INSTITUTO POLITÉCNICO NACIONAL
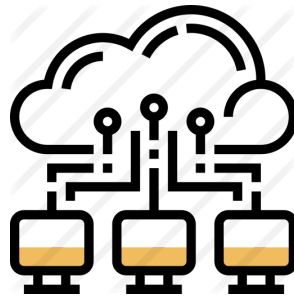
ESCUELA SUPERIOR DE CÓMPUTO

ADMINISTRACIÓN DE SERVICIOS EN RED

Actividad

2_5 Desafío de configuración de ACL's

EQUIPO 1

INTEGRANTES:

Arellano Aguillón Shu Nashy Nizarely

Banderas Solórzano Midori

Montaño Morales Angeles Aranza

Servín Quinterio Damaris Angelina

GRUPO: 4CV12

PROFESORA: Leticia Henestrosa Carrasco

Activity 5.5.2:

Challenge Access Control Lists

NOTE TO USER: This activity is a variation of Lab 5.5.2. Packet Tracer may not support all the tasks specified in the hands-on lab. This activity should not be considered equivalent to completing the hands-on lab. Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Addressing table

Device	Interface	IP address	Subnet Mask	Default Gateway
R1	S0/0/0	10.1.1.0	255.255.255.252	N/A
	Fa0/0	10.1.1.254	255.255.255.0	N/A
R2	S0/0/1	10.1.0.2	255.255.255.252	N/A
	S0/0/1	10.3.0.1	255.255.255.252	N/A
R3	S0/0/1	10.3.0.2	255.255.255.252	N/A
	Fa0/0	10.3.1.254	255.255.255.0	N/A
PC1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC2	NIC	10.3.1.1	255.255.255.0	10.3.1.254

Task 1: Perform Basic Configurations

Step 1. Configure all devices.

Configure all devices according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an encrypted privileged EXEC password of class.
- Configure a message-of-the-day banner
- Configure a password of cisco for console connections.
- Configure a password of cisco for vty connections.
- Configure IP addresses and masks on all devices. Clock rate is 64000.
- Enable OSPF with process ID 1 on all routers for all networks.
- Configure IP addressing and default gateways on each PC.
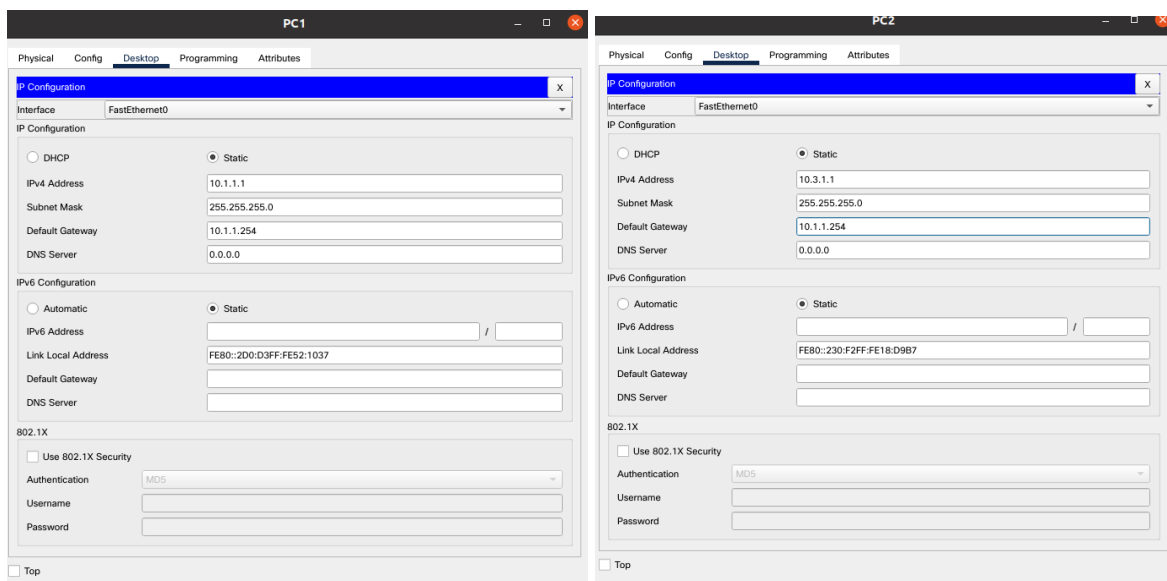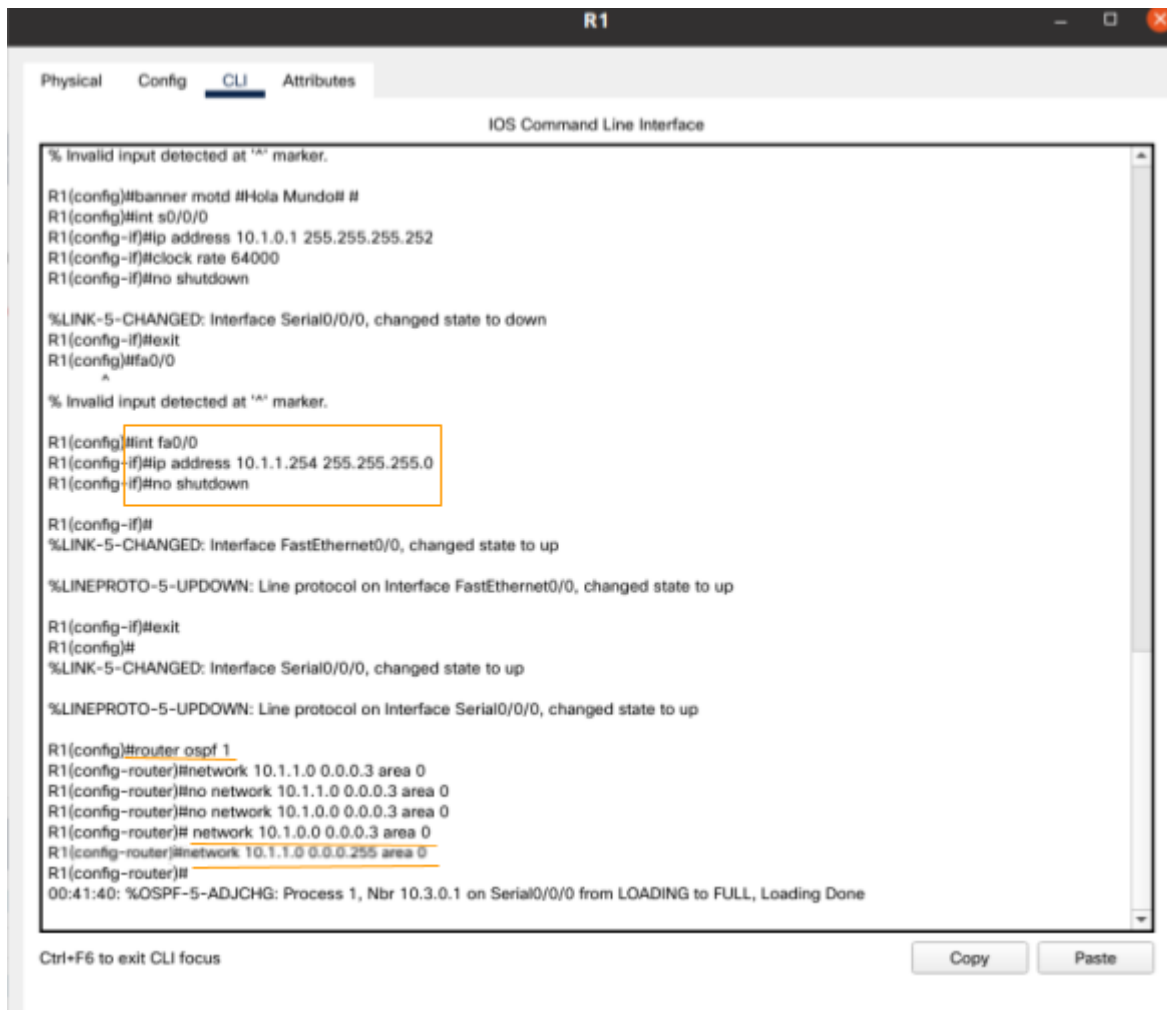- Verify full IP connectivity using the ping command.

ROUTER 1:


```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd ?
  LINE  c banner-text c, where 'c' is a delimiting character
R1(config)#banner ?
  login  Set login banner
  motd   Set Message of the Day banner
R1(config)#banner modt #Hola Mundo#
                ^
% Invalid input detected at '^' marker.

R1(config)#banner modt #Hola Mundo# #
                ^
% Invalid input detected at '^' marker.

R1(config)#banner motd #Hola Mundo# #
R1(config)#int s0/0/0
R1(config-if)#ip address 10.1.0.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
```

R1 — IOS Command Line Interface

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

R1(config)#banner motd #Hola Mundo# #
R1(config)#int s0/0/0
R1(config-if)#ip address 10.1.0.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#fa0/0
         ^
% Invalid input detected at '^' marker.

R1(config)#int fa0/0
R1(config-if)#ip address 10.1.1.254 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#
%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

R1(config)#router ospf 1
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#no network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#no network 10.1.0.0 0.0.0.3 area 0
R1(config-router)# network 10.1.0.0 0.0.0.3 area 0
R1(config-router)#network 10.1.1.0 0.0.0.255 area 0
R1(config-router)#
00:41:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.3.0.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

Ctrl+F6 to exit CLI focus

Copy   Paste

PC1 — IP Configuration

Interface: FastEthernet0

IP Configuration
- DHCP / ● Static
- IPv4 Address: 10.1.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.1.254
- DNS Server: 0.0.0.0

IPv6 Configuration
- Automatic / ● Static
- IPv6 Address: _____ / __
- Link Local Address: FE80::2D0:D3FF:FE52:1037
- Default Gateway:
- DNS Server:

802.1X
- ☐ Use 802.1X Security
- Authentication: MD5
- Username:
- Password:

☐ Top

PC2 — IP Configuration

Interface: FastEthernet0

IP Configuration
- DHCP / ● Static
- IPv4 Address: 10.3.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.1.254
- DNS Server: 0.0.0.0

IPv6 Configuration
- Automatic / ● Static
- IPv6 Address: _____ / __
- Link Local Address: FE80::230:F2FF:FE18:D9B7
- Default Gateway:
- DNS Server:

802.1X
- ☐ Use 802.1X Security
- Authentication: MD5
- Username:
- Password:

☐ Top

Step 2. Check Results.

Your completion percentage should be 85%. If not, click Check Results to see which required components are not yet completed.
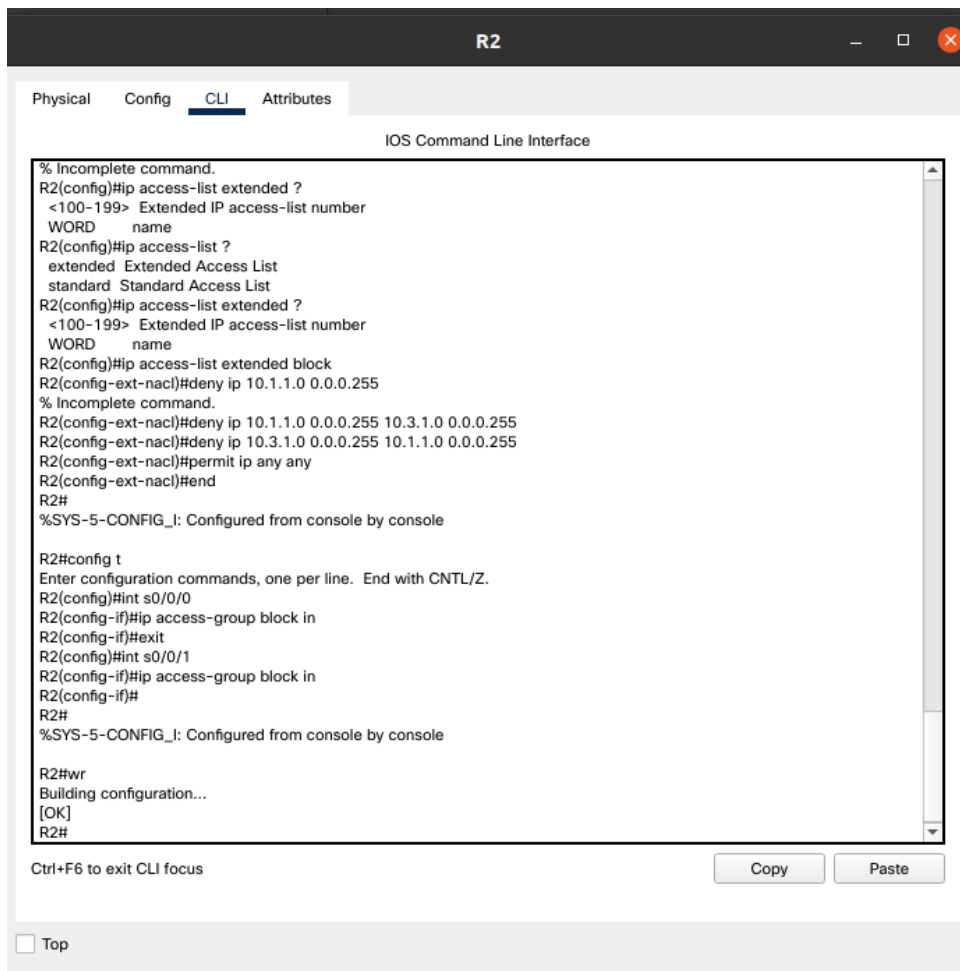
Task 2: Configuring Standard ACLs

Step 1. Configure standard ACLs on R1 and R3.

Configure standard named ACLs on the R1 and R3 vty lines, permitting hosts connected directly to their Fast Ethernet subnets to gain Telnet access. Deny all other connection attempts.Name these standard ACLs VTY-Local. Document your testing procedures.

Step 2. Check Results.

Your completion percentage should be 94%. If not, click Check Results to see which required components are not yet completed.

Task 3: Configuring Extended ACLs

Step 1. Configure extended ACLs on R2.

Using extended ACLs on R2, complete the following requirements:

- Name the ACL block
- Prohibit traffic originating from the R1 connected subnets from reaching the R3 connected subnets.
- Prohibit traffic originating from the R3 connected subnets from reaching the R1 connected subnets.
- Permit all other traffic.

Document your ACL configuration.

Step 2. Check Results.

Your completion percentage should be 100%. If not, click Check Results to see which required components are not yet completed.

Task 4: Verifying an ACL

Step 1. Test telnet.

- PC1 should be able to telnet into R1
- PC3 should be able to telnet into R3
- R2 should be denied telnet access to R1 and R3
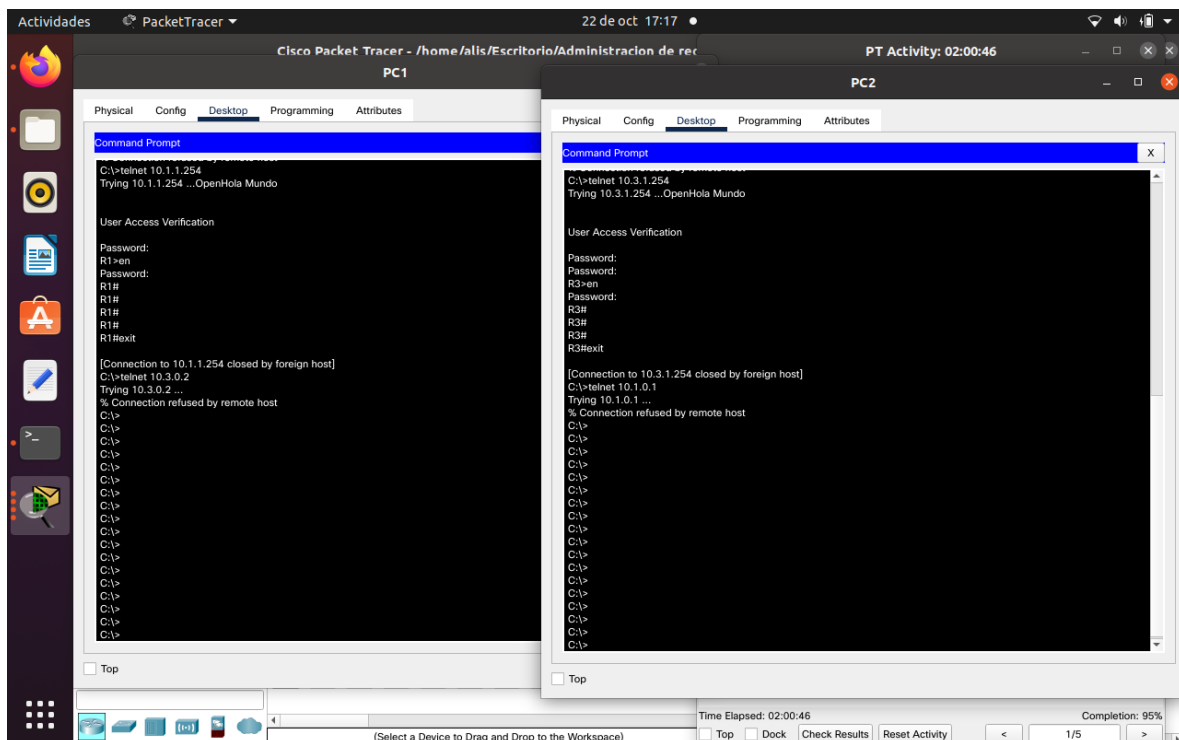
Step 2. Test traffic.

Pings between PC1 and PC3 should fail.
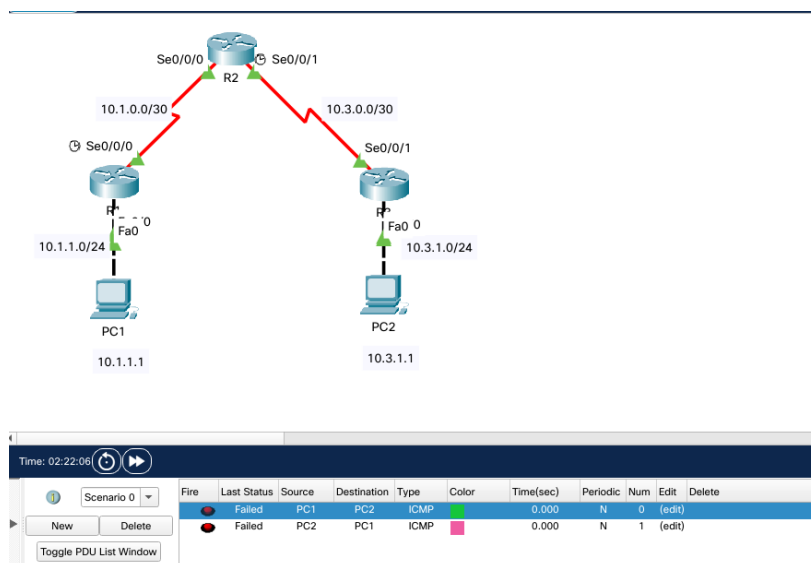
Nota: La actividad no registró la configuración de las Default Gateway pero si está presente.