**Liberty University**

**CSIS 331**

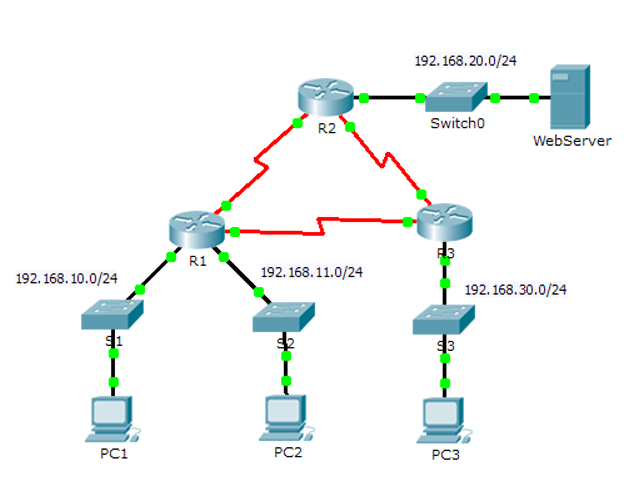
**Lab 14 Instructor**

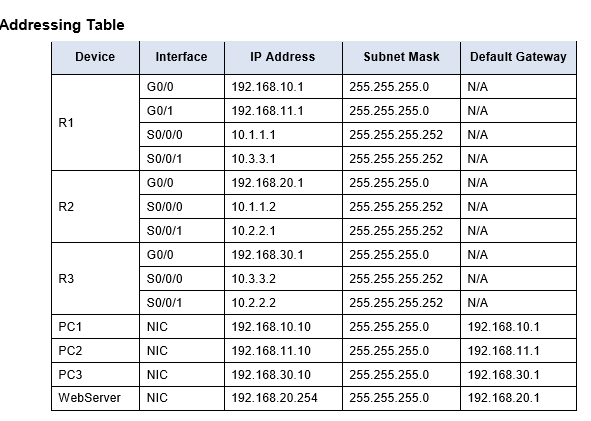
**Packet Tracer:**

*[Adapted from Cisco Networking Academy Routing and Switching 7.2.1.6, 7.2.1.7 & 9.2.2.6]*

*In this lab we will configure ACLs and NAT.*

**Configuring Numbered Standard IPv4 ACLs**

**



**Objectives**

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: Investigate the current network configuration.**

Open “Numbered Standard IPv4 ACLs.pka”. 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. **Record your ping results in Ping Table 1 the Answer Sheet under Numbered IPv4 ACLs.**

**Step 2: Evaluate 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 **WebServer** on 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 **WebServer** at 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 with 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 be 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. Create 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 any rules. 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 GigabitEthernet0/0 R2(config-if)# ip access-group 1 out

**Step 2: Configure and apply a numbered standard ACL on R3.**

a. Create 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 any rules. To permit all other traffic, create a second rule for ACL

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.**

a. 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. **Copy and paste the output of your show command in the Answer Sheet under Numbered IPV4 ACLS.**

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.

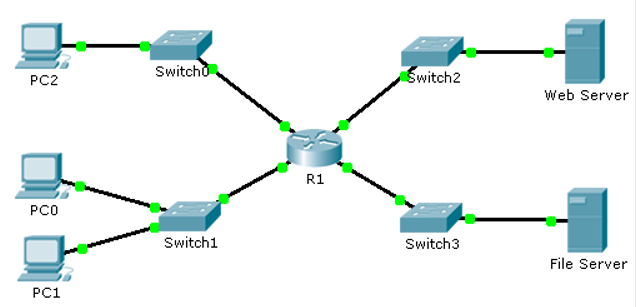
• A ping from 192.168.10.10 to 192.168.30.10 fails.

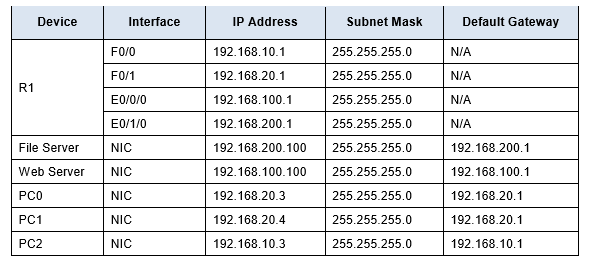
• A ping from 192.168.11.10 to 192.168.30.10 succeeds.

• A ping from 192.168.30.10 to 192.168.20.254 succeeds

**Record your ping results in Ping Table 2 on the Answer Sheet under Numbered IPv4 ACLs.**

**Named IPv4 ACLs**

****

****

**Objectives Part 1: Configure and Apply a Named Standard ACL Part 2: Verify the ACL Implementation**

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.

**Part 1: Configure and Apply a Named Standard ACL**

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

Open “Named IPV4 ACLs.pka”. All three workstations should be able to ping both the Web Server and File Server. **Record your ping results in Ping Table 1 on the Answer Sheet under Named IPv4 ACLs.**

**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 named ACL.**

a. Apply the ACL outbound on the interface Fast Ethernet 0/1.

R1(config-if)# ip access-group File\_Server\_Restrictions out

b. Save the configuration.

**Part 2: 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 fastethernet 0/1** command to verify that the ACL is applied correctly to the interface. **Copy and paste the results of your show command output in the Answer Sheet under Named IPv4 ACLs**

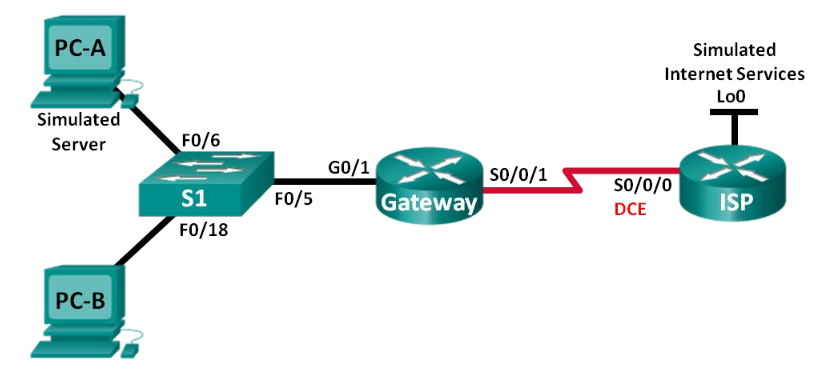
**Step 2: Verify that the ACL is working properly.**

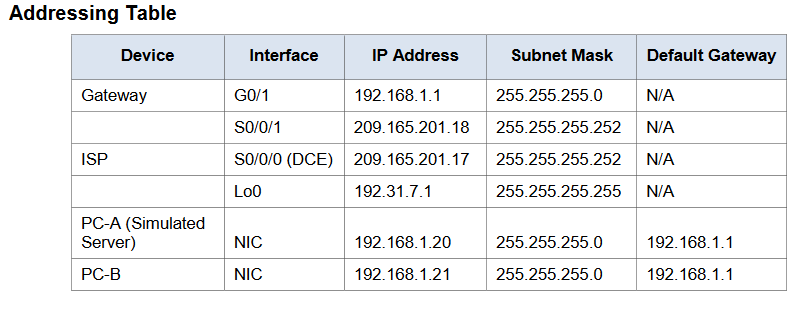
All three workstations should be able to ping the Web Server, but only PC1 should be able to ping the File Server. **Record your ping results in Ping Table 2 on the Answer Sheet under Named IPv4 ACLs.**

**Answer Reflection Q1 on your Answer Sheet.**

**\*\*\*This 3rd Packet Tracer will be done from scratch; you will not have a pre-existing Packet Tracer for this one\*\*\***

**Configuring Dynamic and Static NAT**





**Objectives**

**Part 1: Build the Network and Verify Connectivity**

**Part 2: Configure and Verify Static NAT**

**Part 3: Configure and Verify Dynamic NAT**

**Background / Scenario**

Network Address Translation (NAT) is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited. In this lab, an ISP has allocated the public IP address space of 209.165.200.224/27 to a company. This provides the company with 30 public IP addresses. The addresses, 209.165.200.225 to 209.165.200.241, are for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. A static route is used from the ISP to the gateway router, and a default route is used from the gateway to the ISP router. The ISP connection to the Internet is simulated by a loopback address on the ISP router.

**Note**: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

**Note**: Make sure that the routers and switch have been erased and have no startup configurations. If you are unsure, contact your instructor.

**Required Resources**

• 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

• 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

• 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)

• Console cables to configure the Cisco IOS devices via the console ports

• Ethernet and serial cables as shown in the topology

**Part 1: Build the Network and Verify Connectivity**

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

**Step 1: Cable the network as shown in the topology.**

Attach the devices as shown in the topology diagram, and cable as necessary.

**Step 2: Configure PC hosts.**

**Step 3: Initialize and reload the routers and switches as necessary.**

**Step 4: Configure basic settings for each router.** a. Console into the router and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on the router.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

c. Configure the host name as shown in the topology.

d. Copy the running configuration to the startup configuration.

**Step 5: Create a simulated web server on ISP.** a. Create a local user named **webuser** with an encrypted password of **webpass**.

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

b. Enable the HTTP server service on ISP.

\*\*\*This command may not work on Packet Tracer. If it doesn’t work on 7.2.2 move forward and don’t take too much time on this command. Cisco has never allowed this command to work on Packet Tracer. Document the Answer sheet and move to the next command/configuration\*\*\*

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

c. Configure the HTTP service to use the local user database.

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

**Step 6: Configure static routing.** a. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.

ISP(config)# **ip route 209.165.200.224 255.255.255.224 209.165.201.18**

b. Create a default route from the Gateway router to the ISP router.

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

**Step 7: Save the running configuration to the startup configuration.**

**Step 8: Verify network connectivity.** a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.

b. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

**Part 2: Configure and Verify Static NAT**

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

**Step 1: Configure a static mapping.**

A static map is configured to tell the router to translate between the private inside server address 192.168.1.20 and the public address 209.165.200.225. This allows a user from the Internet to access PC-A. PC-A is simulating a server or device with a constant address that can be accessed from the Internet.

Gateway(config)# **ip nat inside source static 192.168.1.20 209.165.200.225**

**Step 2: Specify the interfaces.**

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

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

Gateway(config-if)# **ip nat inside**

Gateway(config-if)# **interface s0/0/1**

Gateway(config-if)# **ip nat outside**

**Step 3: Test the configuration.**

a. Display the static NAT table by issuing the **show ip nat translations** command.

R2# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.202.130 192.168.20.254 --- ---

**Answer Q1 – Q3 on the Answer Sheet under “NAT”.**

b. From PC-A, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

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 --- ---

A NAT entry was added to the table with ICMP listed as the protocol when PC-A sent an ICMP request (ping) to 192.31.7.1 on ISP.

**Answer Q4 on the Answer Sheet under “NAT”.**

**Note**: It may be necessary to disable the PC-A firewall for the ping to be successful.

c. From PC-A, telnet to the ISP Lo0 interface and display the NAT table.

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 --- ---

**Note**: The NAT for the ICMP request may have timed out and been removed from the NAT table.

**Answer Q5 - Q6 on the Answer Sheet under “NAT”.**

d. Because static NAT was configured for PC-A, verify that pinging from ISP to PC-A at the static NAT public address (209.165.200.225) is successful.

e. On the Gateway router, display the NAT table to verify the translation.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

Icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12209.165.201.17:12

--- 209.165.200.225 192.168.1.20 --- ---

Notice that the Outside local and Outside global addresses are the same. This address is the ISP remote network source address. For the ping from the ISP to succeed, the Inside global static NAT address 209.165.200.225 was translated to the Inside local address of PC-A (192.168.1.20).

f. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat statistics**

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

**Note**: This is only a sample output. Your output may not match exactly.

**Part 3: Configure and Verify Dynamic NAT**

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

**Step 1: Clear NATs.**

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

Gateway# **clear ip nat translation \***

Gateway# **clear ip nat statistics**

**Step 2: Define an access control list (ACL) that matches the LAN private IP address range.**

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

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

**Step 3: Verify that the NAT interface configurations are still valid.**

Issue the **show ip nat statistics** command on the Gateway router to verify the NAT configurations.

**Step 4: Define the pool of usable public IP addresses.**

Gateway(config)# **ip nat pool public\_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224**

**Step 5: Define the NAT from the inside source list to the outside pool.**

**Note**: Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

Gateway(config)# **ip nat inside source list 1 pool public\_access**

**Step 6: Test the configuration.**

a. From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

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 --- ---

**Answer Q7 on the Answer Sheet under “NAT”.**

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

**Answer Q8 on the Answer Sheet under “NAT”**

b. From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as webuser with a password of webpass.

c. Display the NAT table.

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

**Answer Q9 -Q11 on the Answer Sheet under “NAT”.**

d. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat 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\_access refcount 2

pool public\_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

**Note**: This is only a sample output. Your output may not match exactly.

**Step 7: Remove the static NAT entry.**

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

a. Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

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

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

b. Clear the NATs and statistics.

c. Ping the ISP (192.31.7.1) from both hosts.

d. Display the NAT table and statistics.

Gateway# **show ip nat 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\_access refcount 4

pool public\_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 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 --- ---

**Note**: This is only a sample output. Your output may not match exactly.

**Answer Reflection Questions 1 and 2 on the Answer Sheet under “NAT”.**