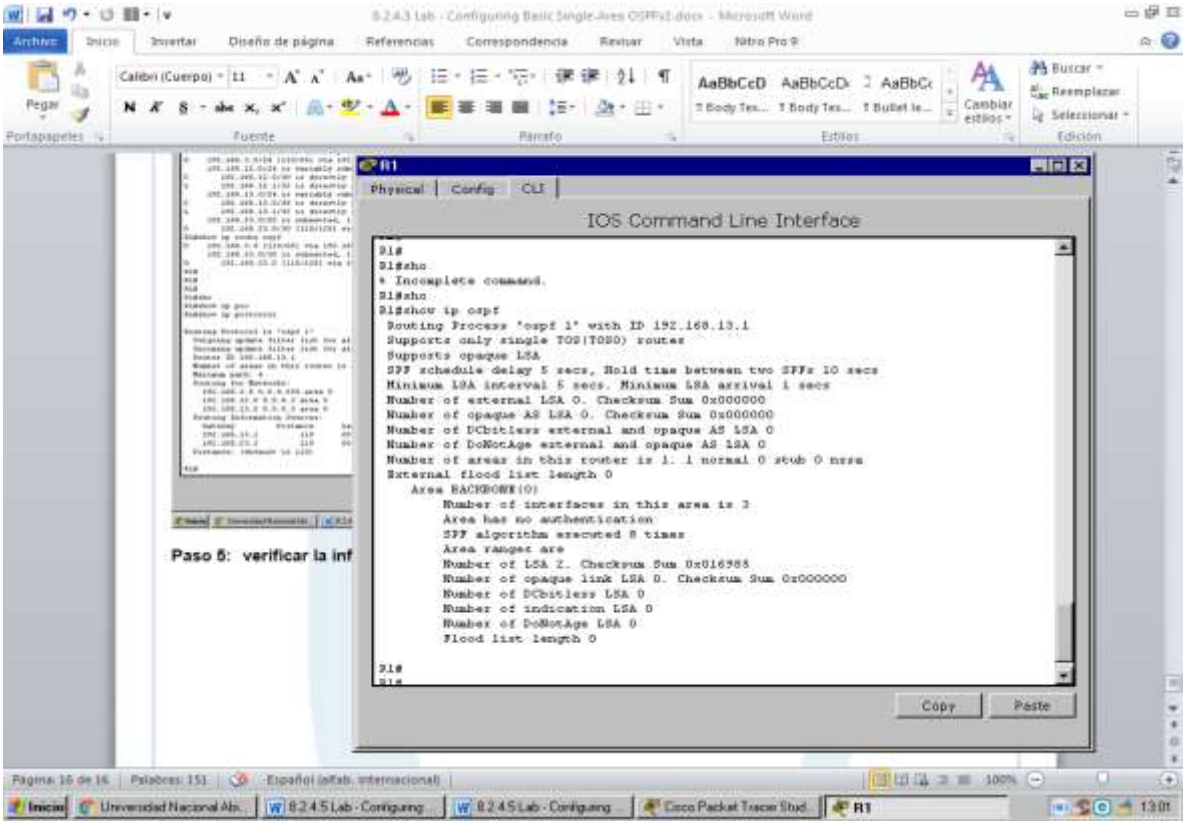


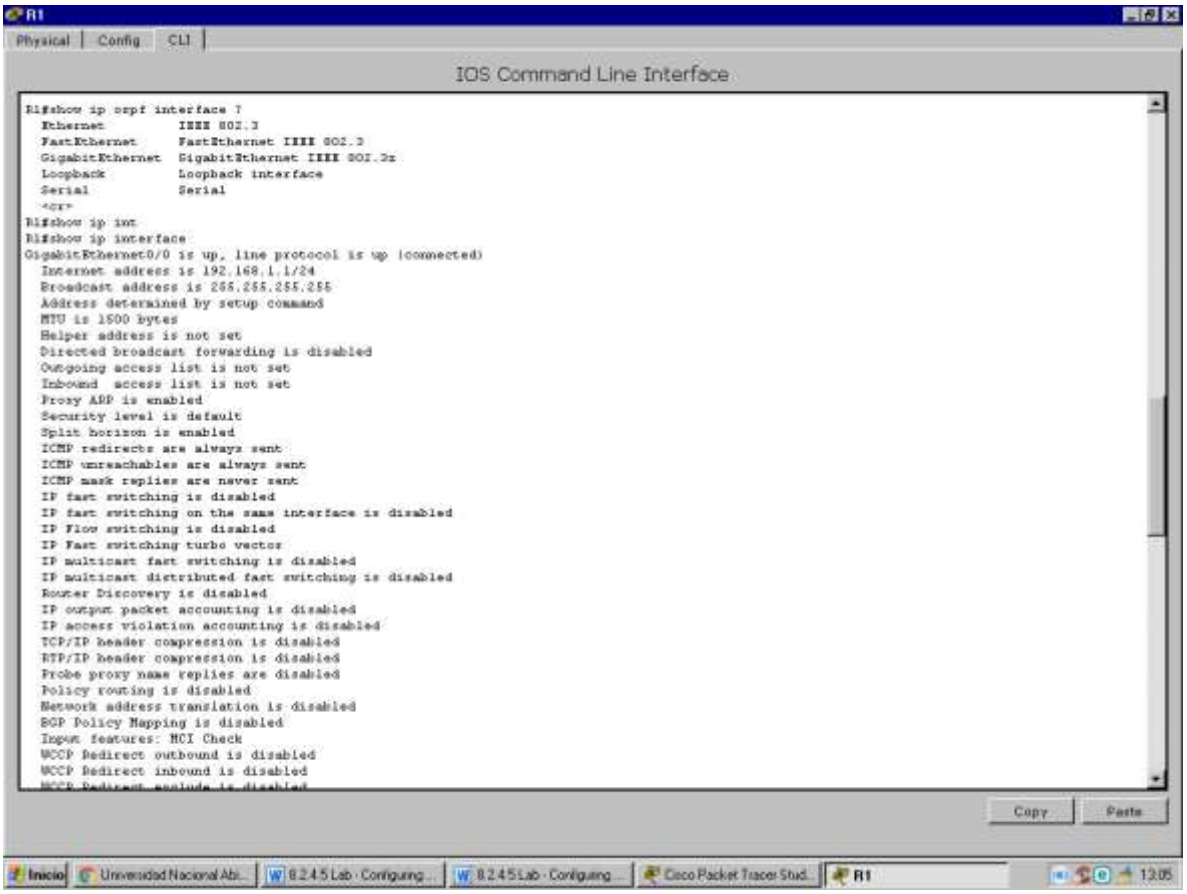
Verificar la configuración del protocolo OSPF.

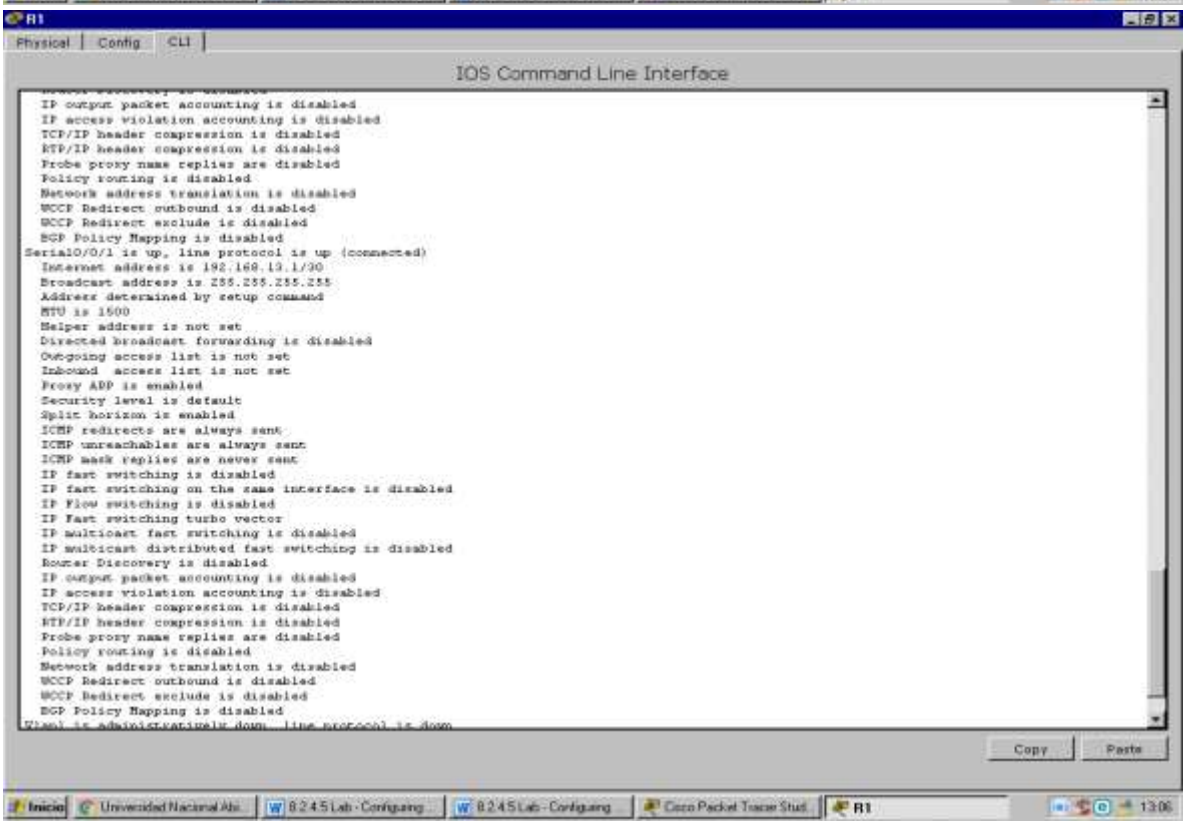
R1



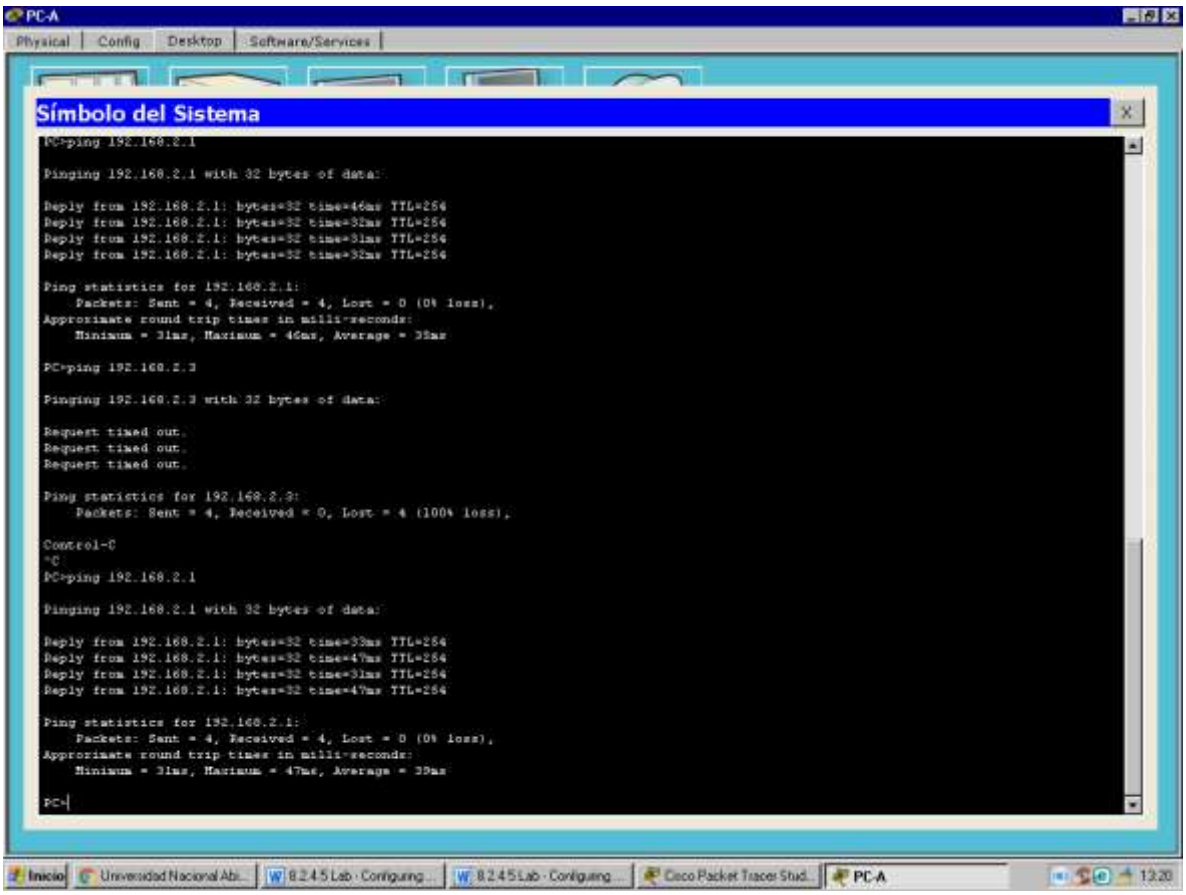
Verificar la información del proceso OSPF.




R1
Physical
Config
CLI
IOS Command Line Interface
R1#show ip ospf interface ?
FastEthernet FastEthernet IEEE 802.3
GigabitEthernet GigabitEthernet IEEE 802.3z
Loopback Loopback interface
Serial Serial
<cr>
R1#show ip int
R1#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
Copy
Paste
Inicio
Universidad Nacional Abi...
8.2.4.5 Lab - Configuring...
8.2.4.5 Lab - Configuring...
Cisco Packet Tracer Stud...
R1
13:05


R1
Physical
Config
CLI
IOS Command Line Interface
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
Internet address is 192.168.13.1/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Vlan1 is administratively down, line protocol is down
Copy
Paste
Inicio
Universidad Nacional Abi...
8.2.4.5 Lab - Configuring...
8.2.4.5 Lab - Configuring...
Cisco Packet Tracer Stud...
R1
13:06

Verificar la conectividad de extremo a extremo



Se procede a realizar la siguiente configuración en los 3 routers igual realizando el reset

#show ip proto
R3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.23.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.3.0 0.0.0.255 area 0
192.168.13.0 0.0.0.3 area 0
192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update

192.168.13.1 110 00:11:26
192.168.23.2 110 00:11:26
Distance: (default is 110)

R3#copy
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#relo
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

_____
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##
######## [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 0 0x00200000 Onboard devices &
buffer pools 0x01E8F000

TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

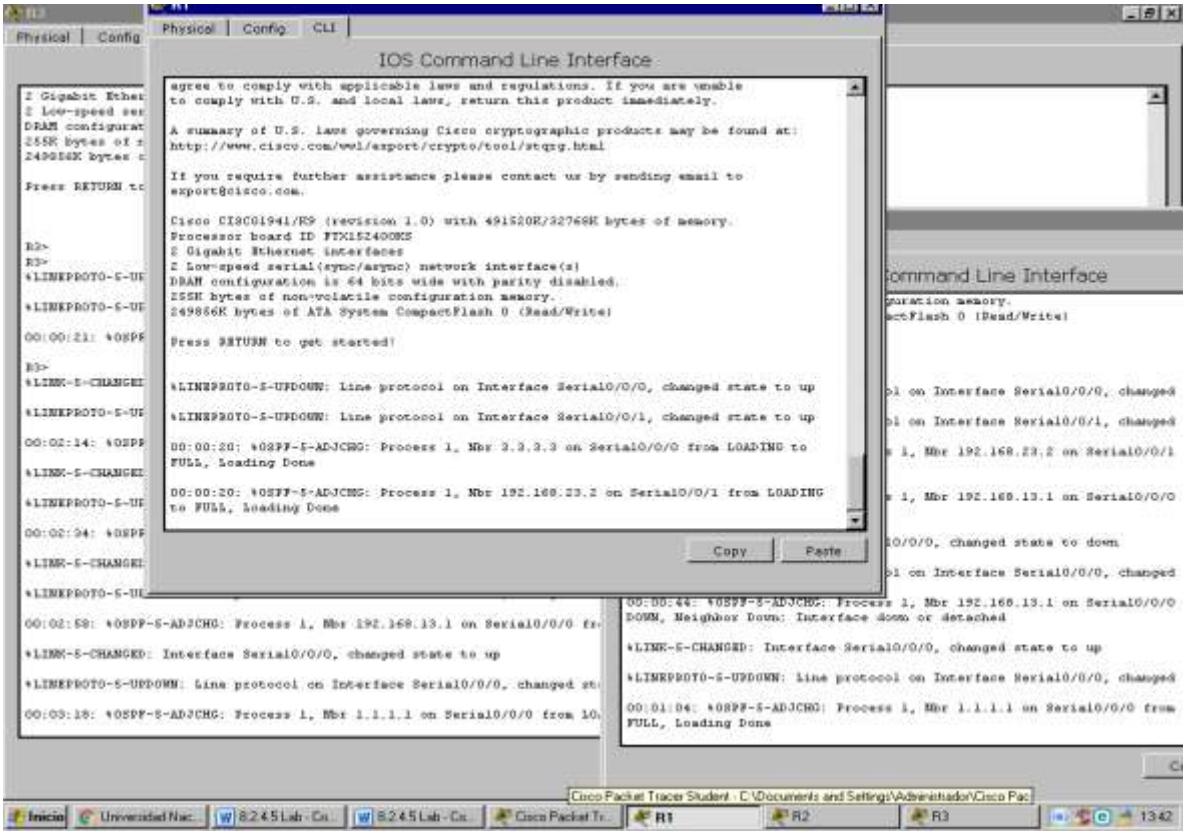
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

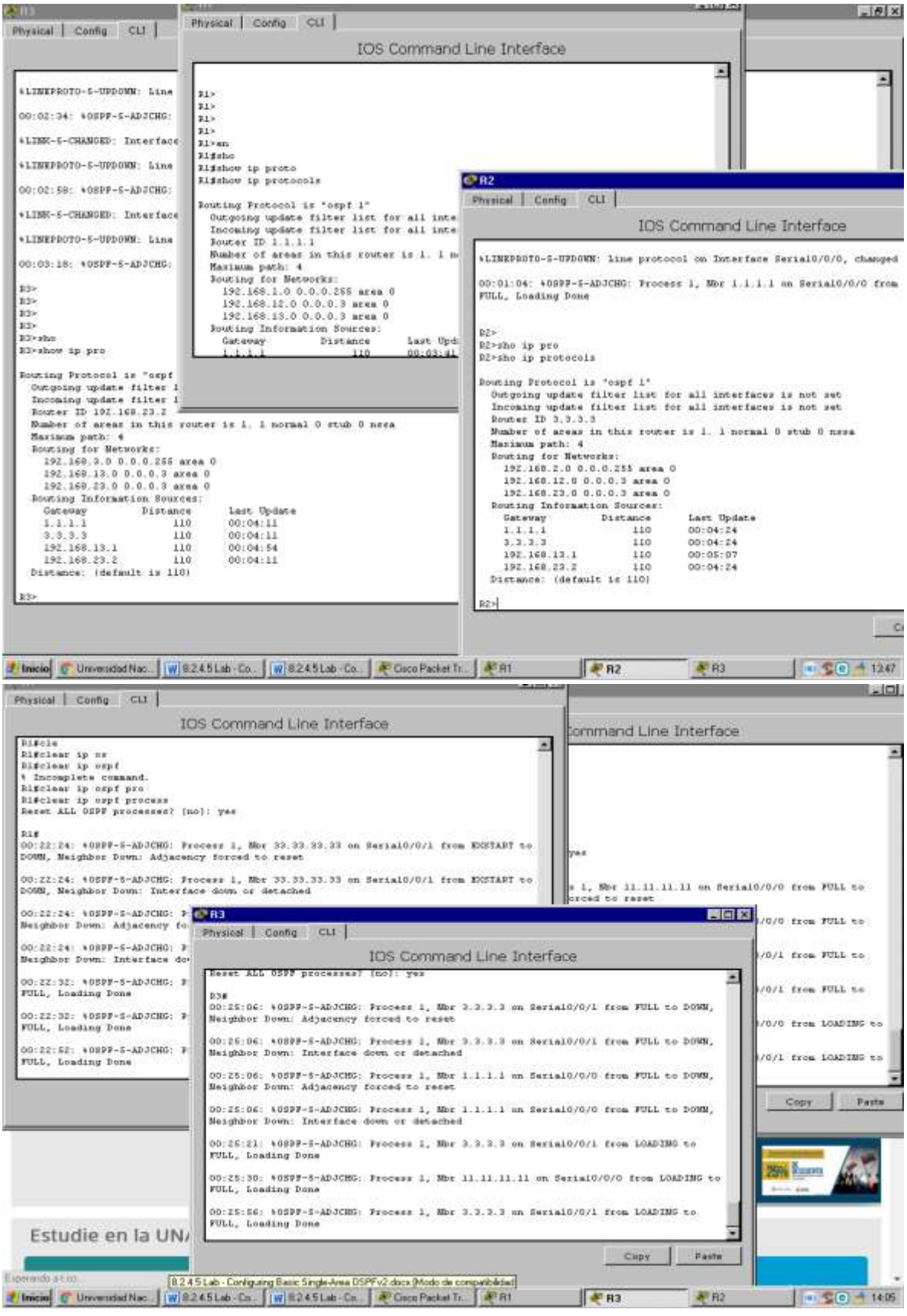
Press RETURN to get started!

R3>
R3>
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

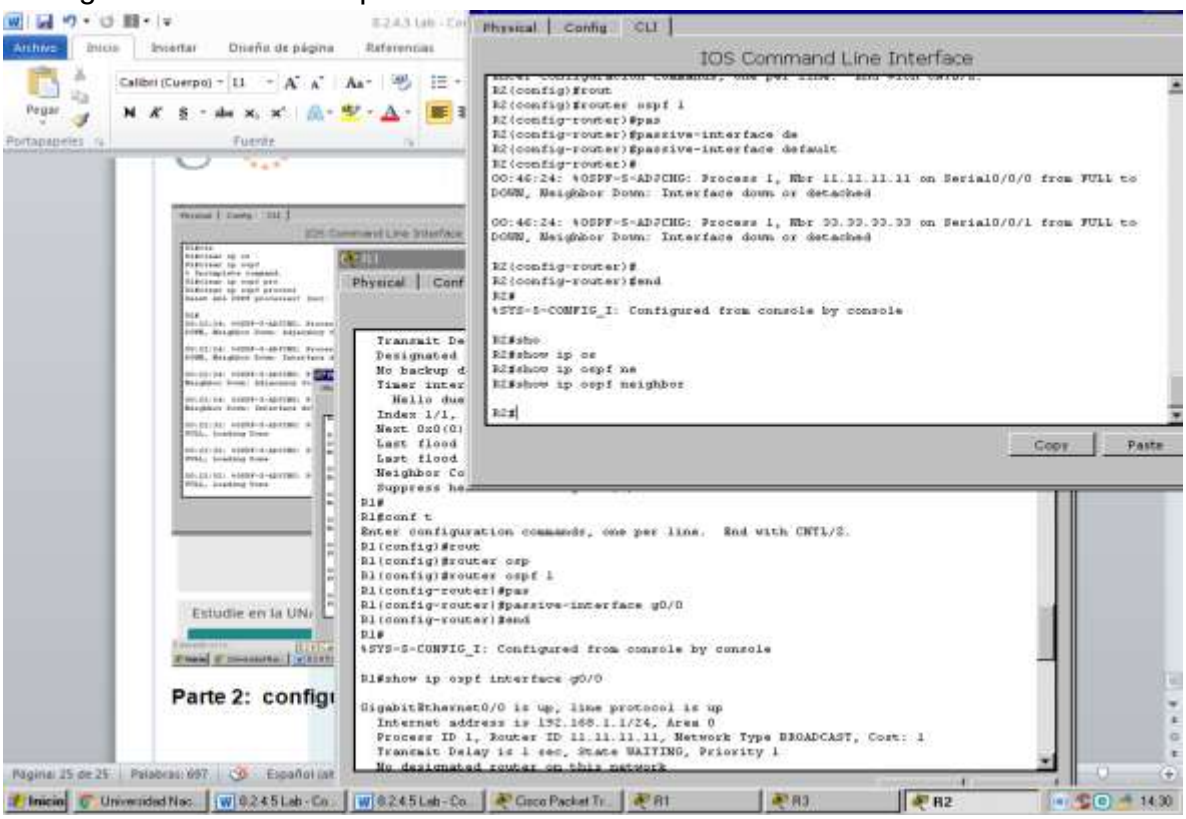
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

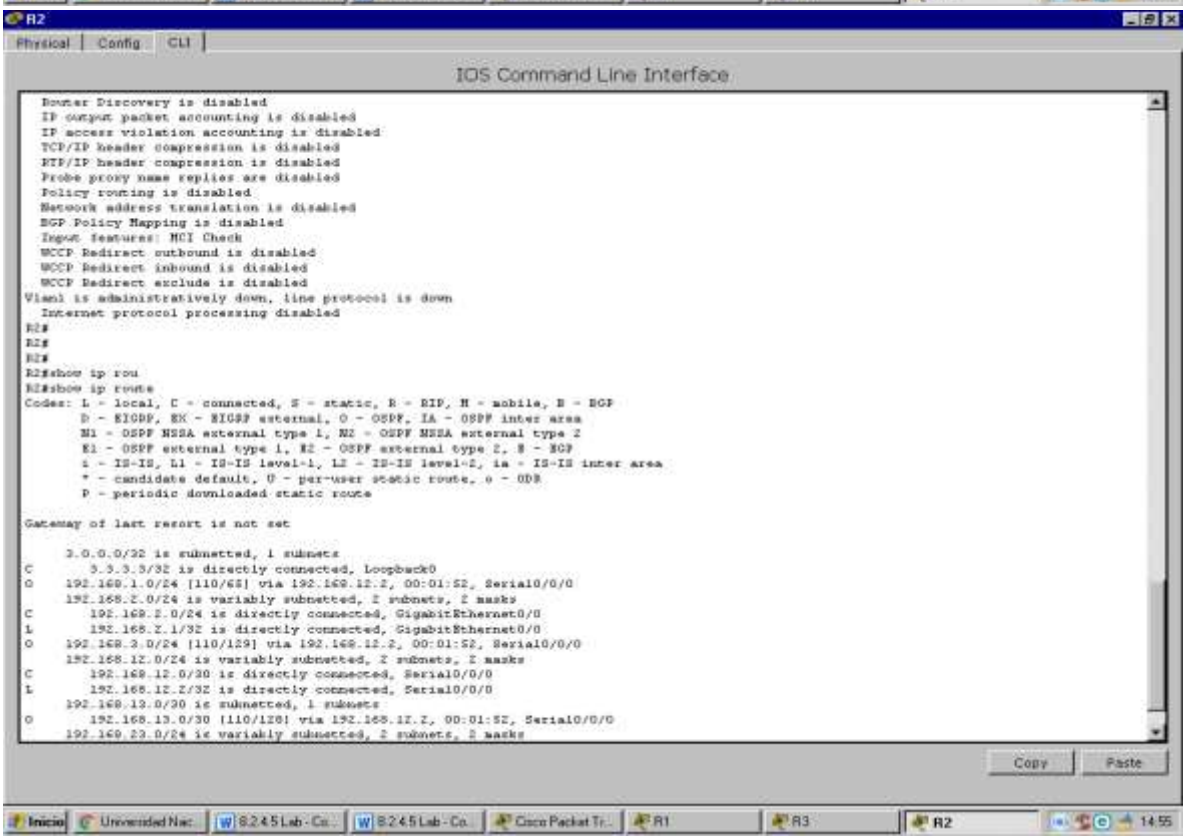
00:00:21: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 from LOADING to FULL, Loading Done

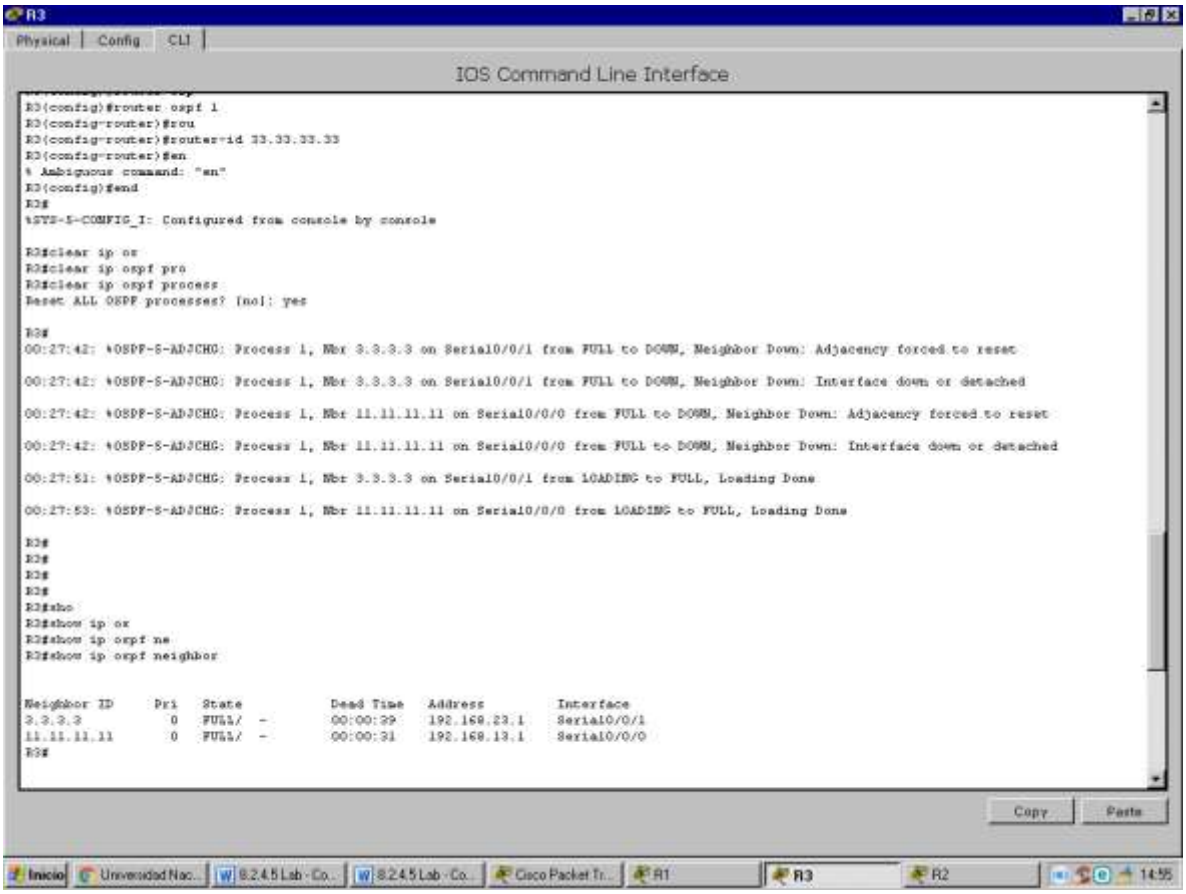



R3
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line
00:02:34: %OSPF-5-ADJCHG:
%LINK-5-CHANGED: Interface
%LINEPROTO-5-UPDOWN: Line
00:02:58: %OSPF-5-ADJCHG:
%LINK-5-CHANGED: Interface
%LINEPROTO-5-UPDOWN: Line
00:03:18: %OSPF-5-ADJCHG:
R3>
R3>
R3>
R3>
R3>sho
R3>show ip pro
Routing Protocol is "ospf
Outgoing update filter l
Incoming update filter l
Router ID 192.168.23.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.3.0 0.0.0.255 area 0
192.168.13.0 0.0.0.3 area 0
192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:04:11
3.3.3.3 110 00:04:11
192.168.13.1 110 00:04:54
192.168.23.2 110 00:04:11
Distance: (default is 110)
R3>
R1>
R1>
R1>
R1>
R1>en
R1#sho
R1#show ip proto
R1#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all inte
Incoming update filter list for all inte
Router ID 1.1.1.1
Number of areas in this router is 1. 1 n
Maximum path: 4
Routing for Networks:
192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Upd
1.1.1.1 110 00:03:41
R2
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: line protocol on Interface Serial0/0/0, changed
00:01:04: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from
FULL, Loading Done
R2>
R2>sho ip pro
R2>sho ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.2.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:04:24
3.3.3.3 110 00:04:24
192.168.13.1 110 00:05:07
192.168.23.2 110 00:04:24
Distance: (default is 110)
R2>
Inicio
Universidad Nac...
8.2.4.5 Lab - Co...
8.2.4.5 Lab - Co...
Cisco Packet Tr...
R1
R2
R3
12:47
IOS Command Line Interface
R1#cle
R1#clear ip ro
R1#clear ip ospf
% Incomplete command.
R1#clear ip ospf pro
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R1#
00:22:24: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from EXCHANGE to
DOWN, Neighbor Down: Adjacency forced to reset
00:22:24: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from EXCHANGE to
DOWN, Neighbor Down: Interface down or detached
00:22:24: %OSPF-5-ADJCHG: P
Neighbor Down: Adjacency fo
00:22:24: %OSPF-5-ADJCHG: P
Neighbor Down: Interface do
00:22:32: %OSPF-5-ADJCHG: P
FULL, Loading Done
00:22:32: %OSPF-5-ADJCHG: P
FULL, Loading Done
00:22:52: %OSPF-5-ADJCHG: P
FULL, Loading Done
R3
Physical
Config
CLI
IOS Command Line Interface
Reset ALL OSPF processes? [no]: yes
R3#
00:25:06: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset
00:25:06: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
00:25:06: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset
00:25:06: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
00:25:21: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done
00:25:30: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to
FULL, Loading Done
00:25:56: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done
Copy
Paste
Estudie en la UN
8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2.docx [Modo de compatibilidad]
Inicio
Universidad Nac...
8.2.4.5 Lab - Co...
8.2.4.5 Lab - Co...
Cisco Packet Tr...
R1
R3
R2
14:05

Configurar las interfaces pasivas de OSPF







¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? Utiliza la interface r3 la serial 0/0/0

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3? Lo realiza por la 129

¿El R2 aparece como vecino OSPF en el R1? Si lo muestra

¿El R2 aparece como vecino OSPF en el R3? No lo muestra por lo que no está activado

¿Qué indica esta información?

Lo que indica es que la red está en modo pasiva y por eso su tráfico lo enVía por r3 a r1 y así llega a r2

Cambie la interfaz S0/0/1 en el R2 para permitir que anuncie las rutas OSPF. Registre los comandos utilizados a continuación.

R2>en

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#route os

R2(config)#route ospf 1

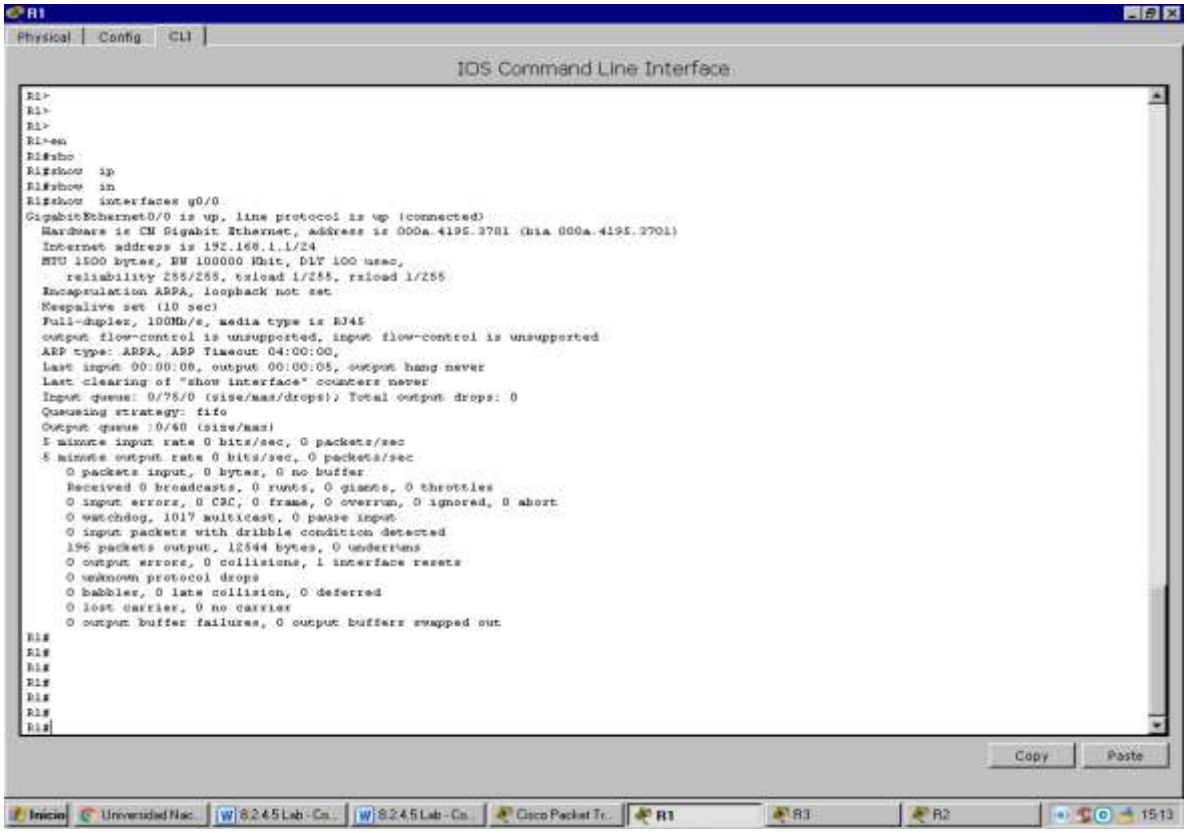
R2(config-router)#no pas

R2(config-router)#no passive-interface

% Incomplete command.

R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
01:25:28: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING to FULL, Loading Done
Vuelva a emitir el comando show ip route en el R3.
¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24?
_____s0/0/1___
¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula? 65 es la métrica. Cambiar las métricas de OSPF

R1



R2#
R2#SH
R2#SHow IP rou
R2#SHow IP route ospf
O 192.168.1.0 [110/65] Vía 192.168.12.2, 00:24:43, Serial0/0/0
O 192.168.3.0 [110/65] Vía 192.168.23.2, 00:07:53, Serial0/0/1
192.168.13.0/30 is subnetted, 1 subnets
O 192.168.13.0 [110/128] Vía 192.168.23.2, 00:07:53, Serial0/0/1
[110/128] Vía 192.168.12.2, 00:07:53, Serial0/0/0
R2#

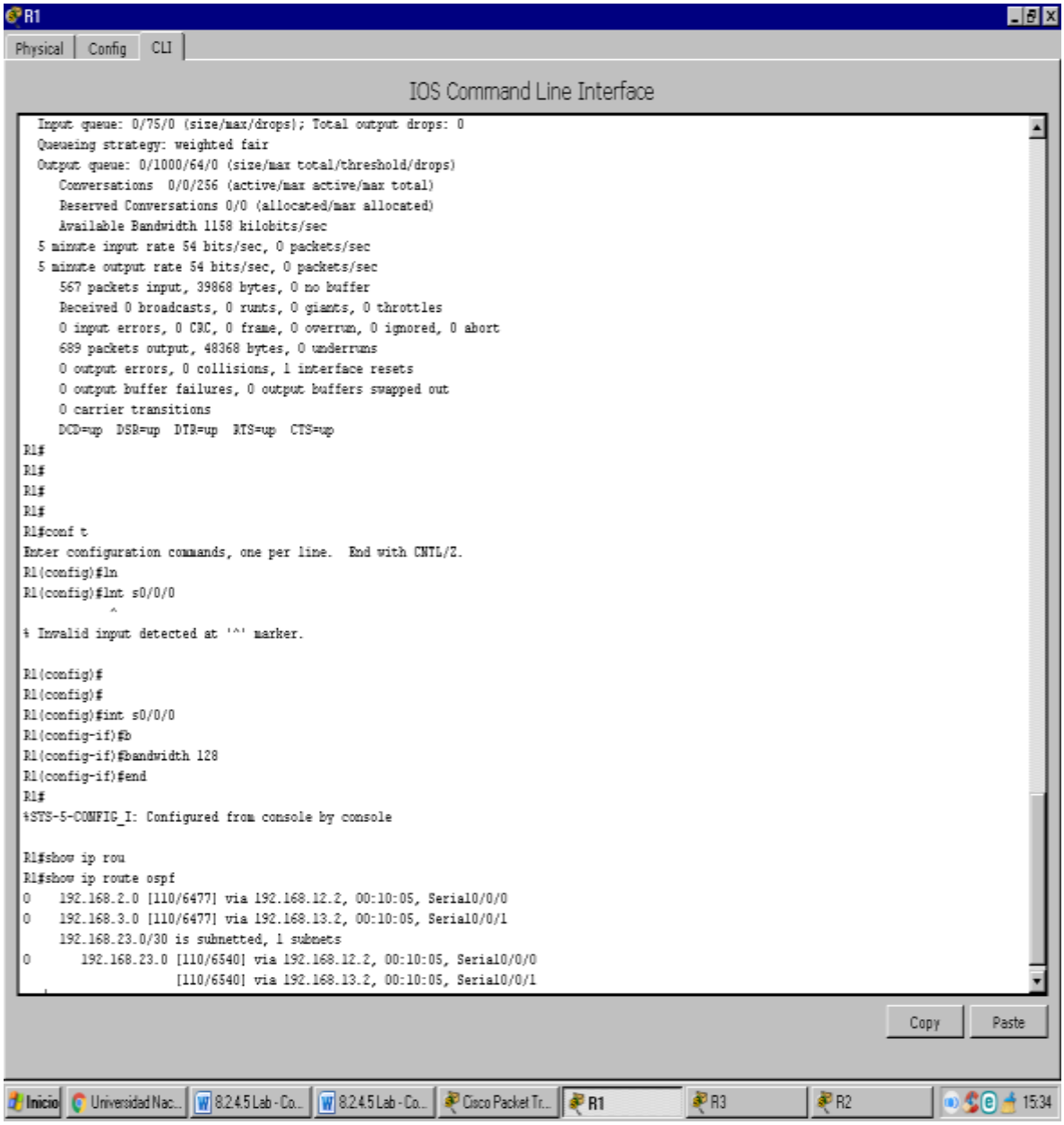
R3
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.1/24, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
R1
192.168.2.0 [110/65] Vía 192.168.12.2, 00:27:50, Serial0/0/0
O 192.168.3.0 [110/65] Vía 192.168.13.2, 01:13:11, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] Vía 192.168.12.2, 00:27:50, Serial0/0/0
[110/128] Vía 192.168.13.2, 00:27:50, Serial0/0/1
R1#SHow IP osp
R1#SHow IP ospf int s0/0/0

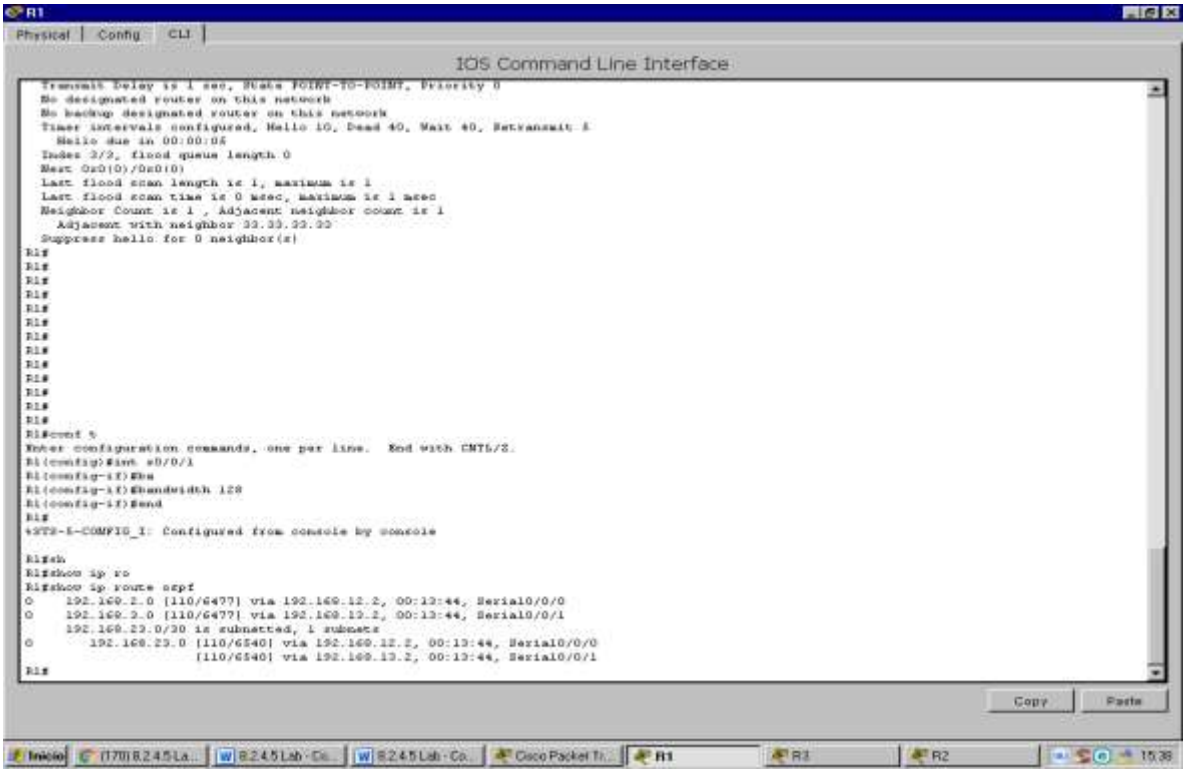
Serial0/0/0 is up, line protocol is up
Internet address is 192.168.12.2/30, Area 0
Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 3.3.3.3
Suppress hello for 0 neighbor(s)
R1#
R1
Incomplete command.
R1(config-router)#auto-cost ref
% Incomplete command.
R1(config-router)#a

R1(config-router)#aut
R1(config-router)#auto-cost r
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#auto-cost reference-bandwidth 1000

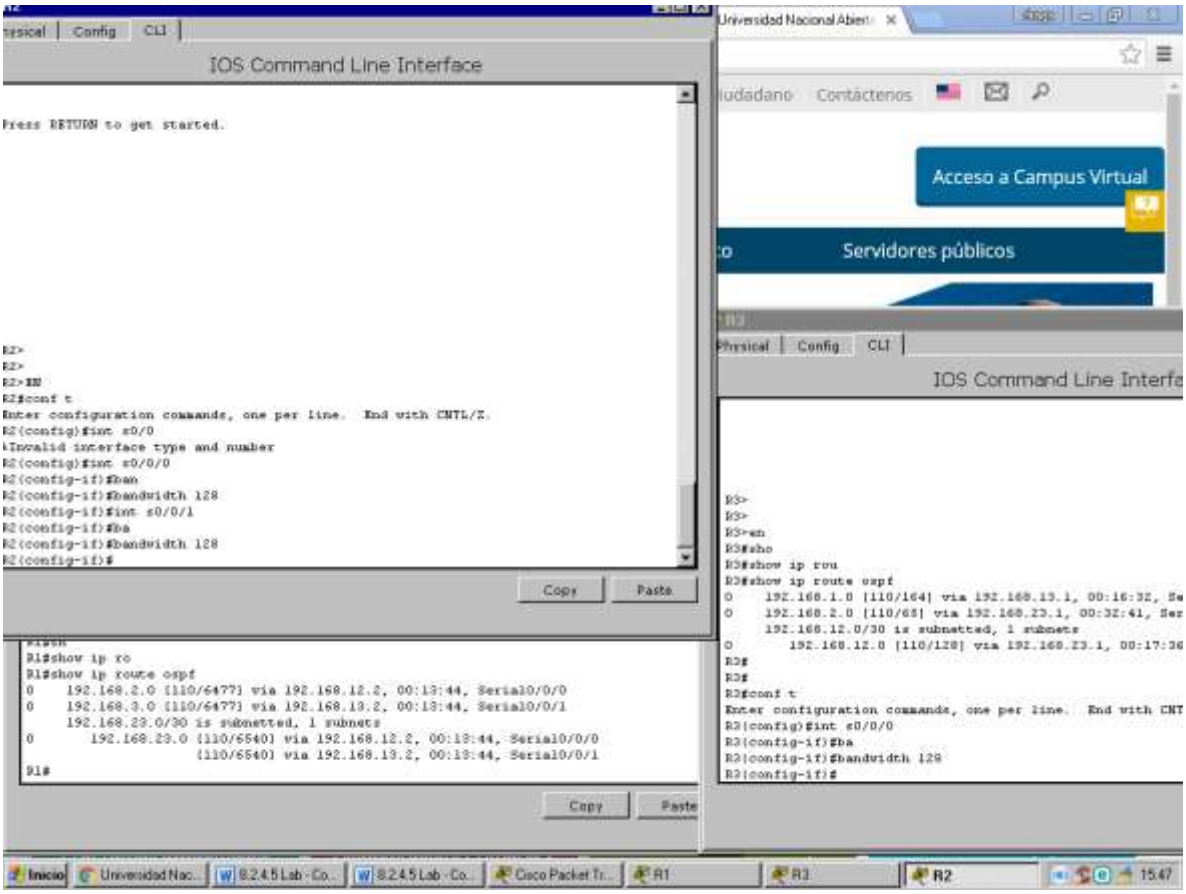
¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?

R/ 1562. Cada enlace serie ahora tiene un costo de 781, y la ruta a la red 192.168.23.0/24 viaja sobre dos enlaces seriales. 781 + 781 = 1.562.





R3
R3>
R3>
R3>en
R3#sho
R3#show ip rou
R3#show ip route ospf
O 192.168.1.0 [110/164] Vía 192.168.13.1, 00:16:32, Serial0/0/0
O 192.168.2.0 [110/65] Vía 192.168.23.1, 00:32:41, Serial0/0/1
192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0 [110/128] Vía 192.168.23.1, 00:17:36, Serial0/0/1
R3#



Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2.

R/ OSPF elegirá la ruta con el menor costo acumulado.

Reflexión

¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF?

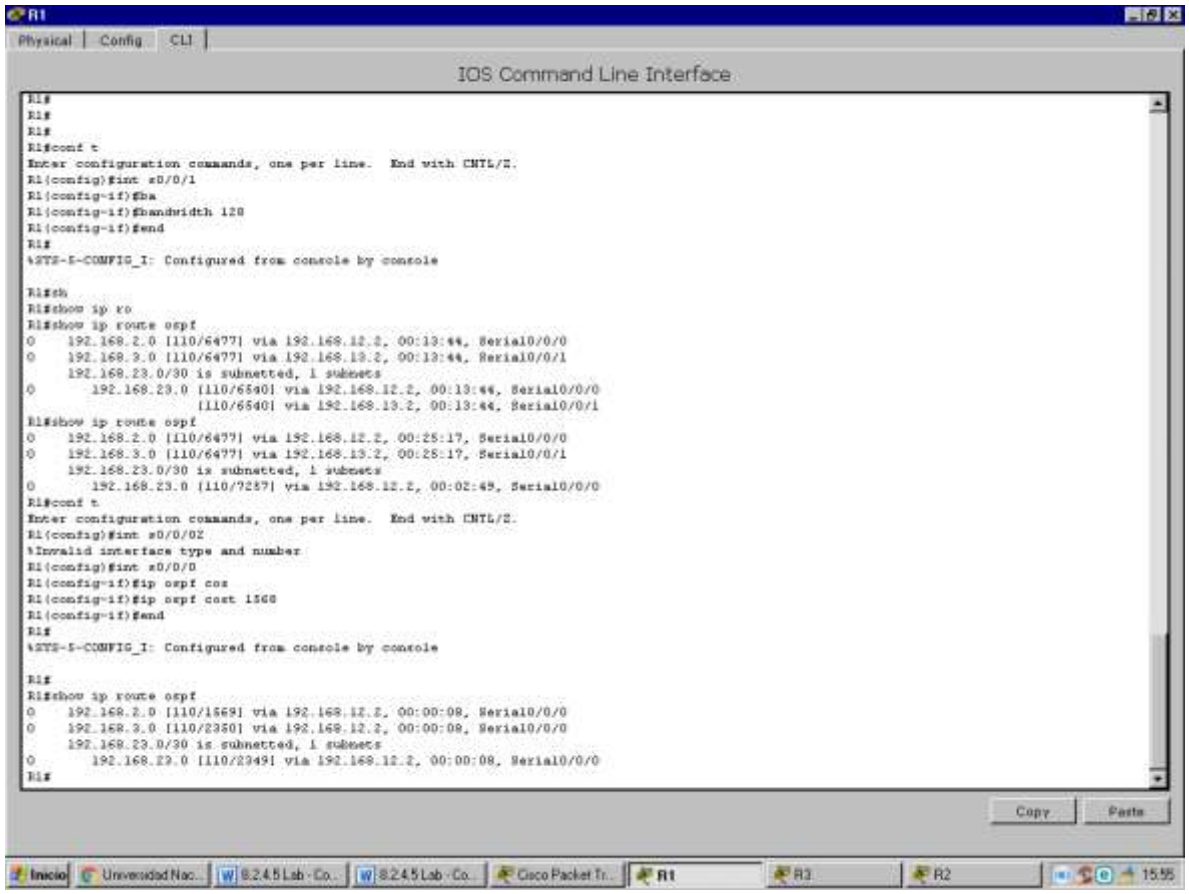
R/ Asignaciones de ID Router controlan el router designado (DR) y BDR (BDR) elección / proceso en una red de acceso múltiple.

¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?

R/El proceso de elección DR / BDR es sólo un problema en una red múltiple acceso como Ethernet o Frame Relay.

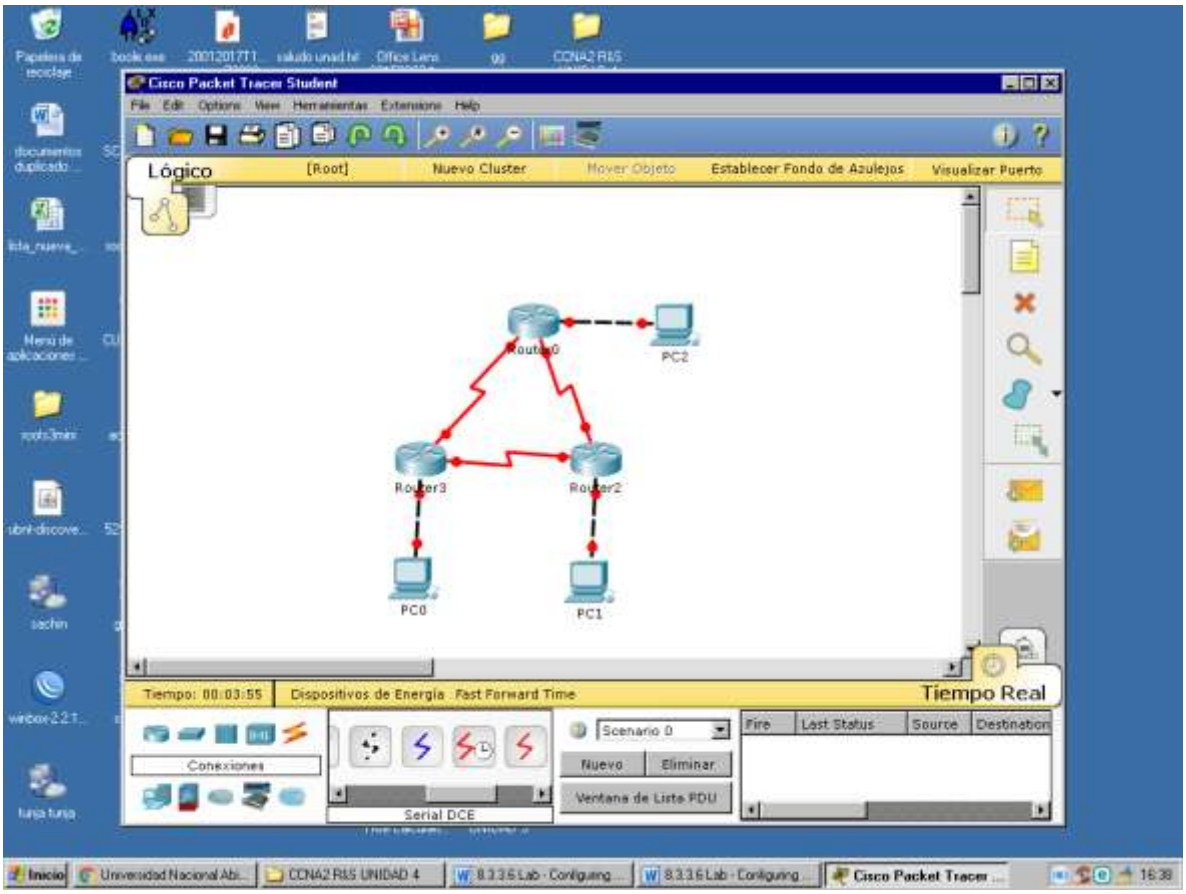
¿Por qué querría configurar una interfaz OSPF como pasiva?

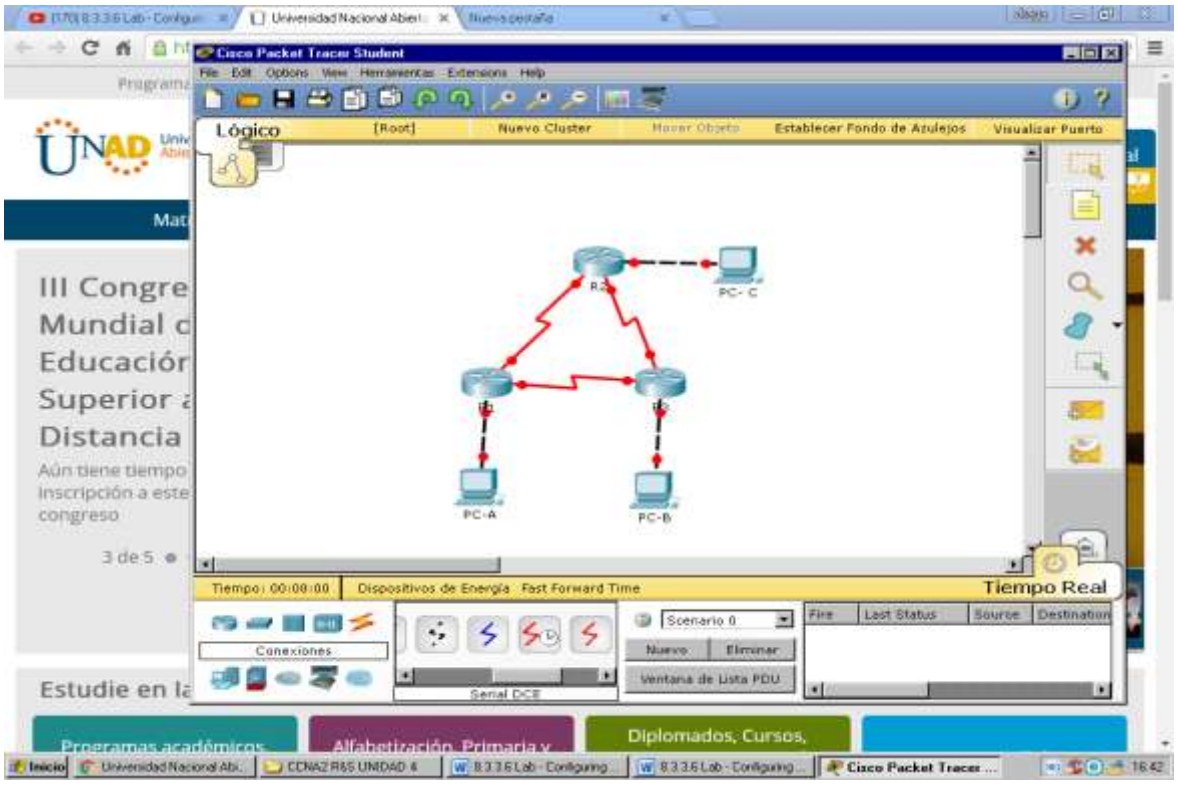
R/ Elimina innecesaria información de enrutamiento OSPF en esa interfaz, liberando ancho de banda



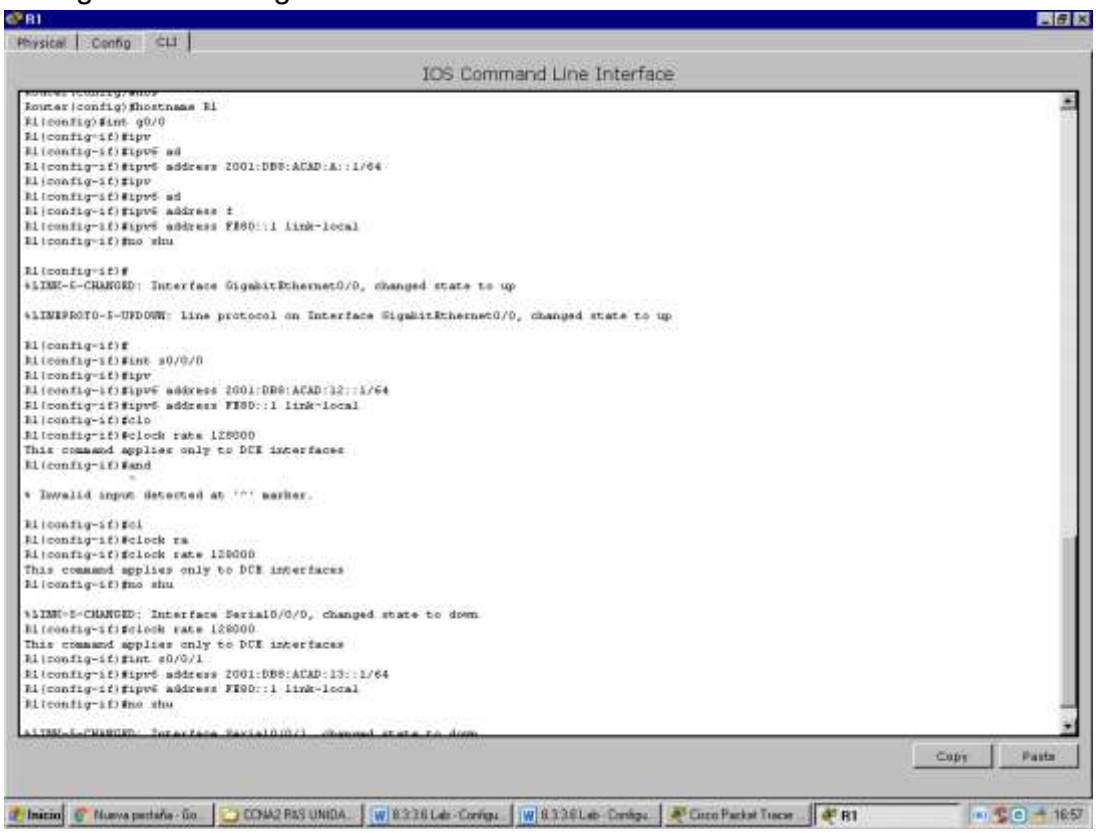
Ejercicio 8.3.3.6

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
Parte 2: configurar y verificar el routing OSPFv3
Parte 3: configurar interfaces pasivas OSPFv3

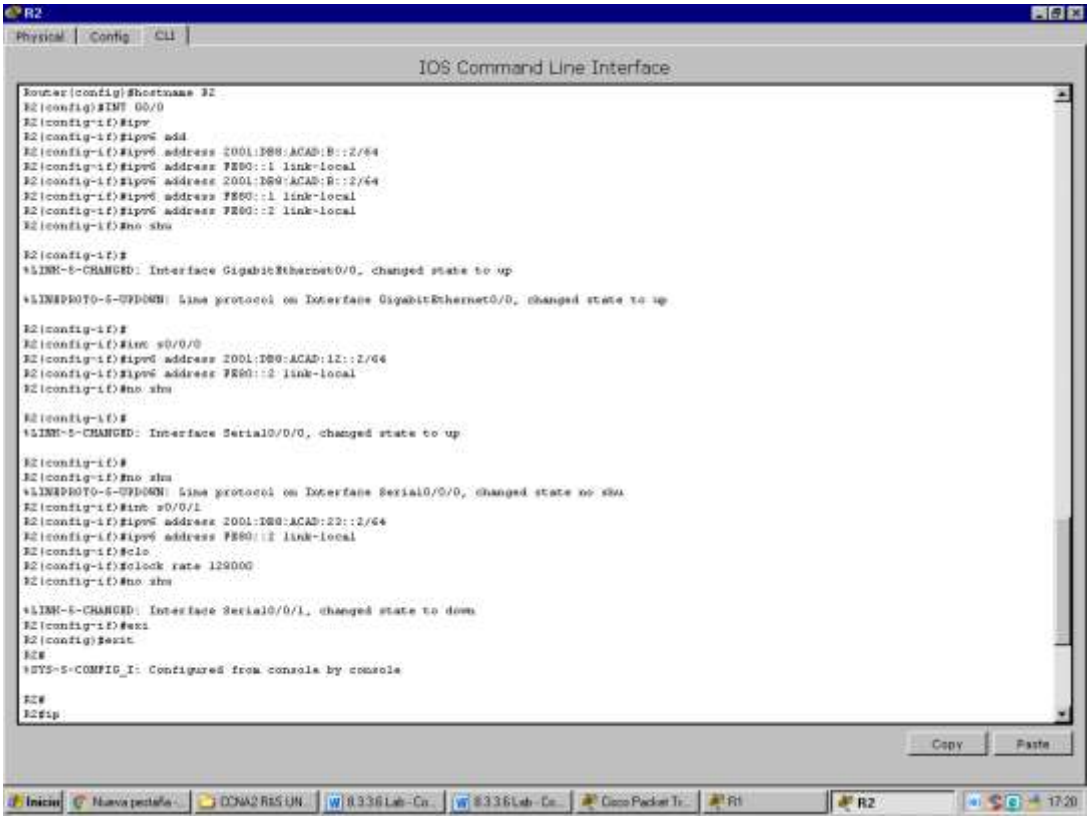

Cisco Packet Tracer Student
File Edit Options View Herramientas Extensiones Help
Lógico
[Root]
Nuevo Cluster
Mover Objeto
Establecer Fondo de Azulejos
Visualizar Puerto
Router0
PC2
Router3
Router2
PC0
PC1
Tiempo: 00:03:55
Dispositivos de Energía Fast Forward Time
Tiempo Real
Conexiones
Serial DCE
Scenario 0
Nuevo
Eliminar
Ventana de Lista PDU
Fire
Last Status
Source
Destination


Cisco Packet Tracer Student
File Edit Options View Herramientas Extensiones Help
Lógico
[Root]
Nuevo Cluster
Mover Objeto
Establecer Fondo de Azulejos
Visualizar Puerto
PC-C
PC-A
PC-B
Tiempo: 00:00:00
Dispositivos de Energía Fast Forward Time
Tiempo Real
Conexiones
Serial DCE
Scenario 0
Nuevo
Eliminar
Ventana de Lista PDU
Fire
Last Status
Source
Destination
III Congre
Mundial d
Educación
Superior a
Distancia
Aún tiene tiempo
Inscripción a este
congreso
3 de 5
Estudie en la
Programas académicos
Alfabetización Primaria y
Diplomados, Cursos,

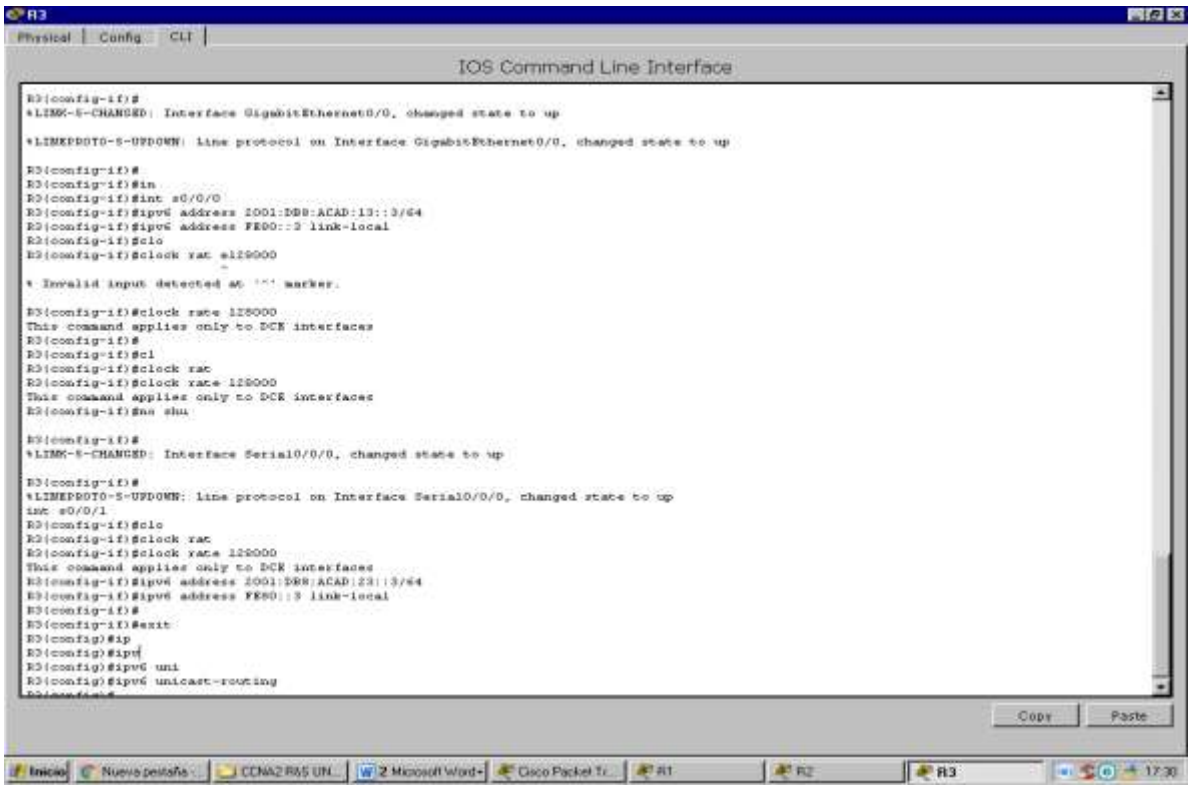
Configurar el routing OSPFv3



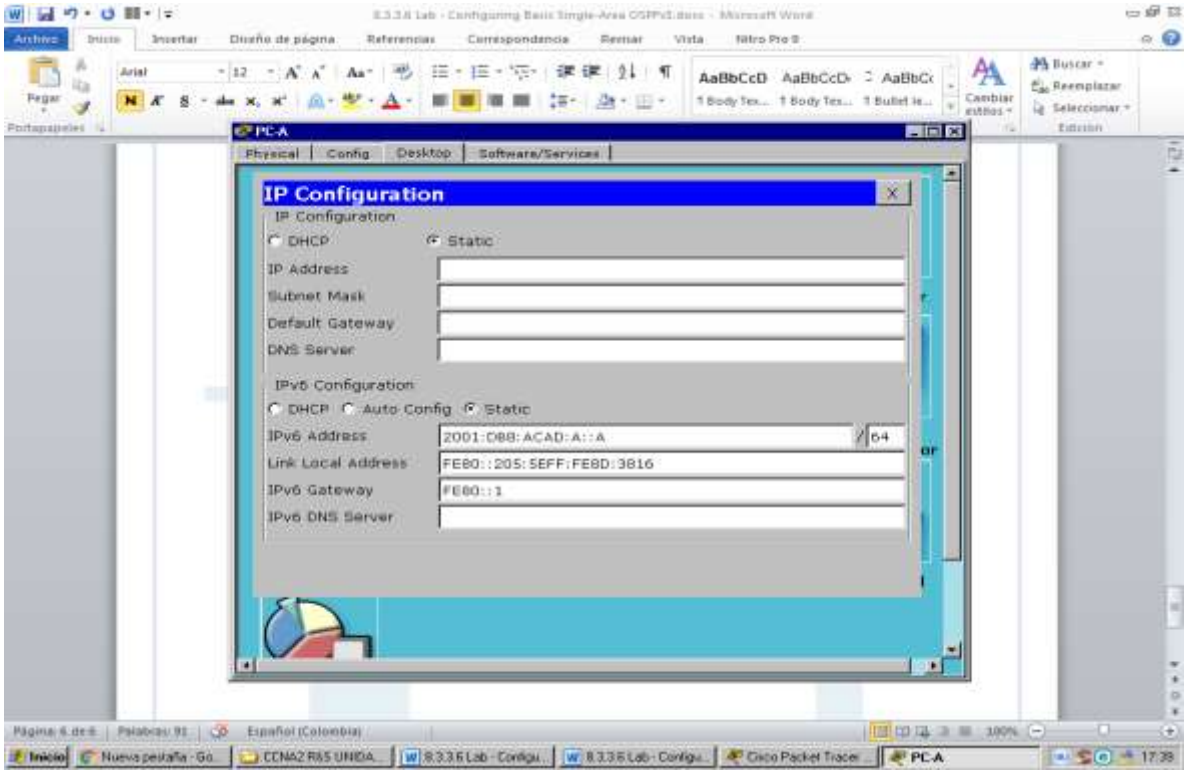
R2



R3



Configurar los equipos host



Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=63ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=32ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255

Verificar vecinos de OSPFv3
R1
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv
R1(config)#ipv6 rout
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R1(config-rtr)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip
R1(config)#ipv
R1(config)#ipv6 rou
R1(config)#ipv6 router ospf 1
R1(config-rtr)#rou
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R2

R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ipv
R2(config)#ipv6 rou
R2(config)#ipv6 router ospf 1
R2(config-rtr)#rou
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#

R3

R3(config-rtr)#exit
R3(config)#ip
R3(config)#ipv
R3(config)#ipv6 router ospf 1
R3(config-rtr)#rout
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#

R2

R2#
R2#show ipv
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

Verificar la configuración del protocolo OSPFv3.

R1

R1>
R1>
R1>en
R1#conf t

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int
R1(config)#interface g0/0
R1(config-if)#ipv
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#
```

R2

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ipv
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
01:38:34: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

R2(config-if)#
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

R3

```
% Incomplete command.
R3(config)#ip
R3(config)#ipv
R3(config)#ipv6 rou
R3(config)#ipv6 router ospf 1
R3(config-rtr)#ro
```

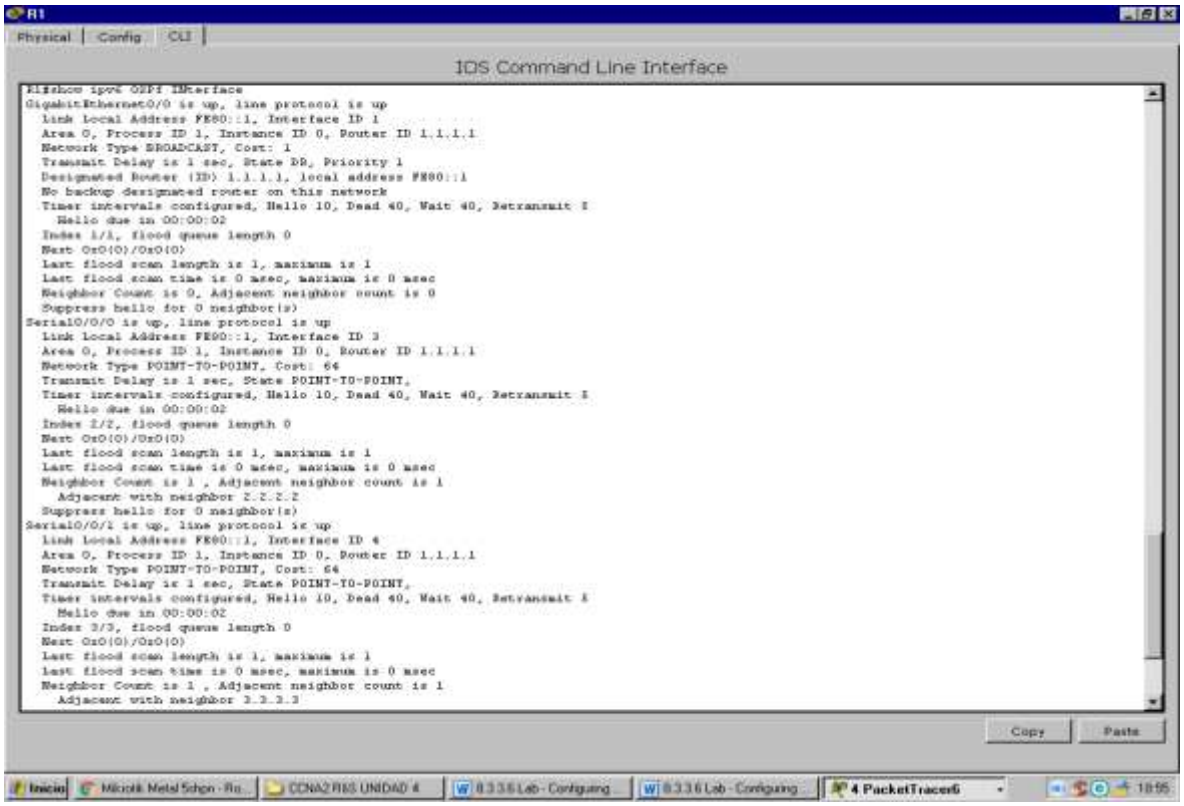
```
R3(config-rtr)#exit
R3(config)#int g0/0
R3(config-if)#ip
R3(config-if)#ipv
R3(config-if)#ipv6 osp
R3(config-if)#ipv6 ospf 1 ar
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:16:26: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

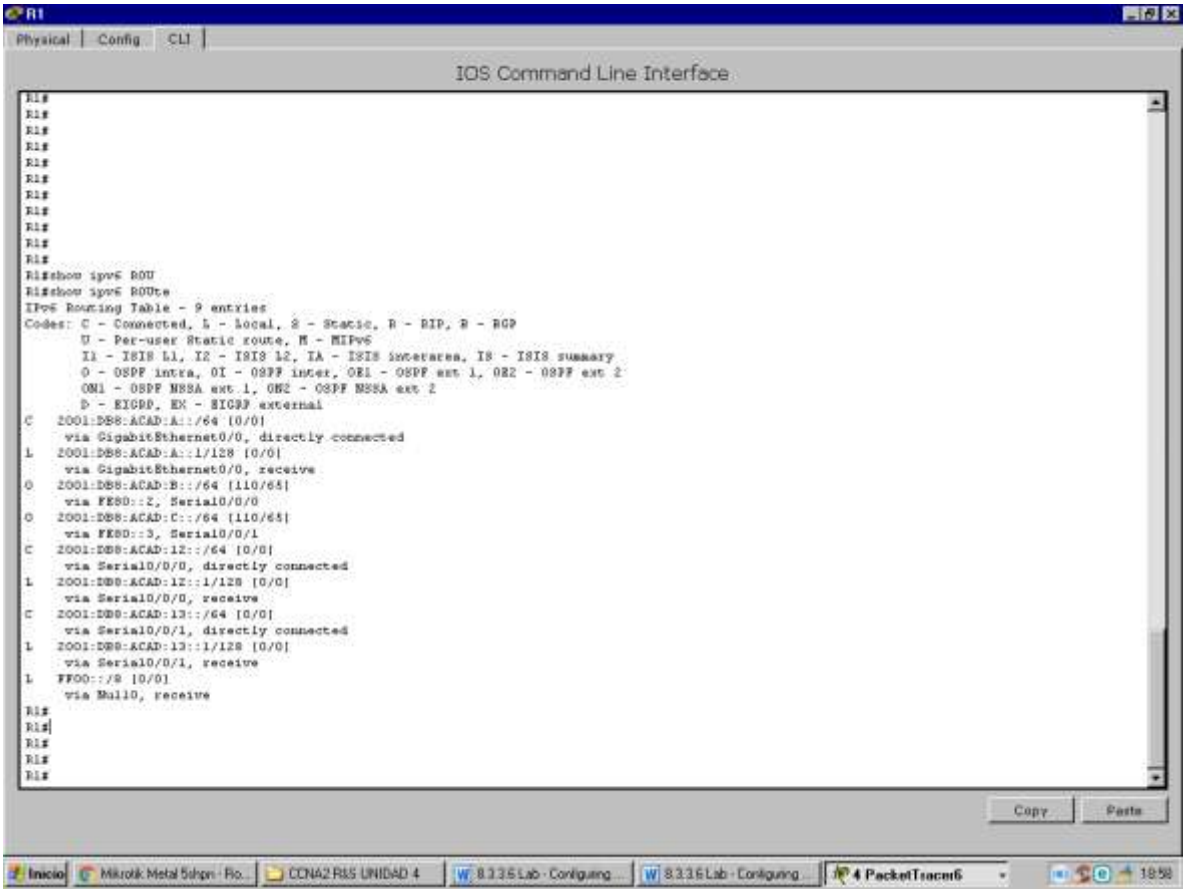
verificar las interfaces OSPFv3.

```
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
```

R1

```
R1#show ip ospf neighbor

R1#sh
R1#show ip
R1#show ipv
R1#show ipv6 pro
R1#show ipv6 pro
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0)
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Redistribution:
None

R1#
```


R1
Physical
Config
CLI
IOS Command Line Interface
R1#show ipv6 OSPF INterface
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Link Local Address FE80::1, Interface ID 4
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 3.3.3.3
Copy
Paste
Inicio
Mikrotik Metal 5shpn - Ro...
CCNA2 R&S UNIDAD 4
8.3.3.6 Lab - Configuring...
8.3.3.6 Lab - Configuring...
4 PacketTracer6
18:55


R1
Physical
Config
CLI
IOS Command Line Interface
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#show ipv6 ROU
R1#show ipv6 ROUte
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/65]
via FE80::2, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
via Serial0/0/1, receive
L FF00::/8 [0/0]
via Null0, receive
R1#
R1#
R1#
R1#
R1#
Copy
Paste
Inicio
Mikrotik Metal 5shpn - Ro...
CCNA2 R&S UNIDAD 4
8.3.3.6 Lab - Configuring...
8.3.3.6 Lab - Configuring...
4 PacketTracer6
18:58

Verificar la tabla de routing IPv6.

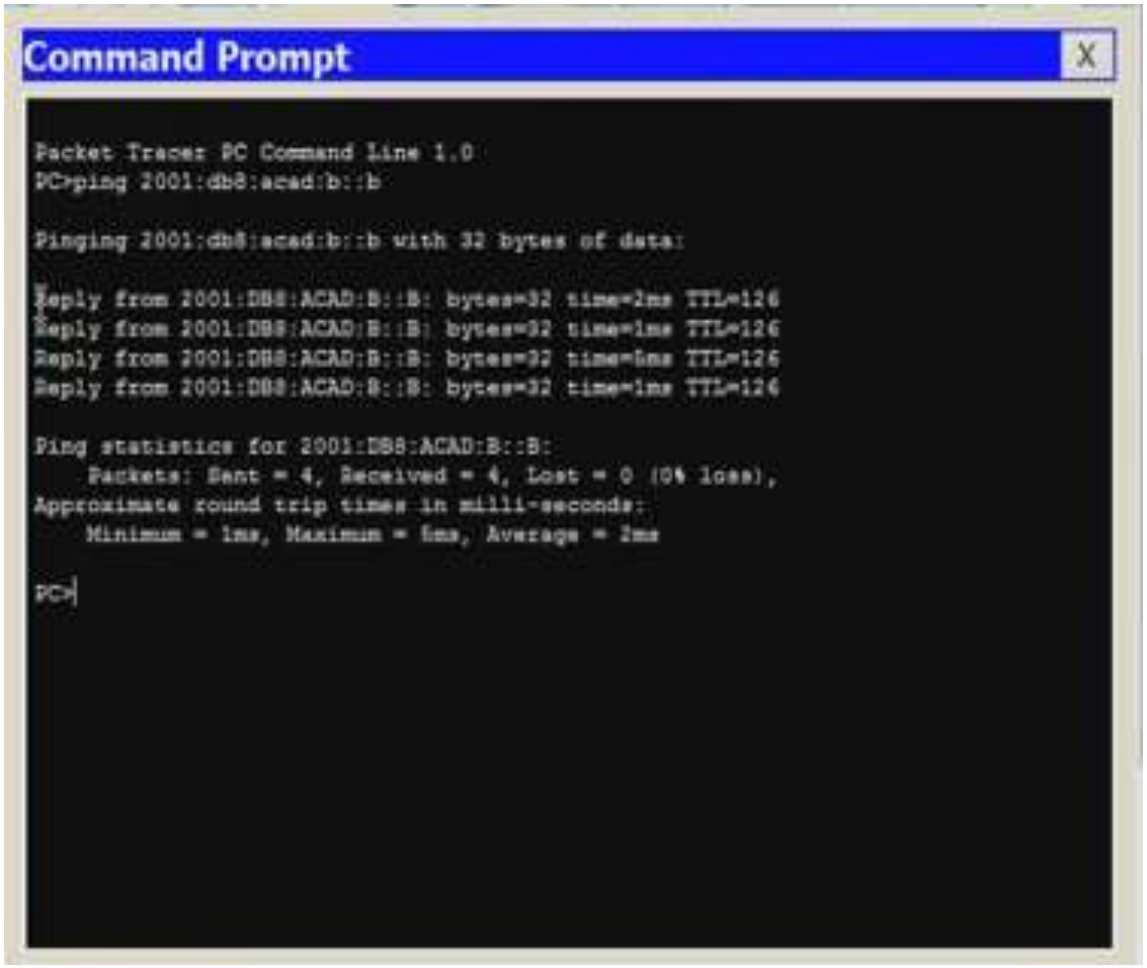
```
R2>SH
R2>SHow IPV
R2>SHow IPV6 ROU
R2>SHow IPV6 ROUte
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
C 2001:DB8:ACAD:B::/64 [0/0]
Vía GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::2/128 [0/0]
Vía GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/129]
Vía FE80::1, Serial0/0/0
C 2001:DB8:ACAD:12::/64 [0/0]
Vía Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::2/128 [0/0]
Vía Serial0/0/0, receive
O 2001:DB8:ACAD:13::/64 [110/128]
Vía FE80::1, Serial0/0/0
L FF00::/8 [0/0]
Vía Null0, receive
```

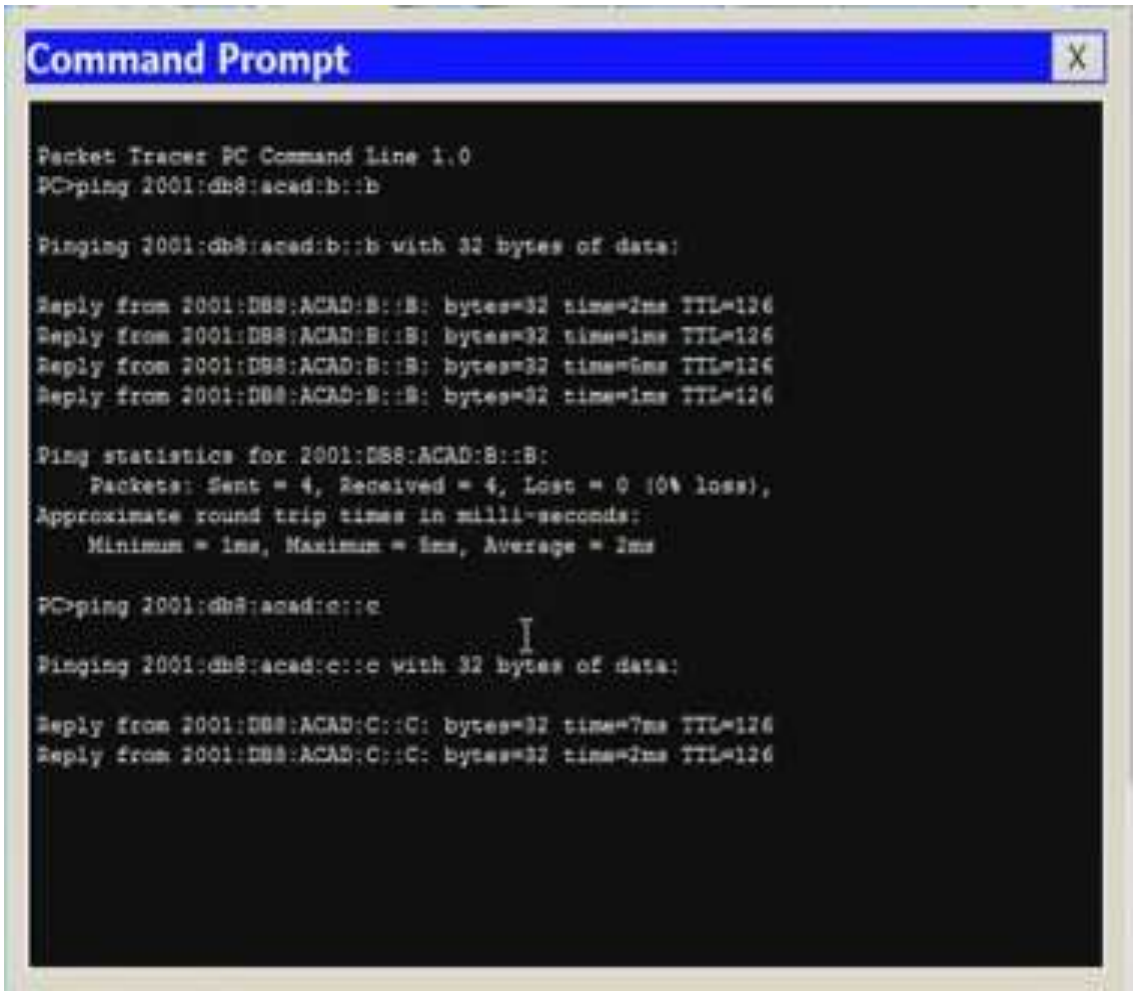
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

```
R2>sho
R2>show ipv
R2>show ipv6 ro
R2>show ipv6 route osp
R2>show ipv6 route ospf
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/129]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:13::/64 [110/128]
Vía FE80::1, Serial0/0/0
R2>

Verificar la conectividad de extremo a extremo



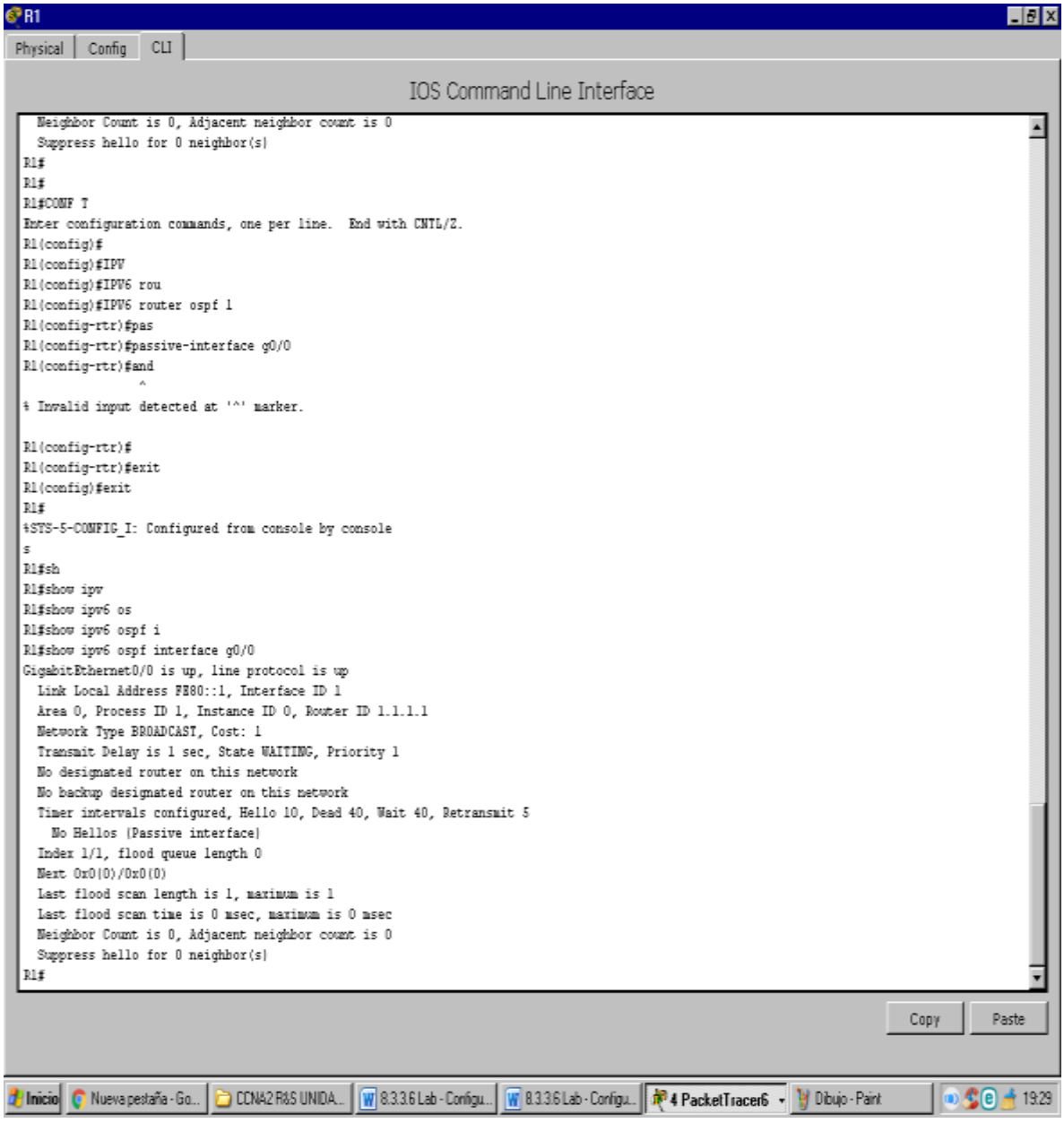


Configurar las interfaces pasivas de OSPFv3

R1

R1>en
R1#sho
R1#show ipv os
R1#show ipv ospf in
R1#show ipv ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
R1#



R2

```
R2>
R2>
R2>en
R2#sho
R2#show ipv
R2#show ipv6 rou
R2#show ipv6 route ospf
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/129]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:13::/64 [110/128]
Vía FE80::1, Serial0/0/0
R2#
```

R3

```
3>en
R3#sh
R3#show ip
R3#show ipv
R3#show ipv6 rou
R3#show ipv6 route os
R3#show ipv6 route ospf
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
```

Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/129]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:12::/64 [110/128]
Vía FE80::1, Serial0/0/0
R3#

R2

R2>
R2>en
R2#sho
R2#show ipv
R2#show ipv6 rou
R2#show ipv6 route ospf
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/129]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:13::/64 [110/128]
Vía FE80::1, Serial0/0/0
R2#
R2#CONF T
R2#CONF Terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv
R2(config)#ipv6 rou
R2(config)#ipv6 router ospf 1
R2(config-rtr)#pas
R2(config-rtr)#passive-interface defa
R2(config-rtr)#passive-interface default
R2(config-rtr)#
02:56:52: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

R2(config-rtr)#

R1

R1#
R1#sho
R1#show ipv
R1#show ipv6 ospf ne
R1#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
3.3.3.3 0 FULL/ - 00:00:39 3 Serial0/0/1
R1#

R2

R2#sho
R2#show ip
R2#show ipv
R2#show ipv6 osp
R2#show ipv6 ospf in
R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
R2#

R3

R3#SHOw IPV6 ROU
R3#SHOw IPV6 ROUte OSPF

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:12::/64 [110/128]
Vía FE80::1, Serial0/0/0
R3#

R2

R3#SHOw IPV6 ROU
R3#SHOw IPV6 ROUte OSPF
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:12::/64 [110/128]
Vía FE80::1, Serial0/0/0
R3#

R1

R1#show ipv
R1#show ipv6 rout
R1#show ipv6 route ospf
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:C::/64 [110/65]
Vía FE80::3, Serial0/0/1
R1#

R2

R2#show ipv6 route ospf
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
R2#
R2#

R3

R3#
R3#SHOw IPV6 ROUte OSPF
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
Vía FE80::1, Serial0/0/0
O 2001:DB8:ACAD:12::/64 [110/128]
Vía FE80::1, Serial0/0/0
R3#

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? S0/0/1
¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1? 129
¿El R2 aparece como vecino OSPFv3 en el R1? R3
¿El R2 aparece como vecino OSPFv3 en el R3? SI

Qué indica esta información?

Que todo el tráfico hacia la red r1 será rutiado hacia r3 y la interface 01 está configurada como pasiva
Por tal razón no envía la información de ruteo
El costo 129 es la acumulación del tráfico que pasa por r3
R2(config-rtr)#
R2(config-rtr)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#sho
R2#show ipv
R2#show ipv6 ospf
R2#show ipv6 ospf ne
R2#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
1.1.1.1 0 FULL/ - 00:00:38 3 Serial0/0/0
R2#

Si la configuración OSPFv6 del R1 tiene la ID de proceso 1 y la configuración OSPFv3 del R2 tiene la ID de proceso 2, ¿se puede intercambiar información de routing entre ambos routers? ¿Por qué

Si debido a el proceso es muy usado para la configuración de los routesr lo utilizan ospf el cual es muy común

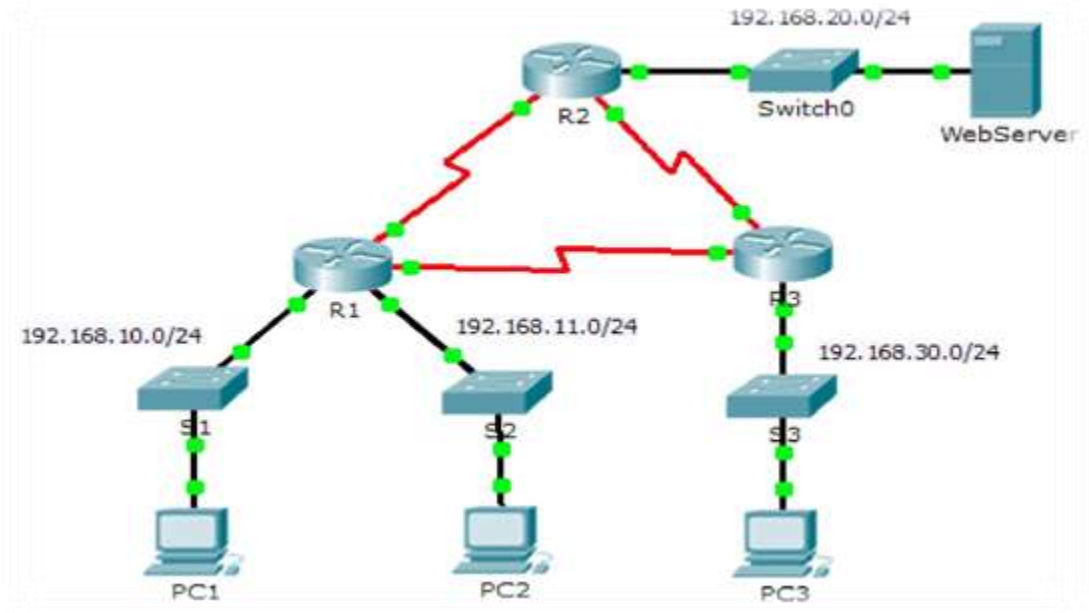
¿Cuál podría haber sido la razón para eliminar el comando network en OSPFv3

Se logra prevenir los errores de las direcciones ipv6 al realizar una ip ospf todas las direcciones se re direccionan lo cual le dará una ruta de ruteo por la tabla asignada

Ejercicio 9.2.1.10

Packet Tracer - Configuring Standard ACLs

Topology



AddressingTable

Device	Interface	IP Address	SubnetMask	Default Gateway
R1	FO/0	192.168.10.1	255.255.255.0	N/A
	FO/1	192.168.11.1	255.255.255.0	N/A
	SO/O/O	10.1.1.1	255.255.255.252	N/A
	SO/0/1	10.3.3.1	255.255.255.252	N/A
R2	FO/0	192.168.20.1	255.255.255.0	N/A
	SO/0/0	10.1.1.2	255.255.255.252	N/A
	SO/0/1	10.2.2.1	255.255.255.252	N/A
R3	FO/0	192.168.30.1	255.255.255.0	N/A
	SO/0/0	10.3.3.2	255.255.255.252	N/A
	SO/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetives
Part 1: Plan an ACL Implementation
Part 2: Configure, Apply, and Verify a Standard ACL
Background / Scenario
Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

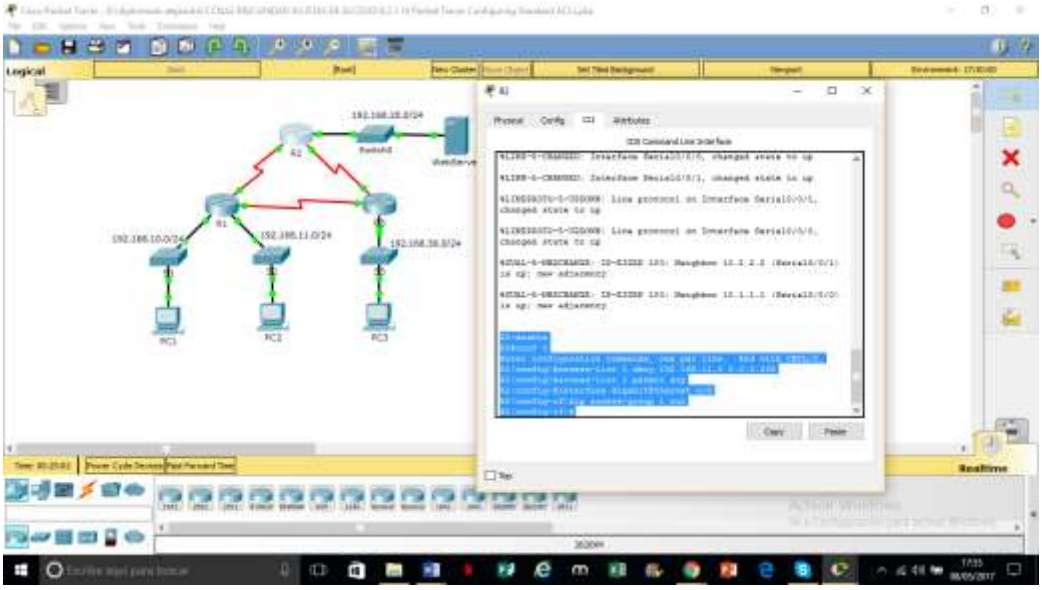
Part 1: Plan an ACL Implementation

Step 1: Investígate the current network configuration.
Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

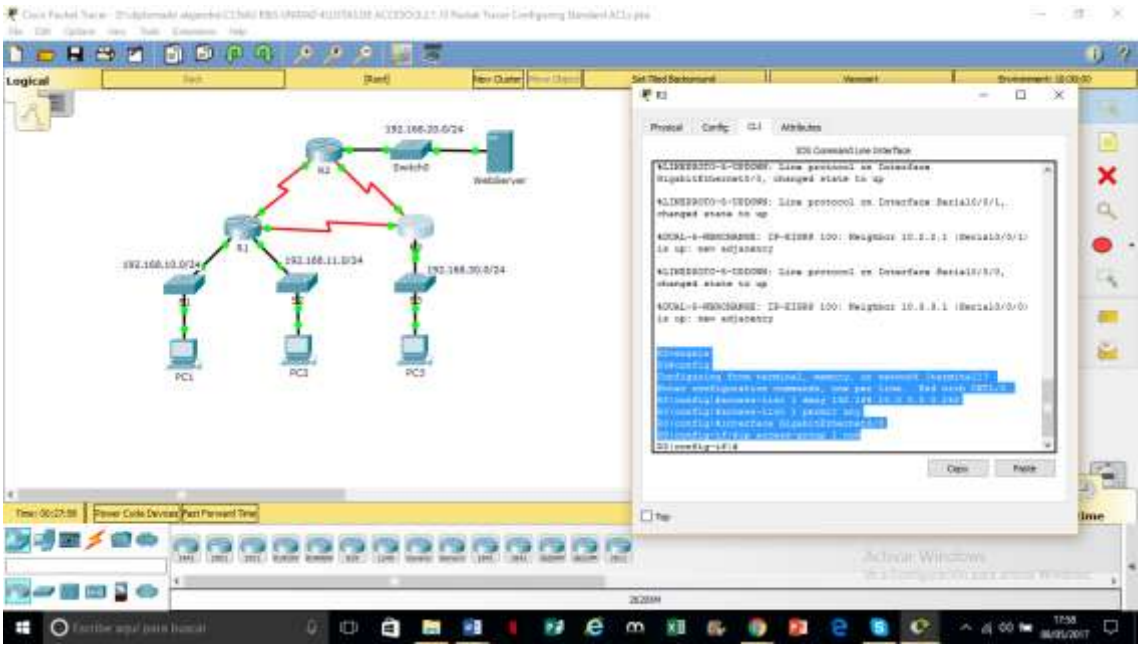
Step 2: Evalúate two network policies and plan ACL implementations.
a. The following network policies are implemented on R2:
The 192.168.11.0/24 network is not allowed access to the WebServeron the 192.168.20.0/24 network.
All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the WebServerat 192.168.20.254 without interfering with other traffic, an ACL must be created on R2. The access list must be placed on the outbound interface to the WebServer. A second rule must be created on R2 to permit all other traffic.
b. The following network policies are implemented on R3:
The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
All other access is permitted.
To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on R3. The ACL must placed on the outbound interface to PC3. A second rule must be created on R3 to permit all other traffic.
Part 2: Configure, Apply, and Verify a Standard ACL
Step 1: Configure and apply a numbered standard ACL on R2.

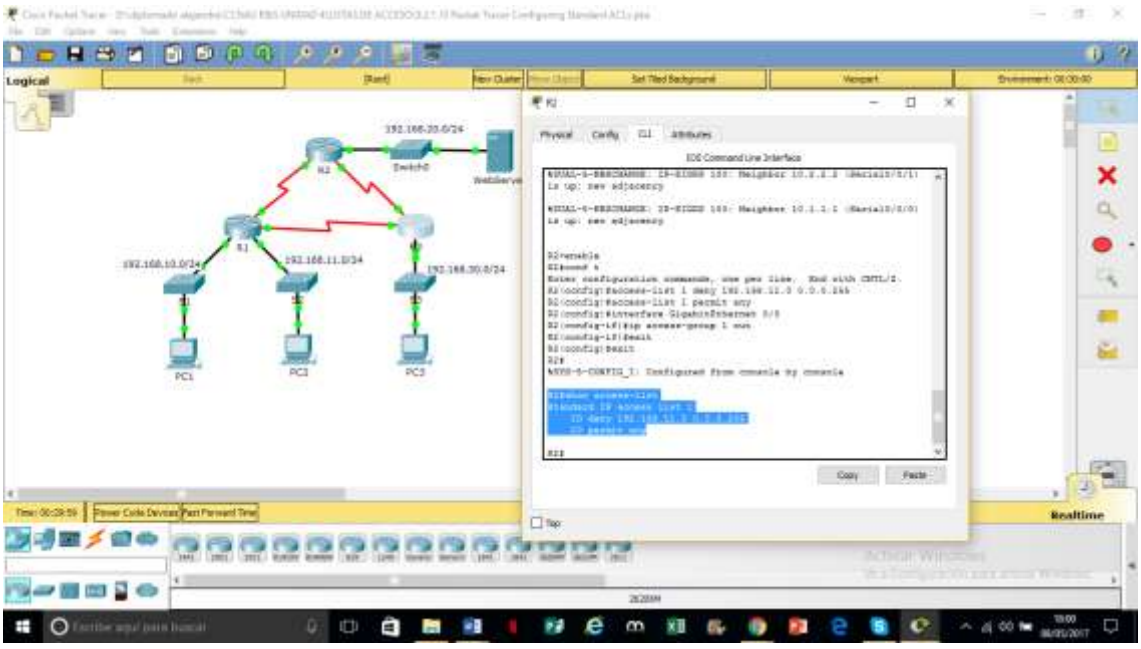
a. Créate an ACL using the number 1 on R2 with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:
R2(config)# access-list 1 permit any
c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing
it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R2(config)# interface GigabitEthernet 0/0
R2(config-if)# ip access-group 1 out

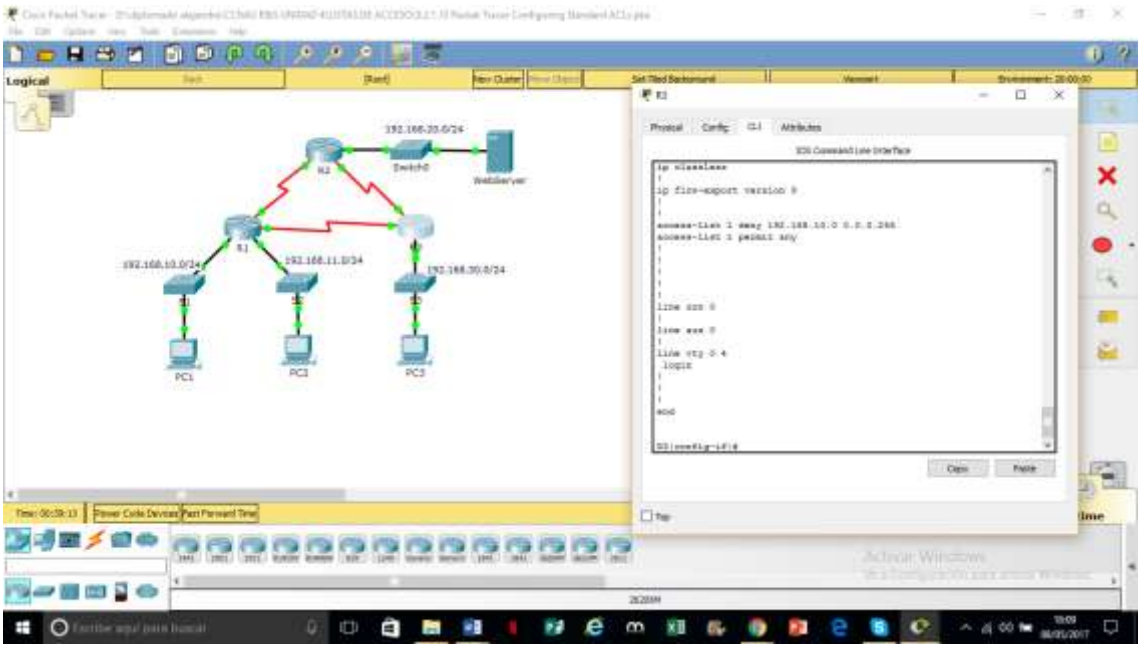


Step 2: Configure and apply a numbered standard ACL on R3.
a. Créate an ACL using the number 1 on R3 with a statement that denies access to the 192.168.30.0/24 network from the PC1 (192.168.10.0/24) network.
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, créate a secondrule for ACL 1.
R3(config)# access-list 1 permit any
c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out

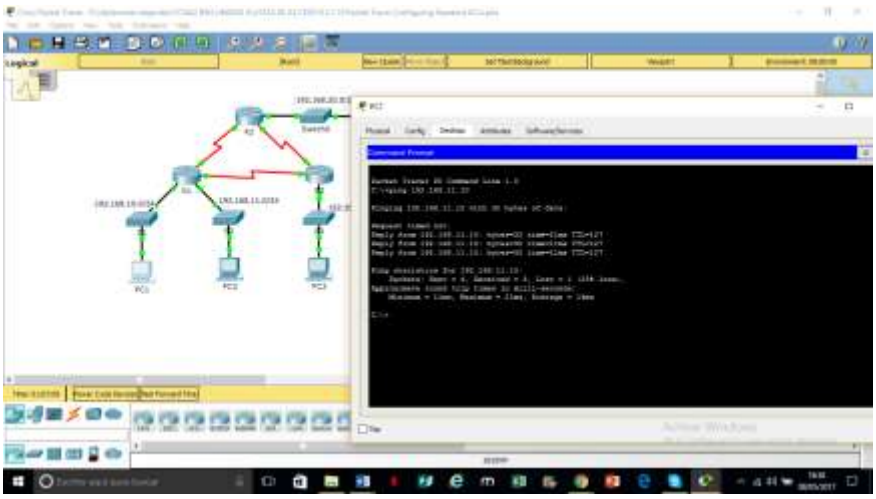


Step 3: Verify ACL configuration and functionality.
On R2 and R3, enter the show access-list command to verify the ACL configurations. Enter the show run or show ip interface gigabitethernet 0/0 command to verify the ACL placements

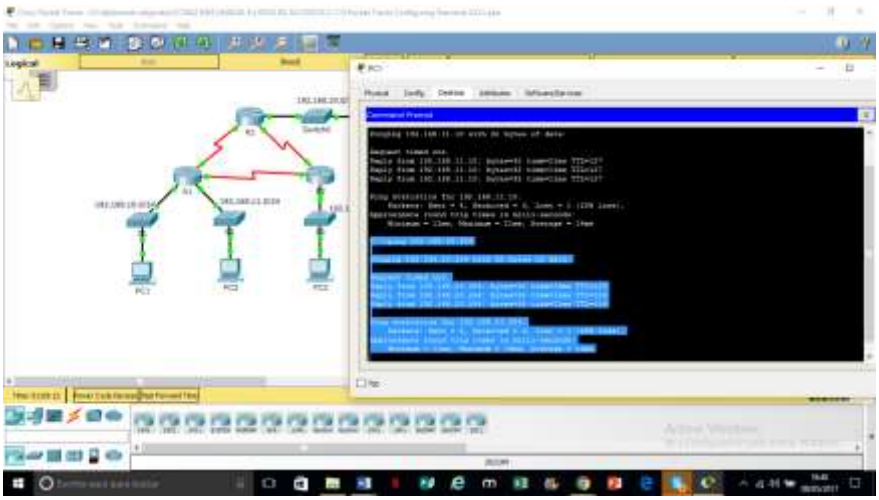




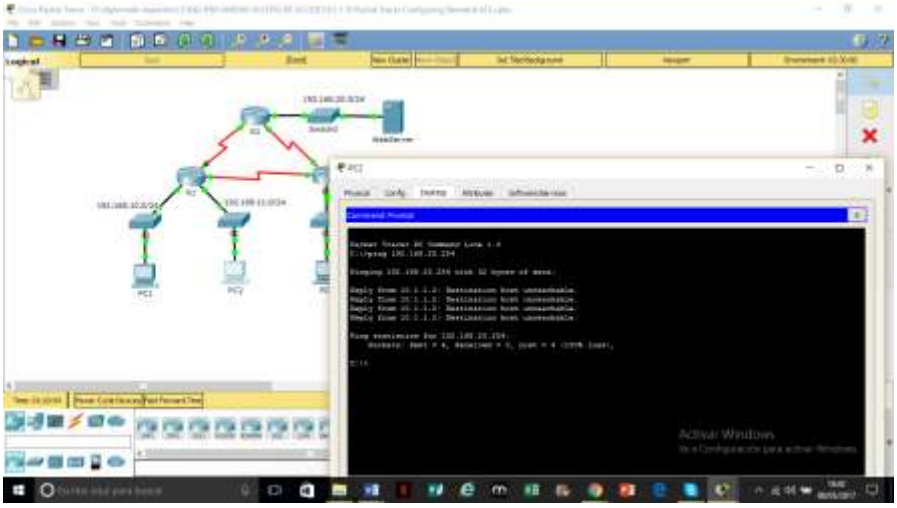
b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:
A ping from 192.168.10.10 to 192.168.11.10 succeeds.



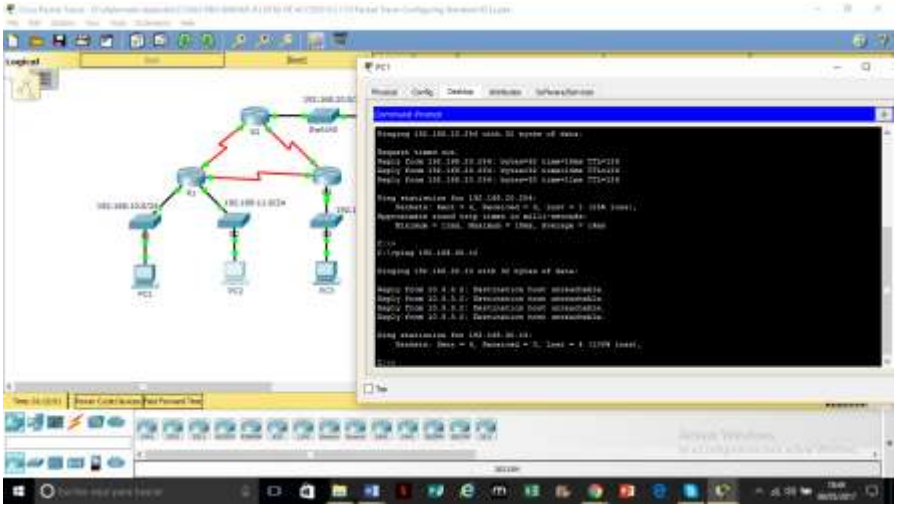
A ping from 192.168.10.10 to 192.168.20.254 succeeds.



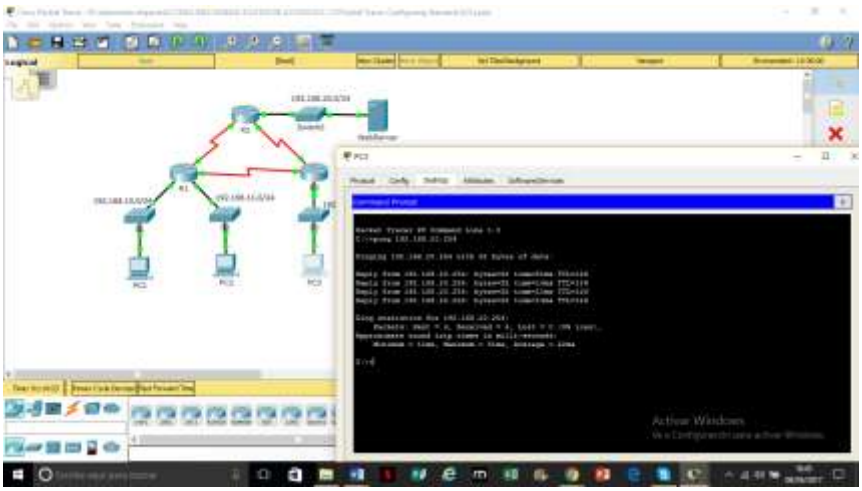
A ping from 192.168.11.10 to 192.168.20.254 fails.



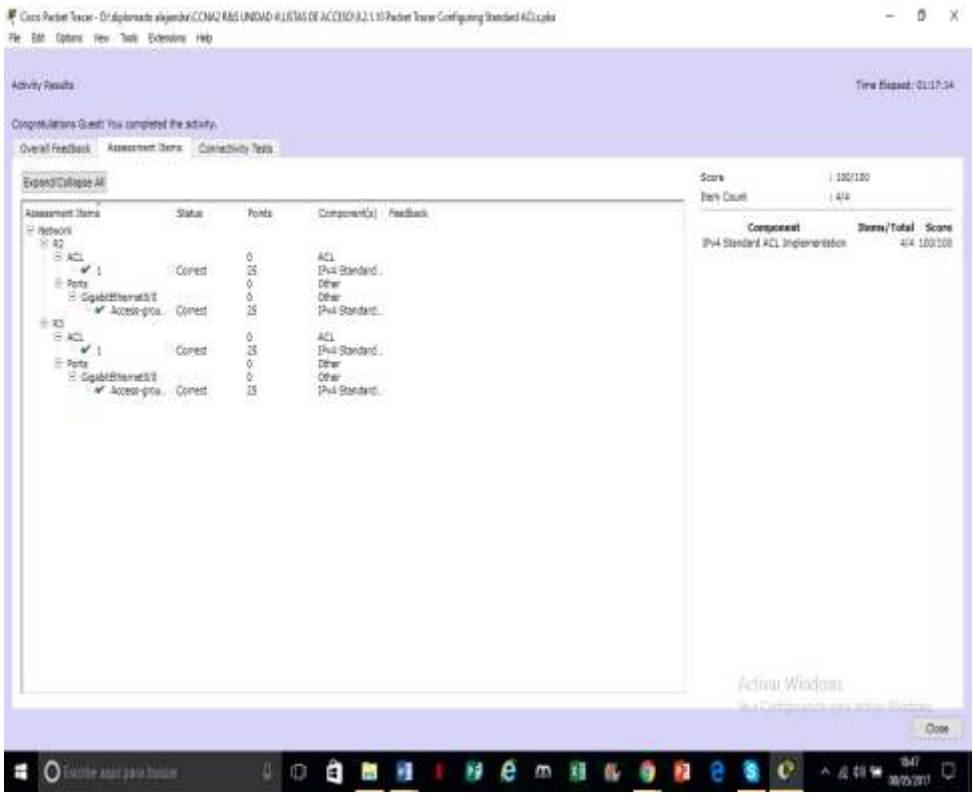
A ping from 192.168.10.10 to 192.168.30.10 fails.



A ping from 192.168.30.10 to 192.168.20.254 succeeds.



Resultados

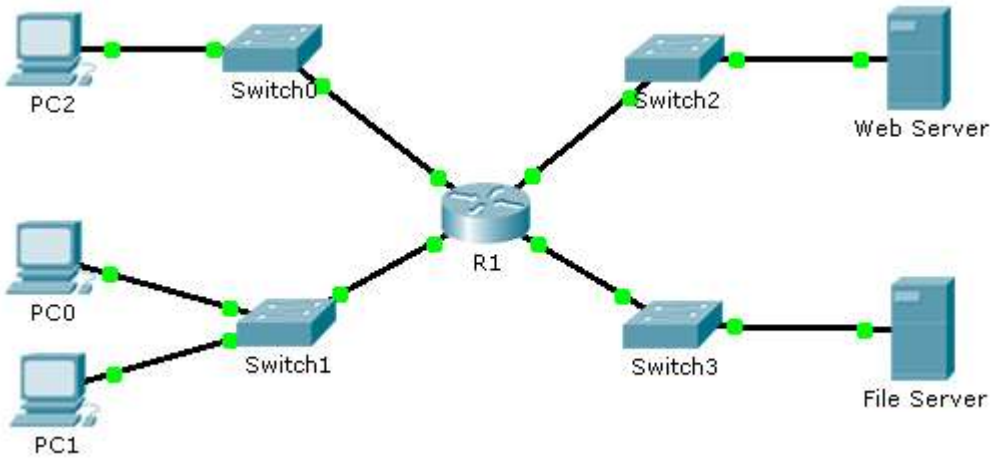


Ejercicio 9.2.1.11

Packet Tracer - Configuring Named Standard ACLs

.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Background / Scenario

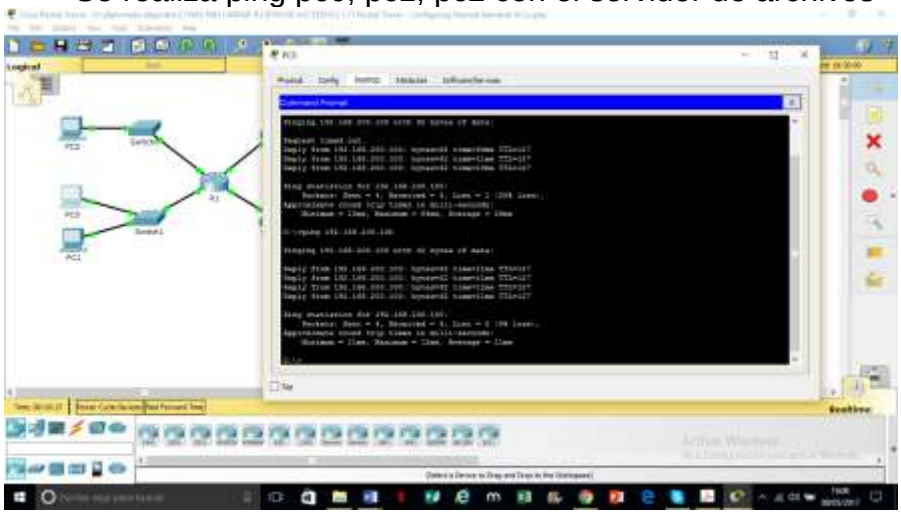
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

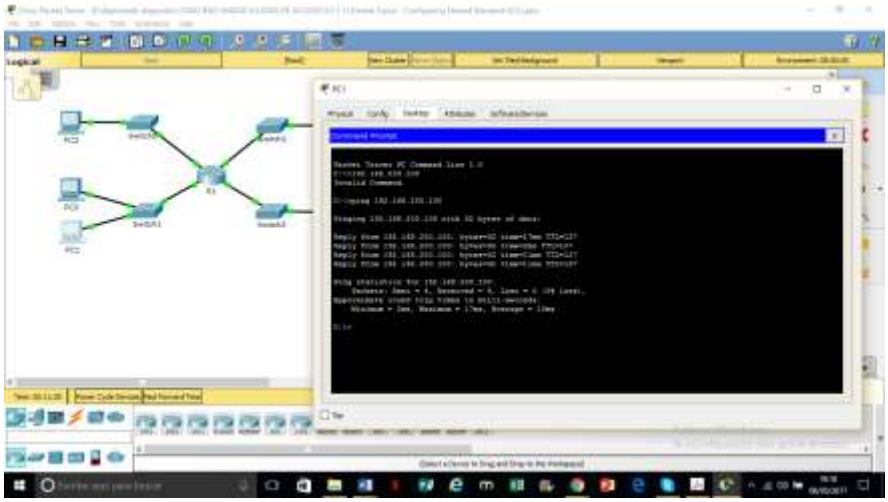
Part1: Configure and Apply a Named Standard ACL

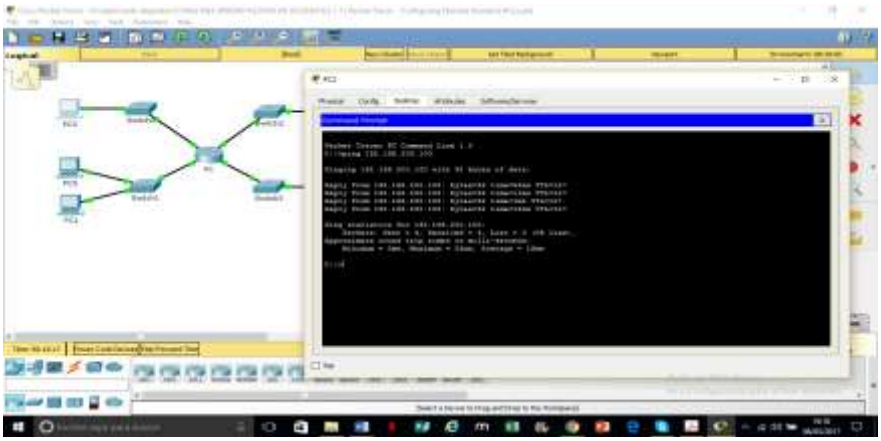
Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the Web Server and File Server.

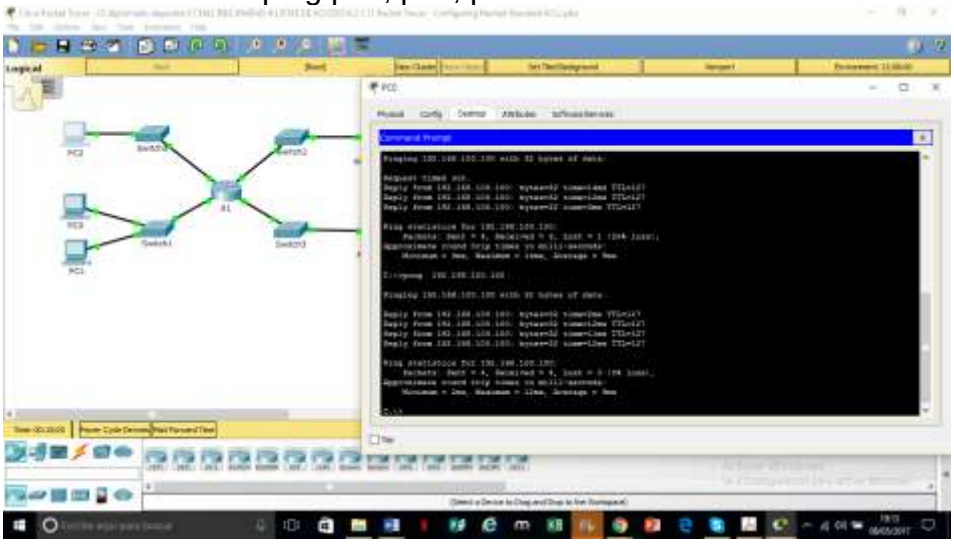
Se realiza ping pc0, pc1, pc2 con el servidor de archivos

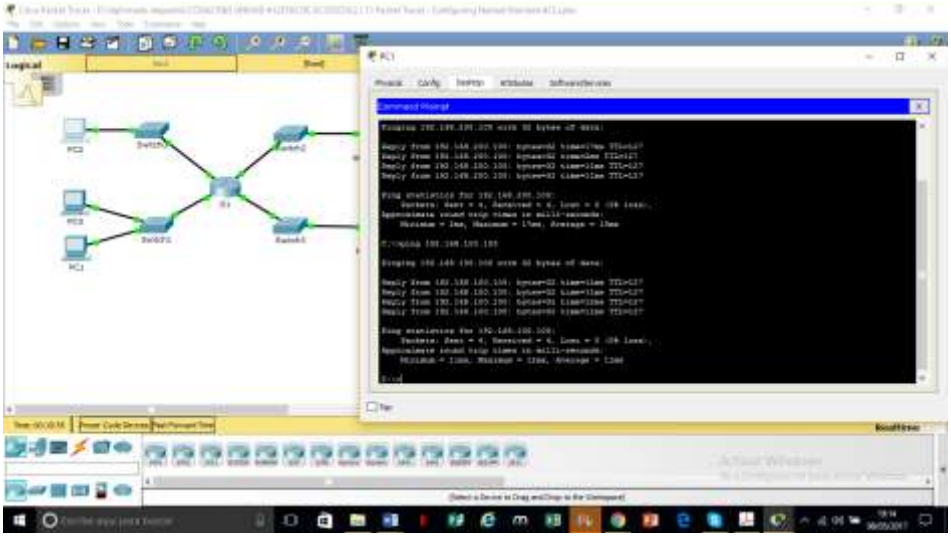


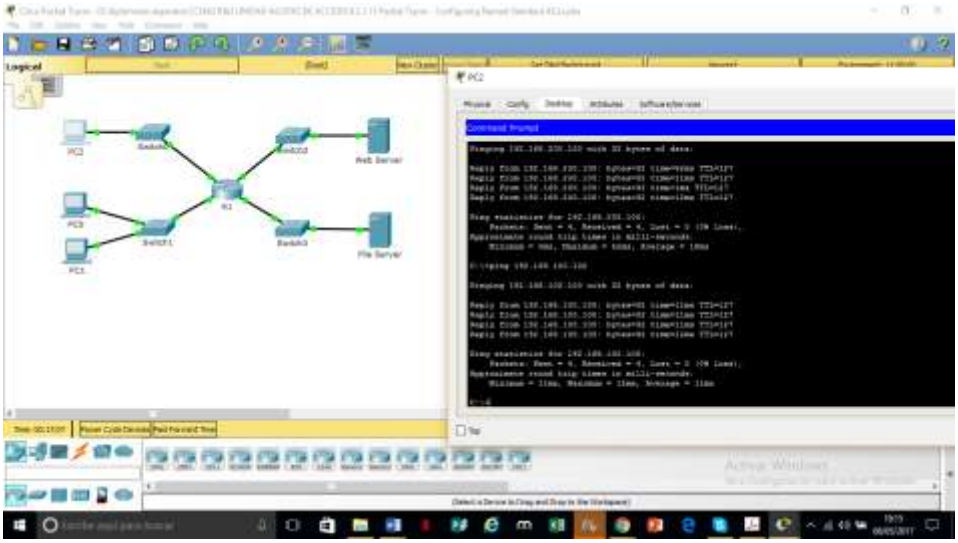




Ahora realizamos ping pc0, pc1, pc2 con el servidor web.



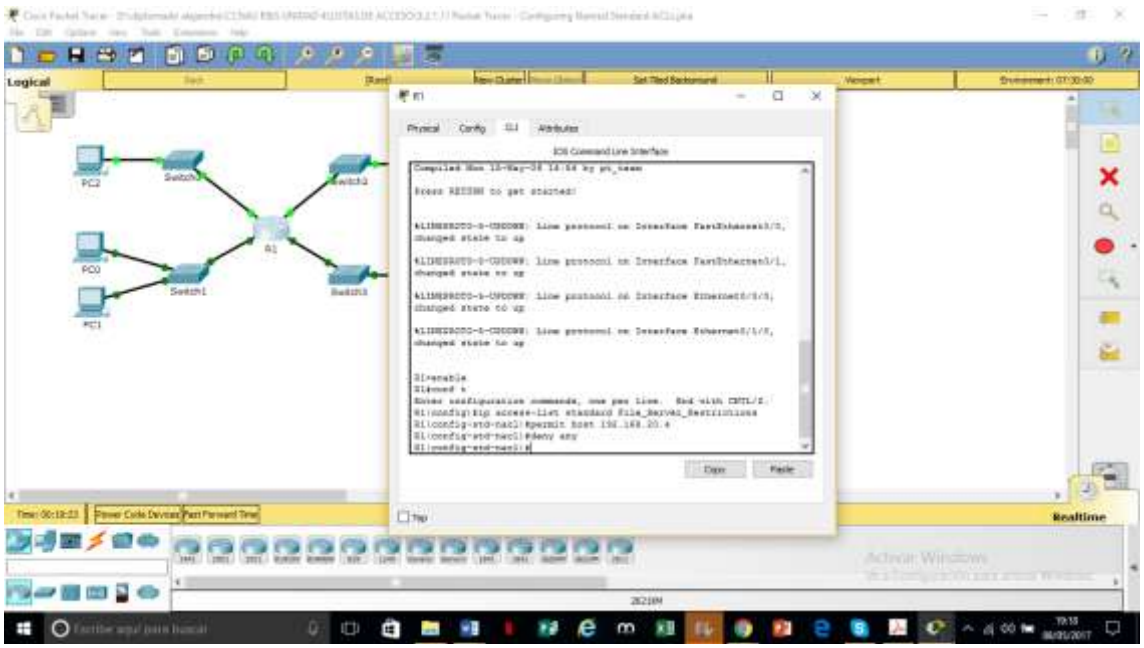




Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.

R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any

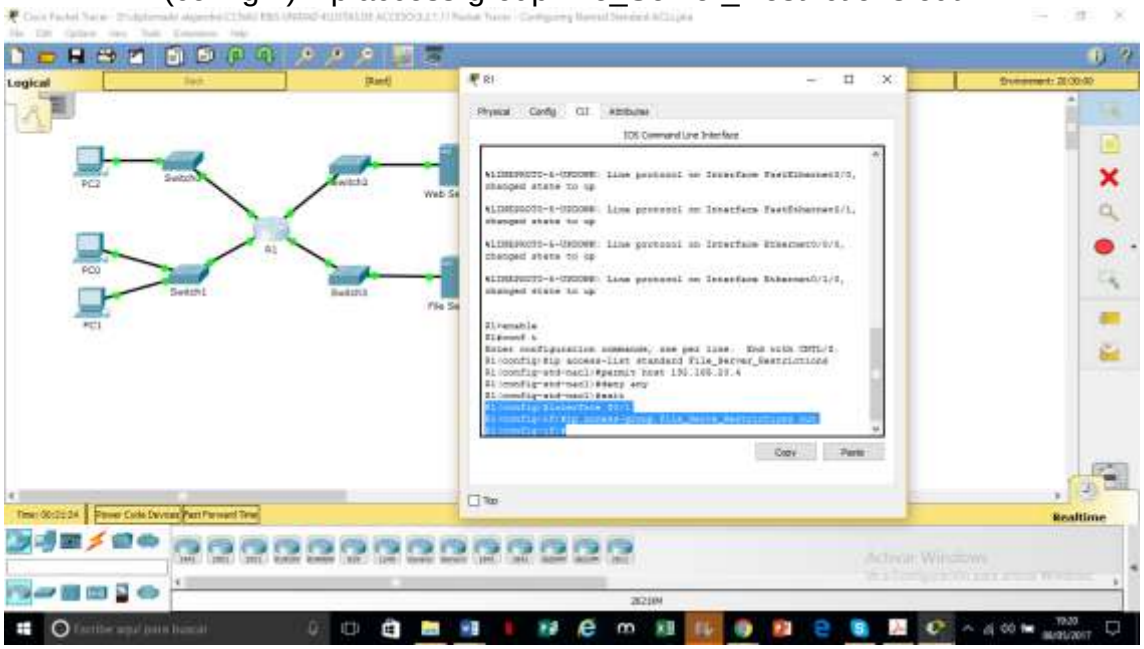


Note: For scoring purposes, the ACL name is case-sensitive.

Step 3: Apply the namedACL.

a. Apply the ACL outbound on the interface Fast Ethernet0/1.

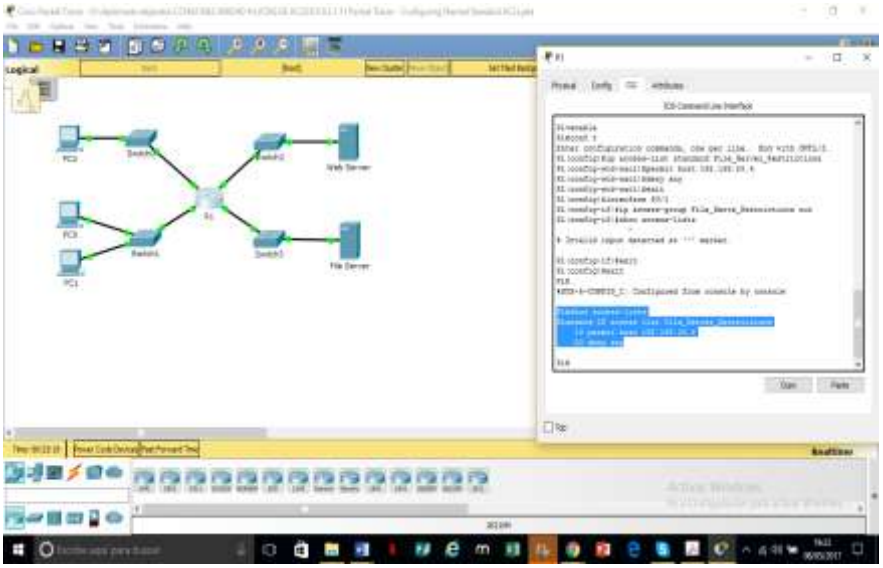
R1(config-if)# ip access-group File_Server_Restrictions out

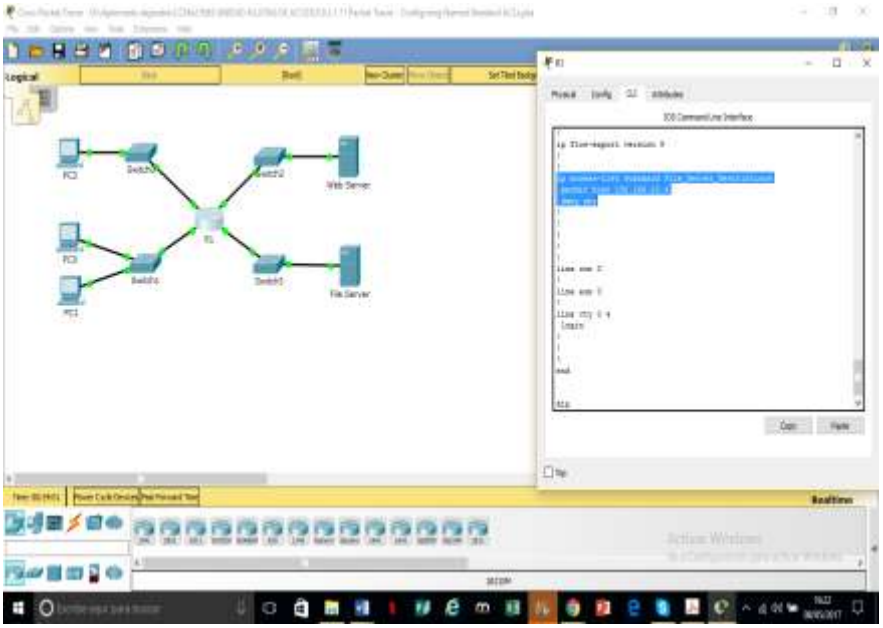


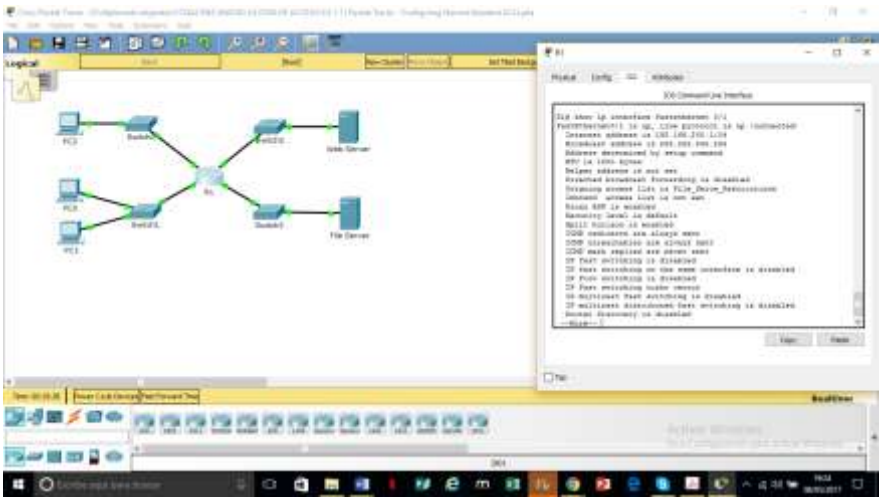
Part2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Use the show access-lists command to verify the ACL configuration. Use the show run or show ip interface fast Ethernet 0/1 command to verify that the ACL is applied correctly to the interface.

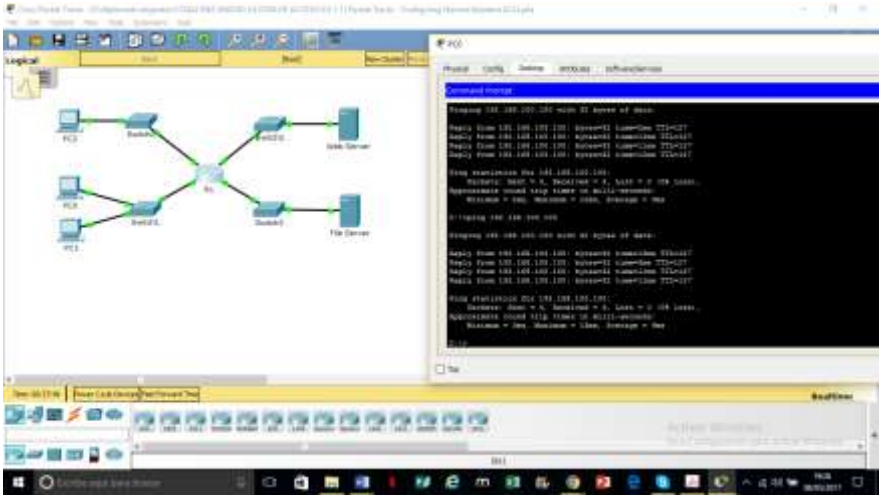


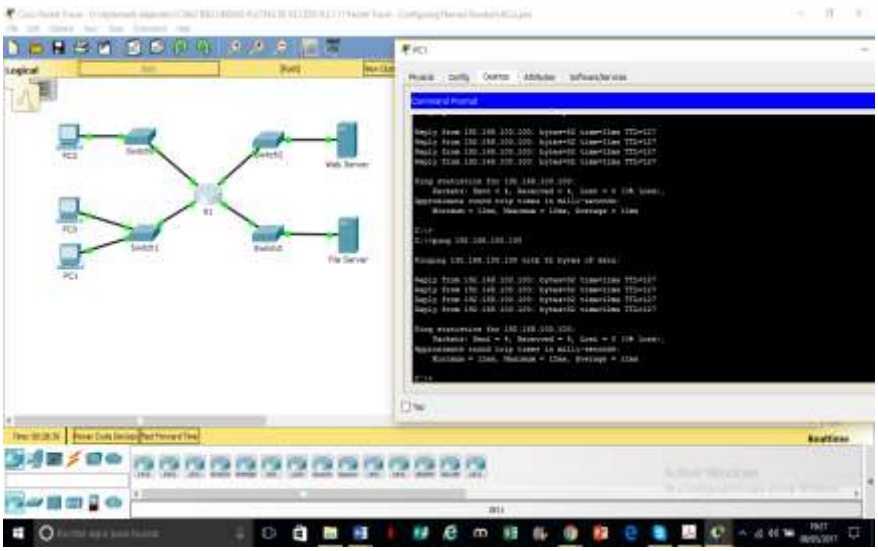


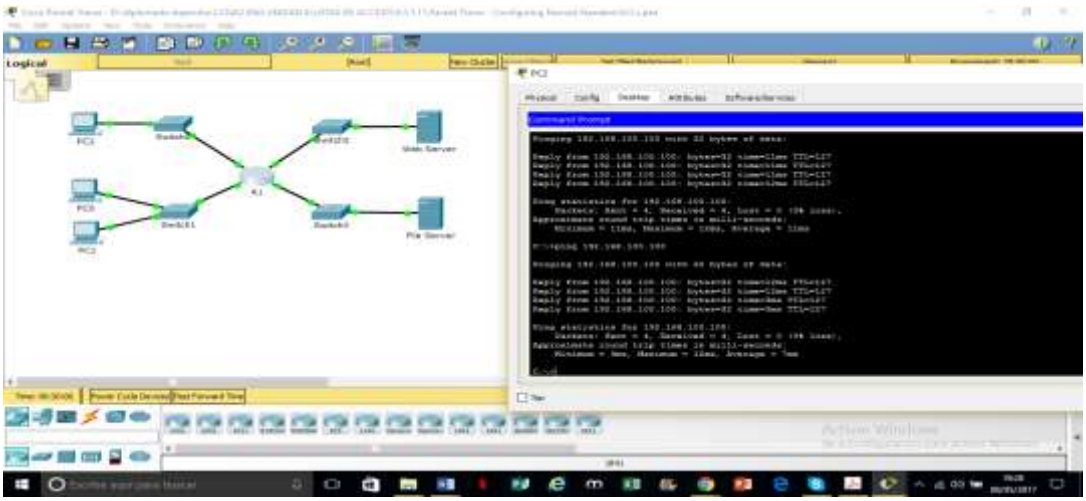


Step 2: Verify that the ACL is workingproperly.

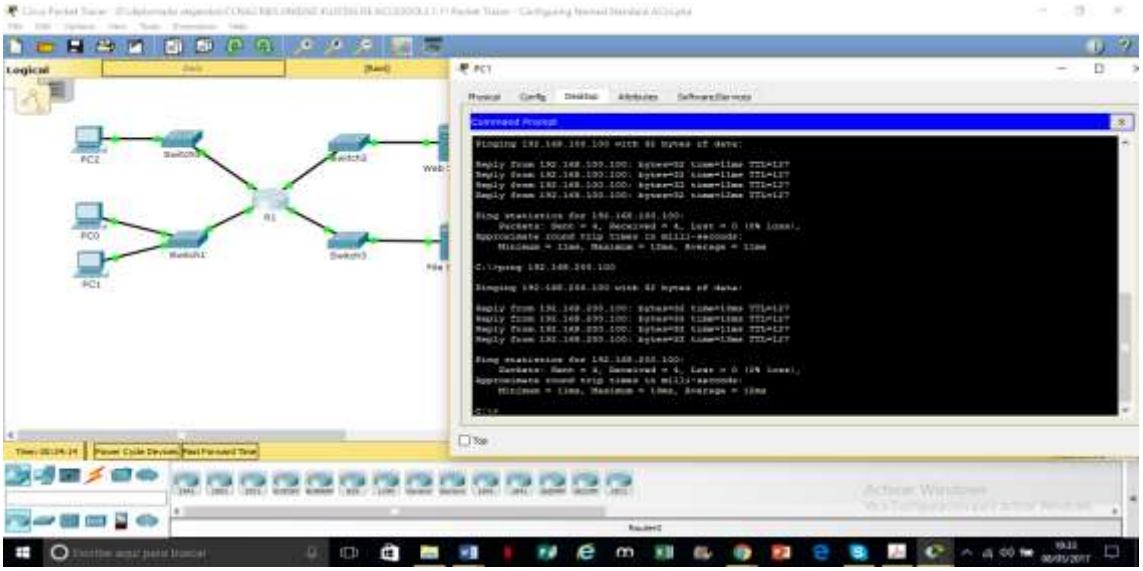
All three workstations should be able to ping the Web Server, but only PC1 should be able to ping the File Server.

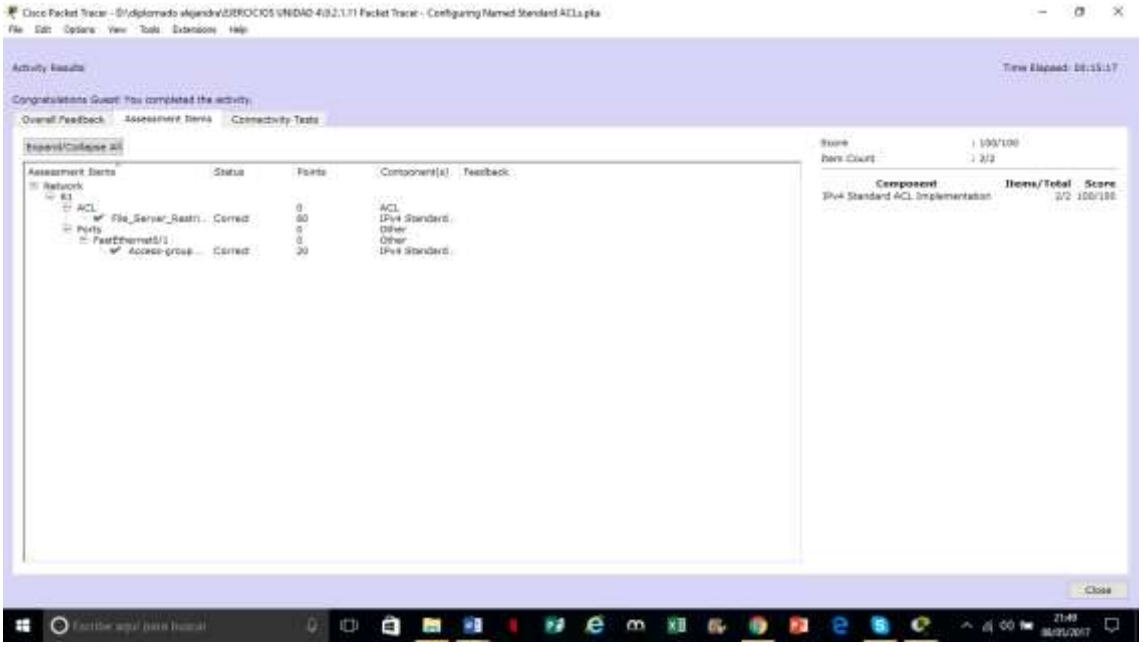






Ahora solo hace ping pc1 al servidor de archivos

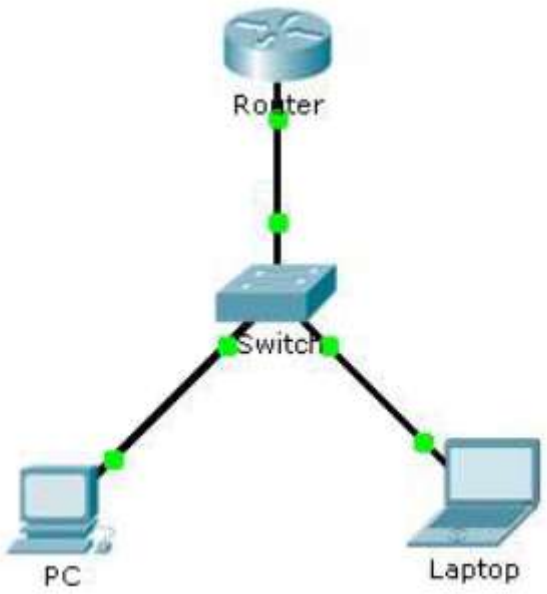




Ejercicio 9.2.3.3

Packet tracer – Configuring an ACL ON VTY LINES

Topology



Part 1: Configure and Apply an ACL to VTY Lines

AddressingTable

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Applyan ACL to VTY Lines
Part 2: Verifythe ACL Implementation

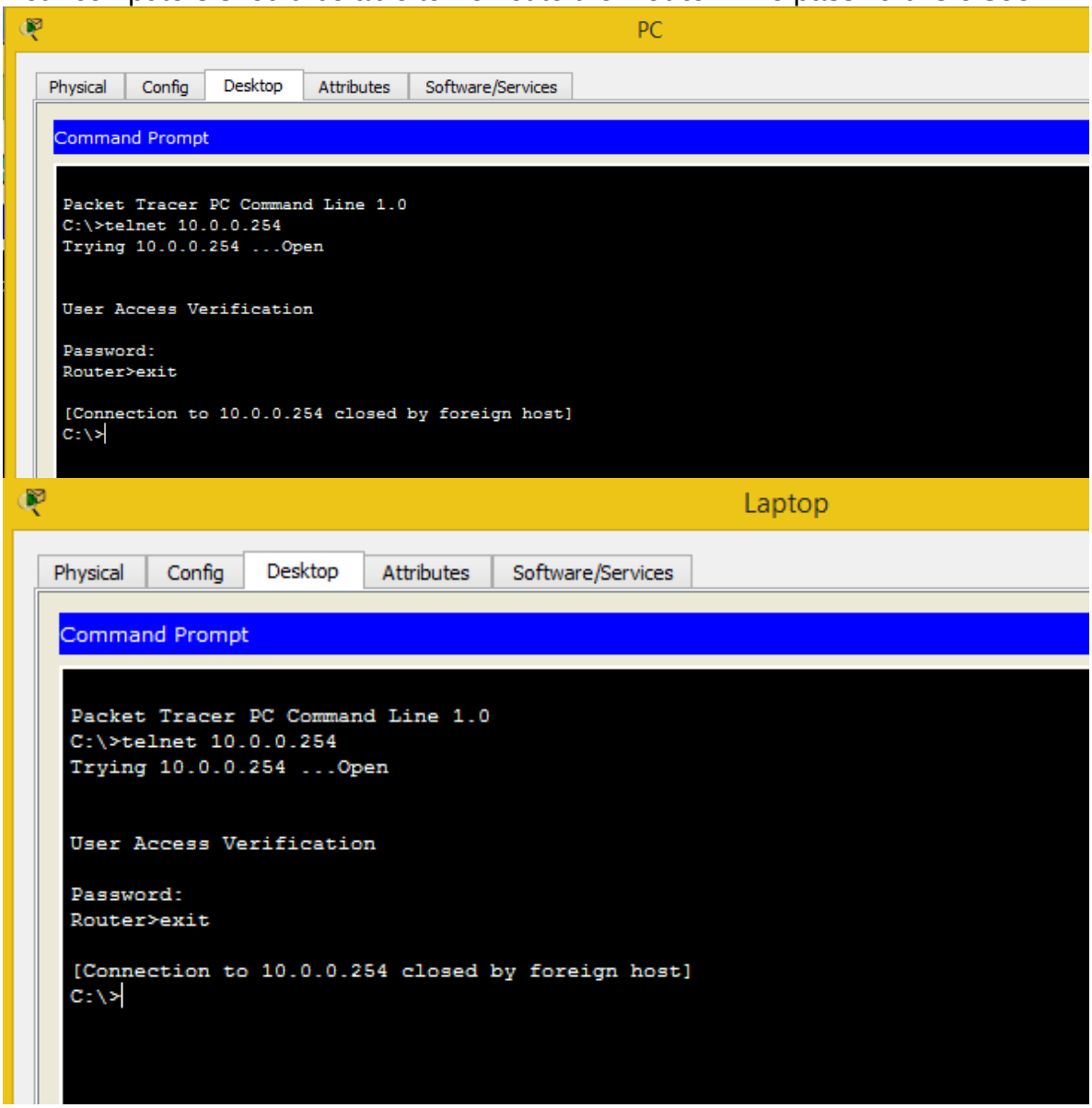
Background

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC** access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL isconfigured

Both computers should be able to Telnet to the **Router**. The password is **cisco**.



Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router**.
Router(config)# **access-list 99 permit host 10.0.0.1**

Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.Rta:/Al final hay un implícito que niega todo lo demás

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#
```

Step 3: Place a named standard ACL on the router.

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

Router(config)# **line vty 0 15**
Router(config-line)# **access-class 99 in**

```
Router(config)#line vty 0 4
Router(config-line)#access-class 99 in
Router(config-line)#
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.

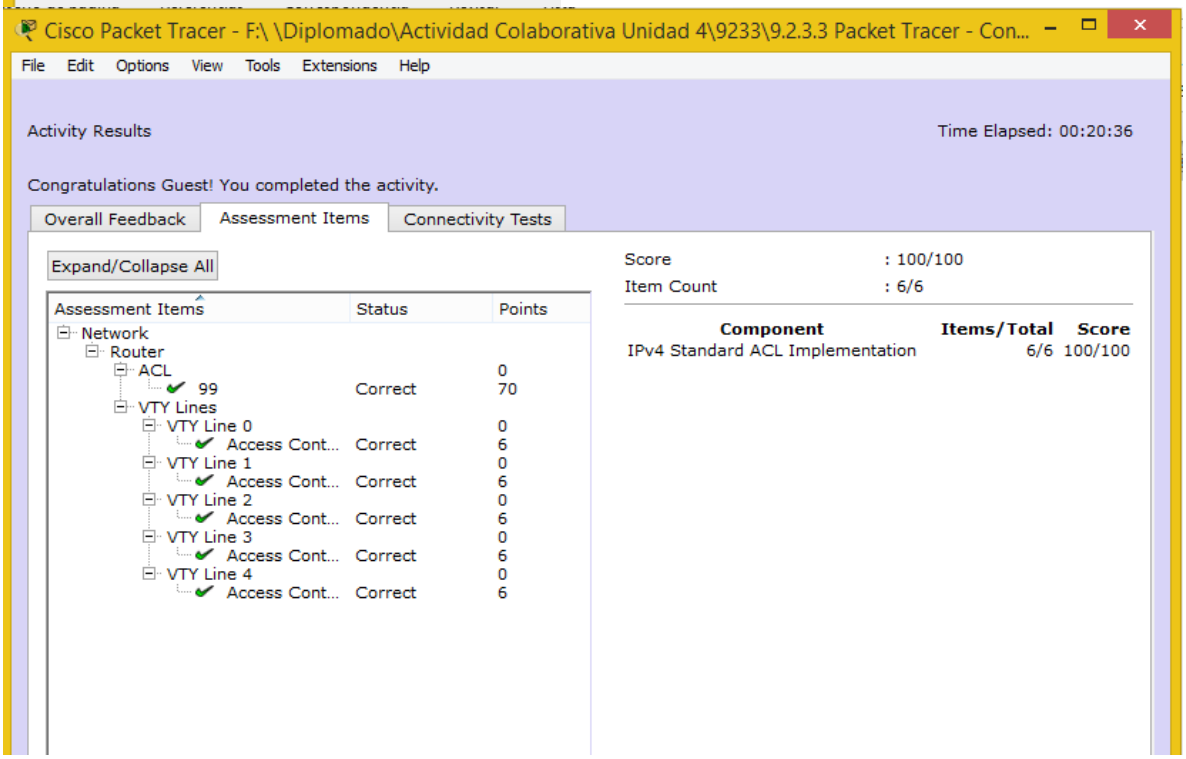
```
Router#show acc
Router#show access-lists
Standard IP access list 99
    10 permit host 10.0.0.1
!
access-list 99 permit host 10.0.0.1
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 password cisco
 login
```

Step 2: Verify that the ACL isworkingproperly.

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.

```
Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

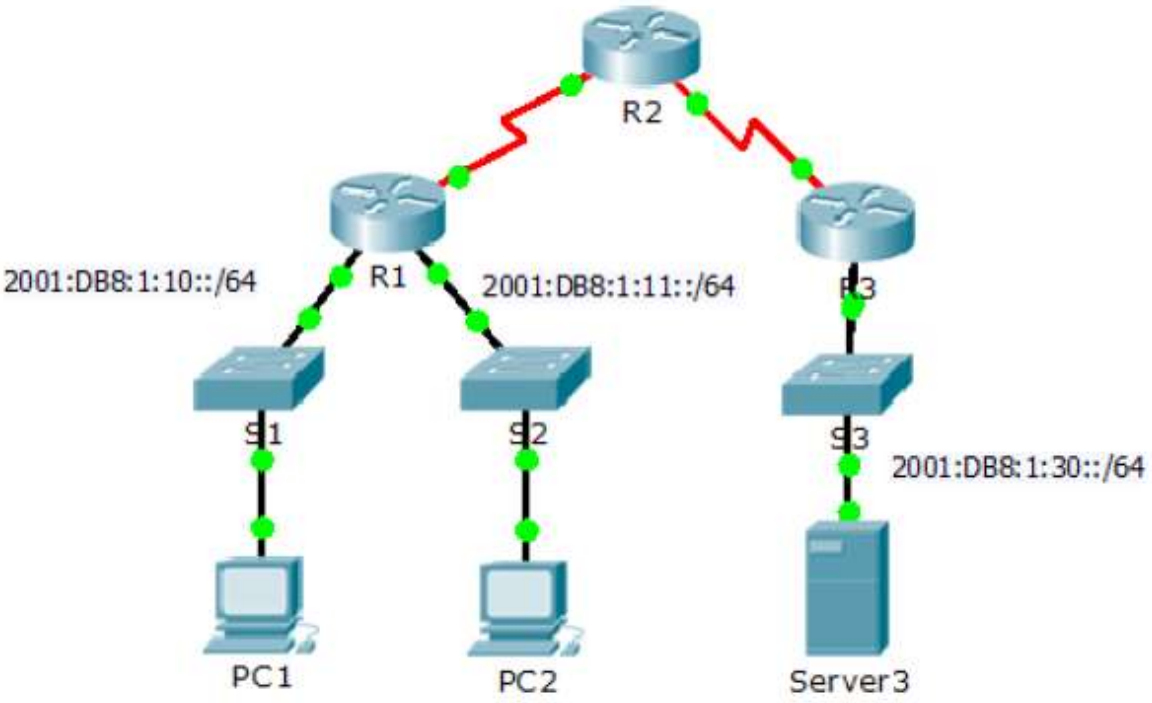
```
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open


User Access Verification

Password:
Router>
```



Ejercicio 9.2.1.11

9.5.2.6 Packet Tracer – Configuring - IPv6 ACLs

Topology



AddressingTable

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verifyan IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#
```

a. Block HTTP and HTTPS traffic from reaching **Server3**.

R1(config)# **deny tcp any host 2001:DB8:1:30::30 eq www**
R1(config)# **deny tcp any host 2001:DB8:1:30::30 eq 443**

```
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443
R1(config-ipv6-acl)#
```

b. Allow all other IPv6 traffic to pass.

R1(config)# **permit ipv6 any any**

```
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#
```

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

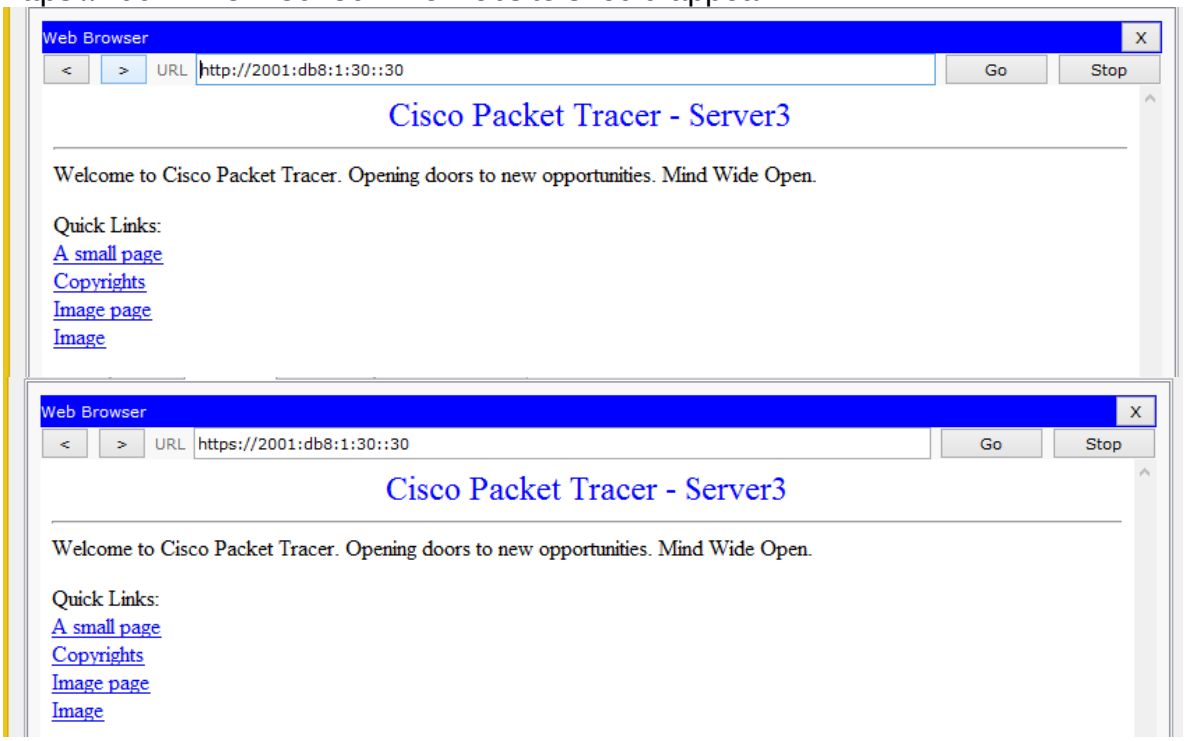
R1(config)# **interface GigabitEthernet0/1**
R1(config-if)# **ipv6 traffic-filter BLOCK_HTTP in**

```
R1(config)#int g0/1
R1(config-if)#ipv6 traffic
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

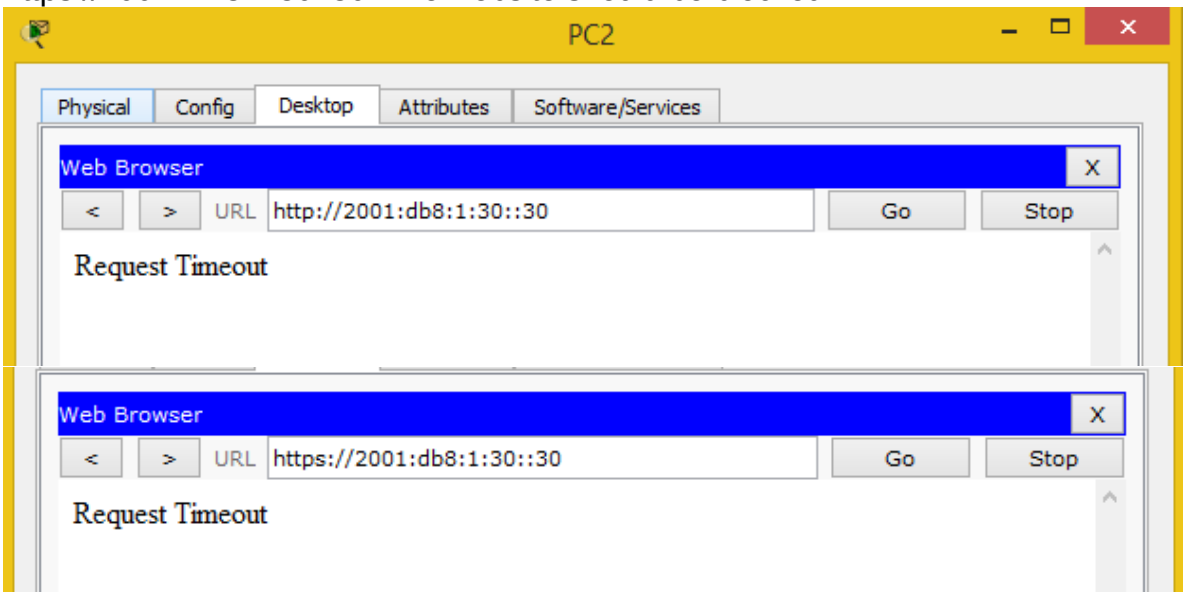
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

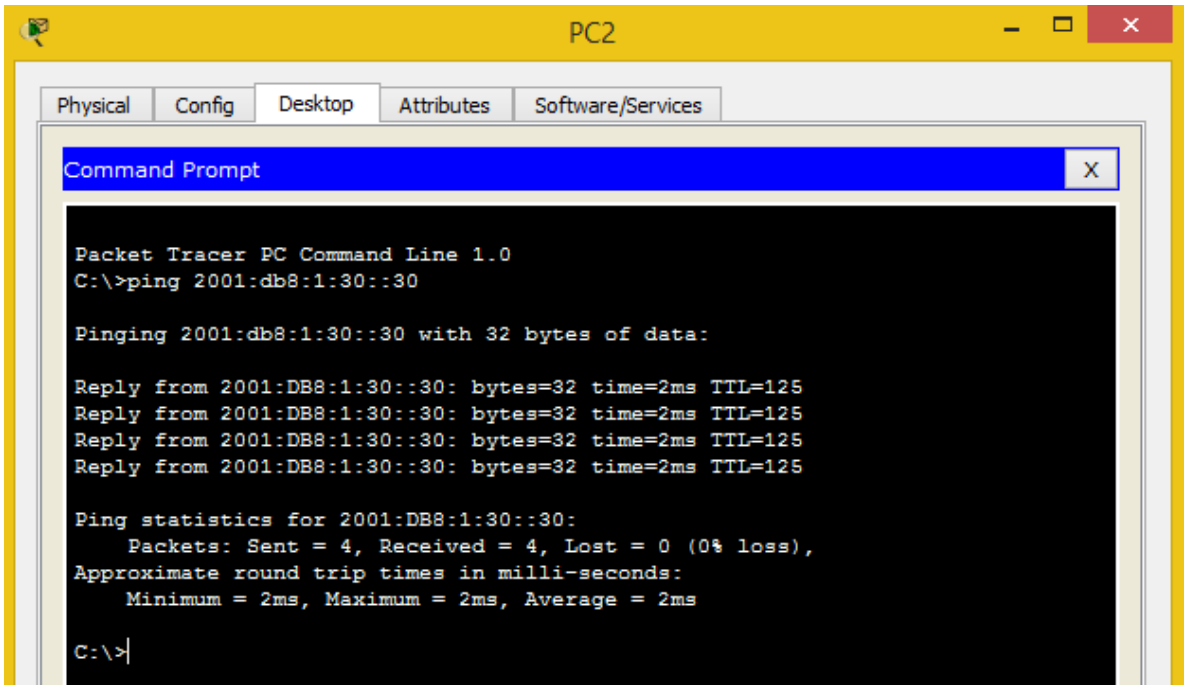
Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.



Open the **web browser** of **PC2** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked



Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.



Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK_ICMP** on **R3** with the following statements:
a. Block all ICMP traffic from any hosts to any destination.

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6
R3(config)#ipv6 acc
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#
```

R3(config)# **deny icmp any any**

b. Allow all other IPv6 traffic to pass.

R3(config)# **permit ipv6 any any**

```
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
```

Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:1:30::1/64
 ipv6 eigrp 1
```

R3(config)# **interface GigabitEthernet0/0**
R3(config-if)# **ipv6 traffic-filter BLOCK_ICMP out**

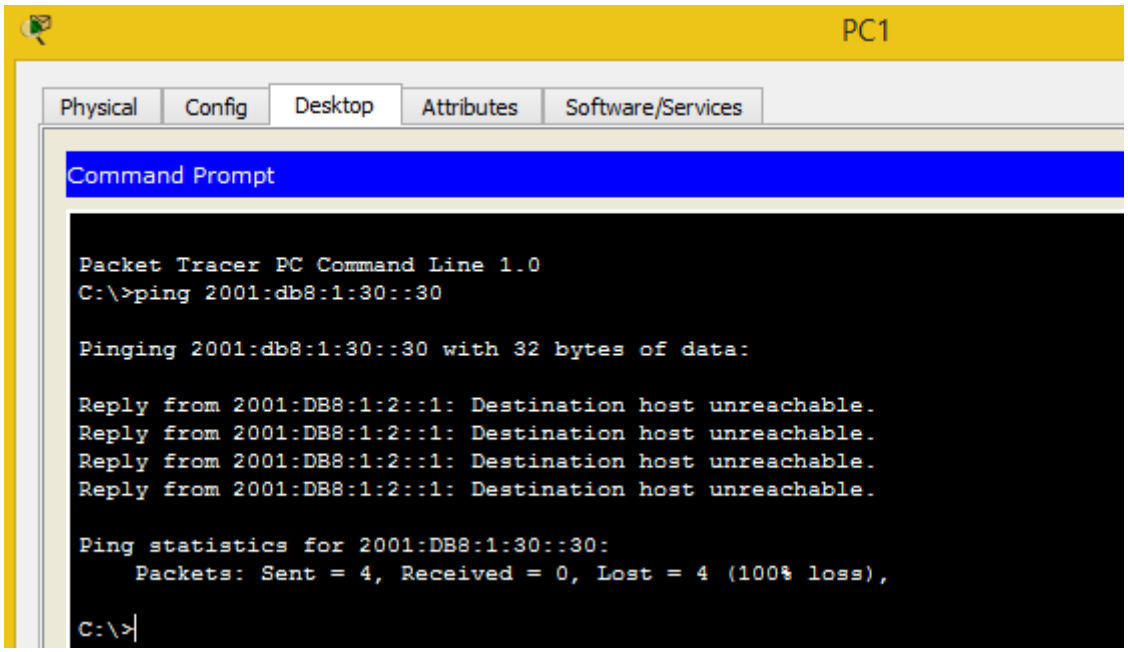
```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traff
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Step 3: Verify that the proper access list functions.

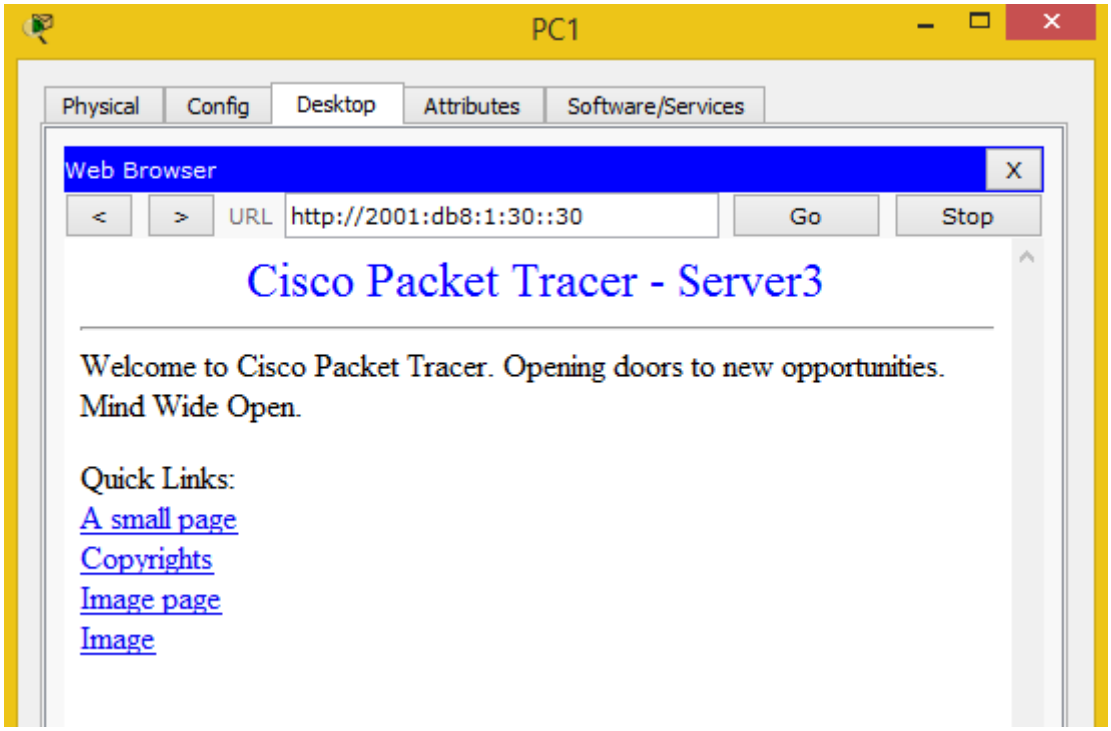
a. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

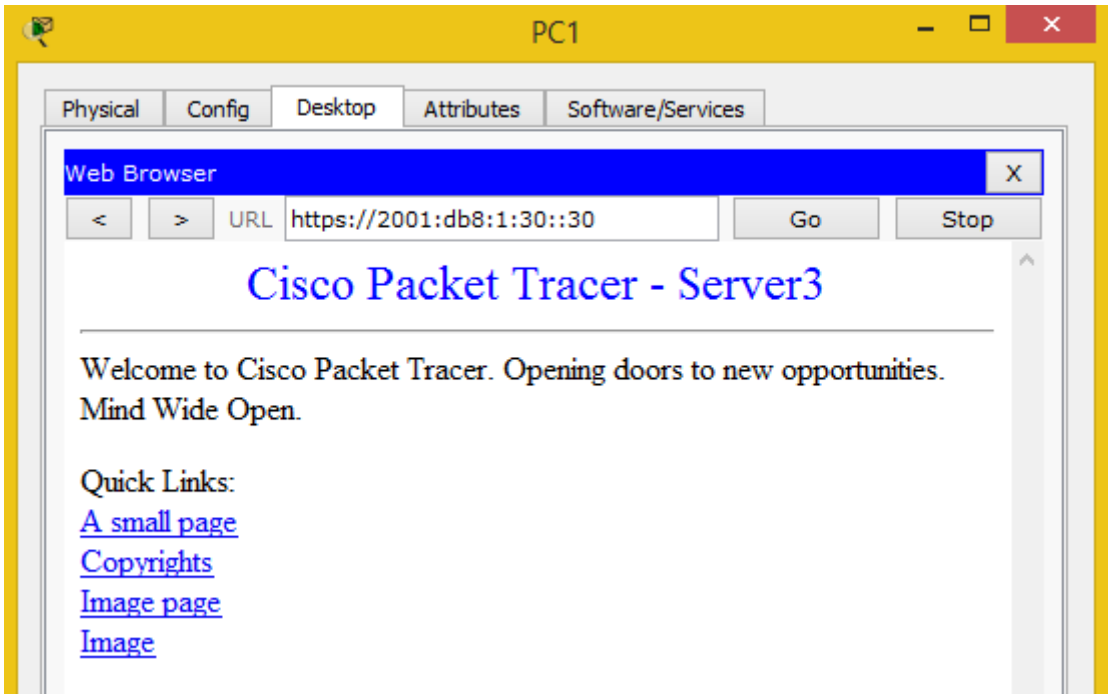
```
C:\>ping 2001:db8:1:30::30

Pinging 2001:db8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

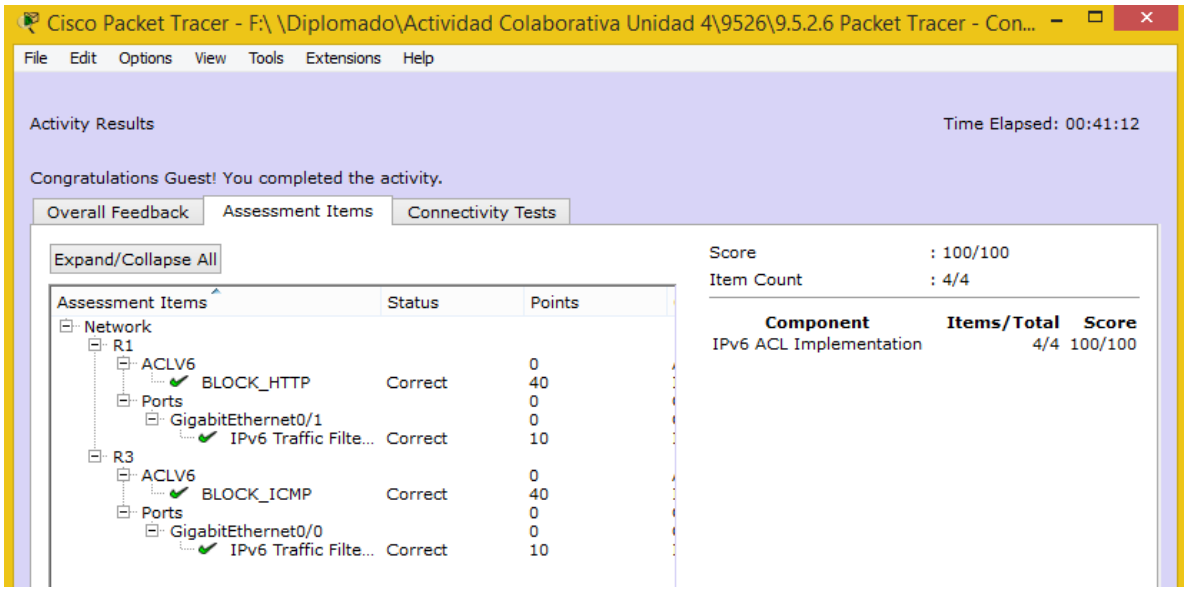
b. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.



Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.




PC1
Physical
Config
Desktop
Attributes
Software/Services
Web Browser
X
<
>
URL
https://2001:db8:1:30::30
Go
Stop
Cisco Packet Tracer - Server3
Welcome to Cisco Packet Tracer. Opening doors to new opportunities.
Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


Cisco Packet Tracer - F:\ \Diplomado\Actividad Colaborativa Unidad 4\9526\9.5.2.6 Packet Tracer - Con...
File
Edit
Options
View
Tools
Extensions
Help
Activity Results
Time Elapsed: 00:41:12
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Network
R1
ACLV6
0
BLOCK_HTTP
Correct
40
Ports
0
GigabitEthernet0/1
0
IPv6 Traffic Filte...
Correct
10
R3
ACLV6
0
BLOCK_ICMP
Correct
40
Ports
0
GigabitEthernet0/0
0
IPv6 Traffic Filte...
Correct
10
Score
: 100/100
Item Count
: 4/4
Component
Items/Total
Score
IPv6 ACL Implementation
4/4
100/100

Ejercicio 10.1.2.4

Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

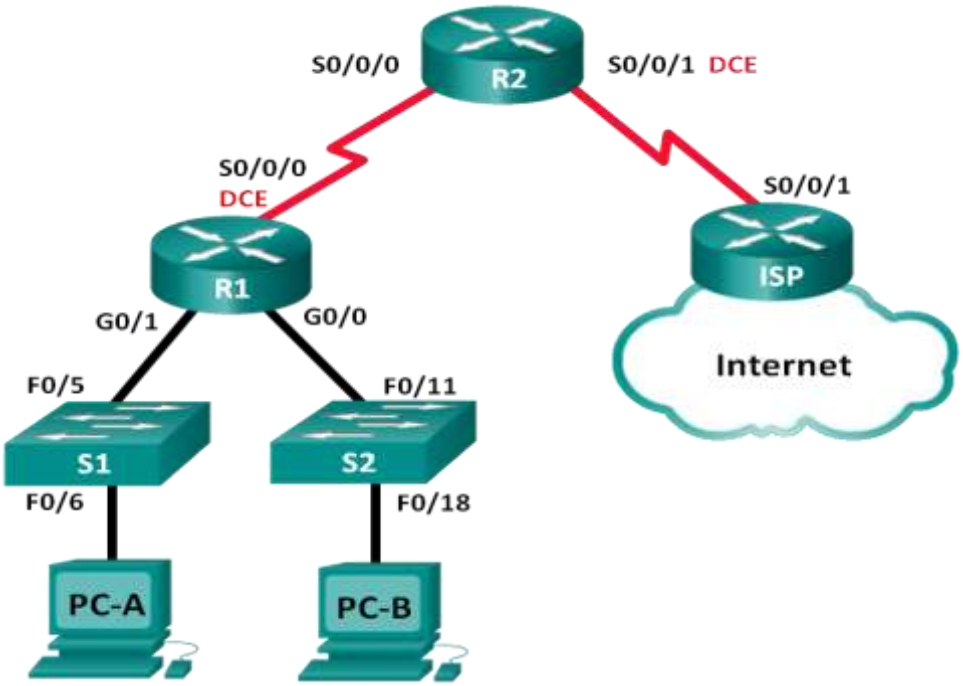


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las

direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y los switches.

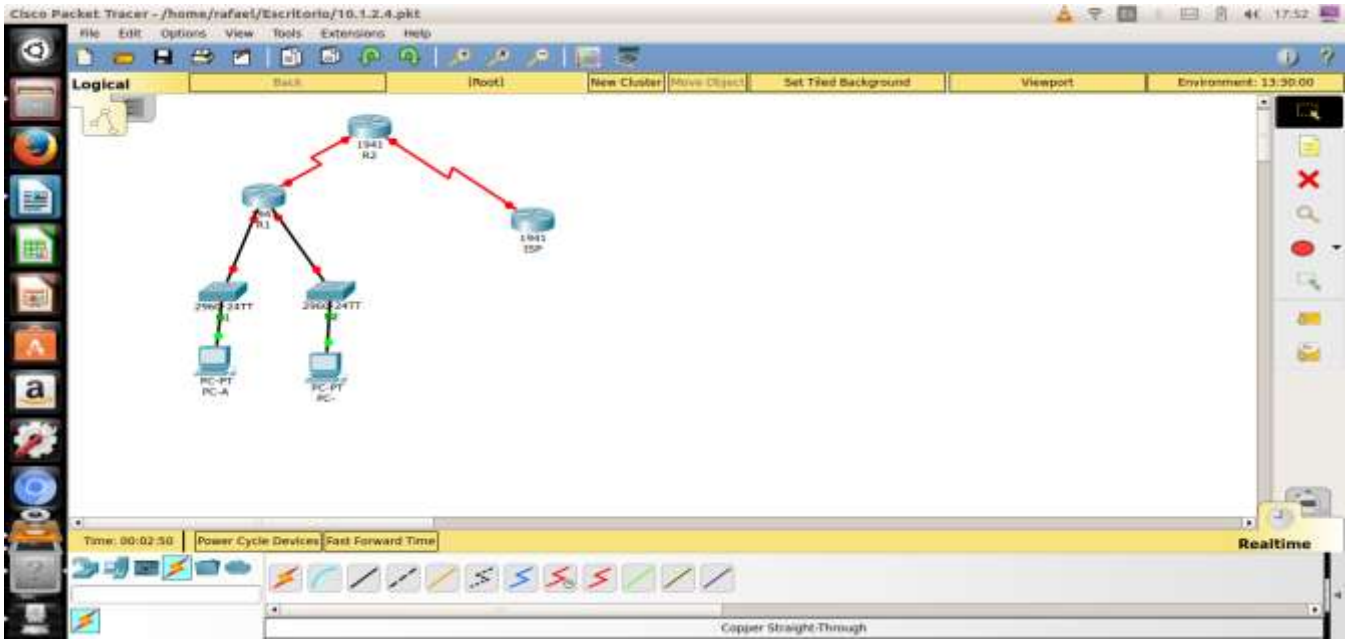
Paso 3: configurar los parámetros básicos para cada router.

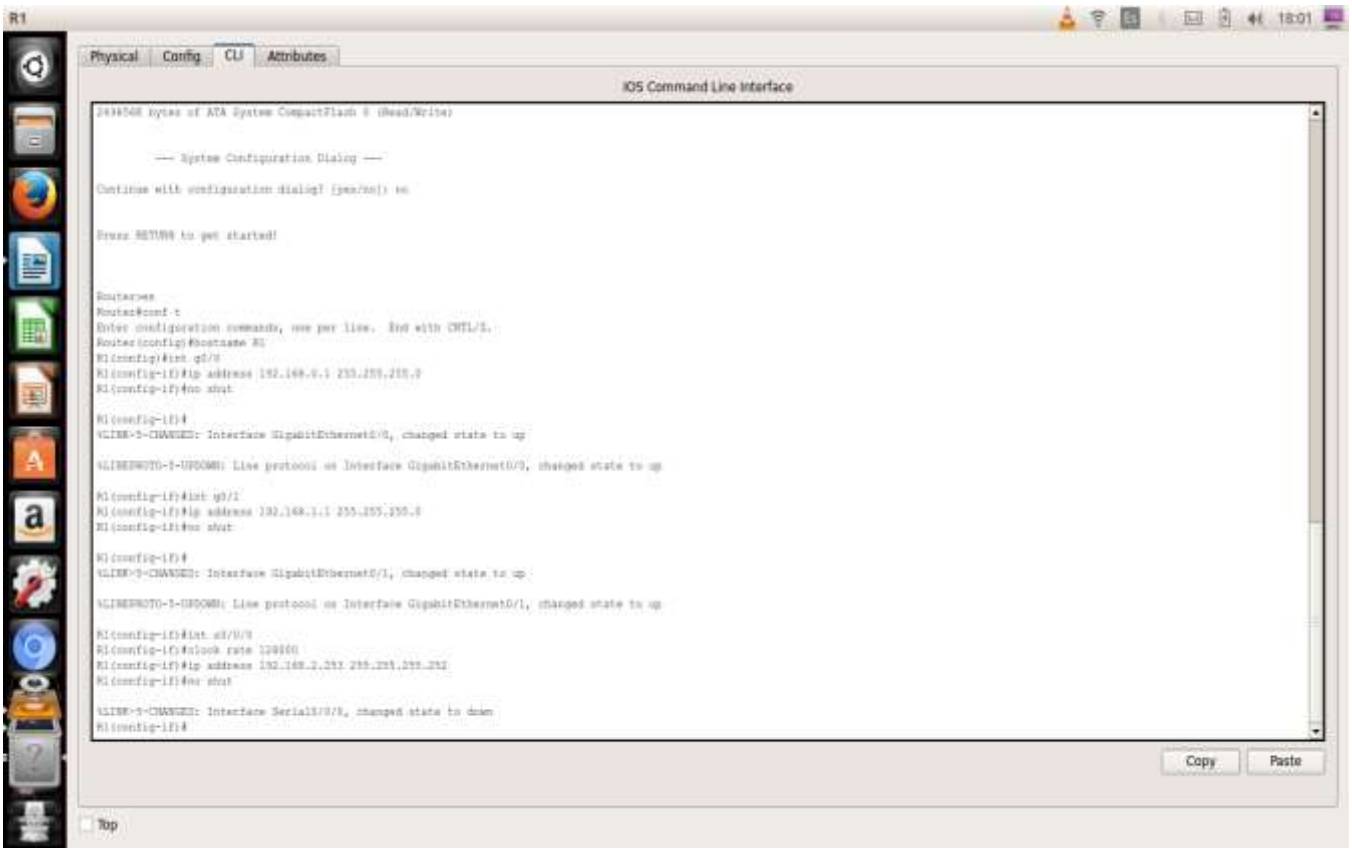
a. Desactive la búsqueda DNS.
b. Configure el nombre del dispositivo como se muestra en la topología.
c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.
h. Configure EIGRP for R1.
   R1(config)# **router eigrp 1**
   R1(config-router)# **network 192.168.0.0 0.0.0.255**
   R1(config-router)# **network 192.168.1.0 0.0.0.255**
   R1(config-router)# **network 192.168.2.252 0.0.0.3**
   R1(config-router)# **no auto-summary**
i. Configure EIGRP y una ruta predeterminada al ISP en el R2.
   R2(config)# **router eigrp 1**
   R2(config-router)# **network 192.168.2.252 0.0.0.3**
   R2(config-router)# **redistribute static**
   R2(config-router)# **exit**
   R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.225**
j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.
   ISP(config)# **ip route 192.168.0.0 255.255.252.0 209.165.200.226**
k. Copie la configuración en ejecución en la configuración de inicio

Paso 4: verificar la conectividad de red entre los routers.

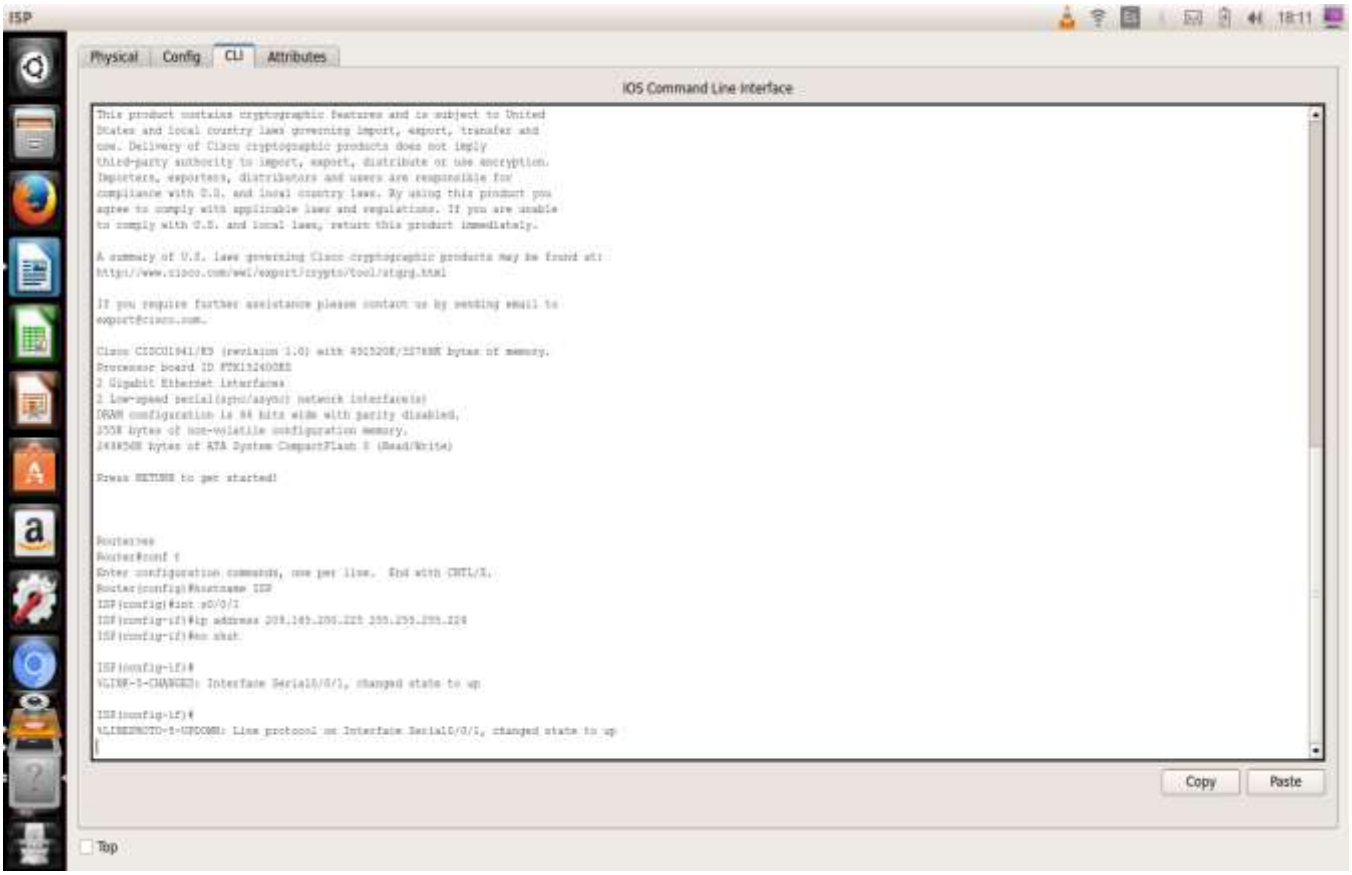
Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos **show ip route** y **show ip interface brief** para detectar posibles problemas.

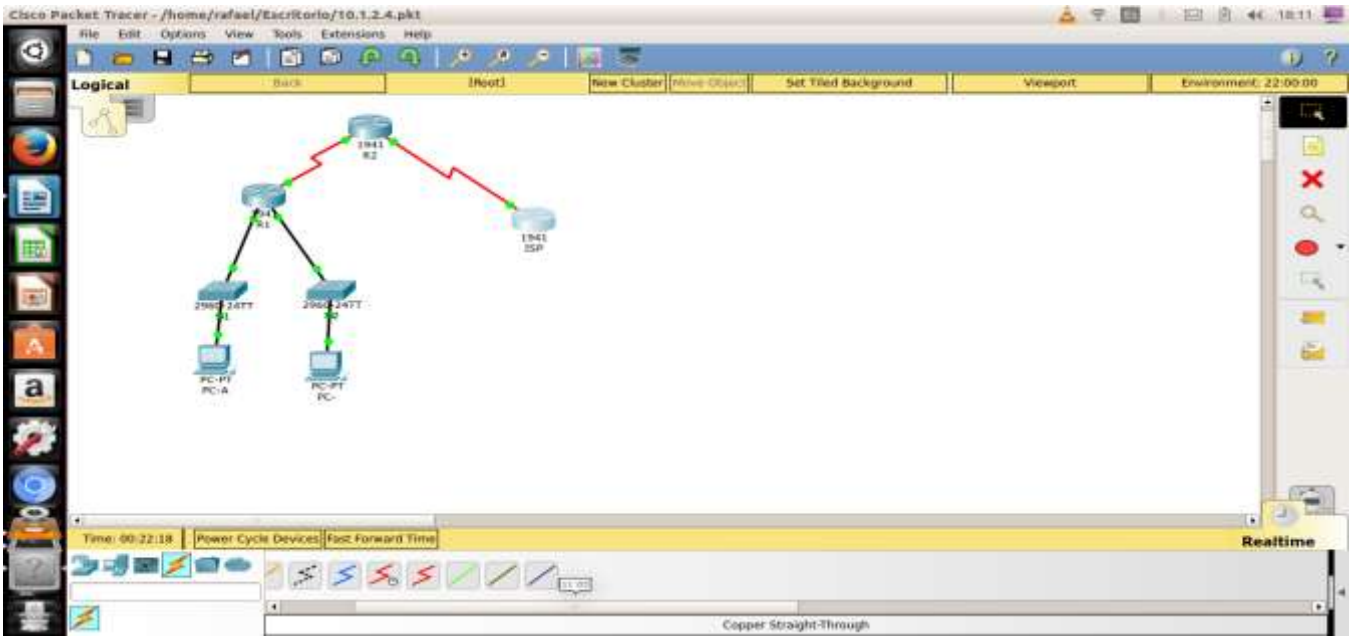
Paso 5: verificar que los equipos host estén configurados para DHCP.

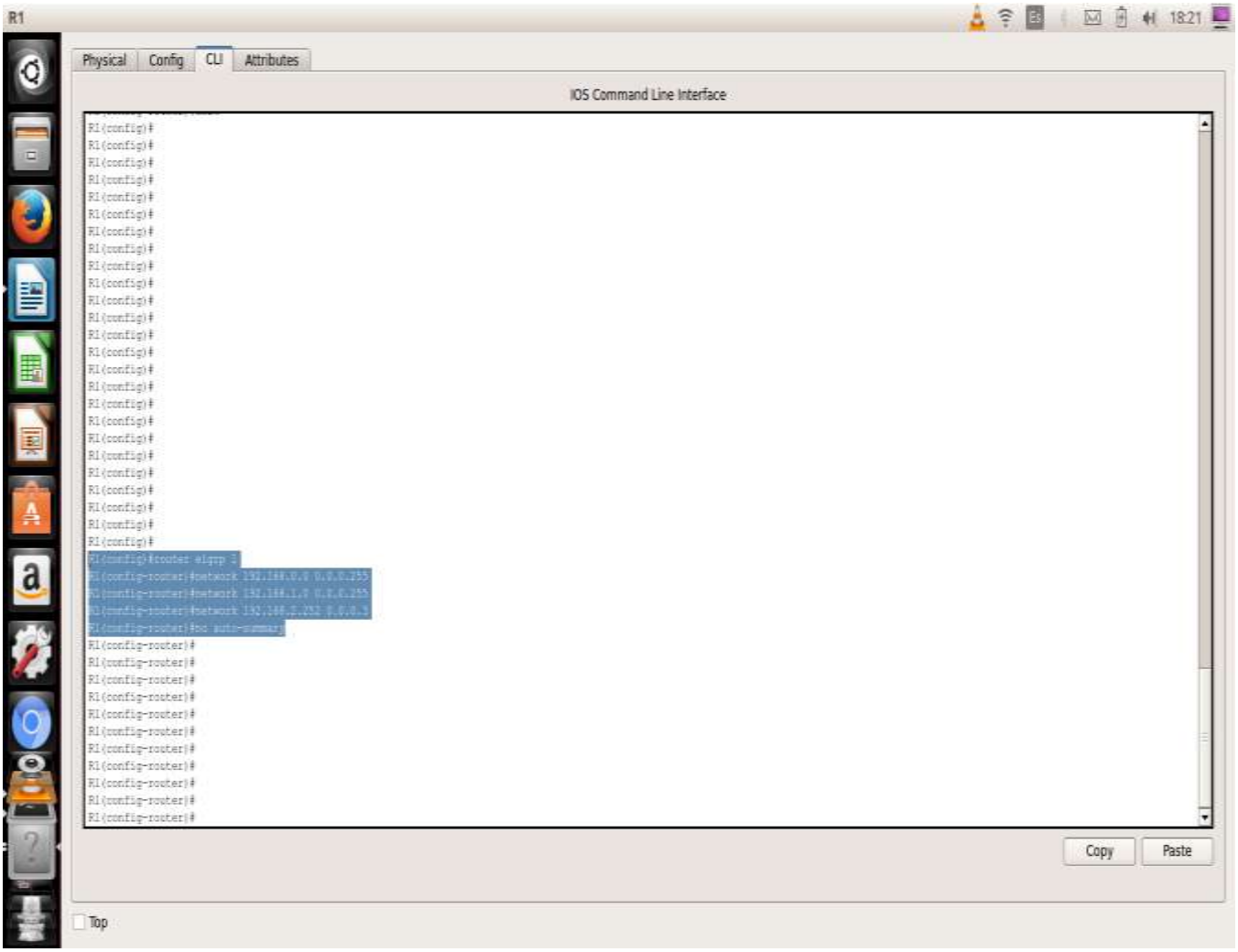


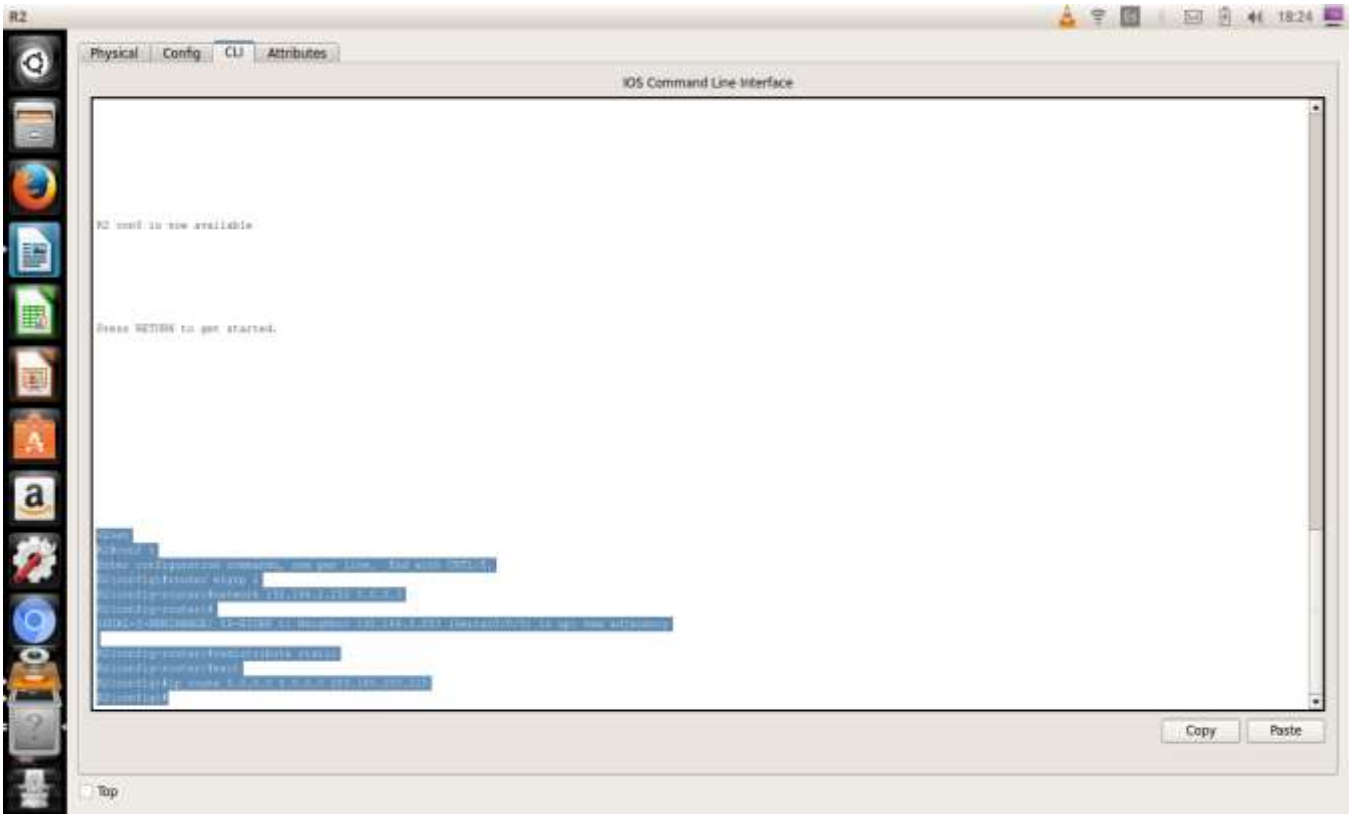


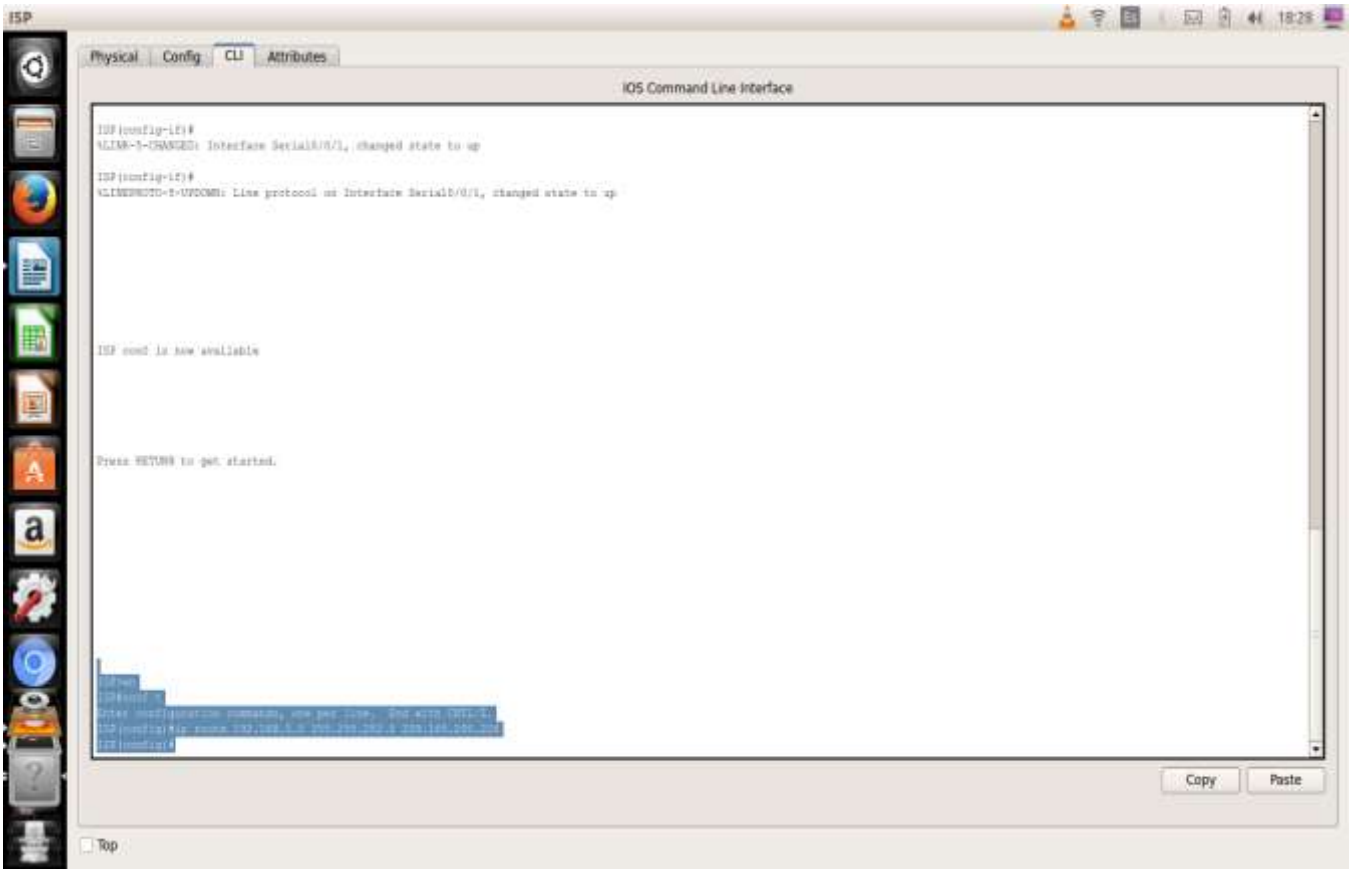

R2
18:08
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top


ISP
18:11
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top


Cisco Packet Tracer - /home/rafael/Escritorio/10.1.2.4.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Set Tiled Background
Viewport
Environment: 22:00:00
Time: 00:22:18
Power Cycle Devices
Fast Forward Time
Realtime
Copper Straight-Through


R1
18:21
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#
Copy
Paste
Top


R2
18:24
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2 conf is now available
Press RETURN to get started.
Copy
Paste
Top


ISP
18:28
Physical
Config
CLI
Attributes
IOS Command Line Interface
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial3/0/1, changed state to up
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0/1, changed state to up
ISP conf is now available
Press RETURN to get started.
Copy
Paste
Top

Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Para asignar automáticamente la información de dirección en la red, configure el R2 como servidor de DHCPv4 y el R1 como agente de retransmisión DHCP.

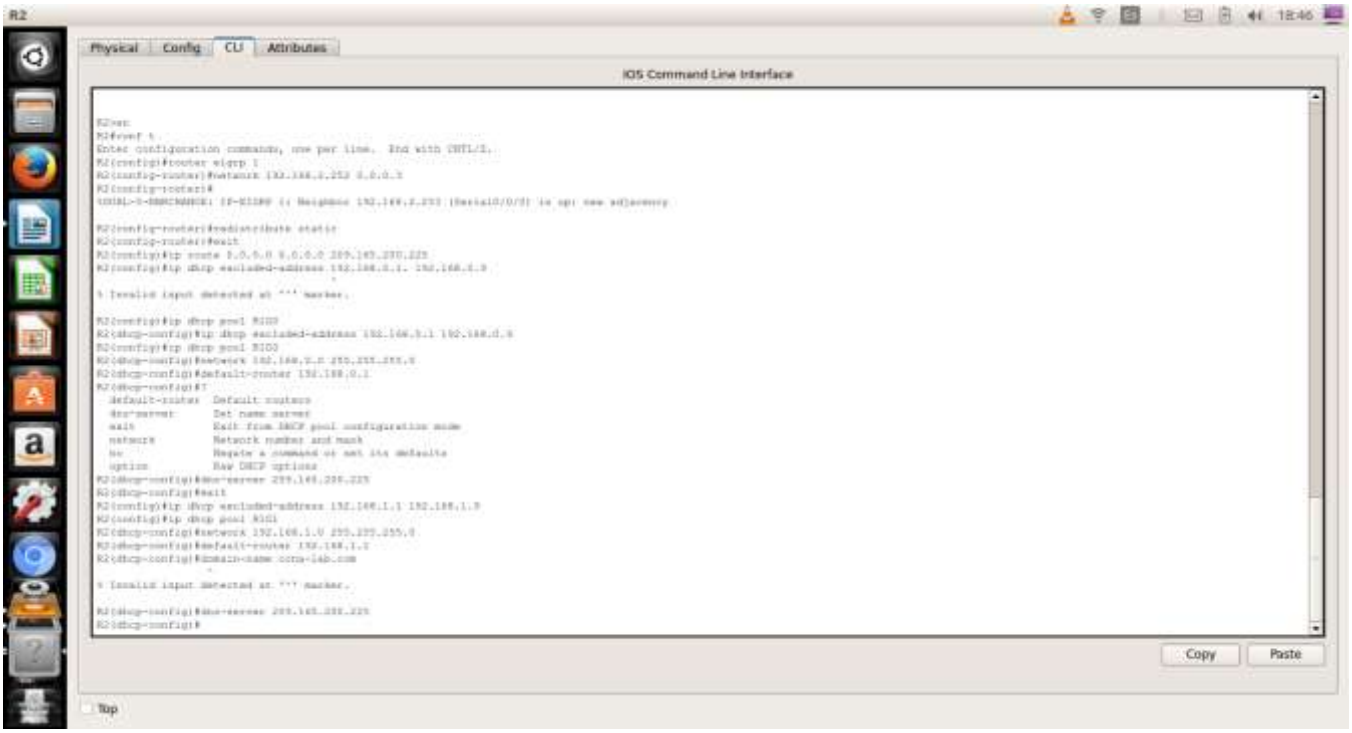
Paso 1: configurar los parámetros del servidor de DHCPv4 en el router R2.

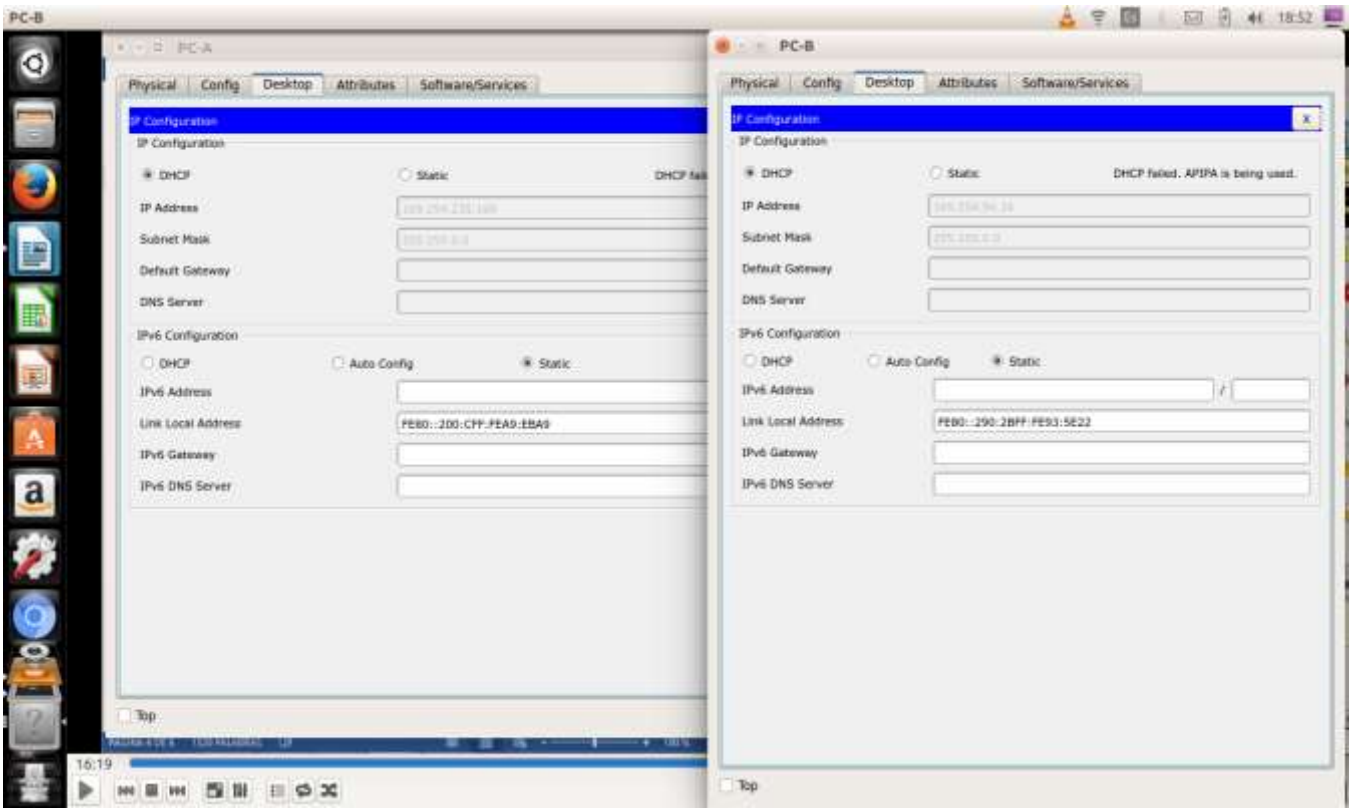
En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

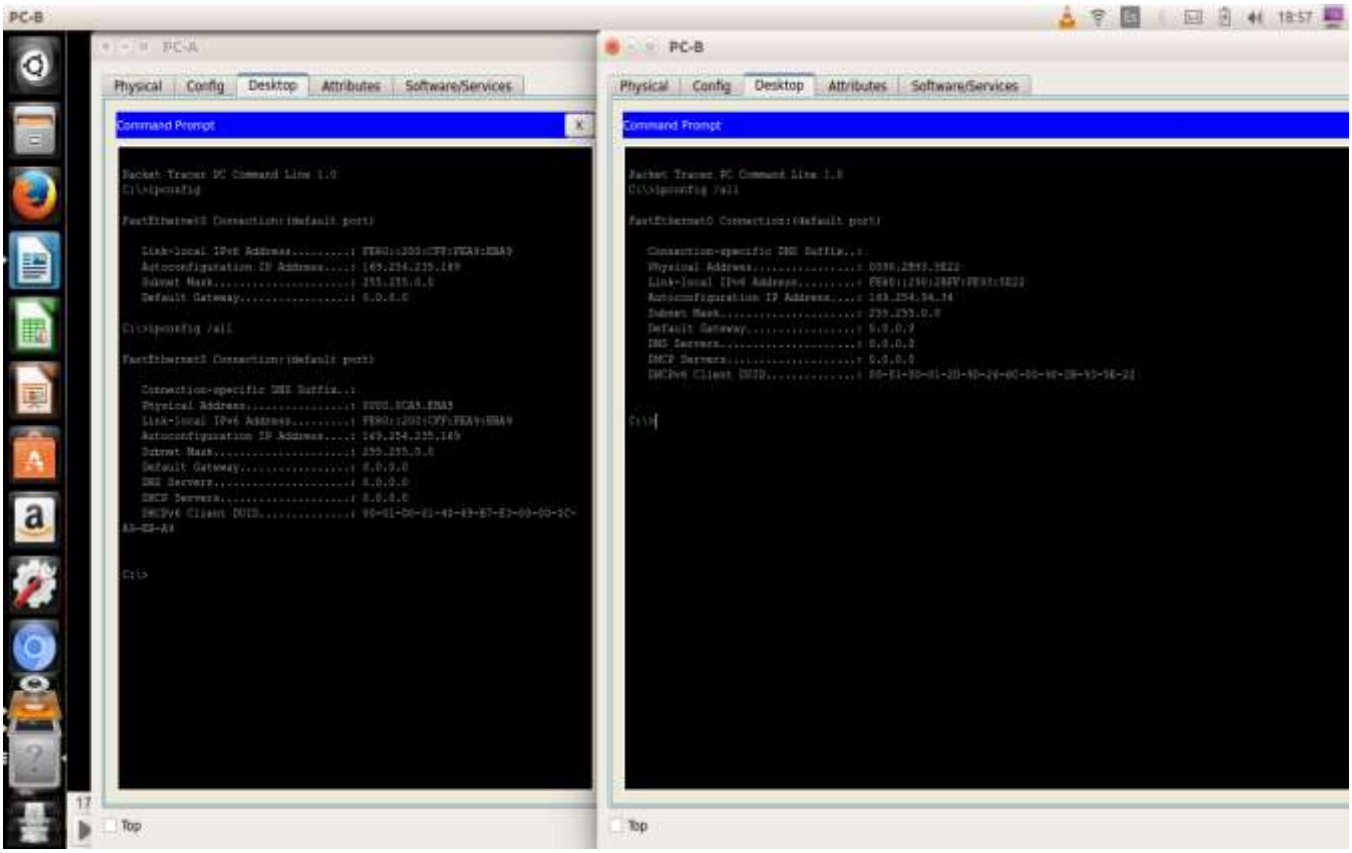
Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio **ccna-lab.com**, un servidor DNS (209.165.200.225) y un tiempo de arrendamiento de dos días.

En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar DHCP en el R1 y el R2 sin consultar el apéndice.




PC-B
PC-A
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
DHCP
Static
DHCP failed. APIPA is being used.
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
Auto Config
IPv6 Address
Link Local Address
FE80::200:CFF:FEA9:EBA9
FE80::290:2BFF:FE93:5E22
IPv6 Gateway
IPv6 DNS Server
Top


PC-B
PC-A
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig
C:\>ipconfig /all
Top

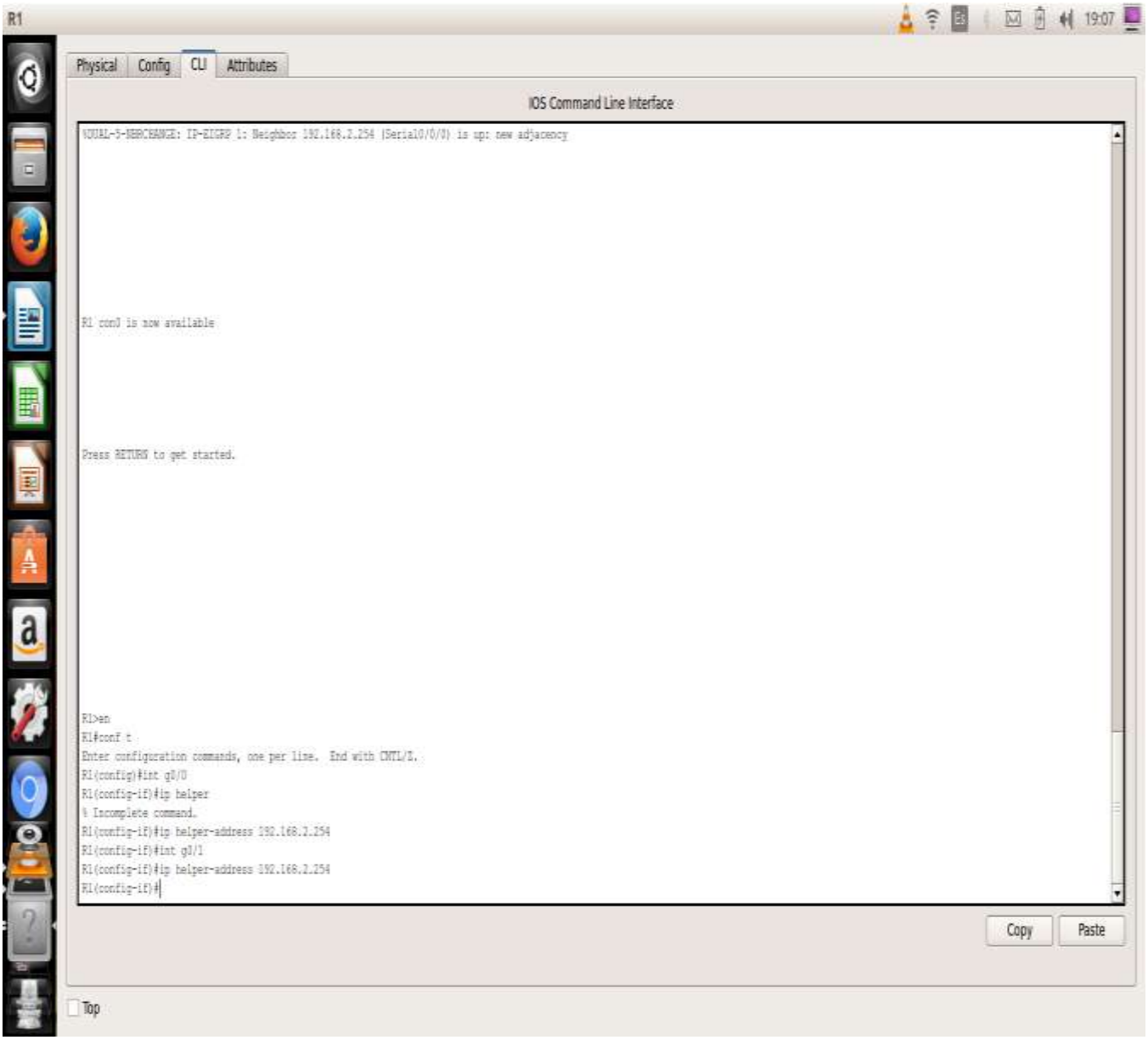
En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

No ha recibido la dirección ip dhcp en R2, hasta que sea configurado agente de ley

Paso 2: configurar el R1 como agente de retransmisión DHCP.

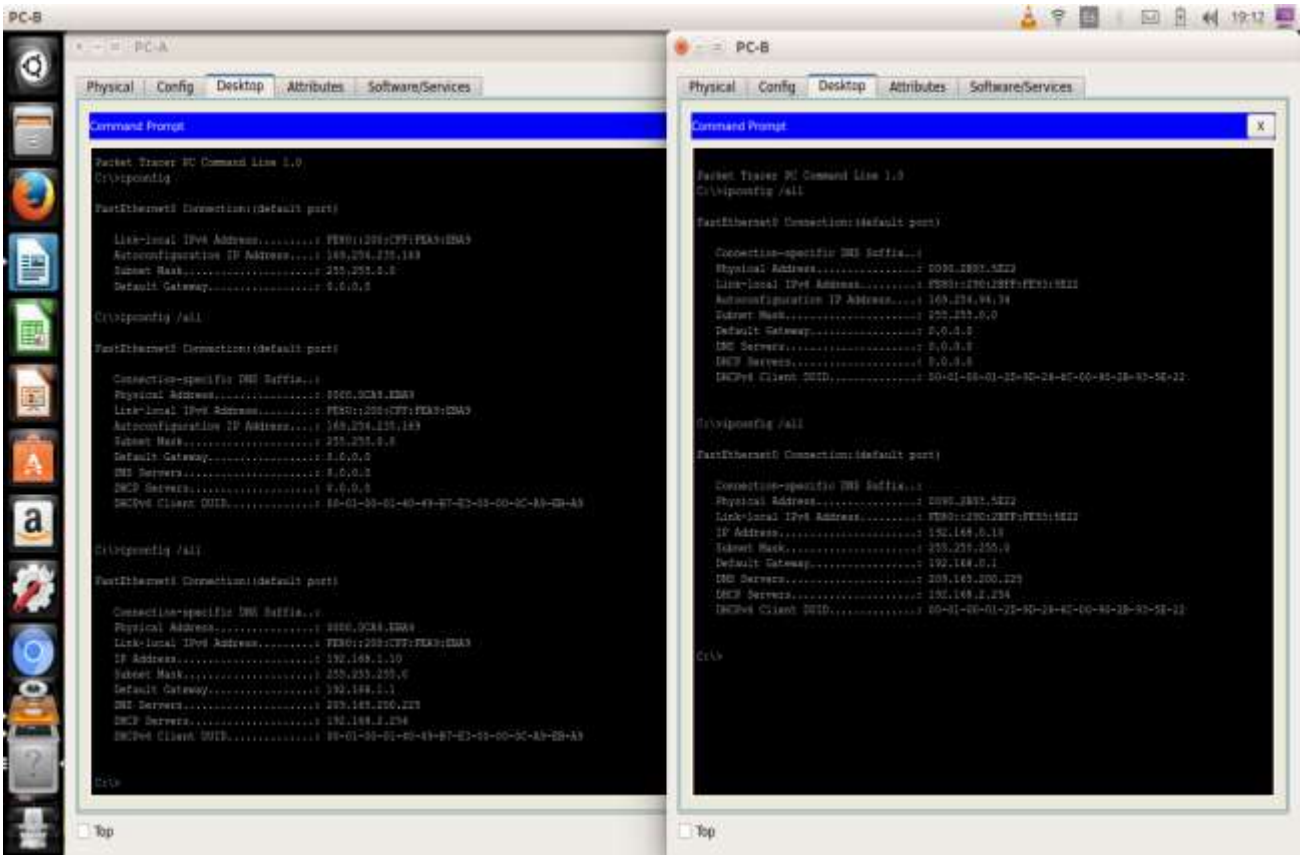
Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2.

En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.



Paso 3: registrar la configuración IP para la PC-A y la PC-B.

En la PC-A y la PC-B, emita el comando **ipconfig /all** para verificar que las computadoras recibieron la información de la dirección IP del servidor de DHCP en el R2. Registre la dirección IP y la dirección MAC de cada computadora.



Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

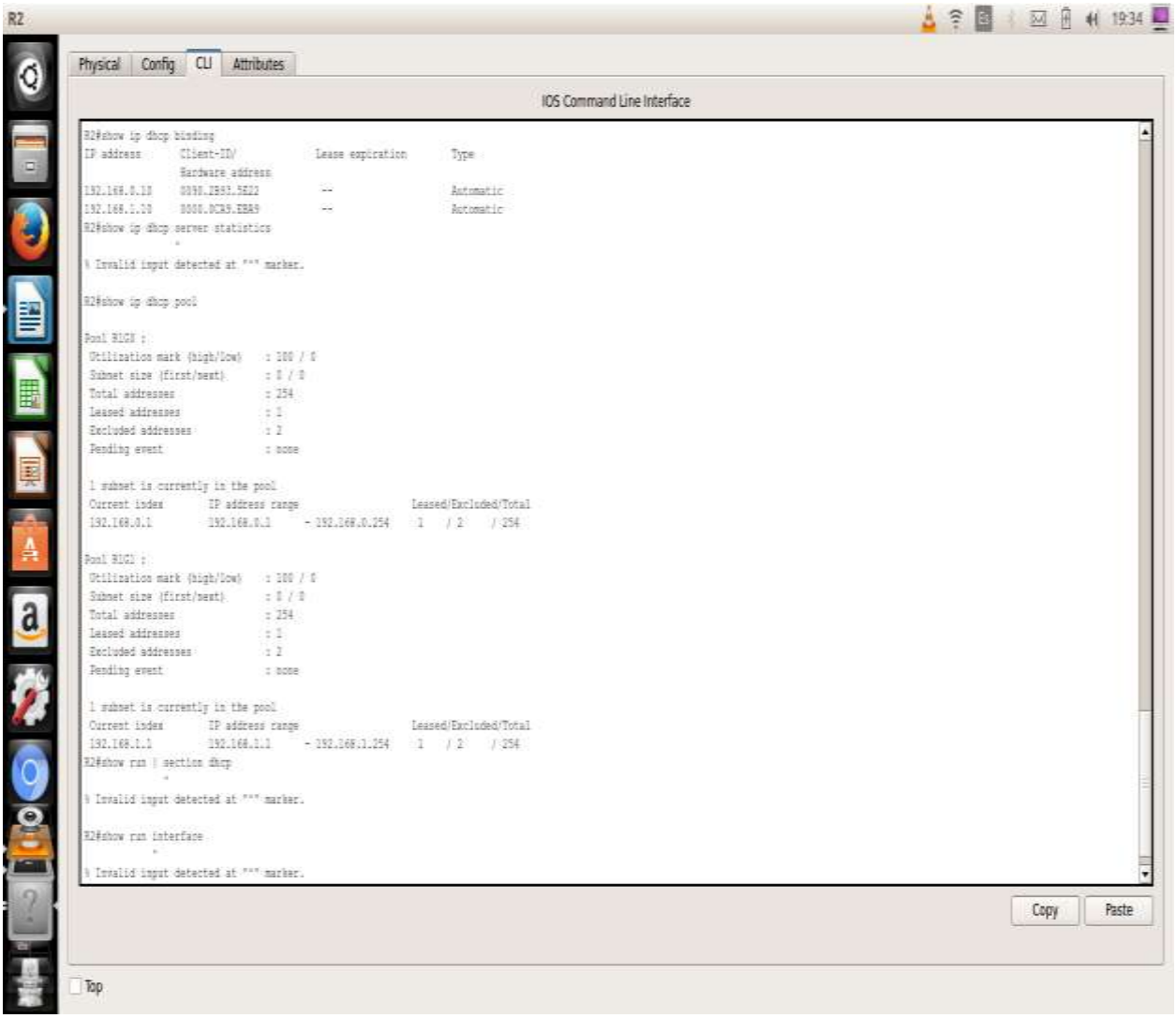
En PC-A 192.168.1.10, En PC-B 192.168.0.10

Paso 4: verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

a. En el R2, introduzca el comando **show ip dhcp binding** para ver los arrendamientos de direcciones DHCP.

Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

Se ve la dirección hardware y física que identifica las pc de la red



b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

10

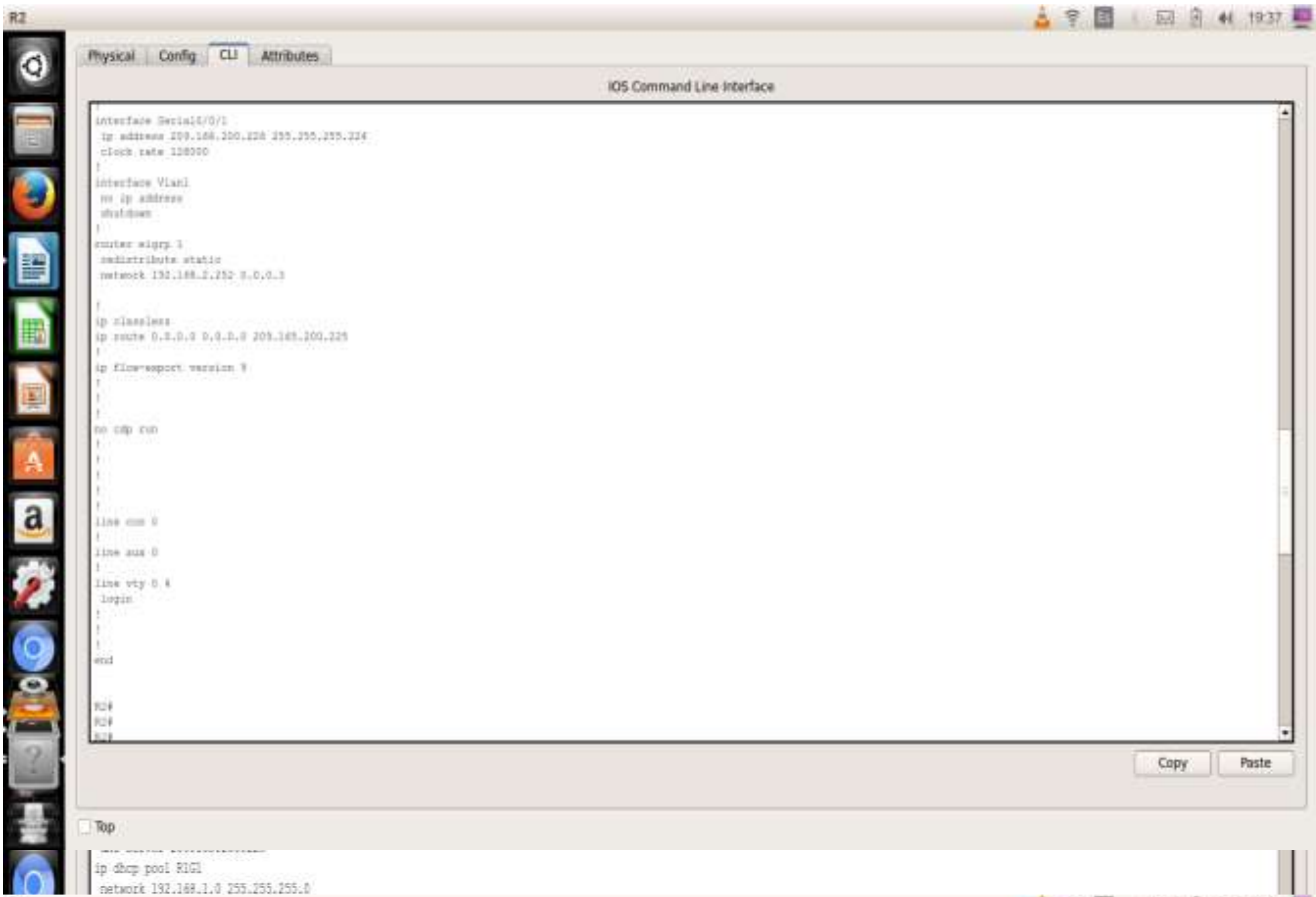
c. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.

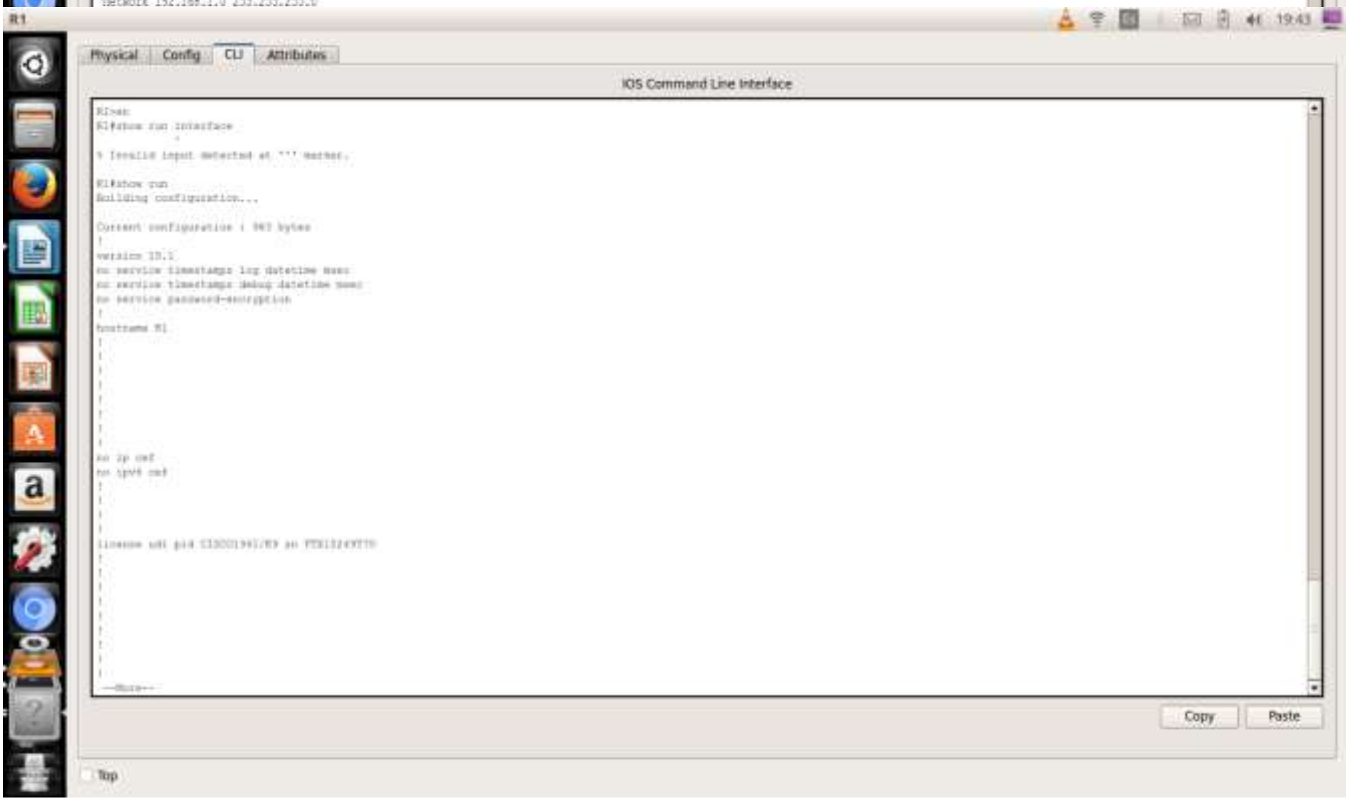
En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current index)?

La dirección ip disponible para ser arrendada

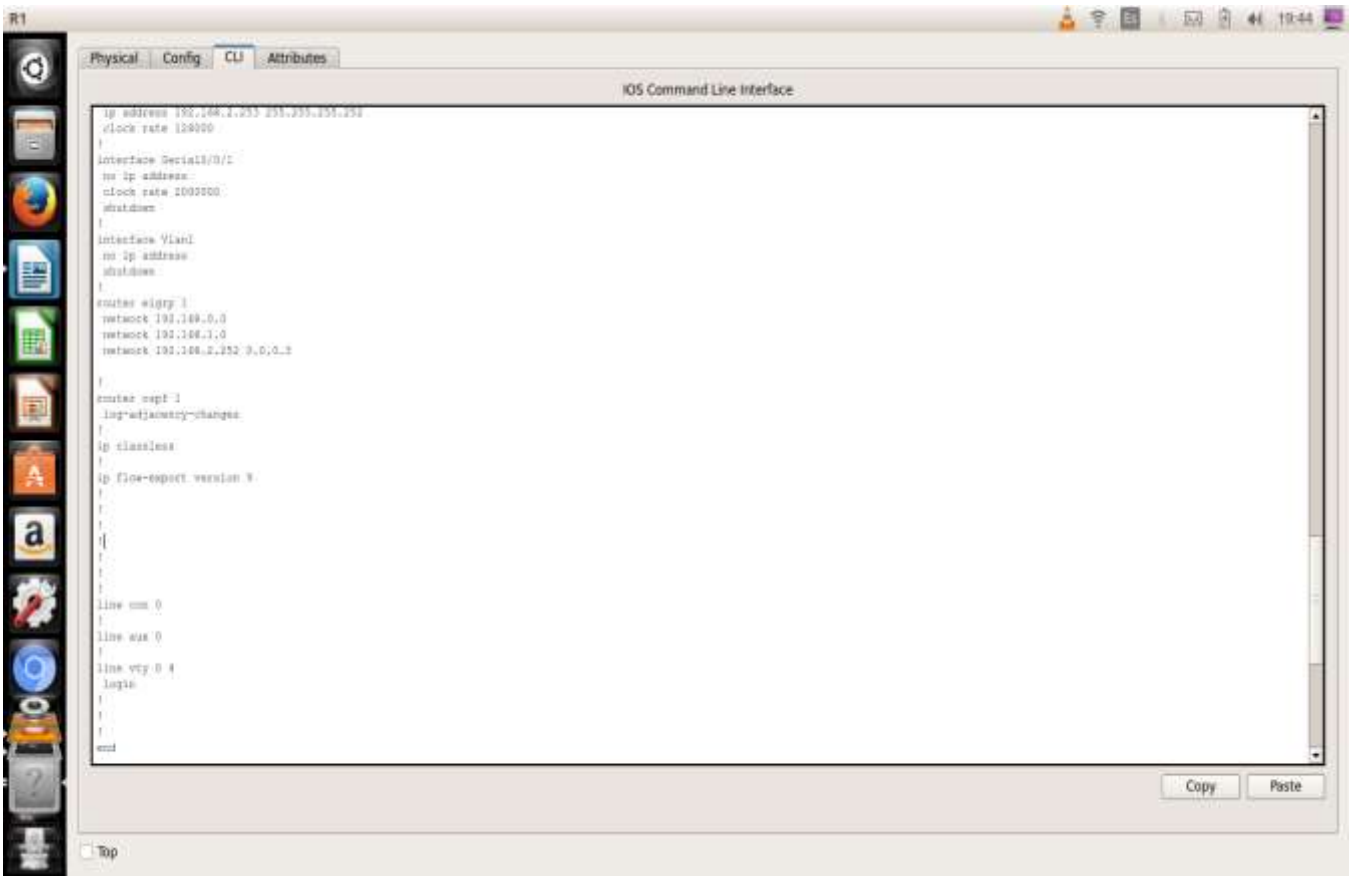
d. Introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.

e. En el R2, introduzca el comando **show run interface** para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.


R2
19:37
Physical
Config
CLI
Attributes
IOS Command Line Interface
interface Serial0/0/1
clock rate 128000
interface Vlan1
no ip address
shutdown
router eigrp 1
redistribute static
ip classless
no cdp run
line con 0
line aux 0
line vty 0 4
login
end
R2#
R2#
Copy
Paste
Top
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0


R1
19:43
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1#show run interface
R1#show run
Building configuration...
hostname R1
--More--
Copy
Paste
Top


R1
19:43
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.253 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 1
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.2.252 0.0.0.3
!
router ospf 1
 log-adjacency-changes
!
ip classless
!
ip flow-export version 9
!
!
--More--
Copy
Paste
Top


R1
19:44
Physical
Config
CLI
Attributes
IOS Command Line Interface
 ip address 192.168.2.253 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 1
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.2.252 0.0.0.3
!
router ospf 1
 log-adjacency-changes
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
Copy
Paste
Top

Reflexión

¿Cuál cree que es el beneficio de usar agentes de retransmisión DHCP en lugar de varios routers que funcionen como servidores de DHCP?
Evita que cada router administre sus propias direcciones dhcp lo que dificultaría la administración de la red

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreVíatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Apéndice A: comandos de configuración de DHCP

Router R1

R1(config)# **interface g0/0**
R1(config-if)# **ip helper-address 192.168.2.254**
R1(config-if)# **exit**
R1(config-if)# **interface g0/1**
R1(config-if)# **ip helper-address 192.168.2.254**

Router R2

R2(config)# **ip dhcp excluded-address 192.168.0.1 192.168.0.9**
R2(config)# **ip dhcp excluded-address 192.168.1.1 192.168.1.9**
R2(config)# **ip dhcp pool R1G1**
R2(dhcp-config)# **network 192.168.1.0 255.255.255.0**
R2(dhcp-config)# **default-router 192.168.1.1**
R2(dhcp-config)# **dns-server 209.165.200.225**
R2(dhcp-config)# **domain-name ccna-lab.com**
R2(dhcp-config)# **lease 2**

R2(dhcp-config)# **exit**
R2(config)# **ip dhcp pool R1G0**
R2(dhcp-config)# **network 192.168.0.0 255.255.255.0**
R2(dhcp-config)# **default-router 192.168.0.1**
R2(dhcp-config)# **dns-server 209.165.200.225**
R2(dhcp-config)# **domain-name ccna-lab.com**
R2(dhcp-config)# **lease 2**

Ejercicio 10.1.2.5

Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología

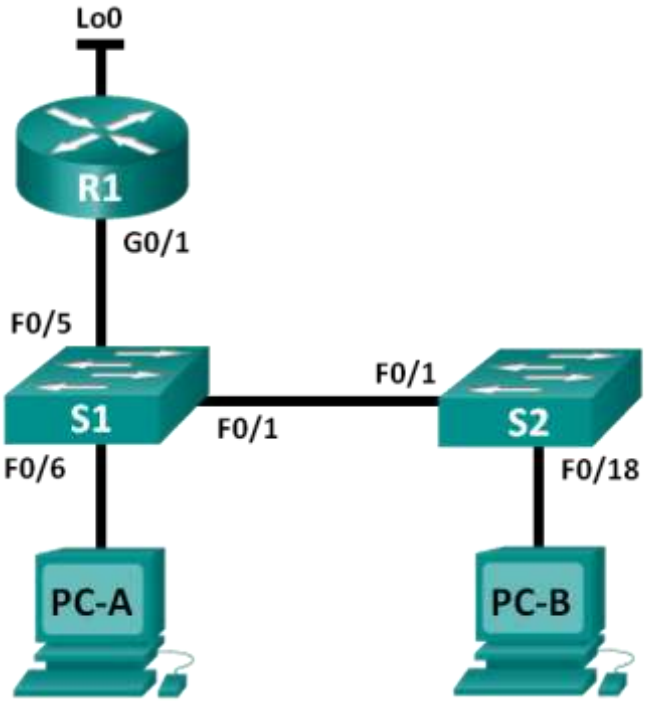


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

Configurar DHCPv4 para la VLAN 1.

Verificar la conectividad y DHCPv4.

Parte 4: configurar DHCP para varias VLAN

Asignar puertos a la VLAN 2.

Configurar DHCPv4 para la VLAN 2.

Verificar la conectividad y DHCPv4.

Parte 5: habilitar el routing IP

Habilite el routing IP en el switch.

Crear rutas estáticas.

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco

versión 15.2 (4) M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0 (2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

1 router (Cisco 1941 con IOS de Cisco versión 15.2 (4) M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco versión 15.0 (2), imagen lanbasek9 o similar)

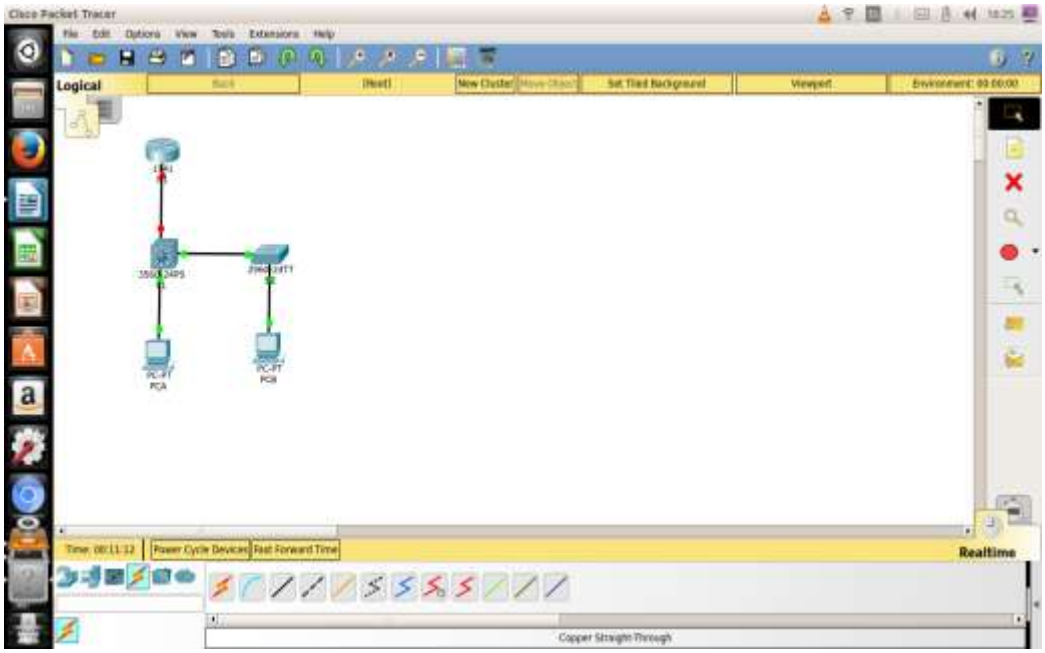
2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet, como se muestra en la topología

Armar la red y configurar los parámetros básicos de los dispositivos

Realizar el cableado de red tal como se muestra en la topología.



Inicializar y volver a cargar los routers y switches.

Configurar los parámetros básicos en los dispositivos.

Asigne los nombres de dispositivos como se muestra en la topología.

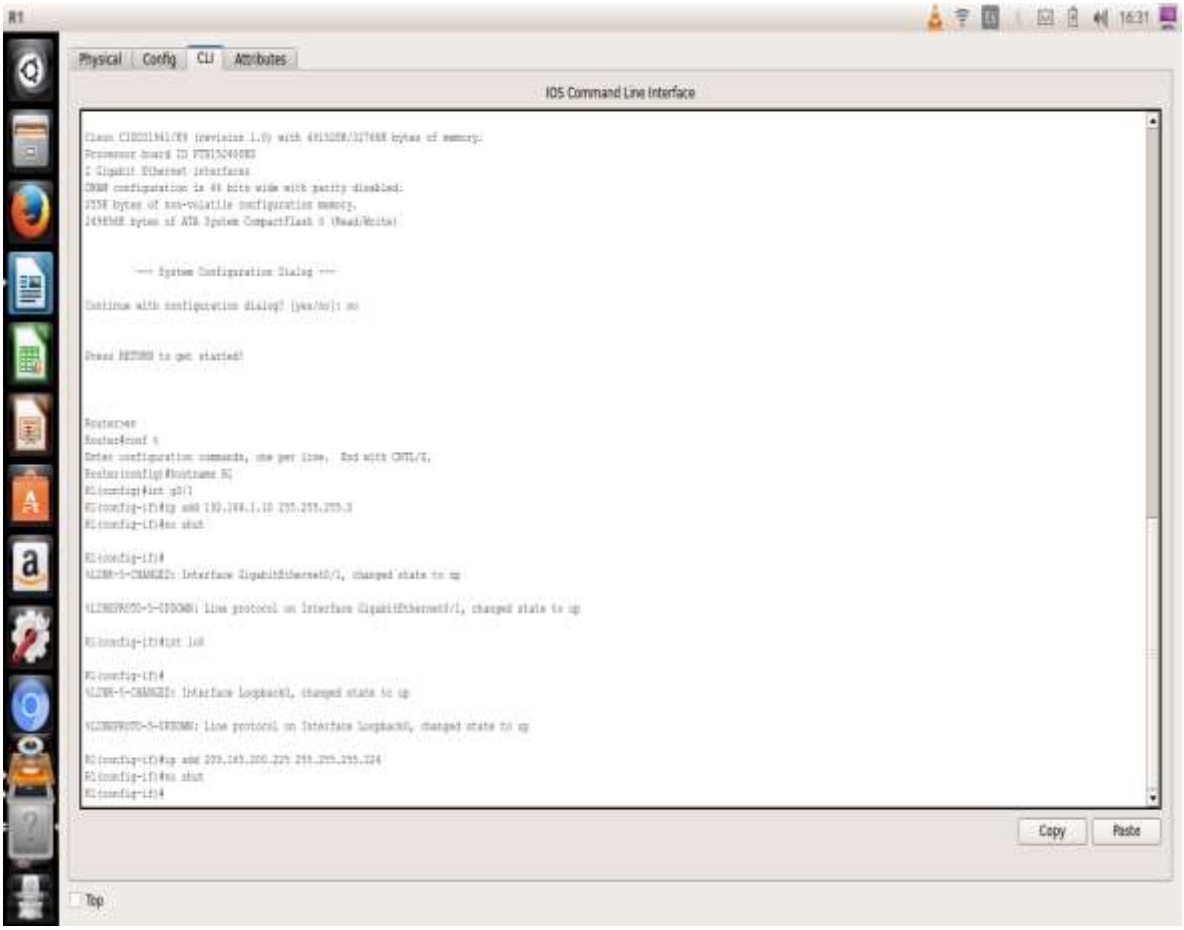
Desactive la búsqueda del DNS.

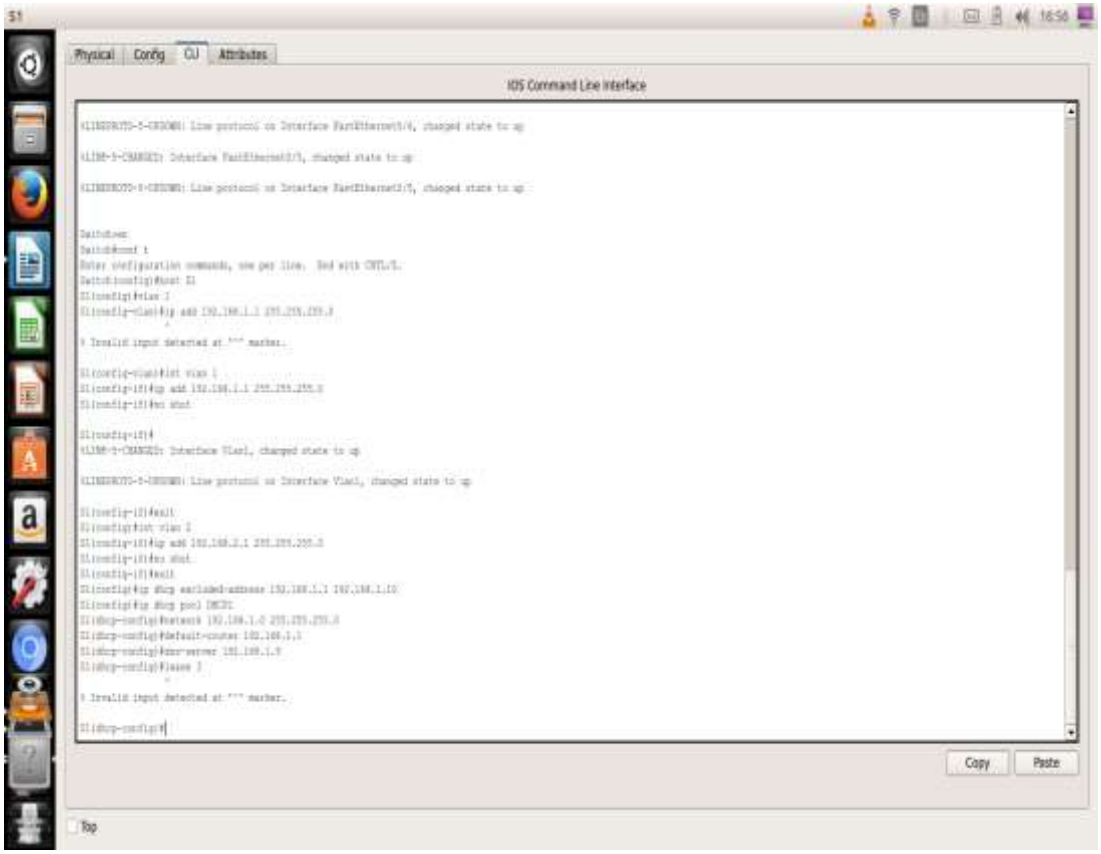
Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.

Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.

Guarde la configuración en ejecución en el archivo de configuración de inicio.





Cambiar la preferencia de SDM

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla lanbase-routing está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

Mostrar la preferencia de SDM en el S1.

En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

S1# **show sdm prefer**

The current template is "default" template.

The selected template optimizes the resources in

The switch to support this level of features for

0 routed interfaces and 255 VLANs.

Number of unicast mac addresses:	8K
Number of IPv4 IGMP groups:	0.25K
Number of IPv4/MAC qos aces:	0.125k
Number of IPv4/MAC security aces:	0.375k

¿Cuál es la plantilla actual?

Default, default dual-ipv4-and-ipv6, lanbase-routing

Cambiar la preferencia de SDM en el S1.

Establezca la preferencia de SDM en **lanbase-routing**. (Si lanbase-routing es la plantilla actual, continúe con la parte 3). En el modo de configuración global, emita el comando **sdm prefer lanbase-routing**.

S1 (config)# **sdm prefer lanbase-routing**

Changes to the running SDM preferences have been stored, but cannot take effect

Until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga? lanbase-routing

Se debe volver a cargar el switch para que la plantilla esté habilitada.

S1# **reload**

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la configuración en ejecución. Para guardar la configuración en ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.

Verificar que la plantilla lanbase-routing esté cargada.

Emita el comando **show sdm prefer** para verificar si la plantilla lanbase-routing se cargó en el S1.

S1# **show sdm prefer**

The current template is "lanbase-routing" template.

The selected template optimizes the resources in

The switch to support this level of features for

0 routed interfaces and 255 VLANs.

Number of unicast mac addresses: 4K

Number of IPv4 IGMP groups + multicast routes: 0.25K

Number of IPv4 unicast routes: 0.75K

Number of directly-connected IPv4 hosts: 0.75K

Number of indirect IPv4 routes: 16

Number of IPv6 multicast groups: 0.375k

Number of directly-connected IPv6 addresses: 0.75K

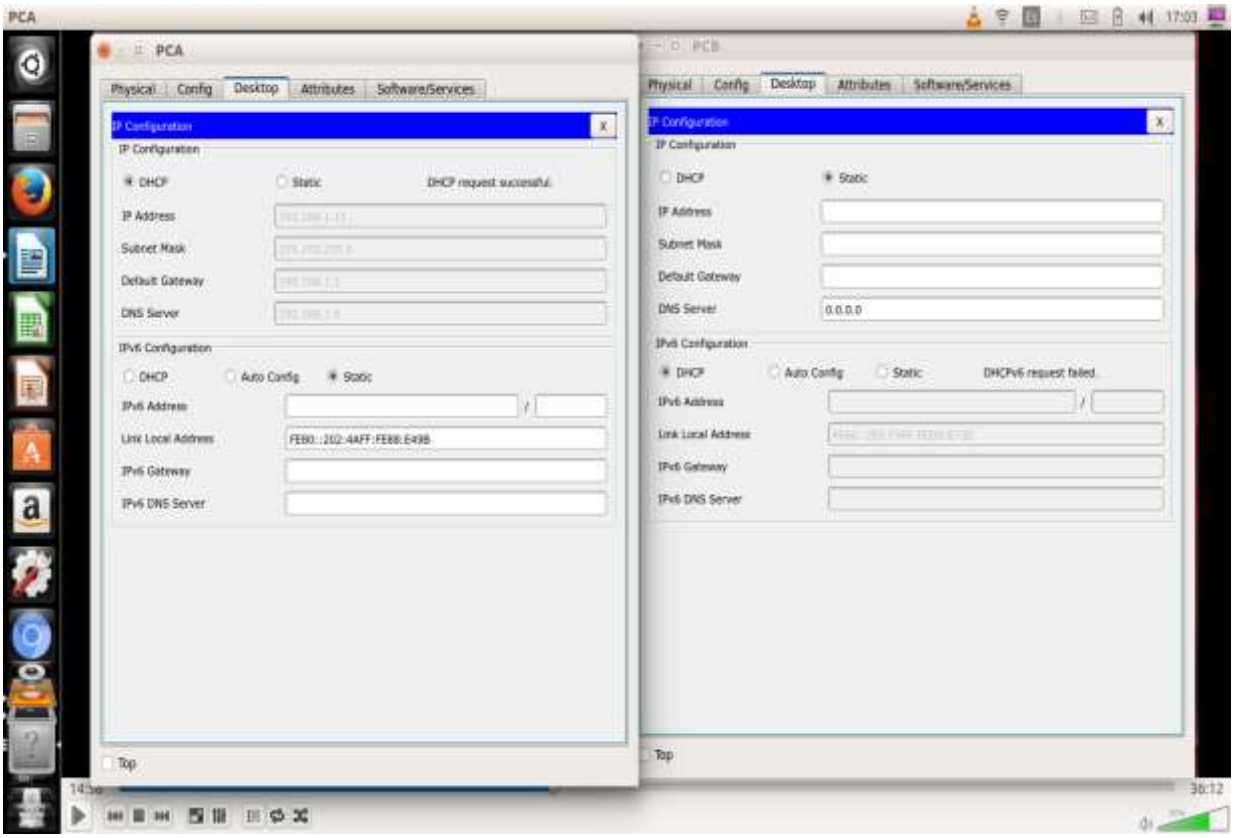
Number of indirect IPv6 unicast routes: 16

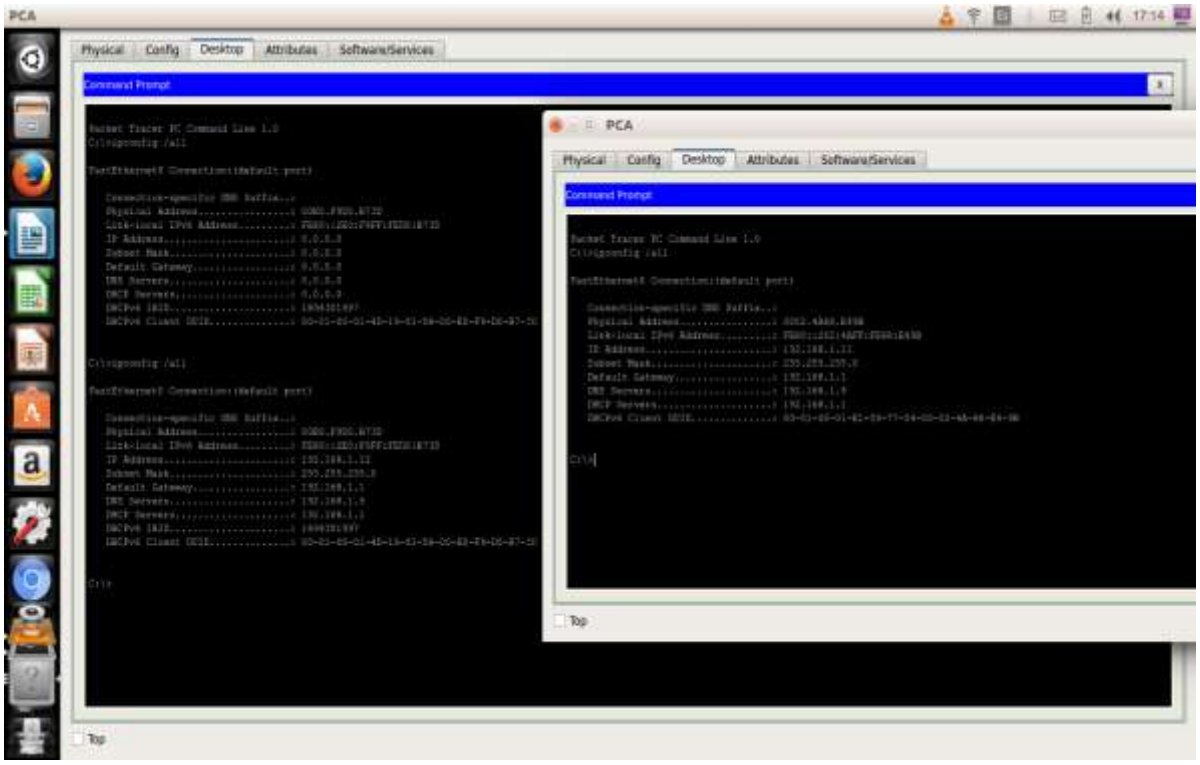
Number of IPv4 policy based routing aces: 0

Number of IPv4/MAC qos aces: 0.125k
Number of IPv4/MAC security aces: 0.375k
Number of IPv6 policy based routing aces: 0
Number of IPv6 qos aces: 0.375k
Number of IPv6 security aces: 127

Configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.





Configurar DHCP para la VLAN 1.

Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10

Cree un pool de DHCP con el nombre DHCP1. En el espacio proporcionado, escriba el comando que utilizó.
S1(config)# ip dhcp pool DHCP1

Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# network 192.168.1.0 255.255.255.0

Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# default-router 192.168.1.1

Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# dns-server 192.168.1.9

Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# lease 3

Guarde la configuración en ejecución en el archivo de configuración de inicio.

Verificar la conectividad y DHCP.

En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

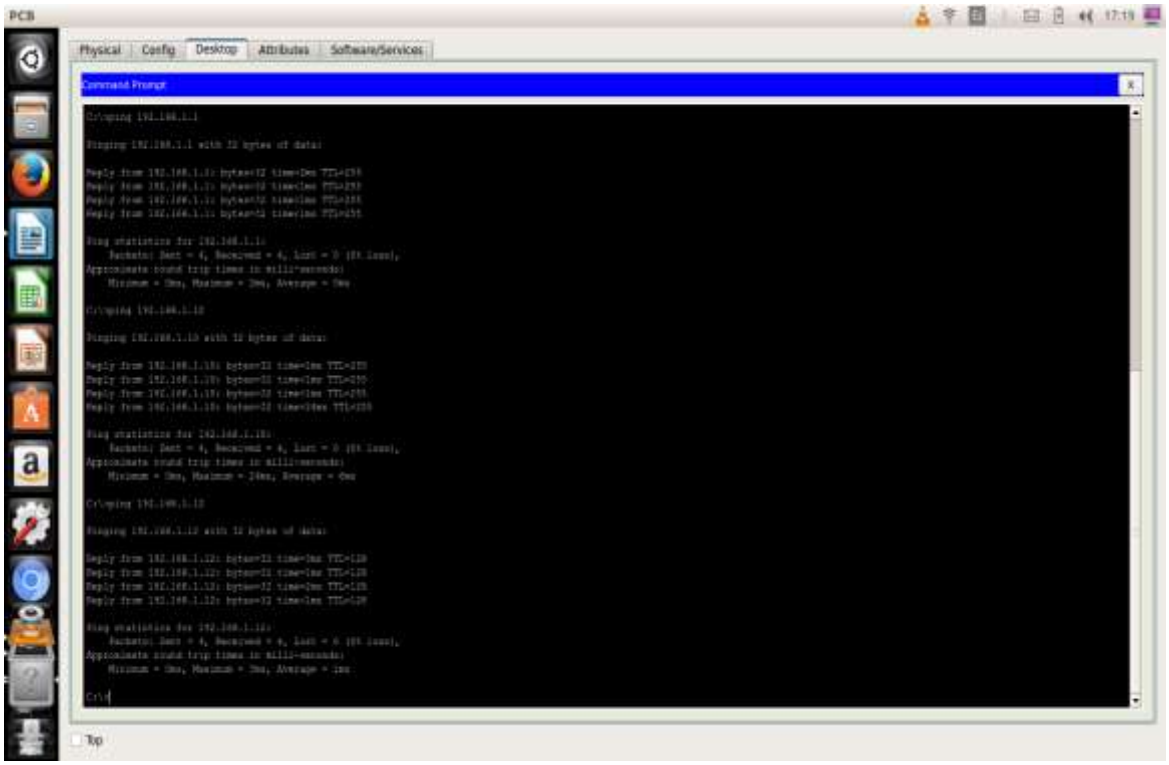
Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? si

¿Es posible hacer ping de la PC-A a la PC-B? si

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? si

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.



Configurar DHCPv4 para varias VLAN

En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Asignar un puerto a la VLAN 2.

Coloque el puerto F0/6 en la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Configurar DHCPv4 para la VLAN 2.

Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10

Cree un pool de DHCP con el nombre DHCP2. En el espacio proporcionado, escriba el comando que utilizó.
S1(config)# ip dhcp pool DHCP2

Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# network 192.168.2.0 255.255.255.0

Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# default-router 192.168.2.1

Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# dns-server 192.168.2.9

Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.
S1(dhcp-config)# lease 3

Guarde la configuración en ejecución en el archivo de configuración de inicio.

Verificar la conectividad y DHCPv4.

En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.2.1

Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? si

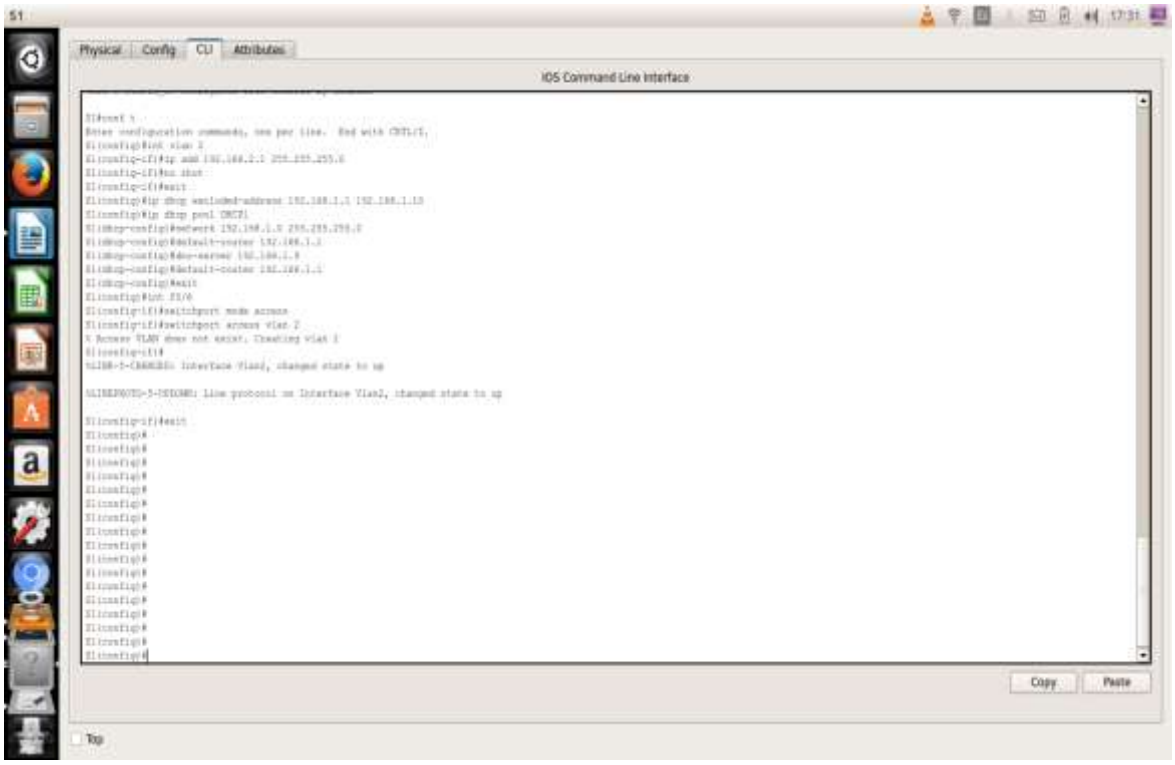
¿Es posible hacer ping de la PC-A a la PC-B? no

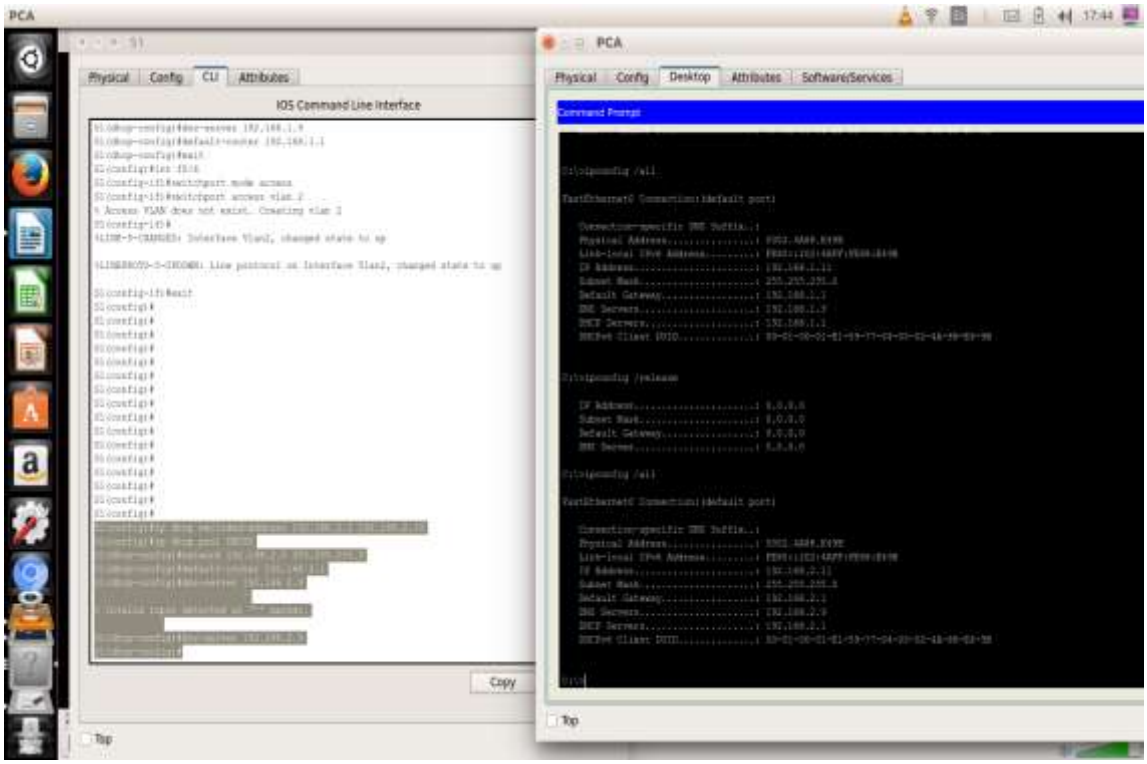
¿Los pings eran correctos? ¿Por qué?

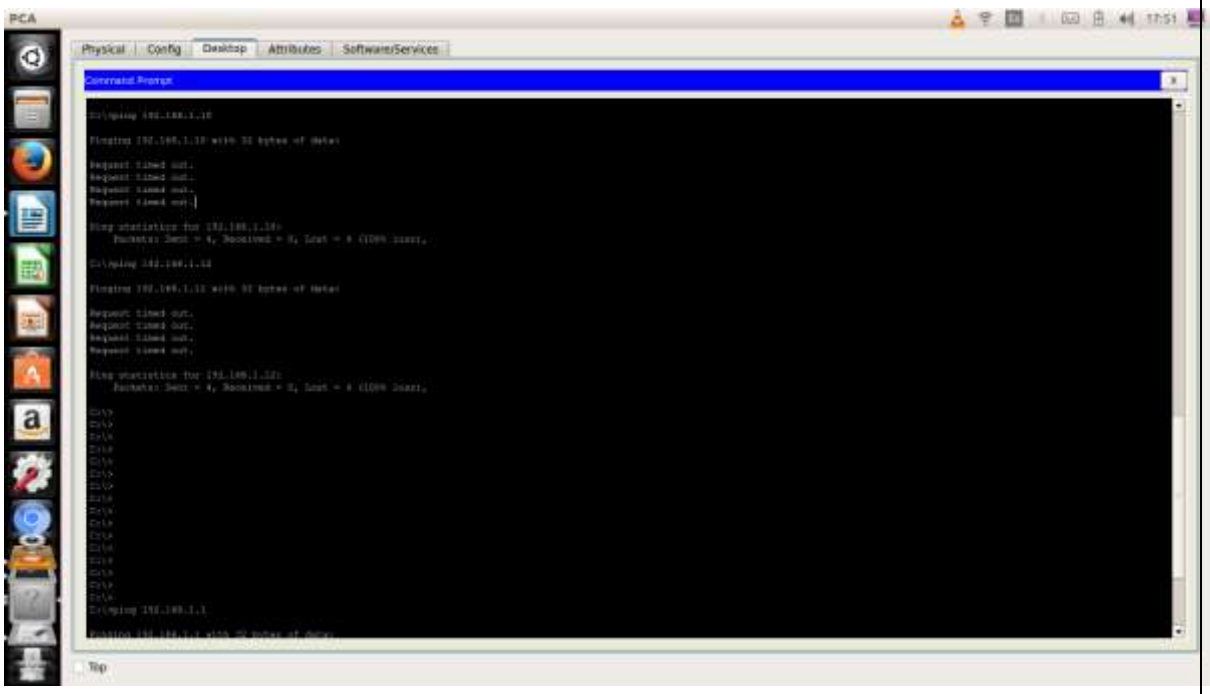
el ping de la PC-A no es correcto, porque PC-B está en una red diferente y PC-A hace ping al gateway predeterminado.

Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?
No se estableció un gateway predeterminado

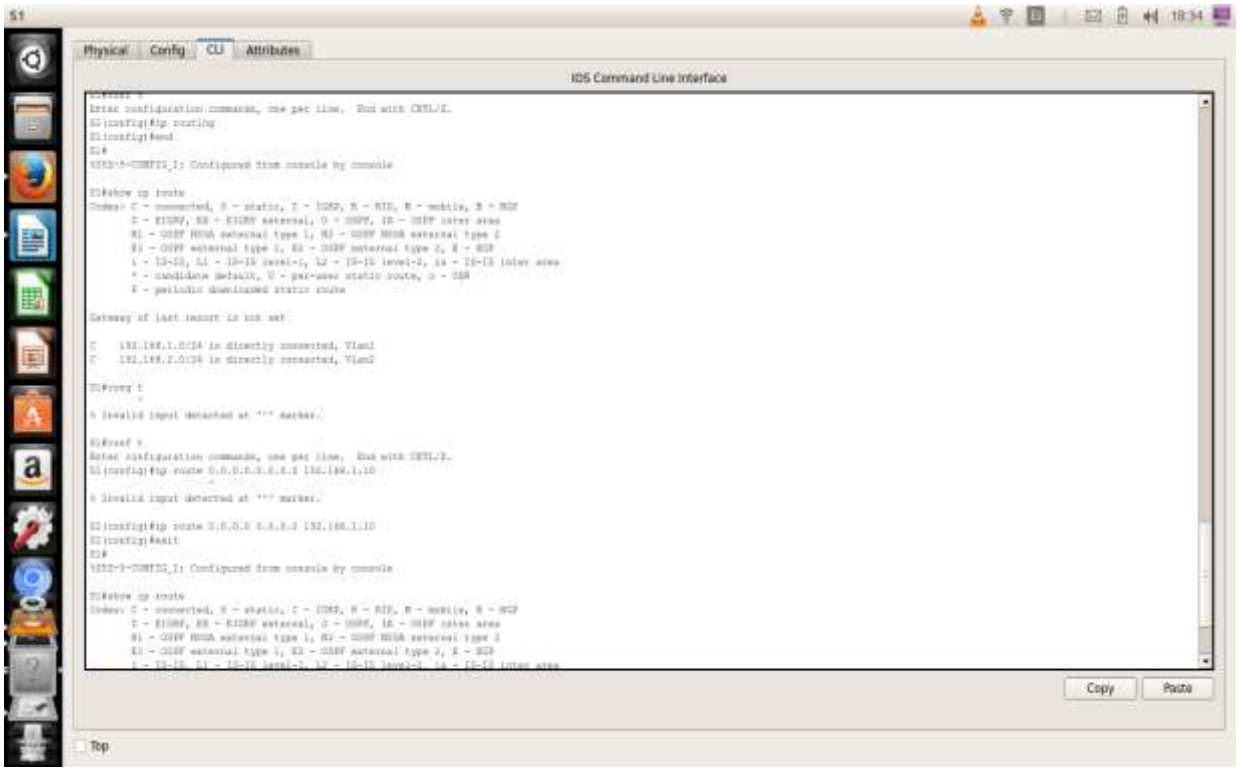


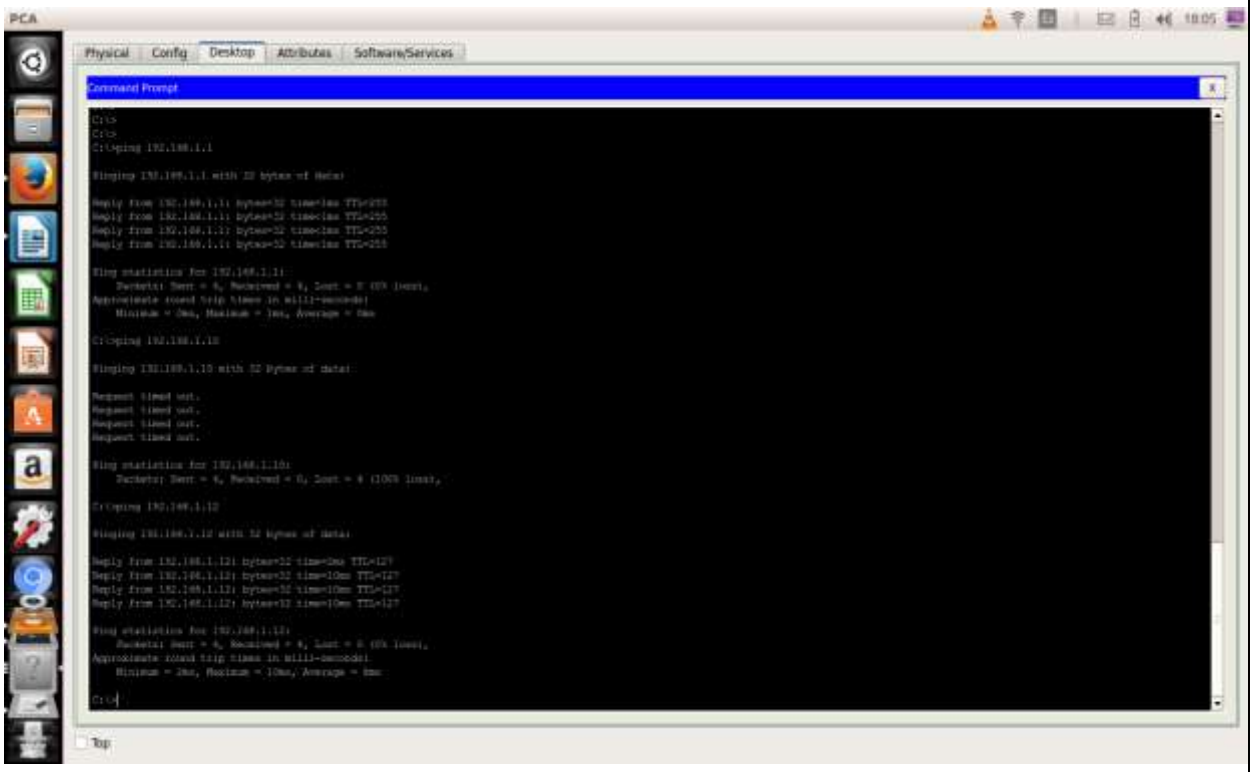




Habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.





Habilitar el routing IP en el S1.

En el modo de configuración global, utilice el comando **ip routing** para habilitar el routing en el S1.

S1(config)# **ip routing**

Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? si

¿Qué función realiza el switch?

routing entre VLAN

Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?

192.168.1.0/24 y 192.168.2.0/24

Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

192.168.1.0 y 209.165.200.224

No tiene entrada 192.168.2.0

¿Es posible hacer ping de la PC-A al R1? no

¿Es posible hacer ping de la PC-A a la interfaz Lo0? no

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

rutas a las tablas de routing.

Asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10

En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/

Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?
Gateway of last resort is 192.168.1.10 to network 0.0.0.0

Vea la información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

192.168.2.0/24, GigabitEthernet0/1

¿Es posible hacer ping de la PC-A al R1? si

¿Es posible hacer ping de la PC-A a la interfaz Lo0? si


R1
S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 192.168.1.10 to network 0.0.0.0
C 192.168.1.0/24 is directly connected, Vlan1
C 192.168.2.0/24 is directly connected, Vlan2
S* 0.0.0.0/0 [1/0] via 192.168.1.10
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1
S 192.168.2.0/24 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0


PCA
18:30
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Minimum = 0ms, Maximum = 10ms, Average = 4ms
C:\>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
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 = 1ms, Average = 0ms
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=1ms TTL=254
Reply from 192.168.1.10: bytes=32 time<1ms TTL=254
Reply from 192.168.1.10: bytes=32 time=1ms TTL=254
Reply from 192.168.1.10: bytes=32 time<1ms TTL=254
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top

Reflexión

Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

Estas pueden pasarse dinámicamente a hosts.

Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

VLAN al puerto que el host esté conectado.

Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?
como un servidor de DHCP y routing estático y entre VLAN.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreVíatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Apéndice A: comandos de configuración

Configurar DHCPv4

S1(config)# **ip dhcp excluded-address 192.168.1.1 192.168.1.10**
S1(config)# **ip dhcp pool DHCP1**
S1(dhcp-config)# **network 192.168.1.0 255.255.255.0**
S1(dhcp-config)# **default-router 192.168.1.1**
S1(dhcp-config)# **dns-server 192.168.1.9**
S1(dhcp-config)# **lease 3**

Configurar DHCPv4 para varias VLAN

S1(config)# **interface f0/6**
S1(config-if)# **switchport access vlan 2**
S1(config)# **ip dhcp excluded-address 192.168.2.1 192.168.2.10**
S1(config)# **ip dhcp pool DHCP2**
S1(dhcp-config)# **network 192.168.2.0 255.255.255.0**
S1(dhcp-config)# **default-router 192.168.2.1**
S1(dhcp-config)# **dns-server 192.168.2.9**
S1(dhcp-config)# **lease 3**

Habilitar routing IP

S1(config)# **ip routing**
S1(config)# **ip route 0.0.0.0 0.0.0.0 192.168.1.10**
R1(config)# **ip route 192.168.2.0 255.255.255.0 g0/1**

Ejercicio 10.2.3.5

Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

Solo mediante configuración automática de dirección sin estado (SLAAC)

Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)

Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

S1# **show sdm prefer**

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

S1# **config t**

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# **end**

S1# **reload**

Recursos necesarios

1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

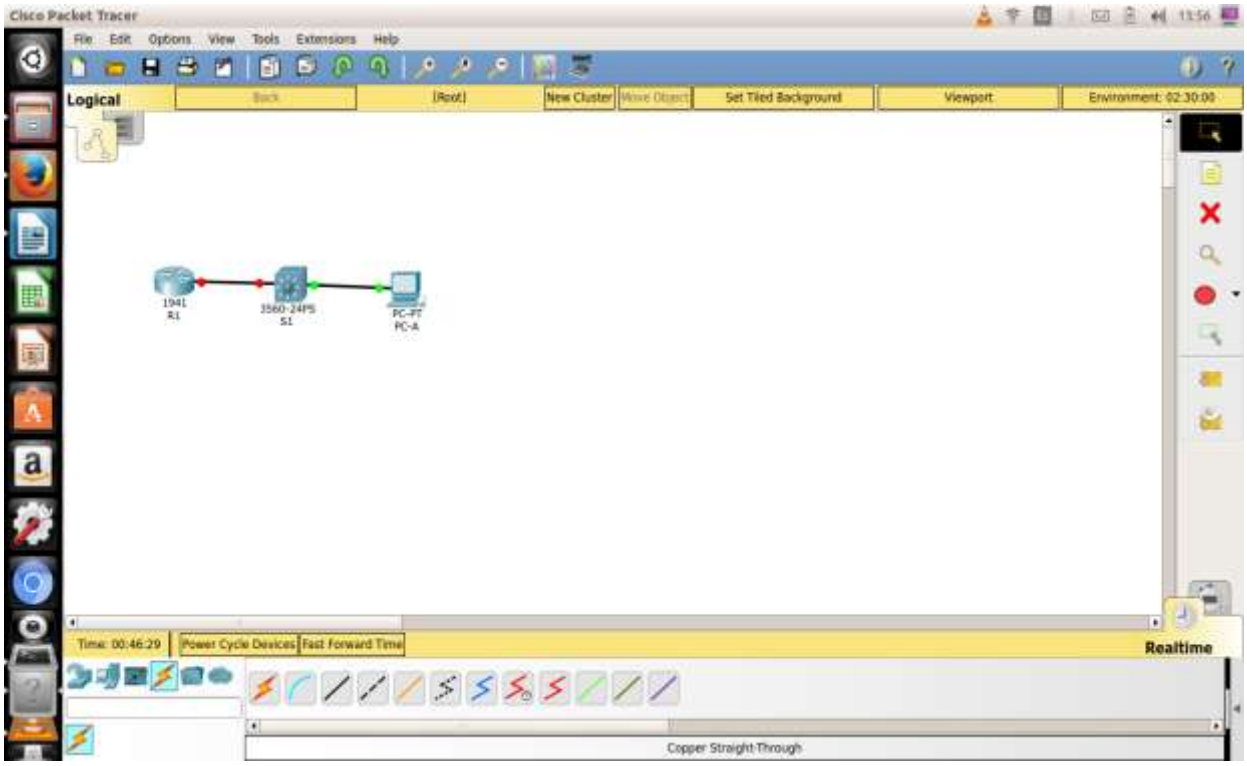
Cables Ethernet, como se muestra en la topología

Nota: los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

Armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

realizar el cableado de red tal como se muestra en la topología.



Inicializar y volver a cargar el router y el switch según sea necesario.

Configurar R1

Desactive la búsqueda del DNS.

Configure el nombre del dispositivo.

Cifre las contraseñas de texto no cifrado.

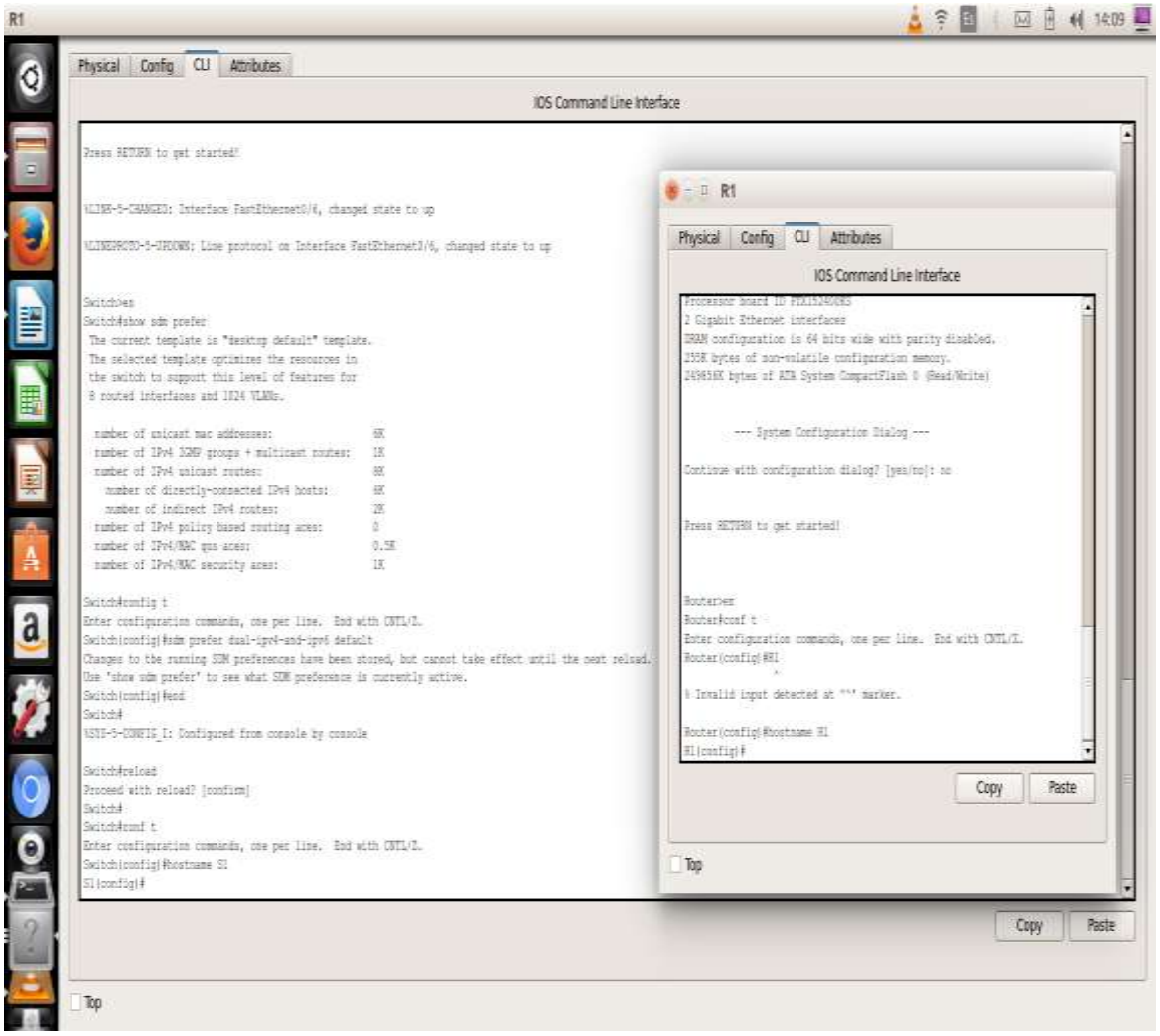
Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

Establezca el inicio de sesión de consola en modo sincrónico.

Guardar la configuración en ejecución en la configuración de inicio.



Configurar el S1.

Desactive la búsqueda del DNS.

Configure el nombre del dispositivo.

Cifre las contraseñas de texto no cifrado.

Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

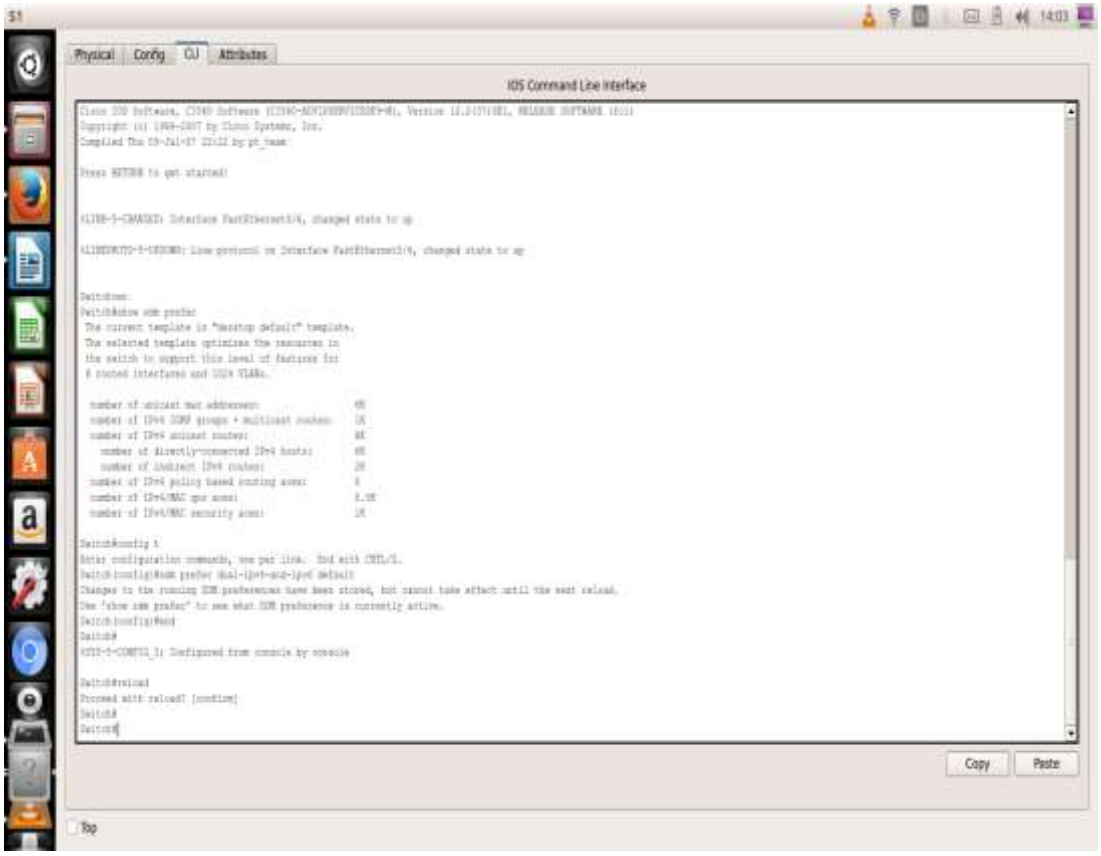
Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

Establezca el inicio de sesión de consola en modo sincrónico.

Desactive administrativamente todas las interfaces inactivas.

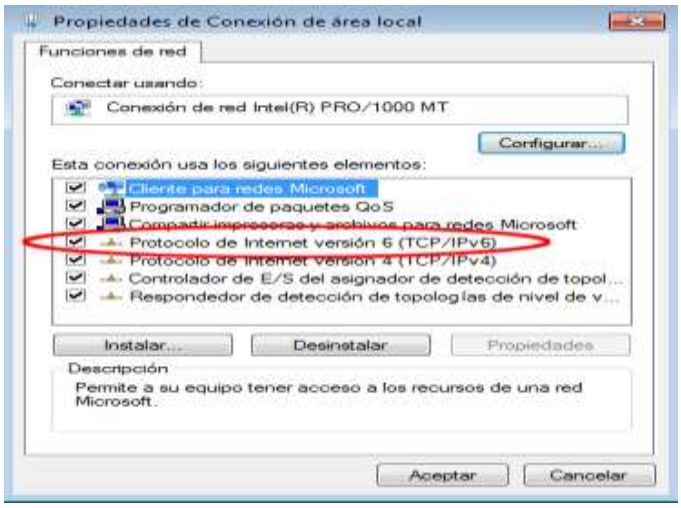
Guarde la configuración en ejecución en la configuración de inicio.



Configurar la red para SLAAC

Preparar la PC-A.

Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.



Inicie una captura del tráfico en la NIC con Wireshark.

Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.

Configurar R1

Habilite el routing de unidifusión IPv6.

Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.

Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.

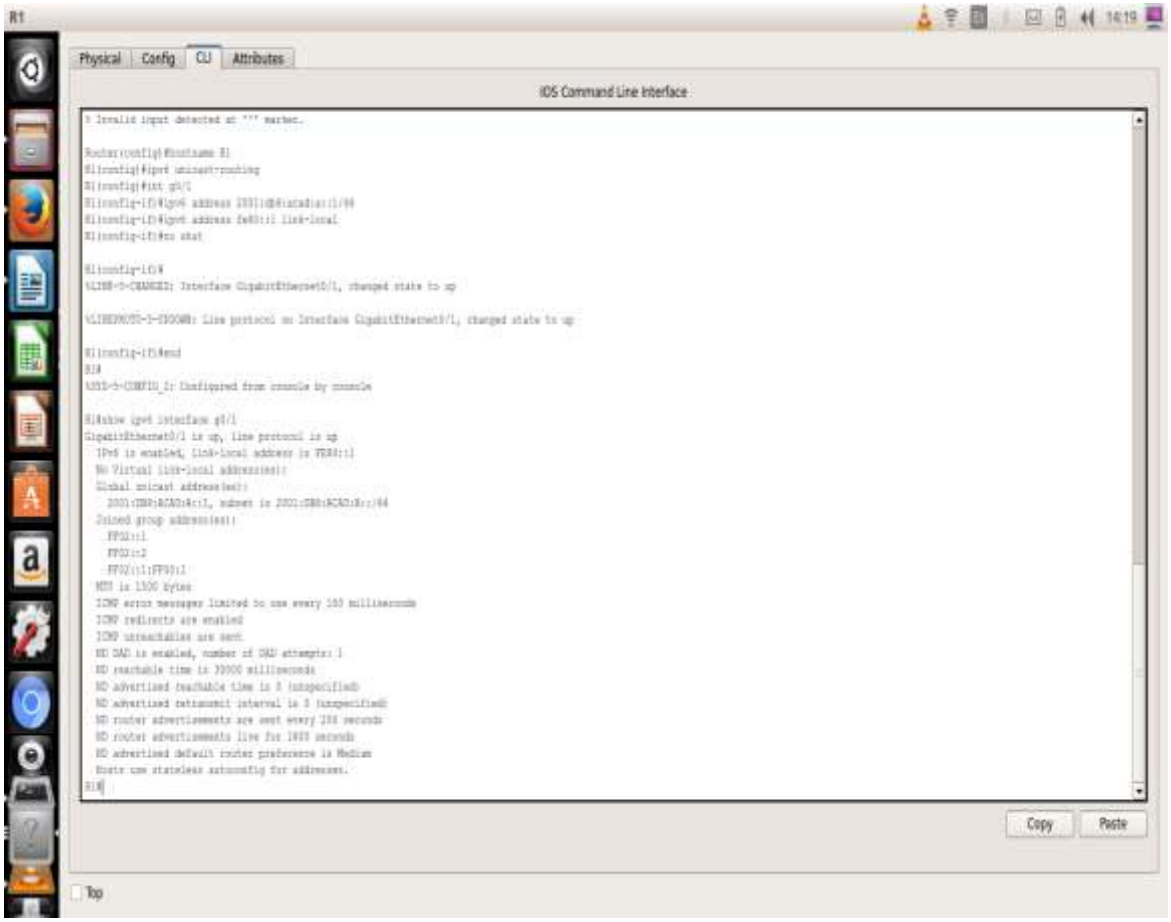
Active la interfaz G0/1.

Verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

R1# **show ipv6 interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
FF02::1
FF02::2

FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.



Configurar el S1.

Use el comando **ipv6 address autoconfig** en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.

S1(config)# **interface vlan 1**
S1(config-if)# **ipv6 address autoconfig**
S1(config-if)# **end**

Verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

S1# **show ipv6 interface**

Vlan1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40

No Virtual link-local address(es):

Stateless address autoconfig enabled

Global unicast address(es):

2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]

Valid lifetime 2591988 preferred lifetime 604788

Joined group address(es):

FF02::1

FF02::1:FFE8:8A40

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

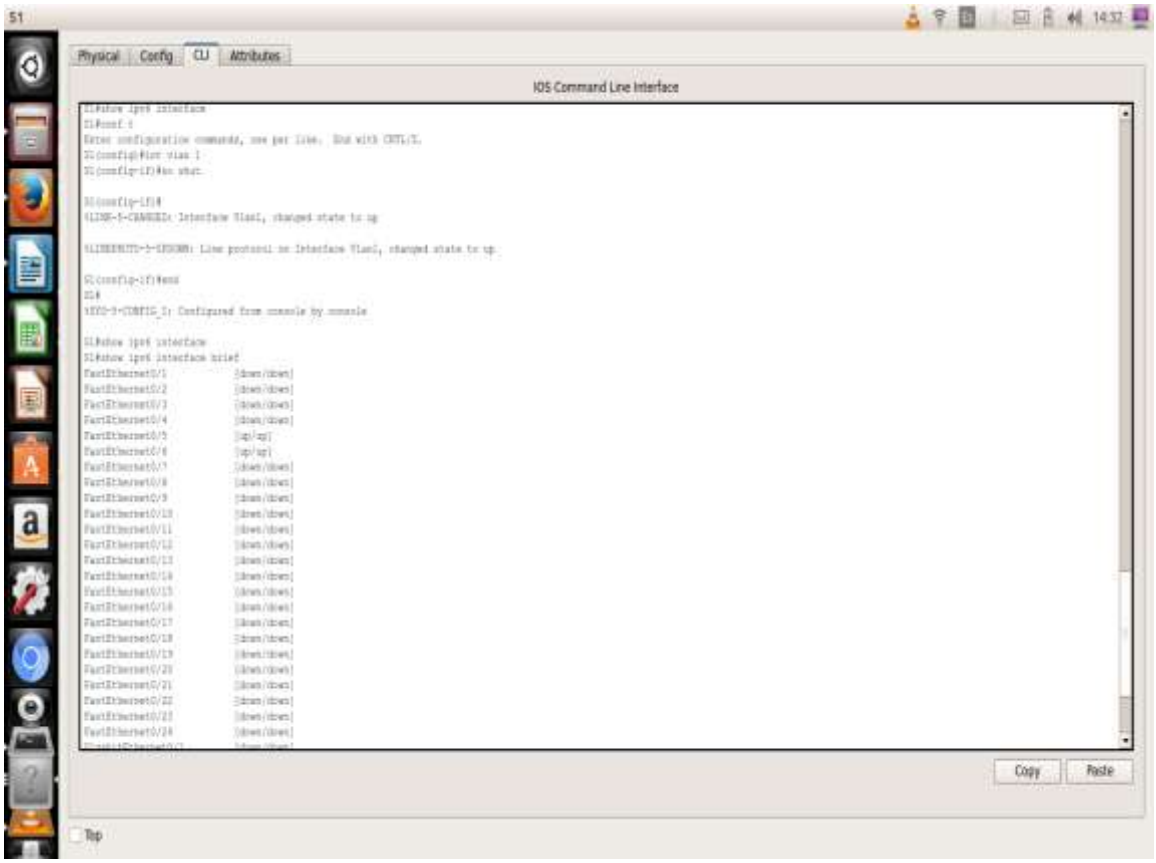
Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

Default router is FE80::1 on Vlan1

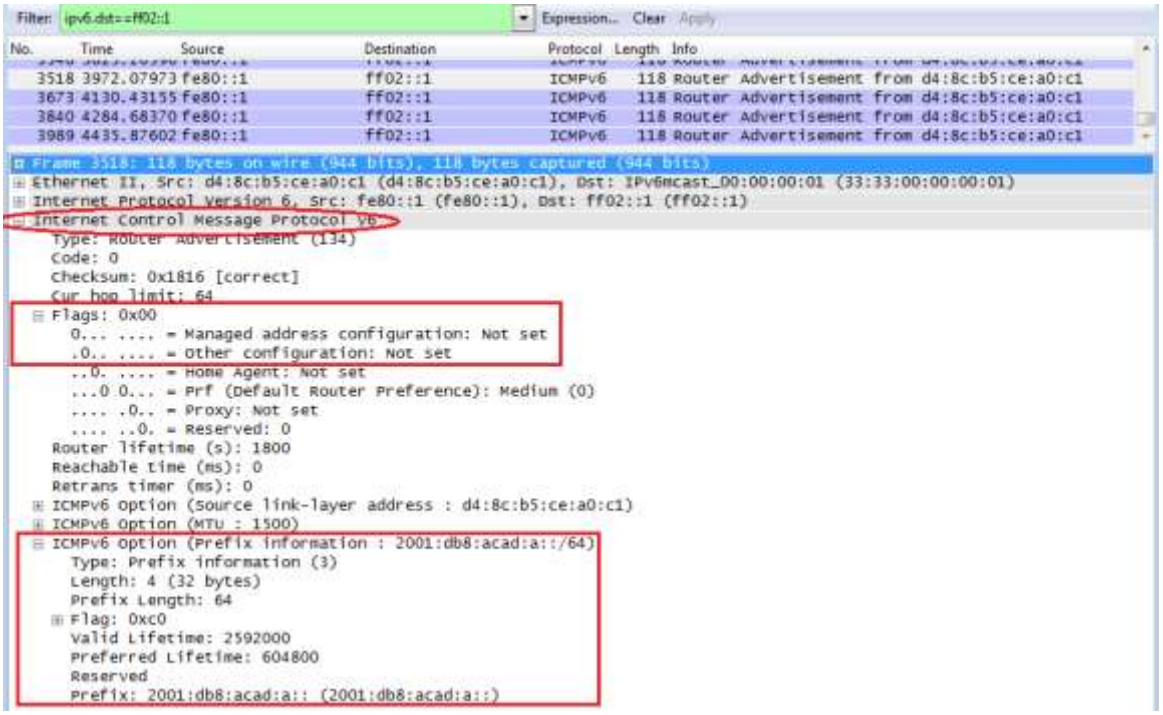


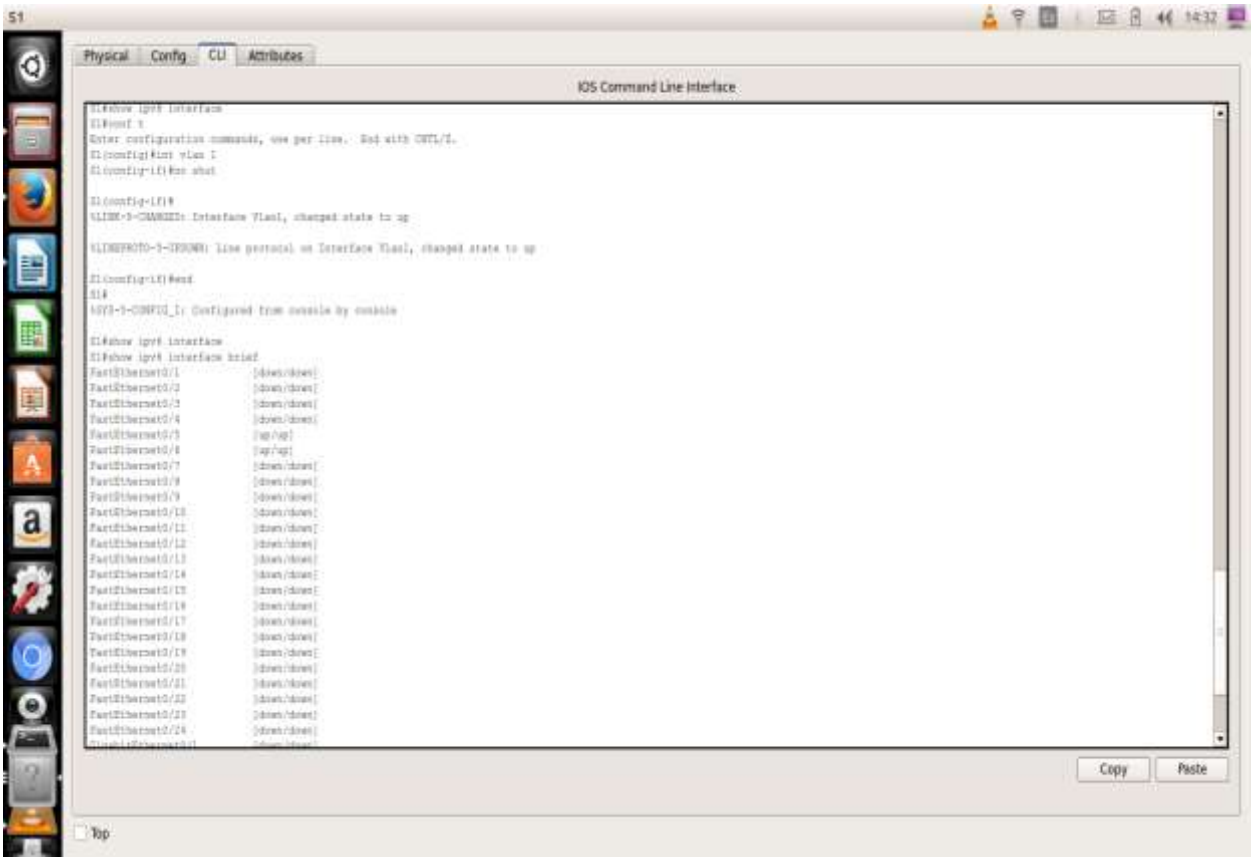
Verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

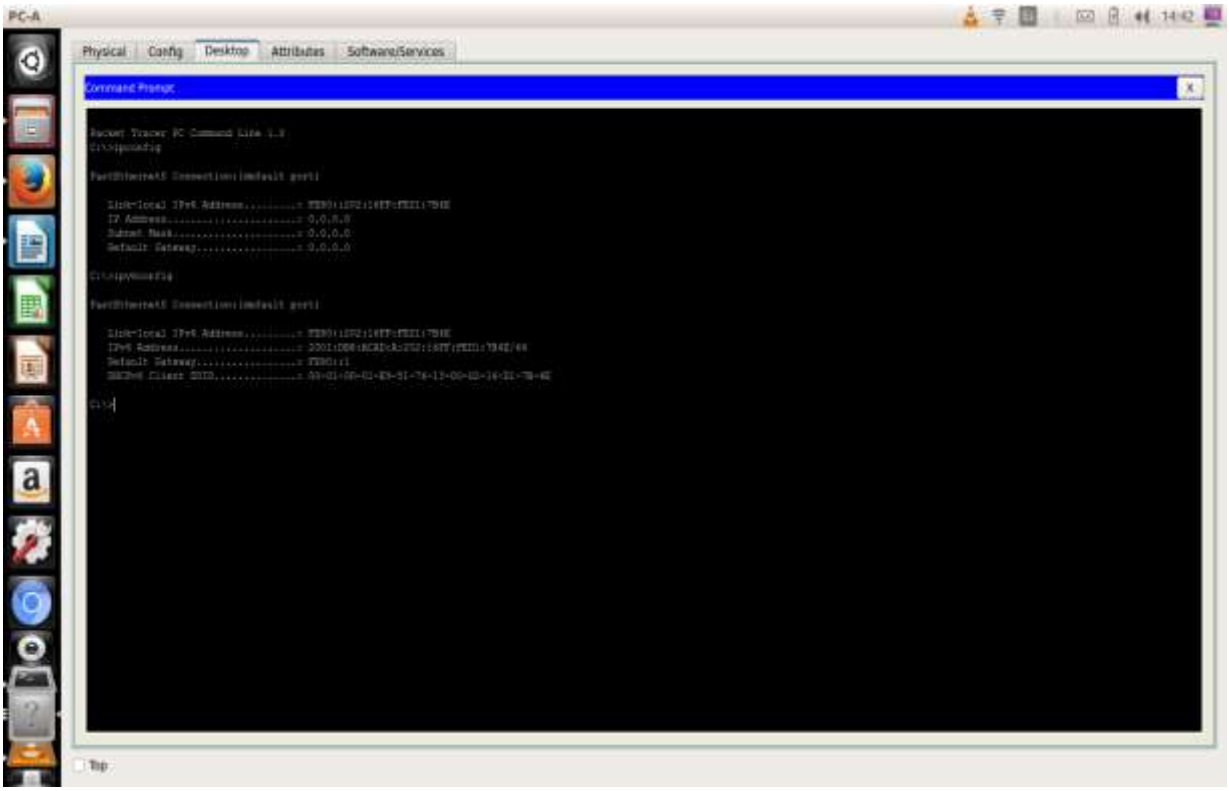
En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                               fec0:0:0:ffff::2%1
                                               fec0:0:0:ffff::3%1
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.


Filter: ipv6.dst==ff02::1
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
3518 3972.07973 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
3673 4130.43155 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
3840 4284.68370 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
3989 4435.87602 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x1816 [correct]
Cur hop limit: 64
Flags: 0x00
0... .... = Managed address configuration: Not set
.0.. .... = Other configuration: Not set
..0. .... = Home Agent: Not set
...0 0... = Prf (Default Router Preference): Medium (0)
.... .0.. = Proxy: Not set
.... ..0. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 option (Source link-layer address : d4:8c:b5:ce:a0:c1)
ICMPv6 option (MTU : 1500)
ICMPv6 option (Prefix information : 2001:db8:acad:a::/64)
Type: Prefix information (3)
Length: 4 (32 bytes)
Prefix Length: 64
Flag: 0xc0
Valid Lifetime: 2592000
Preferred Lifetime: 604800
Reserved
Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top



Configurar la red para DHCPv6 sin estado

Configurar un servidor de DHCP IPv6 en el R1.

Cree un pool de DHCP IPv6.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

Asigne un nombre de dominio al pool.

R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**

Asigne una dirección de servidor DNS.

R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**

R1(config-dhcpv6)# **exit**

Asigne el pool de DHCPv6 a la interfaz.

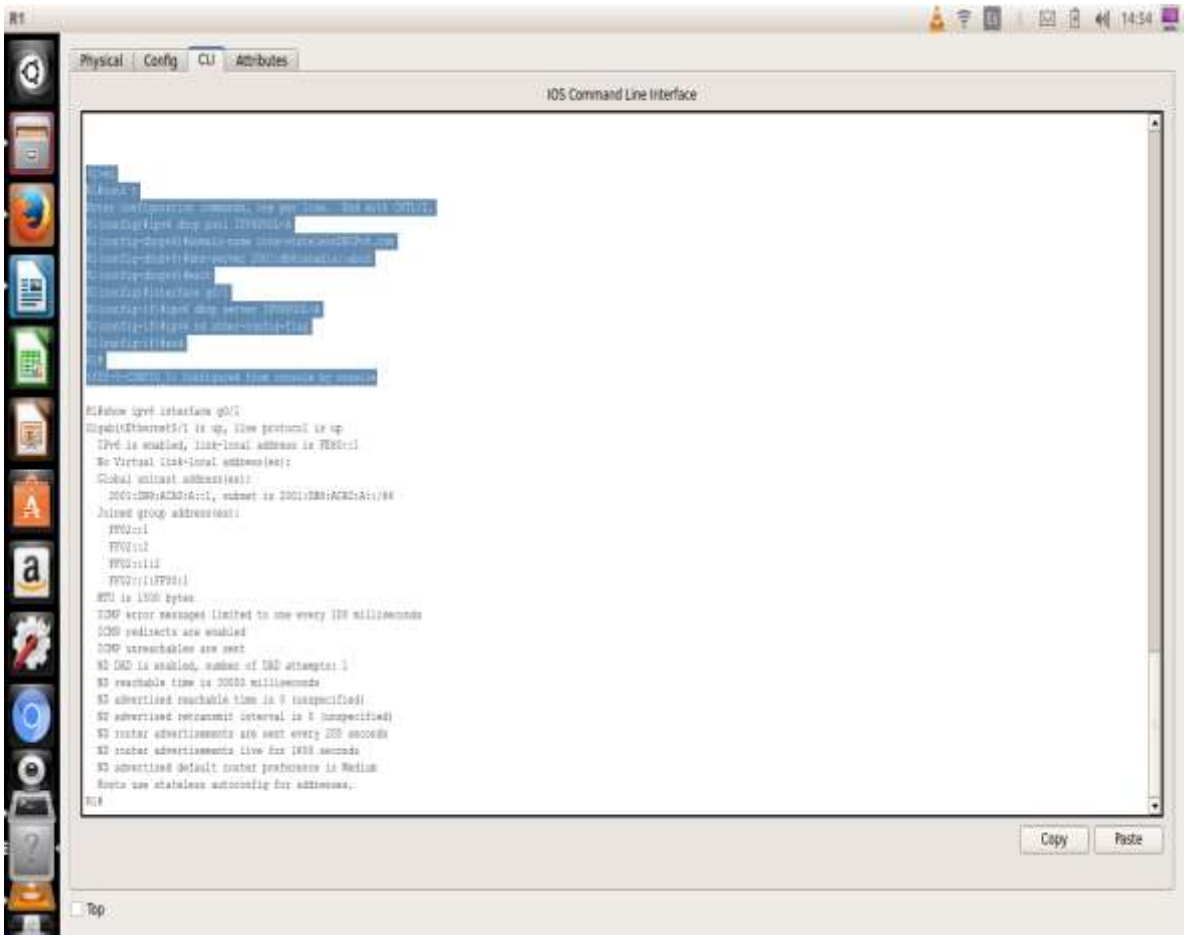
R1(config)# **interface g0/1**

R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.

R1(config-if)# **ipv6 nd other-config-flag**

R1(config-if)# **end**



Verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

R1# **show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:2

FF02::1:FF00:1

FF05::1:3

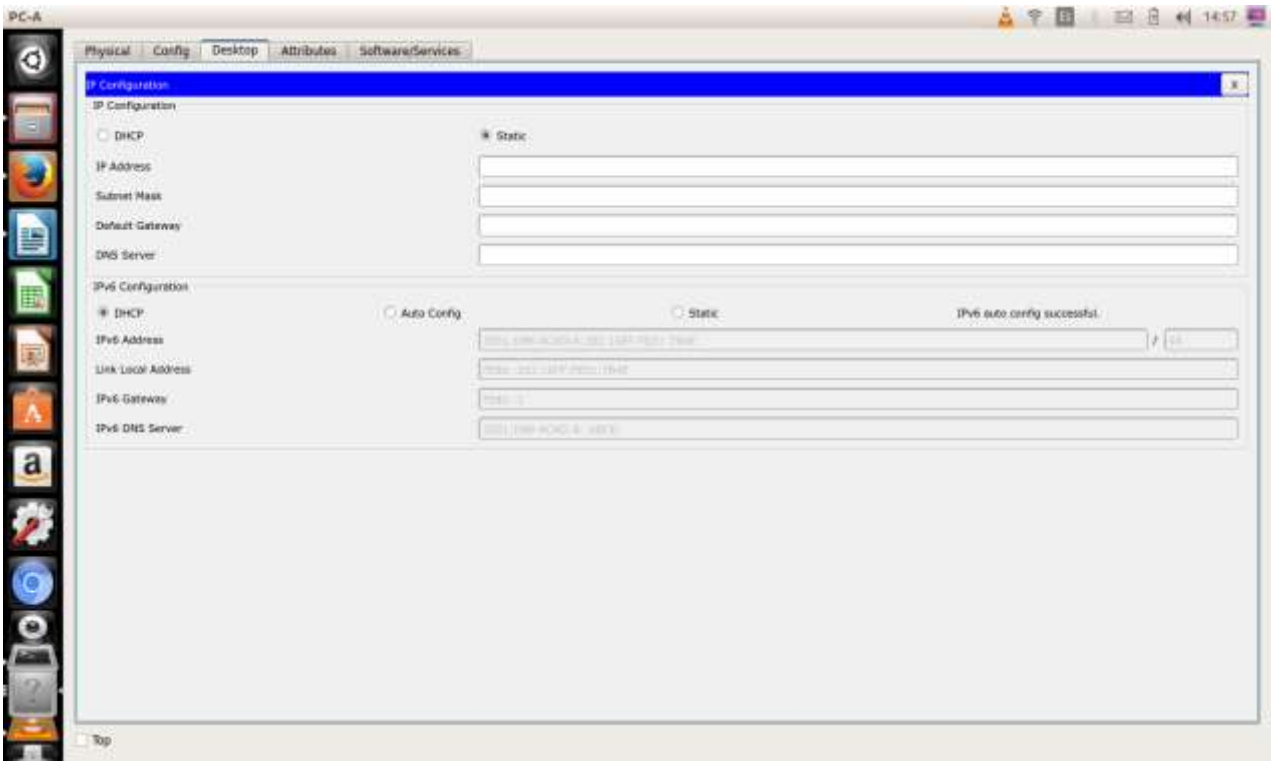
MTU is 1500 bytes

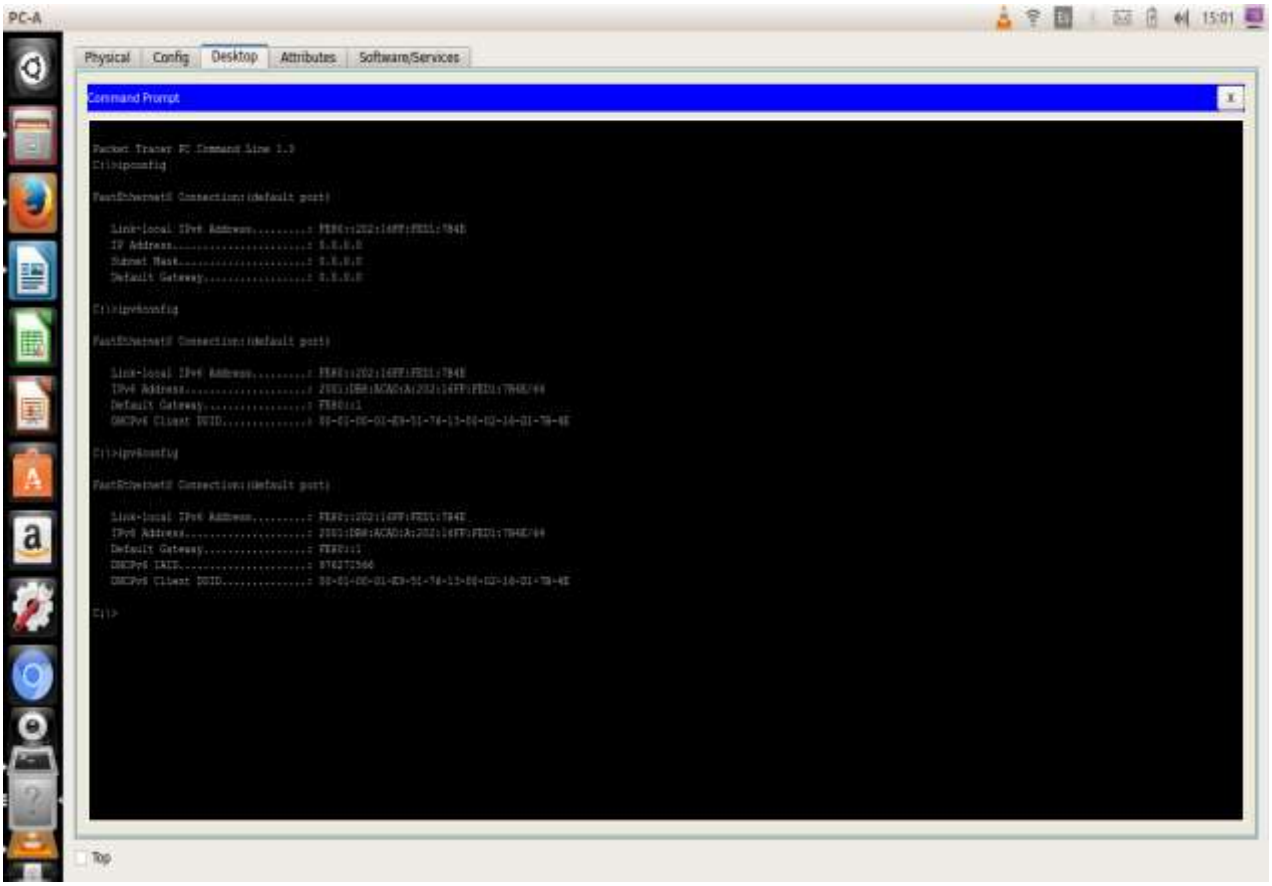
ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.

Ver los cambios realizados en la red en la PC-A.

Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron preVíamente mediante SLAAC.


PC-A
14:57
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 auto config successful.
IPv6 Address
Link Local Address
IPv6 Gateway
IPv6 DNS Server
Top


PC-A
15:01
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::202:16FF:FE11:784E
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
C:\>ipv6config
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::202:16FF:FE11:784E
IPv6 Address.....: 2001:DB8:ACAD:A:202:16FF:FE11:784E/64
Default Gateway.....: FE80::1
DHCPv6 Client DUID.....: 00-03-00-01-E9-51-74-13-00-02-16-D1-78-4E
C:\>ipv6config
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::202:16FF:FE11:784E
IPv6 Address.....: 2001:DB8:ACAD:A:202:16FF:FE11:784E/64
Default Gateway.....: FE80::1
DHCPv6 IAID.....: 876272366
DHCPv6 Client DUID.....: 00-03-00-01-E9-51-74-13-00-02-16-D1-78-4E
C:\>
Top

Ver los mensajes RA en Wireshark.

Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.

Verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

R1# **show ipv6 dhcp binding**

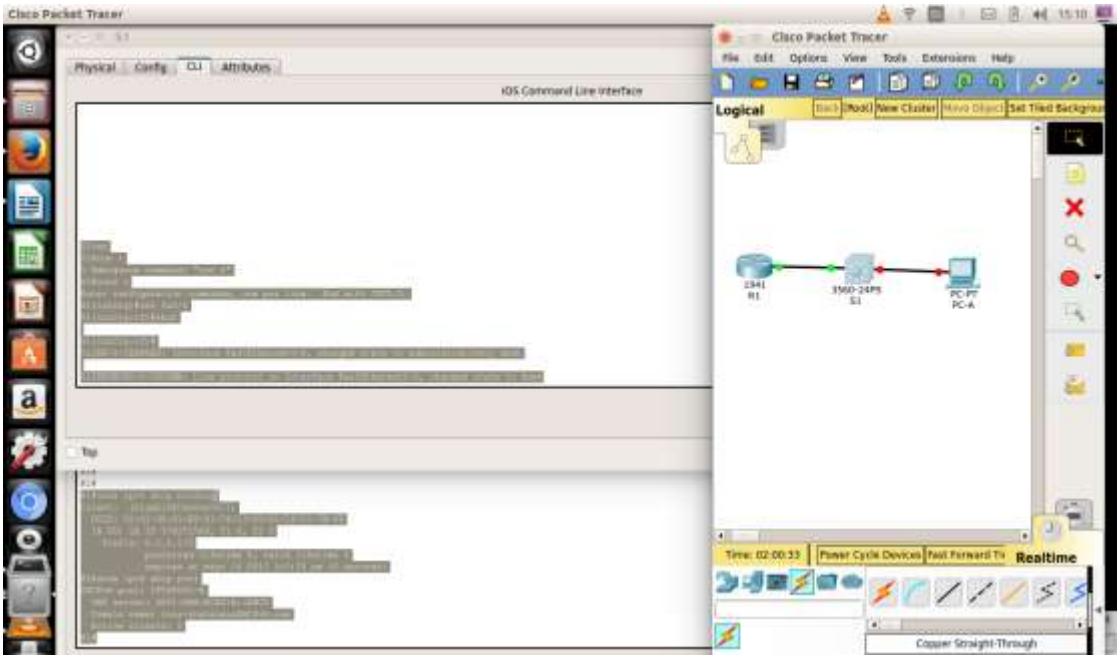
R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

Active clients: 0



Restablecer la configuración de red IPv6 de la PC-A.

Desactive la interfaz F0/6 del S1.

Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

S1(config)# **interface f0/6**

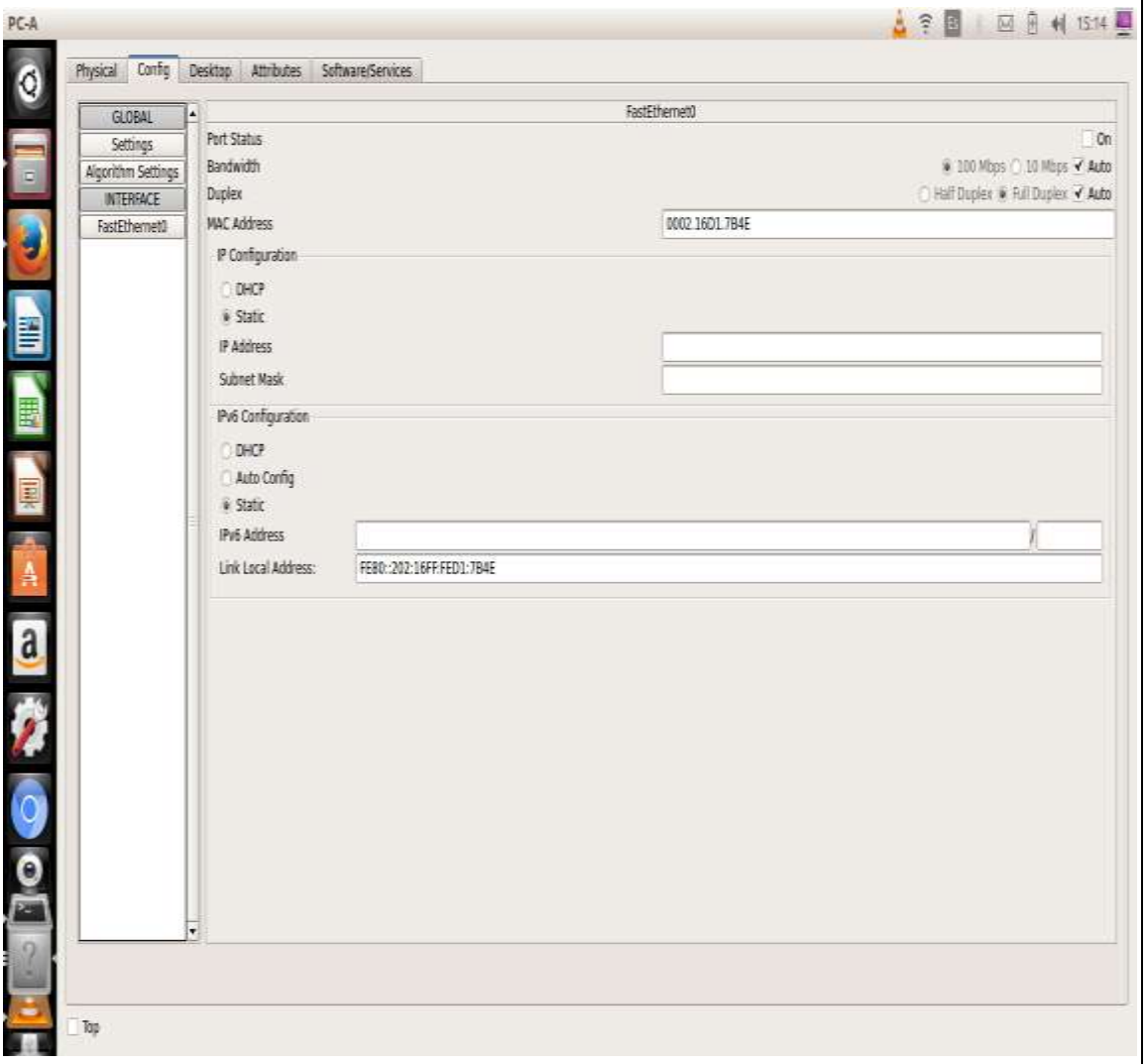
S1(config-if)# **shutdown**

Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.

Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.

Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.



Configurar la red para DHCPv6 con estado

Preparar la PC-A.

Inicie una captura del tráfico en la NIC con Wireshark.

Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.

Cambiar el pool de DHCPv6 en el R1.

Agregue el prefijo de red al pool.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

R1(config-dhcpv6)# **address prefix 2001:db8:acad:a::/64**

Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

Nota: debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

R1(config-dhcpv6)# **no domain-name ccna-statelessDHCPv6.com**

R1(config-dhcpv6)# **domain-name ccna-StatefulDHCPv6.com**

R1(config-dhcpv6)# **end**

Verifique la configuración del pool de DHCPv6.

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 0

Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

R1# **debug ipv6 dhcp detail**

IPv6 DHCP debugging is on (detailed)

Establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

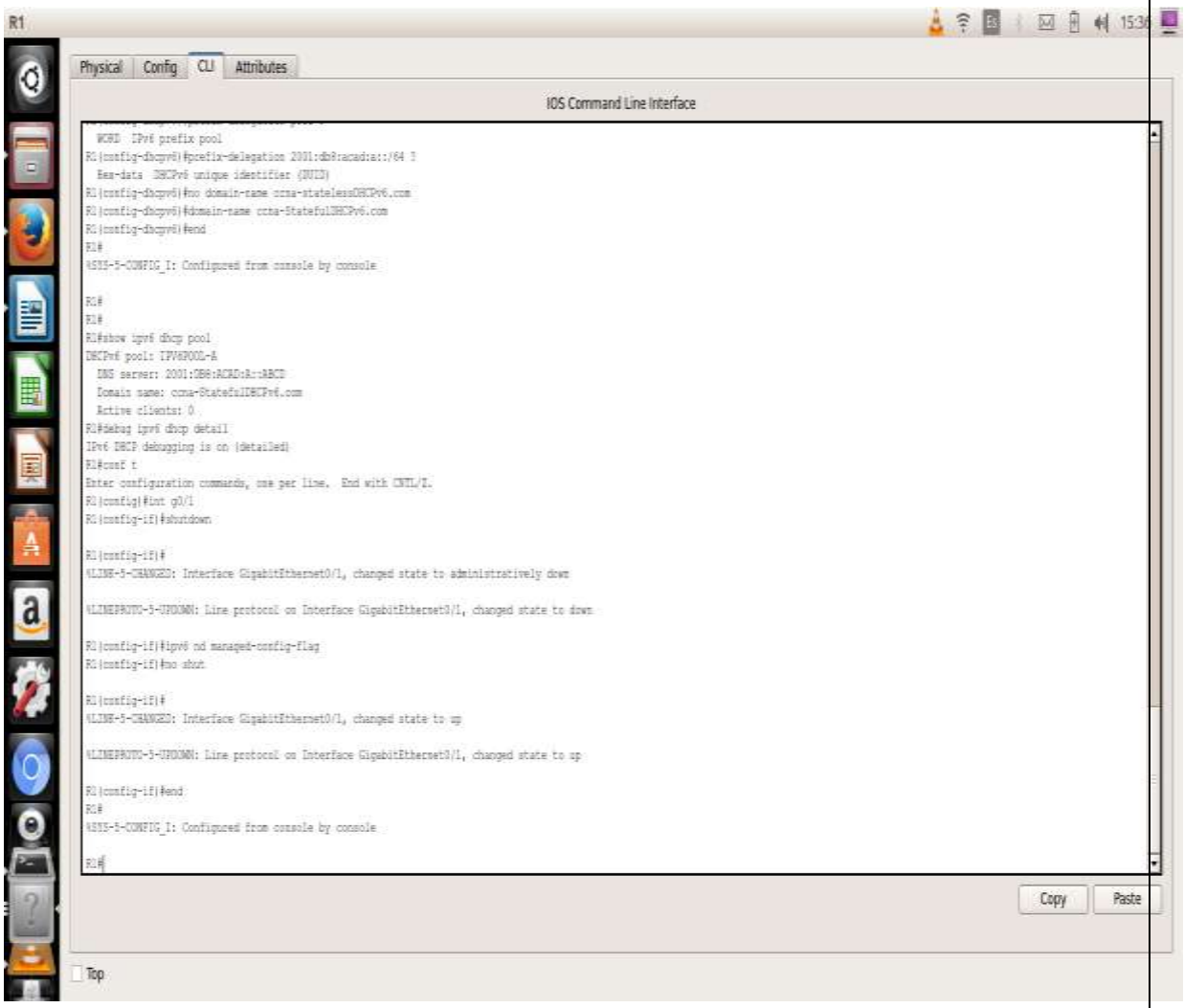
R1(config)# **interface g0/1**

R1(config-if)# **shutdown**

R1(config-if)# **ipv6 nd managed-config-flag**

R1(config-if)# **no shutdown**

R1(config-if)# **end**



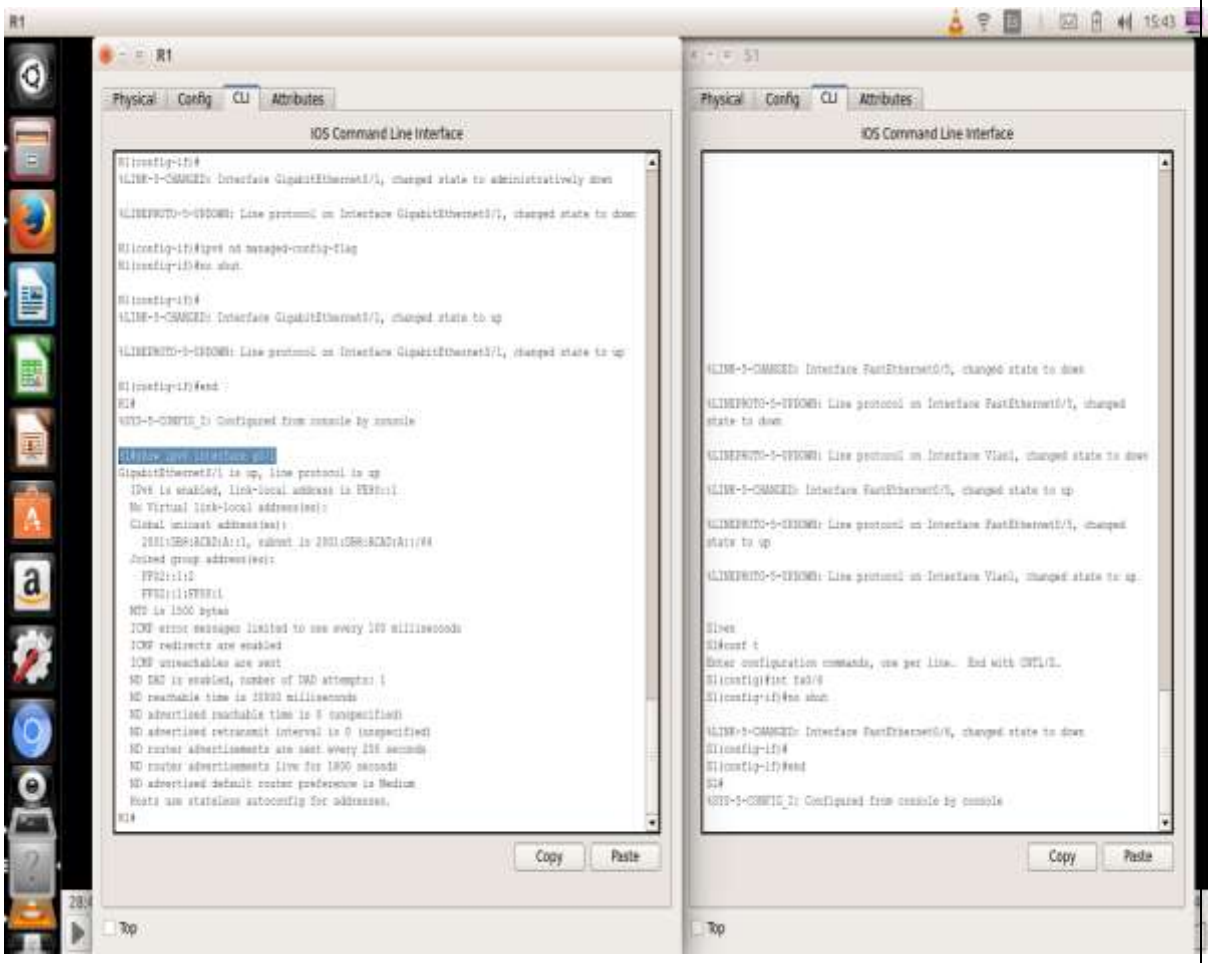
Paso 4: habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

S1(config)# **interface f0/6**

S1(config-if)# **no shutdown**

S1(config-if)# **end**



Paso 1. Paso 5: verificar la configuración de DHCPv6 con estado en el R1.

Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

R1# **show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:2

FF02::1:FF00:1

FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
Hosts use DHCP to obtain other configuration.

En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.

Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

R1# **show ipv6 dhcp pool**
DHCPv6 pool: IPV6POOL-A
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 1

Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**
Client: FE80::D428:7DE2:997C:B05A
DUID: 0001000117F6723D000C298D5444
Username : unassigned
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE
preferred lifetime 86400, valid lifetime 172800
expires at Mar 07 2013 04:09 PM (171595 seconds)

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce(Pref
erido)
   Concesión obtenida. . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:07:59
   La concesión expira . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:38:03
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a%11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   IAID DHCPv6 . . . . . . . . . . . . . . . : 234884137
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
   Servidores DNS. . . . . . . . . . . . . . : 2001:db8:acad:a::abcd
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Emita el comando **undebug all** en el R1 para detener la depuración de DHCPv6.

Nota: escribir **u all** es la forma más abreViada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebug all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

Examine el mensaje de solicitud de la PC-A que solicita información de red.

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

*Mar 5 16:42:39.775: dst FF02::1:2

*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

*Mar 5 16:42:39.775: elapsed-time 6300

*Mar 5 16:42:39.775: option CLIENTID(1), len 14

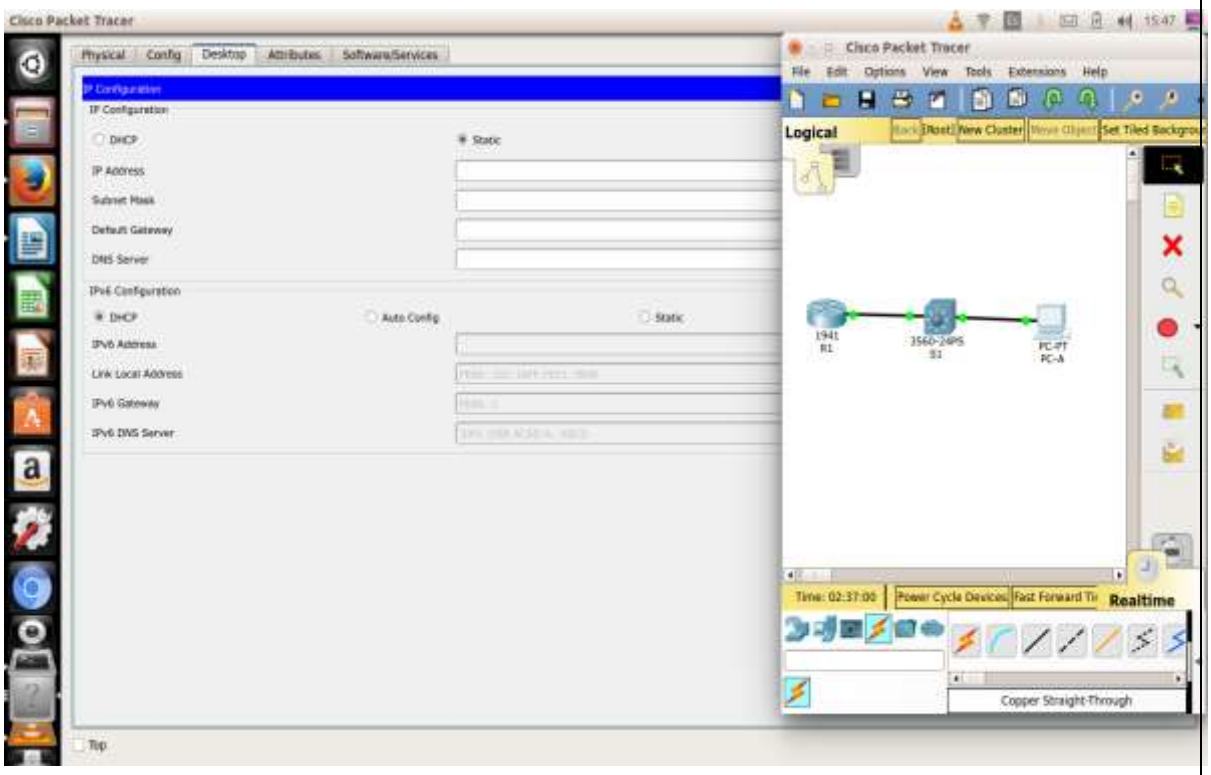
Examine el mensaje de respuesta enViado a la PC-A con la información de red DHCP.

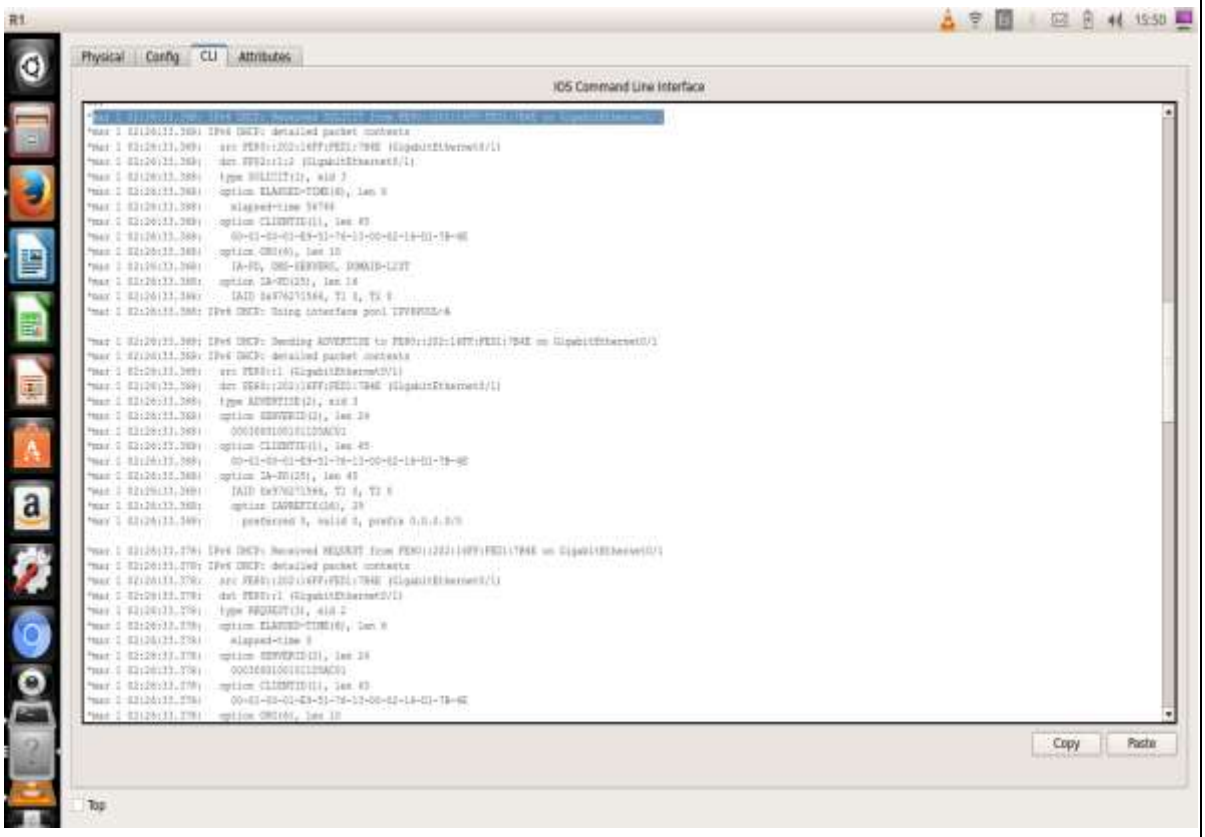
*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

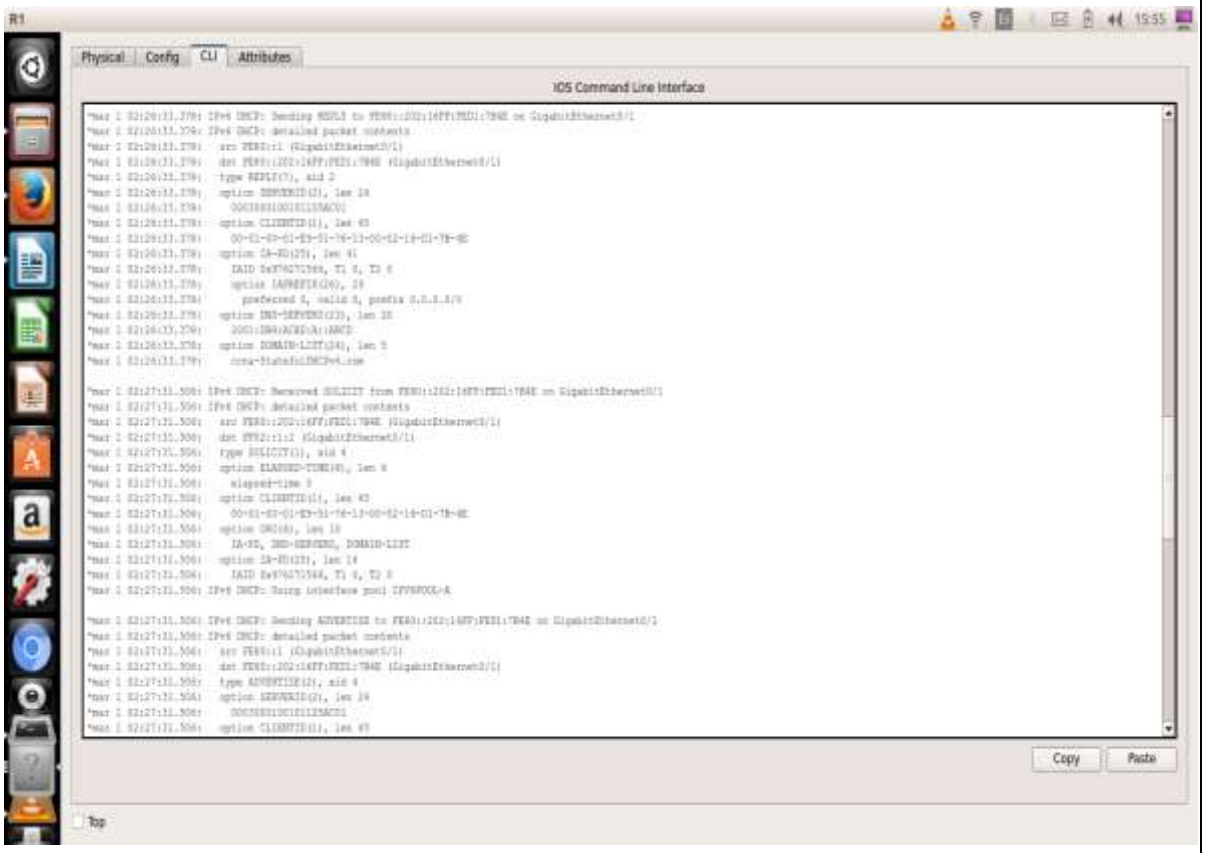
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents

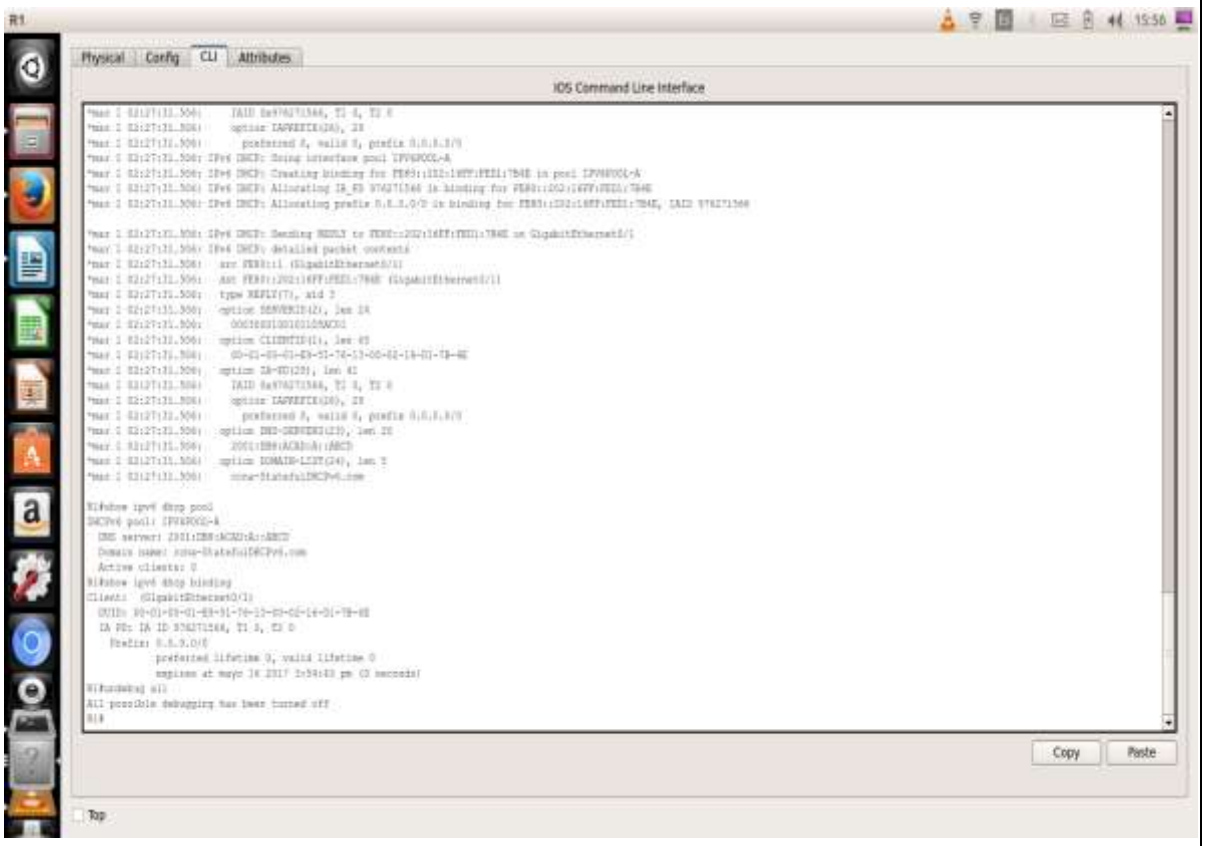
*Mar 5 16:42:39.779: src FE80::1

*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001 R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com




R1
15:50
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top

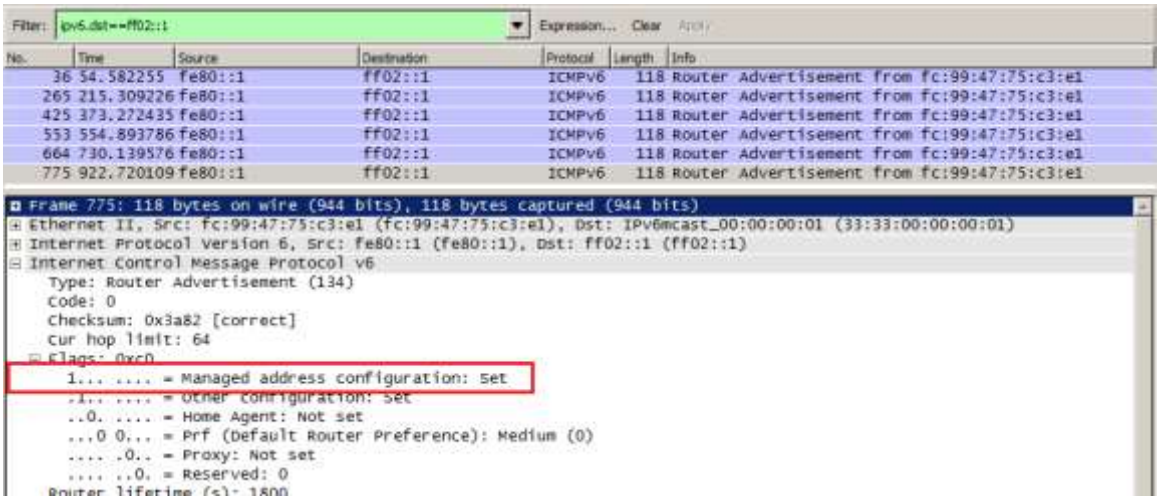

R1
15:55
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top



Paso 2. Paso 6: verificar DHCPv6 con estado en la PC-A.

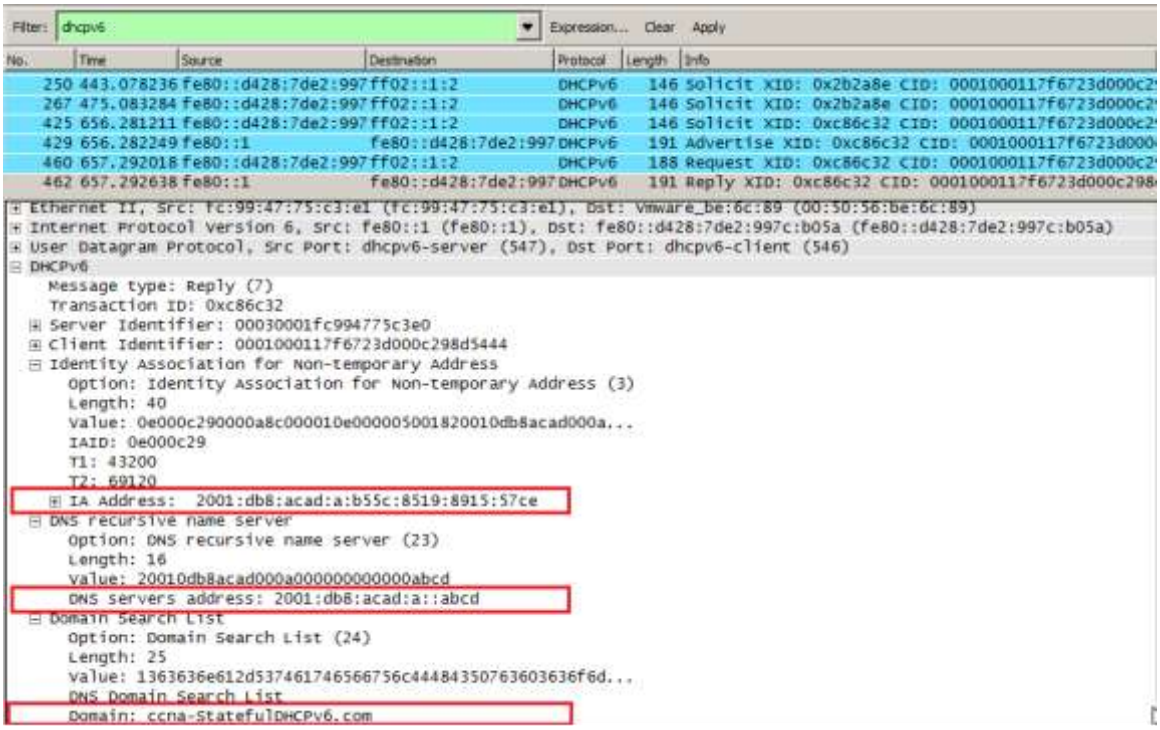
Detenga la captura de Wireshark en la PC-A.

Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información

de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.



Reflexión

¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?

con estado se usa más recursos de memoria, esto requiere que el router guarde información acerca de los clientes

¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

Sin estado

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreVíatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Ejercicio 10.3.1.1

IdT y DHCP

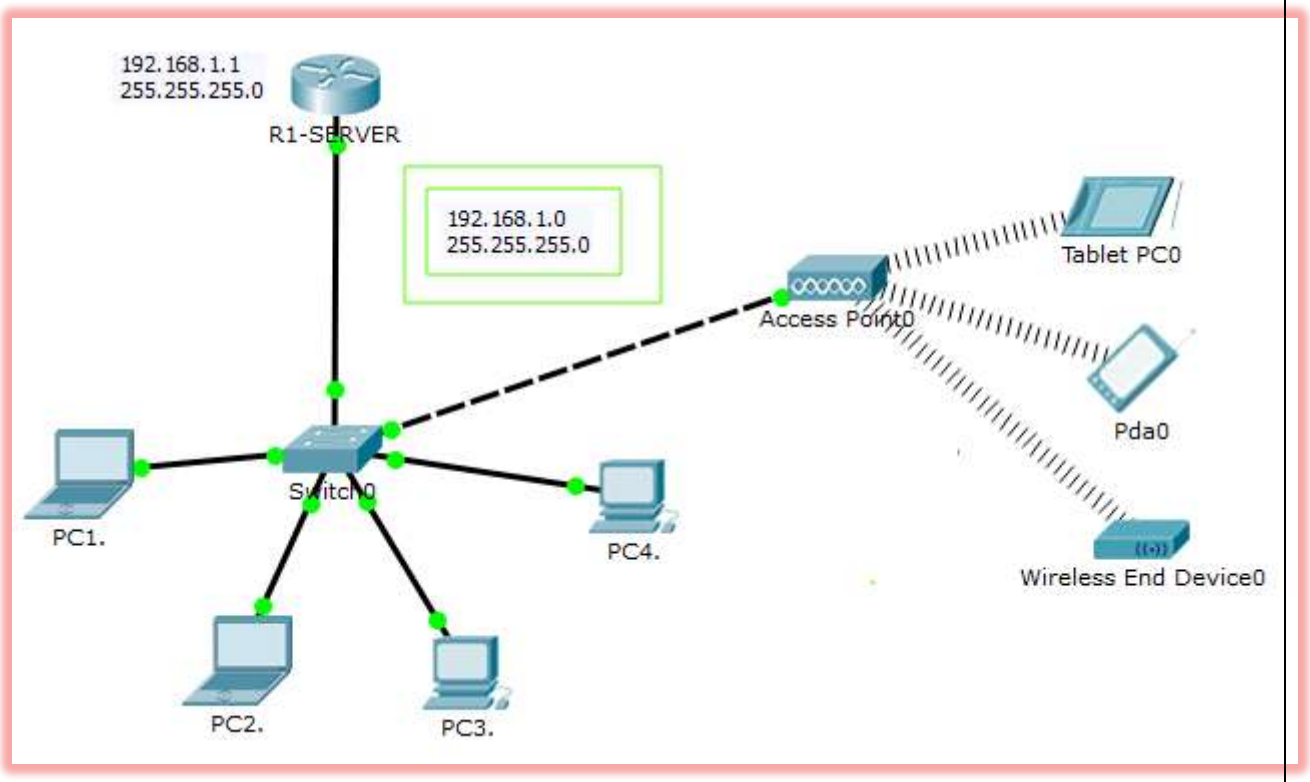
Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

Situación

En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos.

Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.



Con PacketTracer, realice las siguientes tareas para esta actividad de creación de modelos:

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.

Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.

Presente sus conclusiones a un compañero de clase o a la clase.

Recursos necesarios

Software de PacketTracer

Reflexión

¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

En este caso empleando el router 1941 que nos brinda la posibilidad de configurar el servicio DHCP, nos ahorra el hecho de tener que adquirir un dispositivo adicional que haga el papel de servidor DHCP.

¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluVía de ideas, piense y registre cinco respuestas posibles.

- Con DHCP lo que hacemos es ahorrar tiempo de administración junto con la posibilidad de conectar diferentes tipos de dispositivos.
- El crecimiento de internet y el crecimiento en la cantidad de dispositivos que están conectados a la red, se ha visto necesario la posibilidad de ampliar los mismo empleando el direccionamiento IPV6 y junto con DCHP se hace este de manera automática sin o con poca intervención del usuario.
- Tenemos en la actualidad la posibilidad de tener acceso a la información en tiempo real, los dispositivos los podemos manejar de manera distante gracias a que cada uno de ellos está conectado a la red, lo podemos modificar de acuerdo a las necesidades que nosotros tengamos.
- Todas las empresas están sacando el mayor provecho de las tecnologías que surgen en el momento, muchas de las tareas de las mismas ya se realizan conectadas, actualizando y teniendo acceso a infinidad de información que se les refleja en utilidades para la misma.

Gracias a la tecnología el crecimiento que han vivido las empresas ha sido posible, hay mucho más control de cada una de sus parte posibilitando el crecimiento en muchas casos de manera automática con una simple autorización.

Ejercicio 11.2.26

Práctica de laboratorio: configuración de NAT dinámica y estática

Topología

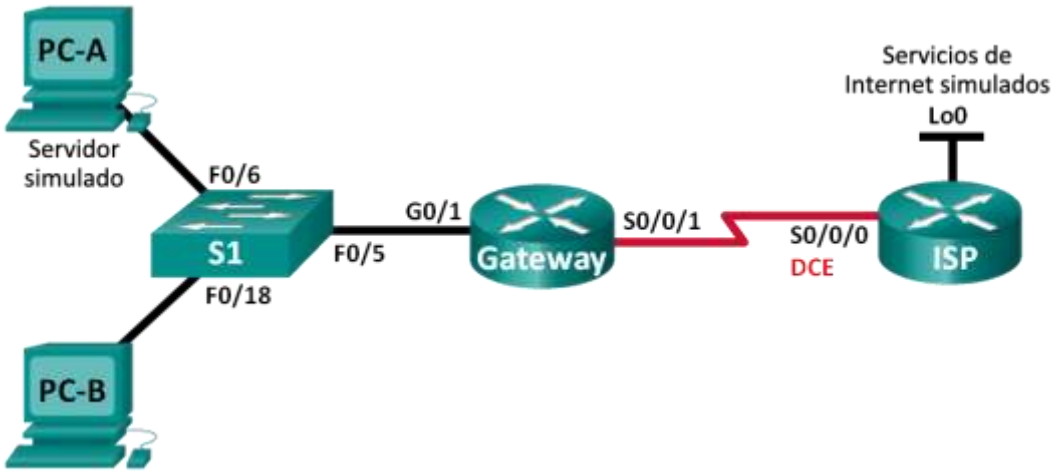


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una

organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

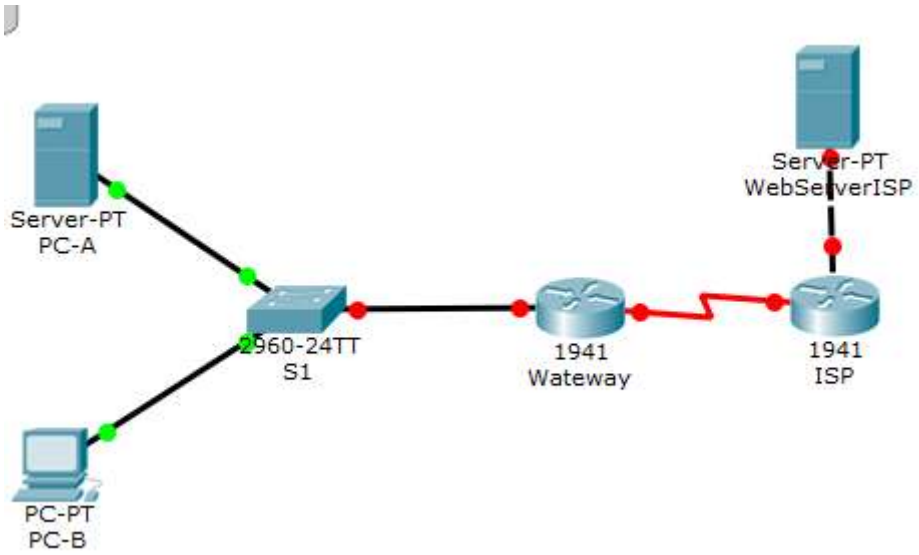
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Armar la red y verificar la conectividad

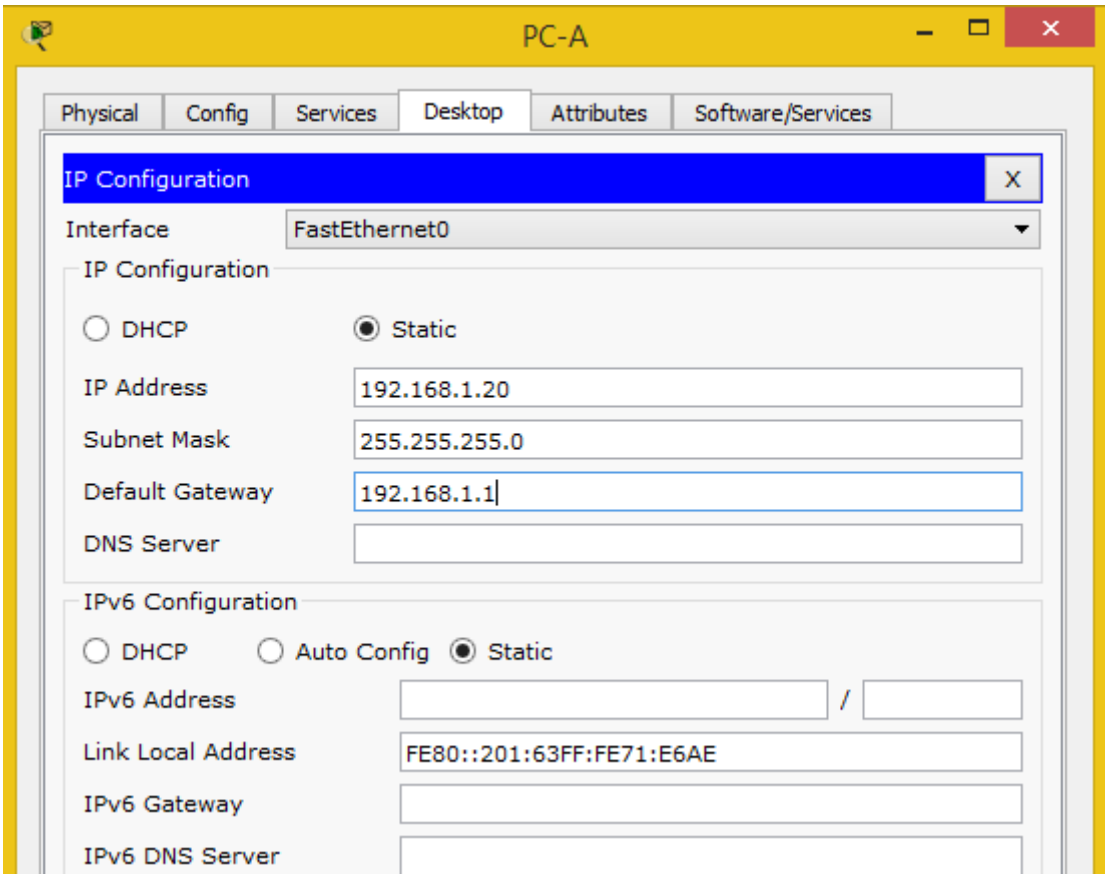
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

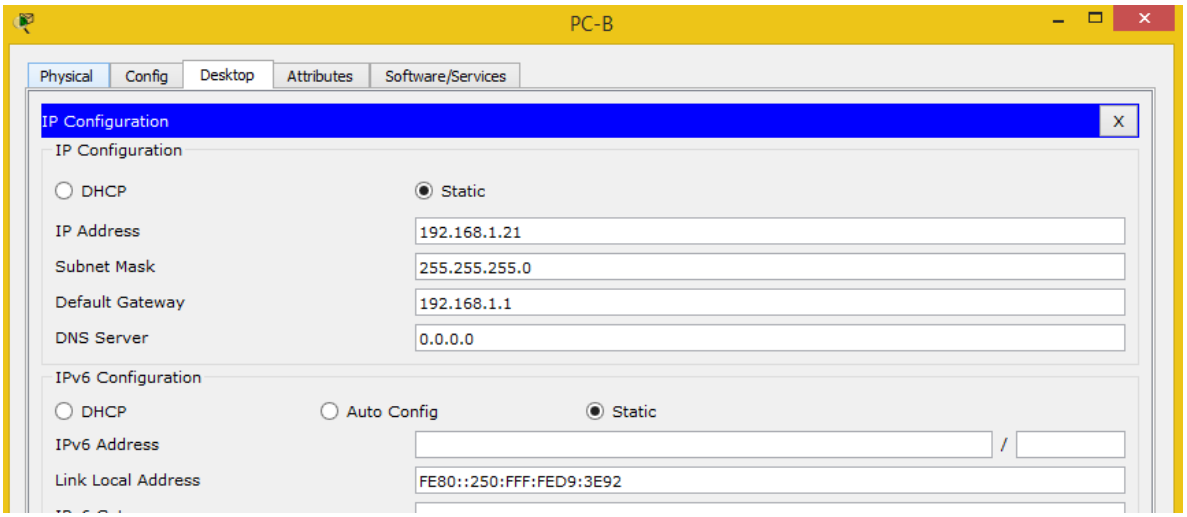
Realizar el cableado de red tal como se muestra en la topología.

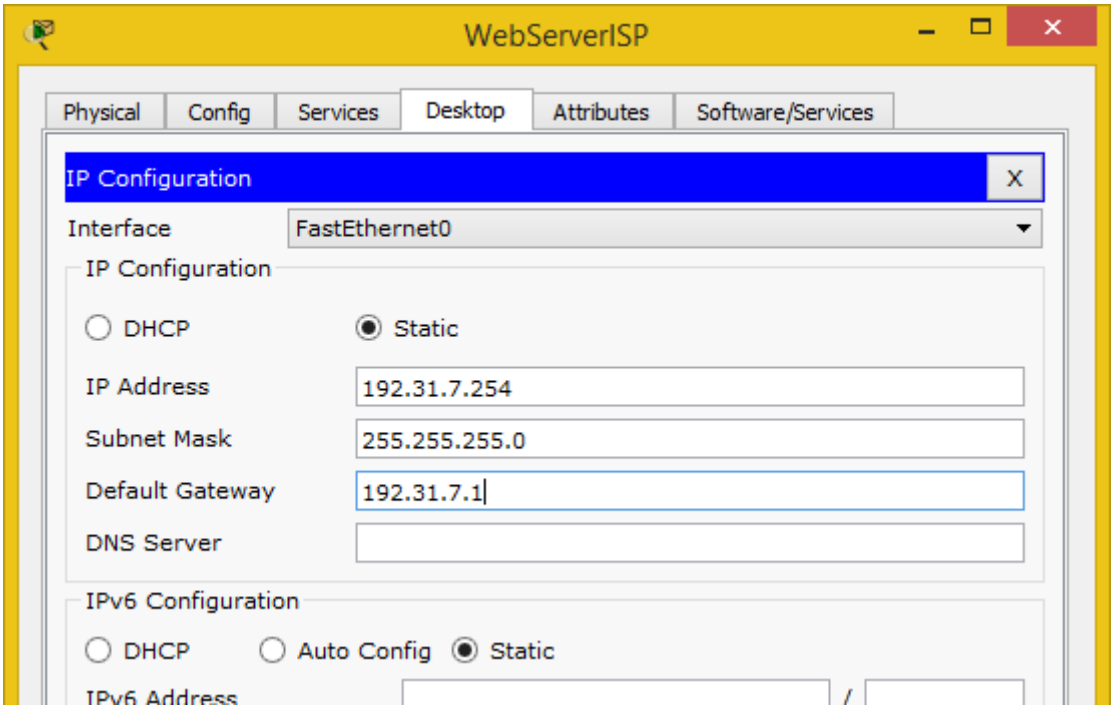
Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.



Configurar los equipos host.







Inicializar y volver a cargar los routers y los switches según sea necesario.

Configurar los parámetros básicos para cada router.

Desactive la búsqueda del DNS.

```
Gateway(config)#no ip domain-lookup
```

Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

```
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shut

Gateway(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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#
```

Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

```
Gateway(config-if)#clock rate 1280000
```

Configure el nombre del dispositivo como se muestra en la topología.

```
Router(config)#hostname Gateway
```

Asigne **cisco** como la contraseña de consola y la contraseña de vty.

```
Gateway(config-line)#line console 0
Gateway(config-line)#pass
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config)#
```

```
Gateway(config)#line vty 0 15
Gateway(config-line)#cisco
                     ^
% Invalid input detected at '^' marker.

Gateway(config-line)#pass
Gateway(config-line)#password cisco
Gateway(config-line)#
```

Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

```
Gateway(config)#enable pass
Gateway(config)#enable password cisco
Gateway(config)#exit
```

```
Gateway(config)#service pass
Gateway(config)#service password-encryption
Gateway(config)#exit
```

```
!
enable password 7 0822455D0A16
!
```

Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

```
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#
```

El router ISP

```
ISP(config)#line console 0
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#
```

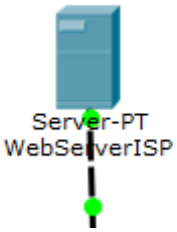
```
Router(config)#hostname ISP
ISP(config)#
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 1280000
Unknown clock rate
ISP(config-if)#clock rate 128000
ISP(config-if)#int g0/0
ISP(config-if)#ip address 192.31.7.1 255.255.255.0
ISP(config-if)#no shut

ISP(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

ISP(config-if)#
```

```
ISP(config-if)#no ip domain-loo
ISP(config-if)#no ip domain-lookup
ISP(config)#line console 0
ISP(config-line)#pass
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#pass
ISP(config-line)#password cisco
ISP(config-line)#exit
ISP(config)#enable pass
ISP(config)#enable password cisco
ISP(config)#exit
ISP#
```

```
ISP(config)#service password-encryption
ISP(config)#exit
```

```
enable password 7 0822455D0A16
!
```

Crear un servidor web simulado en el ISP.



Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.

ISP(config)# **username webuser privilege 15 secret webpass**

Habilite el servicio del servidor HTTP en el ISP.

ISP(config)# **ip http server**

Configure el servicio HTTP para utilizar la base de datos local.

ISP(config)# **ip http authentication local**

Se creaesteservidor web ISP yaque packet tracer no es compatible con estoscomandos

Configurar el routing estático.

Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

ISP(config)# **iproute 209.165.200.224 255.255.255.224 209.165.201.18**

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224
209.165.201.18
ISP(config)#
```

Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# **iproute 0.0.0.0 0.0.0.0 209.165.201.17**

```
Gateway#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

Guardar la configuración en ejecución en la configuración de inicio.

Verificar la conectividad de la red

Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=51ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 51ms, Average = 12ms

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

```
Gateway#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.201.17

Gateway#
```

```
ISP(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.31.7.0/24 is directly connected, GigabitEthernet0/0
L       192.31.7.1/32 is directly connected, GigabitEthernet0/0
     209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 [1/0] via 209.165.201.18
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0

ISP(config)#
```

Configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

Gateway(config)# **ipnat inside source static 192.168.1.20 209.165.200.225**

```
Gateway#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20
209.165.200.225
Gateway(config)#
```

Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

Gateway(config)# **interface g0/1**
Gateway(config-if)# **ipnat inside**
Gateway(config-if)# **interface s0/0/1**
Gateway(config-if)# **ipnat outside**

```
Gateway(config)#int g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#
```

Probar la configuración.

Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

Gateway# **show ipnat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local
Outside global
---  209.165.200.225   192.168.1.20       ---                ---

Gateway#
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = **209.165.200.225**

¿Quién asigna la dirección global interna?

Está asignada por el router y al mismo tiempo nos asigna el proveedor de internet

¿Quién asigna la dirección local interna?

La asignamos nosotros como administradores de red

En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=25ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 25ms, Average = 7ms
```

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1

--- 209.165.200.225 192.168.1.20 --- ---

```
Gateway#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:10192.168.1.20:10    192.31.7.2:10      192.31.7.2:10
icmp 209.165.200.225:11192.168.1.20:11    192.31.7.2:11      192.31.7.2:11
icmp 209.165.200.225:12192.168.1.20:12    192.31.7.2:12      192.31.7.2:12
icmp 209.165.200.225:5 192.168.1.20:5     192.31.7.1:5       192.31.7.1:5
icmp 209.165.200.225:6 192.168.1.20:6     192.31.7.1:6       192.31.7.1:6
icmp 209.165.200.225:7 192.168.1.20:7     192.31.7.1:7       192.31.7.1:7
icmp 209.165.200.225:8 192.168.1.20:8     192.31.7.1:8       192.31.7.1:8
icmp 209.165.200.225:9 192.168.1.20:9     192.31.7.2:9       192.31.7.2:9
---  209.165.200.225   192.168.1.20       ---                ---

Gateway#
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? **10**

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

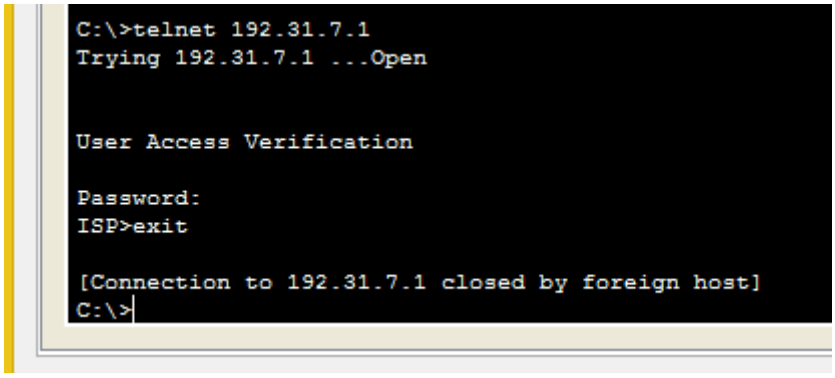
En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

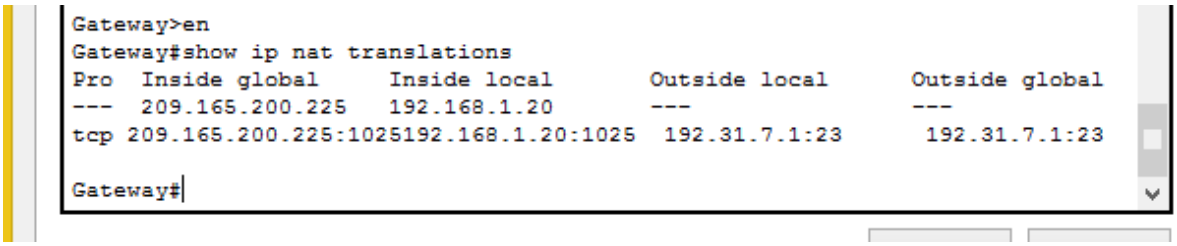
Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1

tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23

--- 209.165.200.225 192.168.1.20 --- ---





Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

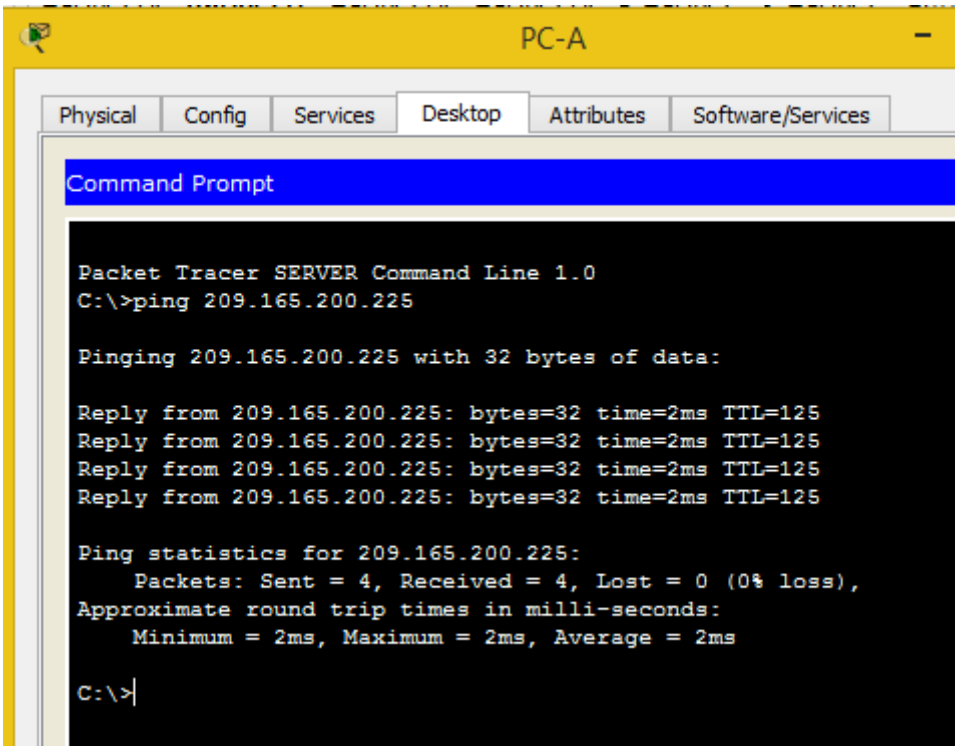
¿Qué protocolo se usó para esta traducción? **Telnet**

¿Cuáles son los números de puerto que se usaron?

Global/local interno: **1025**

Global/local externo: **23**

Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.



En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# **show ipnat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12

--- 209.165.200.225 192.168.1.20 --- ---

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ipnat statics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

```
Gateway#show ip nat statistics
Total translations: 4 (1 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36  Misses: 19
Expired translations: 16
Dynamic mappings:
Gateway#
```

Configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

Gateway# **clear ipnat translation ***

Gateway# **clearipnatstatistics**

No se pudo realizar

Definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

```
Gateway(config)#access-list 1 permit 192.168.1.2 0.0.0.225
```

Verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

Definir el conjunto de direcciones IP públicas utilizables.

Gateway(config)#**ipnat pool public_access 209.165.200.242209.165.200.254 netmask 255.255.255.224**

```
Gateway(config)#ip nat pool public_address 209.165.200.242
209.165.200.254 netmask 255.255.255.224
Gateway(config)#
```

Definir la NAT desde la lista de origen interna hasta el conjunto externo.

Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

Gateway(config)# **ipnat inside source list 1 pool public_access**

```
Gateway(config)#ip nat inside source list 1 pool public_address
Gateway(config)#
```

Probar la configuración.

En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = _____

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? **5-6-7-8**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---

Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:5 192.168.1.21:5     192.31.7.2:5       192.31.7.2:5
icmp 209.165.200.242:6 192.168.1.21:6     192.31.7.2:6       192.31.7.2:6
icmp 209.165.200.242:7 192.168.1.21:7     192.31.7.2:7       192.31.7.2:7
icmp 209.165.200.242:8 192.168.1.21:8     192.31.7.2:8       192.31.7.2:8
---  209.165.200.225   192.168.1.20       ---                ---
```

En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

Muestre la tabla de NAT.

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80

--- 209.165.200.242 192.168.1.22 --- ---

¿Qué protocolo se usó en esta traducción? **http**

¿Qué números de puerto se usaron?

Interno: **1025**

Externo: **80**

¿Qué número de puerto bien conocido y qué servicio se usaron? **80**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.2:80      192.31.7.2:80

Gateway#
```

Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ipnat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_accessrefcount 2

poolpublic_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12  Misses: 35
Expired translations: 4
Dynamic mappings:
-- Inside Source
access-list 1 pool public_address refCount 0
 pool public_address: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 0 (0%),
misses 0
Gateway#
```

Eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

Gateway (config)# **no ipnat inside source static 192.168.1.20 209.165.200.225**

```
Gateway#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#no ip nat inside source static 192.168.1.20
209.165.200.225
Gateway(config)#
```

Static entry in use, do you want to delete child entries? [no]: **yes**

Borre las NAT y las estadísticas.

Haga ping al ISP (192.31.7.1) desde ambos hosts.

Muestre la tabla y las estadísticas de NAT.

Gateway# **show ipnat statistics**

Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 00:00:43 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 16 Misses: 0

CEF Translated packets: 285, CEF Punted packets: 0

Expired translations: 11

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_accessrefcount 4

poolpublic_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12  Misses: 35
Expired translations: 4
Dynamic mappings:
-- Inside Source
access-list 1 pool public_address refCount 0
 pool public_address: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 0 (0%),
misses 0
Gateway#
```

Gateway# **show ipnat translation**

Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512 192.31.7.1:512
--- 209.165.200.243 192.168.1.20 --- ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512 192.31.7.1:512
--- 209.165.200.242 192.168.1.21 --- ---

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión

¿Por qué debe utilizarse la NAT en una red?

Porquecada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet

¿Cuáles son las limitaciones de NAT?

Puede que no se pueda reduzca el rendimiento de las ip de extremo a extremo

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreVíatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Ejercicio 11.2.3.7

Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

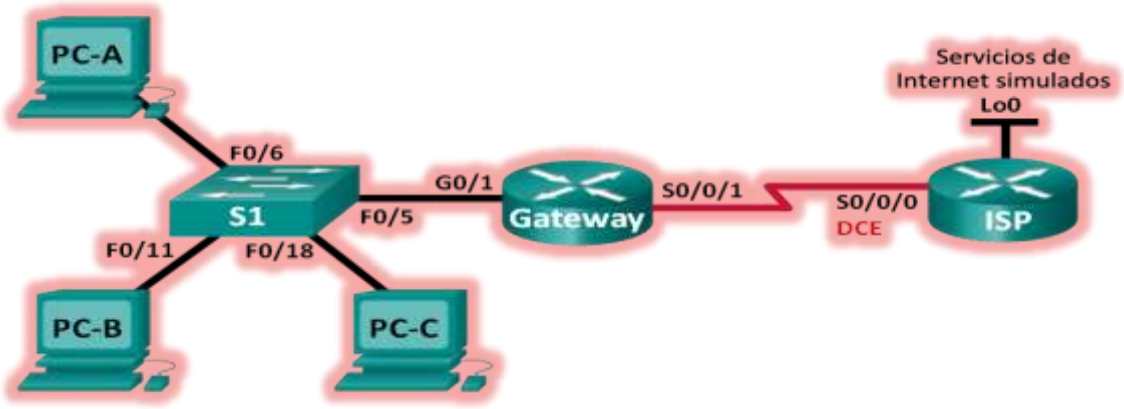


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

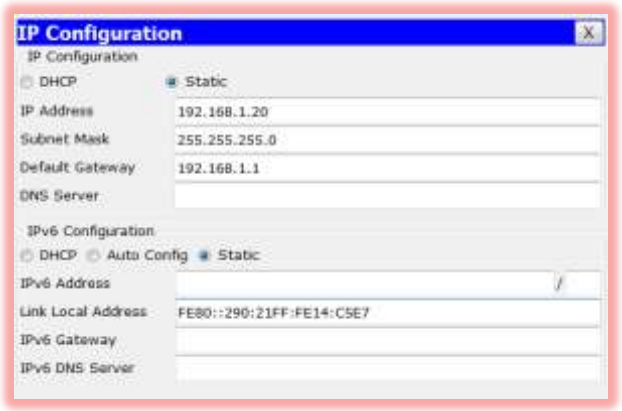
Cables Ethernet y seriales, como se muestra en la topología

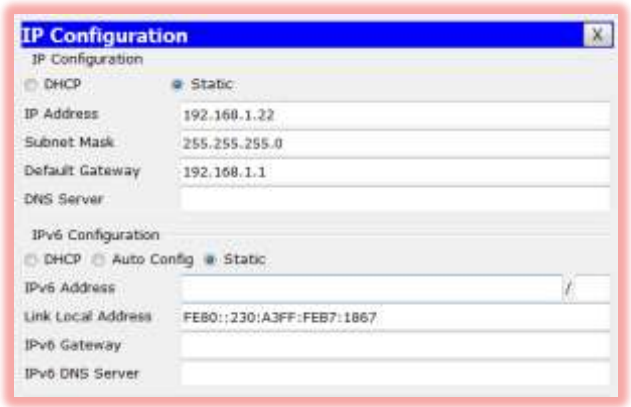
Armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Realizar el cableado de red tal como se muestra en la topología.

Configurar los equipos host.





Inicializar y volver a cargar los routers y los switches.

Configurar los parámetros básicos para cada router.

Desactive la búsqueda del DNS.

Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

Configure el nombre del dispositivo como se muestra en la topología.

Asigne **cisco** como la contraseña de consola y la contraseña de vty.

Asigne**class** como la contraseña cifrada del modo EXEC privilegiado.

Configure**loggingsynchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Configurar el routing estático.

Cree una ruta estática desde el router ISP hasta el router Gateway.

ISP(config)# **iproute 209.165.200.224 255.255.255.248 209.165.201.18**

```
ISP(config)#
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

Cree una ruta predeterminada del router Gateway al router ISP.

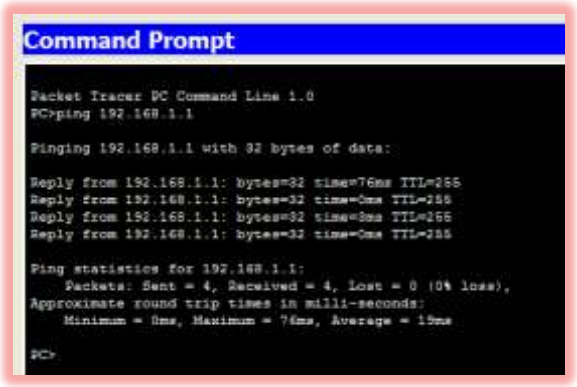
Gateway(config)# **iproute 0.0.0.0 0.0.0.0 209.165.201.17**

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

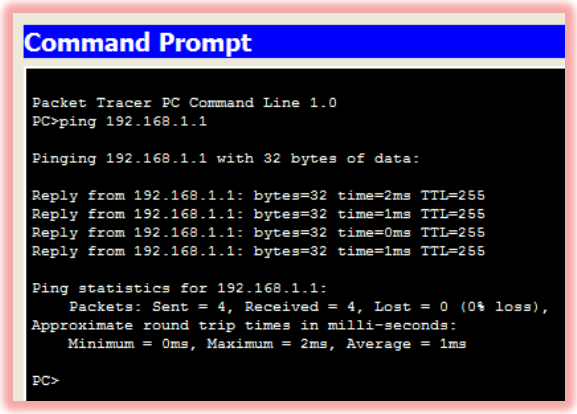
Verificar la conectividad de la red

Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

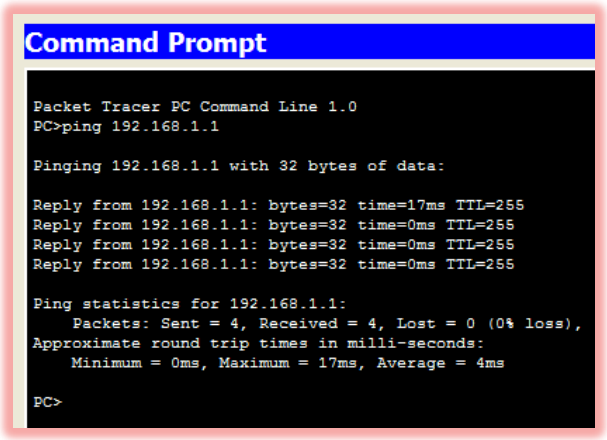
PC-A



PC-B



PC-C



Verifique que las rutas estáticas estén bien configuradas en ambos routers.

```
Gateway#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.201.17
Gateway#
```

```
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.31.7.0/24 is directly connected, GigabitEthernet0/0
L       192.31.7.1/32 is directly connected, GigabitEthernet0/0
     209.165.200.0/29 is subnetted, 1 subnets
S       209.165.200.224/29 [1/0] via 209.165.201.18
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0
ISP#
```

Configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

```
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#
```

Definir el conjunto de direcciones IP públicas utilizables.

Gateway(config)#**ipnat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

```
Gateway(config)#ip nat pool public_access 209.165.200.225  209.165.200.230 netmask 255.255.255.248
Gateway(config)#
```

Definir la NAT desde la lista de origen interna hasta el conjunto externo.

Gateway(config)# **ipnat inside source list 1 pool public_access overload**

```
Gateway(config)#ip nat inside source list 1 pool public_access overload
Gateway(config)#
```

Especifique las interfaces.

Emita los comandos **ipnatinside** e **ipnatoutside** en las interfaces.

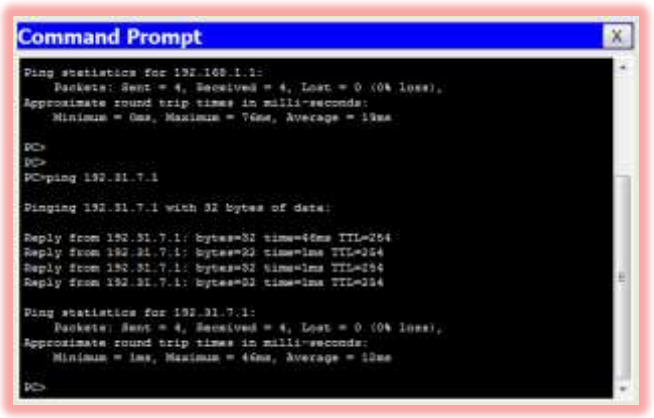
Gateway(config)# **interface g0/1**
Gateway(config-if)# **ipnat inside**
Gateway(config-if)# **interface s0/0/1**
Gateway(config-if)# **ipnat outside**

```
Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/1
Gateway(config-if)#ip nat outside
```

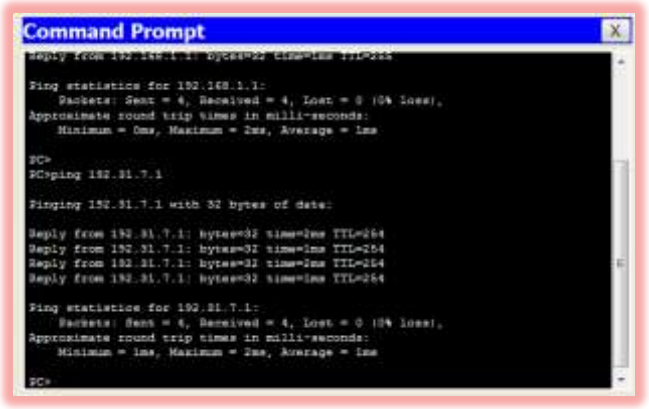
Verificar la configuración del conjunto de NAT con sobrecarga.

Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

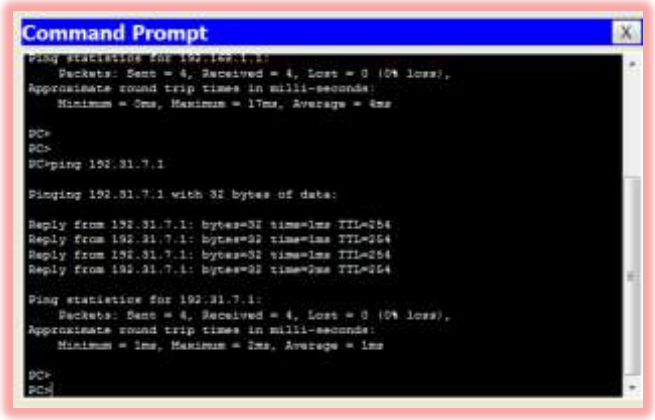
PC-A



PC-B



PC-C



Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ipnat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_accessrefcount 3
poolpublic_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
QueuedPackets: 0

```
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36  Misses: 36
Expired translations: 24
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 12
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 1 (16%), misses 0
Gateway#
```

Muestre las NAT en el router Gateway.

Gateway# **show ipnat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:0	192.168.1.20:1	192.31.7.1:1	192.31.7.1:0
icmp	209.165.200.225:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.200.225:2	192.168.1.22:1	192.31.7.1:1	192.31.7.1:2

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:1024192.168.1.21:17   192.31.7.1:17      192.31.7.1:1024
icmp 209.165.200.225:1025192.168.1.21:18   192.31.7.1:18      192.31.7.1:1025
icmp 209.165.200.225:1026192.168.1.21:19   192.31.7.1:19      192.31.7.1:1026
icmp 209.165.200.225:1027192.168.1.21:20   192.31.7.1:20      192.31.7.1:1027
icmp 209.165.200.225:1028192.168.1.22:17   192.31.7.1:17      192.31.7.1:1028
icmp 209.165.200.225:1029192.168.1.22:18   192.31.7.1:18      192.31.7.1:1029
icmp 209.165.200.225:1030192.168.1.22:19   192.31.7.1:19      192.31.7.1:1030
icmp 209.165.200.225:1031192.168.1.22:20   192.31.7.1:20      192.31.7.1:1031
icmp 209.165.200.225:17192.168.1.20:17     192.31.7.1:17      192.31.7.1:17
icmp 209.165.200.225:18192.168.1.20:18     192.31.7.1:18      192.31.7.1:18
icmp 209.165.200.225:19192.168.1.20:19     192.31.7.1:19      192.31.7.1:19
icmp 209.165.200.225:20192.168.1.20:20     192.31.7.1:20      192.31.7.1:20

Gateway#
```

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?

- 3

¿Cuántas direcciones IP globales internas se indican?

- 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?

- 4

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

- En este caso el PING falla, ya que no conocemos la dirección IP interna, solo se conoce la dirección local a la cual se realiza la traducción.

```
ISP#ping 192.168.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ISP#
```

Configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Borrar las NAT y las estadísticas en el router Gateway.

Gateway#clearipnat translation *

Verificar la configuración para NAT.

Verifique que se hayan borrado las estadísticas.

Show ipnatstatis.

```
Gateway#Show ip nat statis
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 48  Misses: 48
Expired translations: 48
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#
```

Verifique que las interfaces externa e interna estén configuradas para NAT.

Verifique que la ACL aún esté configurada para NAT.

```
Gateway#Show ip nat statis
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 48  Misses: 48
Expired translations: 48
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#
```

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Gateway# show ipnat statistics

Eliminar el conjunto de direcciones IP públicas utilizables.

Gateway(config)# **noipnat pool public_access 209.165.200.225209.165.200.230 netmask 255.255.255.248**

```
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
%Pool public_access in use, cannot destroy
Gateway(config)#
```

Eliminar la traducción NAT de la lista de origen interna al conjunto externo.

Gateway(config)# **no ipnat inside source list 1 pool public_access overload**

```
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
Gateway(config)#
```

Asociar la lista de origen a la interfaz externa.

Gateway(config)# **ipnat inside source list 1 interface serial 0/0/1 overload**

```
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
Gateway(config)#
```

Probar la configuración PAT.

Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ipnat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
QueuedPackets: 0

```
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60  Misses: 60
Expired translations: 48
Dynamic mappings:
Gateway#
Gateway#
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60  Misses: 60
Expired translations: 48
Dynamic mappings:
Gateway#
```

Muestre las traducciones NAT en el Gateway.

Gateway# **show ipnat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

```
Gateway#
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.18:1024192.168.1.21:25   192.31.7.1:25      192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.21:26   192.31.7.1:26      192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.21:27   192.31.7.1:27      192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.22:25   192.31.7.1:25      192.31.7.1:1027
icmp 209.165.201.18:1028192.168.1.21:28   192.31.7.1:28      192.31.7.1:1028
icmp 209.165.201.18:1029192.168.1.22:26   192.31.7.1:26      192.31.7.1:1029
icmp 209.165.201.18:1030192.168.1.22:27   192.31.7.1:27      192.31.7.1:1030
icmp 209.165.201.18:1031192.168.1.22:28   192.31.7.1:28      192.31.7.1:1031
icmp 209.165.201.18:25 192.168.1.20:25    192.31.7.1:25      192.31.7.1:25
icmp 209.165.201.18:26 192.168.1.20:26    192.31.7.1:26      192.31.7.1:26
icmp 209.165.201.18:27 192.168.1.20:27    192.31.7.1:27      192.31.7.1:27
icmp 209.165.201.18:28 192.168.1.20:28    192.31.7.1:28      192.31.7.1:28

Gateway#
```

Reflexión

¿Qué ventajas tiene la PAT?

Con esto minimizamos la cantidad de direcciones IP públicas que necesitamos para dar salida a internet anuestros equipos de la red local.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreVíatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Conclusiones

La tarea propuesta logro ampliar el conocimiento correspondiente al diseño e implementación de soluciones integradas LAN / WAN, donde pudimos desarrollar parámetros satisfactoriamente, comprendiendo de manera apropiada el contorno a los proyectos planteados de este tipo.

El conocimiento pertinente, oportuno y completo sobre las redes ofrece posibilidades de instalación segura de las mismas, estrategias y protocolos de seguridad. Ya sean cableadas o inalámbricas; una red requiere elementos básicos, tanto de físicos como lógicos.

En esta unidad nos enfocamos al enrutamiento de redes de datos el cual es muy importante ya que se transfiere información a través de una red por medio de router quienes se encargan de transferir los paquetes de una red a otra.

El comando para configurar una ruta estática es "iproute" y su sintaxis más simple esla siguiente: Router(config)# iproutedireccion-red mascara-subred { direccion-ip | interfaz-salida }

Aprender la configuración La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. Permite que los dispositivos externos inicien conexiones a los dispositivos internos mediante la dirección pública asignada de forma estática.

Bibliografía

Copyright © 2006 - 2016 - Oscar Gerometta . Todos los derechos reservados.. Tema Awesome Inc.. Con tecnología de Blogger.

New Riders Pub; Edición: 2 (1 de junio de 2000) ISBN-10: 0735709998

ISBN-13: 978-0735709997

B. Hill, "Manual de referencia CISCO. McGraw-Hill, pp. 631-700, 2002.

G. Meyer. S. Sherry "Triggered Extensions to RIP to Support Demand Circuits" RFC 2091 "Request for Comments: 2091", pp. 1-21, Ene. 1997.

Malkin. "RIP Version 2 Protocol analysis" RFC 1387 "Request for Comments: 1387". pp. 1-3, Ene. 1997.

Principios Básicos de Networking para Redes Cisco IOS - Oscar Gerometta

Academia de Networking de Cisco Systems: Guía del primer año CCNA 1 y 2". 3º Edición. Cisco Press, Madrid, 2008.

Cisco Security Appliance Command Line ConfigurationGuide, Version 8_! " Configuring NA# $Cisco ASA %%!!"& Series 'ire(alls)

Copyright 2000-2017 Firewall.cx - All Rights Reserved
Information and images contained on this site is copyrighted material.

Firewall.cx - Cisco Networking, VPN - IPSec, Security, Best VPN Service, Cisco Switching, Cisco Routers, Cisco VoIP- CallManager Express, Windows Server, Virtualization, Hyper-V, Web Security, Linux Administration

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-data-acl-12-4t-book/sec-cntrl-acc-vtl.html

Routing dinámico, Cisco networking

https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.1.3.6

CCNA 1 Powertraining : ICND1/CCENT

http://bibliotecavirtual.unad.edu.co:2110/ehost/detail/detail?sid=b65a840b-6d84-4d38-b13c-67d16e182184%40sessionmgr4006&vid=0&hid=4107&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=979032&db=e000xww

CCENT/CCNA ICND1

http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf