Cajiga Gutiérrez Edgar Uriel 4CV3
Zepeda Flores Alejandro de Jesús

Activity 7.4.1:

Basic DHCP and NAT Configuration

Introducción

NAT

Network Address Translator, o en español traductor de direcciones de red. Su función es precisamente esa, traducir las direcciones para que sean posibles las conexiones. Cada uno de los dispositivos que hay conectados en nuestra red tienen una dirección IP única. Esto es necesario para que esté conectado a Internet y el router lo detecte y pueda funcionar con normalidad. El traductor de direcciones de red lo que hace (ya sea en el router, módem o dispositivo que sea) es proporcionar una dirección IP pública a toda esa red, a todo el conjunto de equipos.

Podemos decir que en vez de tener que asignar una dirección IP diferente para cada uno de estos dispositivos, el NAT lo que hace es dar una única para todos. Hay que tener en cuenta que NAT actúa únicamente sobre direcciones IPv4. Como sabemos existe también la opción de IPv6, más adaptados y con mejores características. En este caso no se necesitaría traducir las direcciones de red.

DHCP

El DHCP (Dynamic Host Configuration Protocol) se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales.

La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables. Este servidor, componente de cualquier router ADSL moderno, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos:

- Dirección IP única
- Máscara de subred
- Puerta de enlace estándar
- Servidores DNS
- Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol)

NOTE TO USER: This activity is a variation of Lab 7.4.1. 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**	10.1.1.1	255.255.255.252	N/A
	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
R2	**S0/0/0**	10.1.1.2	255.255.255.252	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
	Fa0/0	192.168.20.1	255.255.255.0	N/A
ISP	**S0/0/1**	209.165.200.226	255.255.255.252	N/A

Learning Objectives

Upon completion of this lab, you will be able to:

- Perform basic router configurations.
- Configure a Cisco IOS DHCP server.
- Configure static and default routing.
- Configure static NAT.
- Configure dynamic NAT with a pool of addresses.
- Configure NAT overload.

Scenario

In this lab, you will configure the DHCP and NAT IP services. One router is the DHCP server. The other router forwards DHCP requests to the server. You will also configure both static and dynamic NAT configurations, including NAT overload. When you have completed the configurations, verify the connectivity between the inside and outside addresses.

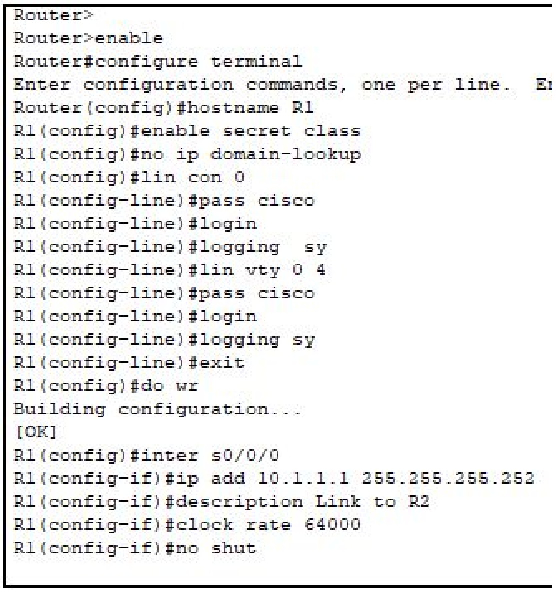
Task 1: Perform Basic Router Configurations

Step 1: Configure the routers.

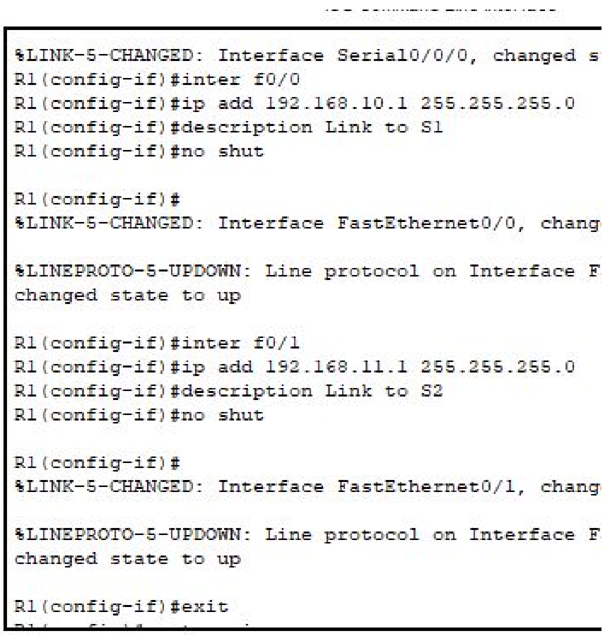
Configure the R1, R2, and ISP routers according to the following guidelines:

- Configure the device hostname.
- Disable DNS lookup.
- Configure a priviledged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for the console connections.
- Configure a password for all vty connections.
- Configure IP addresses on all routers. The PCs receive IP addressing from DHCP later in the activity.
- Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

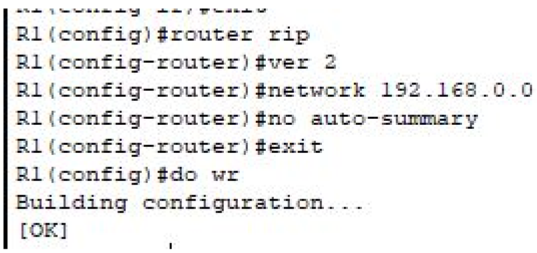
Para el R1



```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  E
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#no ip domain-lookup
R1(config)#lin con 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#logging  sy
R1(config-line)#lin vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#logging sy
R1(config-line)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#inter s0/0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#description Link to R2
R1(config-if)#clock rate 64000
R1(config-if)#no shut
```

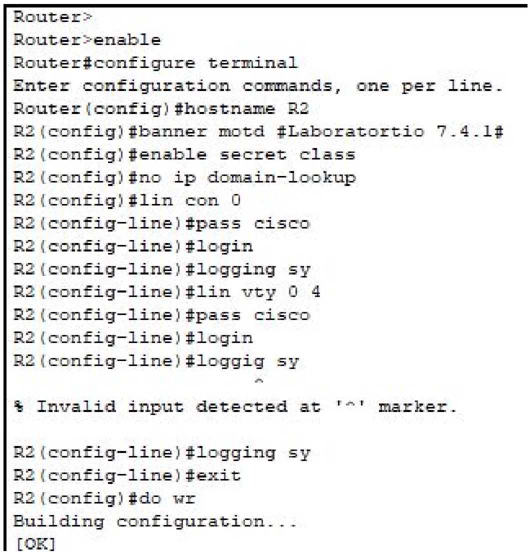


```
%LINK-5-CHANGED: Interface Serial0/0/0, changed s
R1(config-if)#inter f0/0
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#description Link to S1
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, chang

%LINEPROTO-5-UPDOWN: Line protocol on Interface F
changed state to up

R1(config-if)#inter f0/1
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#description Link to S2
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, chang

%LINEPROTO-5-UPDOWN: Line protocol on Interface F
changed state to up

R1(config-if)#exit
```

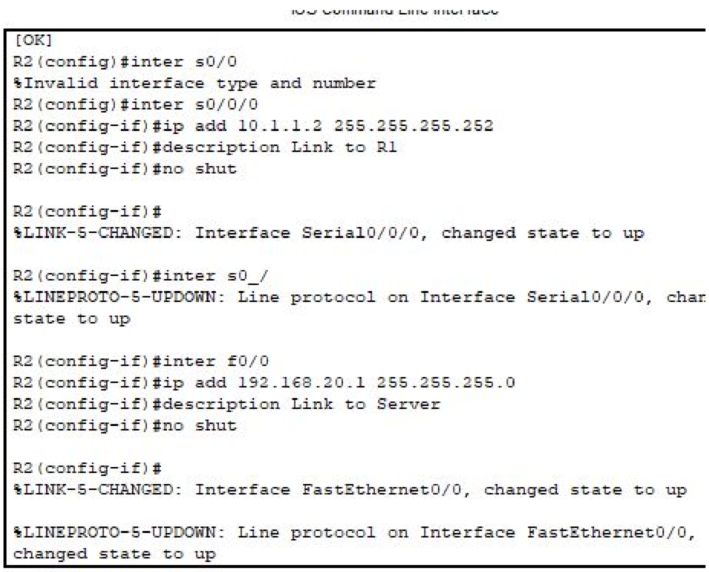


```
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#network 192.168.0.0
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#do wr
Building configuration...
[OK]
```

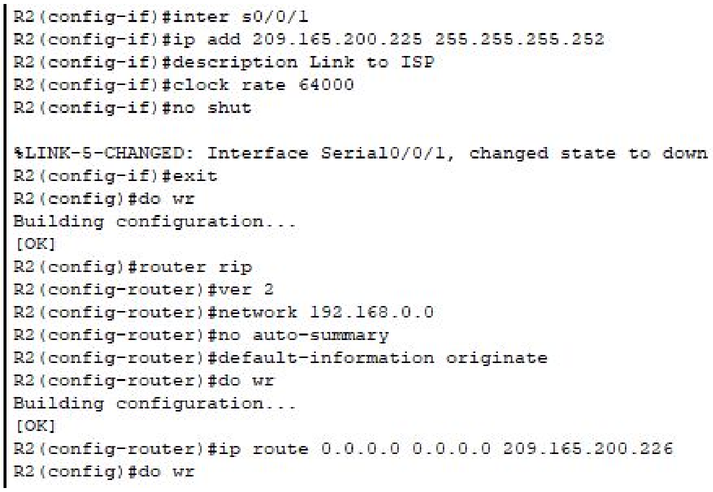
Para el R2



```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.
Router(config)#hostname R2
R2(config)#banner motd #Laboratortio 7.4.1#
R2(config)#enable secret class
R2(config)#no ip domain-lookup
R2(config)#lin con 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#logging sy
R2(config-line)#lin vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#loggig sy
                       ^
% Invalid input detected at '^' marker.

R2(config-line)#logging sy
R2(config-line)#exit
R2(config)#do wr
Building configuration...
[OK]
```

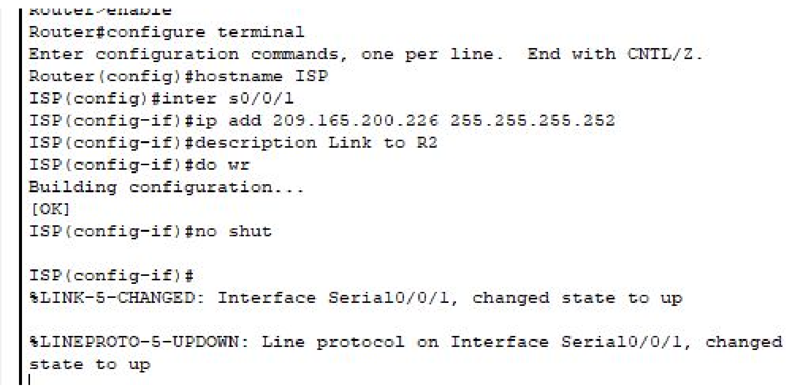


```
[OK]
R2(config)#inter s0/0
%Invalid interface type and number
R2(config)#inter s0/0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#description Link to R1
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#inter s0_/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, char
state to up

R2(config-if)#inter f0/0
R2(config-if)#ip add 192.168.20.1 255.255.255.0
R2(config-if)#description Link to Server
R2(config-if)#no shut

R2(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
```



```
R2(config-if)#inter s0/0/1
R2(config-if)#ip add 209.165.200.225 255.255.255.252
R2(config-if)#description Link to ISP
R2(config-if)#clock rate 64000
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#do wr
Building configuration...
[OK]
R2(config)#router rip
R2(config-router)#ver 2
R2(config-router)#network 192.168.0.0
R2(config-router)#no auto-summary
R2(config-router)#default-information originate
R2(config-router)#do wr
Building configuration...
[OK]
R2(config-router)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#do wr
```

Para el ISP



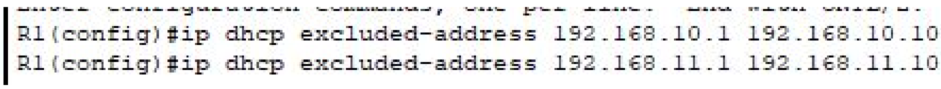
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#inter s0/0/1
ISP(config-if)#ip add 209.165.200.226 255.255.255.252
ISP(config-if)#description Link to R2
ISP(config-if)#do wr
Building configuration...
[OK]
ISP(config-if)#no shut

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

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

Task 2: Configure a Cisco IOS DHCP Server

Step 1: Exclude statically assigned addresses.

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. These IP address are usually static addresses reserved for the router interface, switch management IP address, servers, and local network printer. The **ip dhcp excluded-address** command prevents the router from assigning IP addresses within the configured range. The following commands exclude the first 10 IP addresses from each pool for the LANs attached to R1. These addresses will not be assigned to any DHCP clients.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

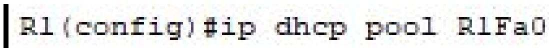


```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Step 2: Configure the pool.

Create the DHCP pool using the **ip dhcp pool** command and name it **R1Fa0**.

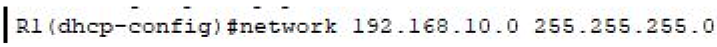
```
R1(config)#ip dhcp pool R1Fa0
```



```
R1(config)#ip dhcp pool R1Fa0
```

Specify the subnet to use when assigning IP addresses. DHCP pools automatically associate with an interface based on the network statement. The router now acts as a DHCP server, handing out addresses in the 192.168.10.0/24 subnet starting with 192.168.10.1.

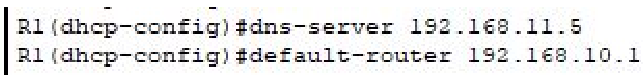
```
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
```



```
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure the default router and domain name server for the network. Clients receive these settings via DHCP, along with an IP address.

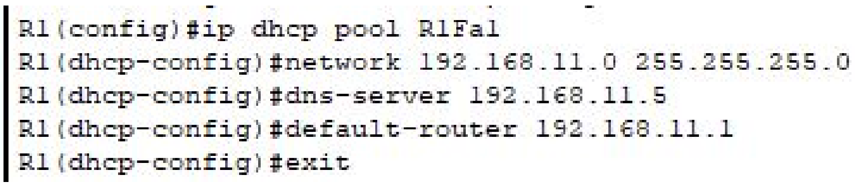
```
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.10.1
```



```
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.10.1
```

Note: There is not a DNS server at 192.168.11.5. You are configuring the command for practice only.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

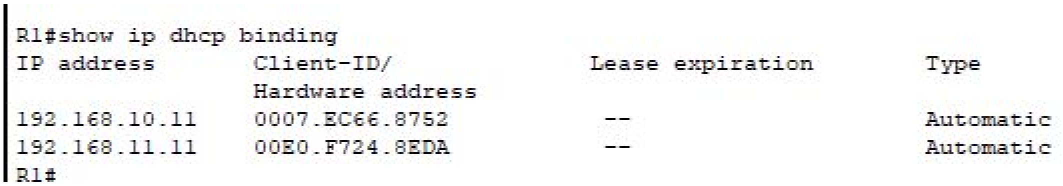


```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
R1(dhcp-config)#exit
```

Step 3: Verify the DHCP configuration.

You can verify the DHCP server configuration in several different ways. The most basic way is to configure a host on the subnet to receive an IP address via DHCP. You can then issue commands on the router to get more information. The **show ip dhcp bindingcommand** provides information on all currently assigned DHCP addresses. For instance, the following output shows that the IP address 192.168.10.11 has been assigned to MAC address 3031.632e.3537.6563. The IP lease expires on September 14, 2007 at 7:33 pm.

```
R1#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA -- Automatic
R1#
```



```
R1#show ip dhcp binding
IP address       Client-ID/           Lease expiration       Type
                 Hardware address
192.168.10.11    0007.EC66.8752        --                    Automatic
192.168.11.11    00E0.F724.8EDA        --                    Automatic
R1#
```

Task 3: Configure Static and Default Routing

Step 1. Configure static and default routes

ISP uses static routing to reach all networks beyond R2. However, R2 translates private addresses into public addresses before sending traffic to ISP. Therefore, ISP must be configured with the public addresses that are part of the NAT configuration on R2. Enter the following static route on ISP:

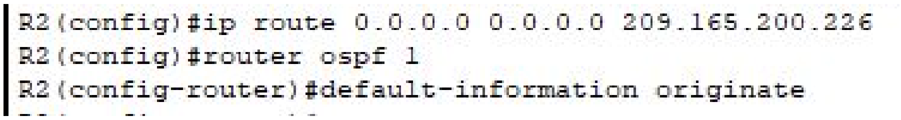
```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

This static route includes all addresses assigned to R2 for public use.

Configure a default route on R2 and propagate the route in OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```



```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

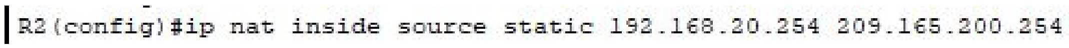
Allow a few seconds for R1 to learn the default route from R2 and then check the R1 routing table. Alternatively, you can clear the routing table with the **clear ip route *** command. A default route pointing to R2 should appear in the R1 routing table. From R1, ping the serial 0/0/1 interface on R2 (209.165.200.225). The pings should be successful. Troubleshoot if the pings fail.

Task 4: Configure Static NAT

Step 1: Statically map a public IP address to a private IP address.

The inside server attached to R2 is accessible by outside hosts beyond ISP. Statically assign the public IP address 209.165.200.254 as the address for NAT to use to map packets to the private IP address of the inside server at 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

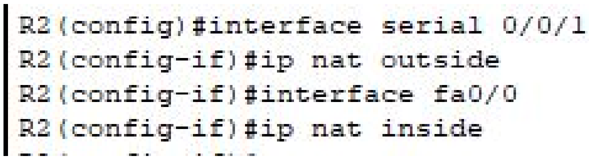


```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Step 2: Specify inside and outside NAT interfaces.

Before NAT can work, you must specify which interfaces are inside and which interfaces are outside.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```



```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Step 3: Verify the static NAT configuration.

From ISP, ping the public IP address 209.165.200.254.

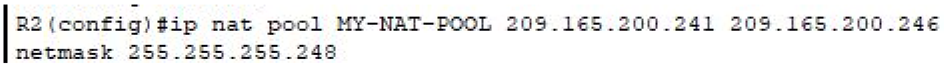
Task 5: Configure Dynamic NAT with a Pool of Addresses

While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool.

Step 1: Define a pool of global addresses.

Create a pool of addresses to which matched source addresses are translated. The following command creates a pool named **MY-NAT-POOL** that translates matched addresses to an available IP address in the 209.165.200.241 - 209.165.200.246 range.

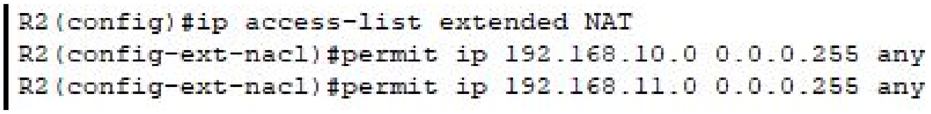
```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246
netmask 255.255.255.248
```



```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246
netmask 255.255.255.248
```

Step 2: Create a standard access control list to identify which inside addresses are translated.

```
R2(config)#ip access-list extended NAT
R2(config-std-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-std-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

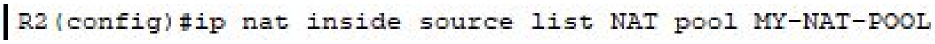


```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Step 3: Establish dynamic source translation by binding the pool with the access control list.

A router can have more than one NAT pool and more than one ACL. The following command tells the router which address pool to use to translate hosts that are allowed by the ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

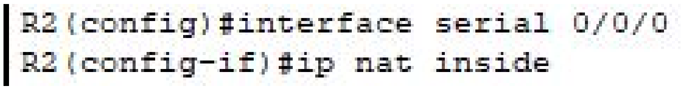


```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Step 4: Specify inside and outside NAT interfaces.

You have already specified the inside and outside interfaces for your static NAT configuration. Now add the serial interface linked to R1 as an inside interface.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```



```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Step 5: Verify the configuration.

Ping ISP from PC1 and PC2. Then use the **show ip nat translations** command on R2 to verify NAT.

```
R2#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
---  209.165.200.241    192.168.10.11      ---                ---
---  209.165.200.242    192.168.11.11      ---                ---
---  209.165.200.254    192.168.20.254     ---                ---
```

Task 6: Configure NAT Overload

In the previous example, what would happen if you needed more than the six public IP addresses that the pool allows?

By tracking port numbers, NAT overloading allows multiple inside users to reuse a public IP address.

In this task, you will remove the pool and mapping statement configured in the previous task. Then you will configure NAT overload on R2 so that all internal IP addresses are translated to the R2 S0/0/1 address when connecting to any outside device.

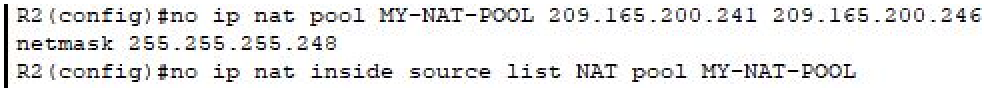
Step 1: Remove the NAT pool and mapping statement.

Use the following commands to remove the NAT pool and the map to the NAT ACL.

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246
netmask 255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

If you receive the following message, clear your NAT translations.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```



```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246
netmask 255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

Step 2: Configure PAT on R2 using the serial 0/0/1 interface public IP address.

The configuration is similar to dynamic NAT, except that instead of a pool of addresses, the **interface** keyword is used to identify the outside IP address. Therefore, no NAT pool is defined. The **overload** keyword enables the addition of the port number to the translation.

Because you already configured an ACL to identify which inside IP addresses to translate as well as which interfaces are inside and outside, you only need to configure the following:

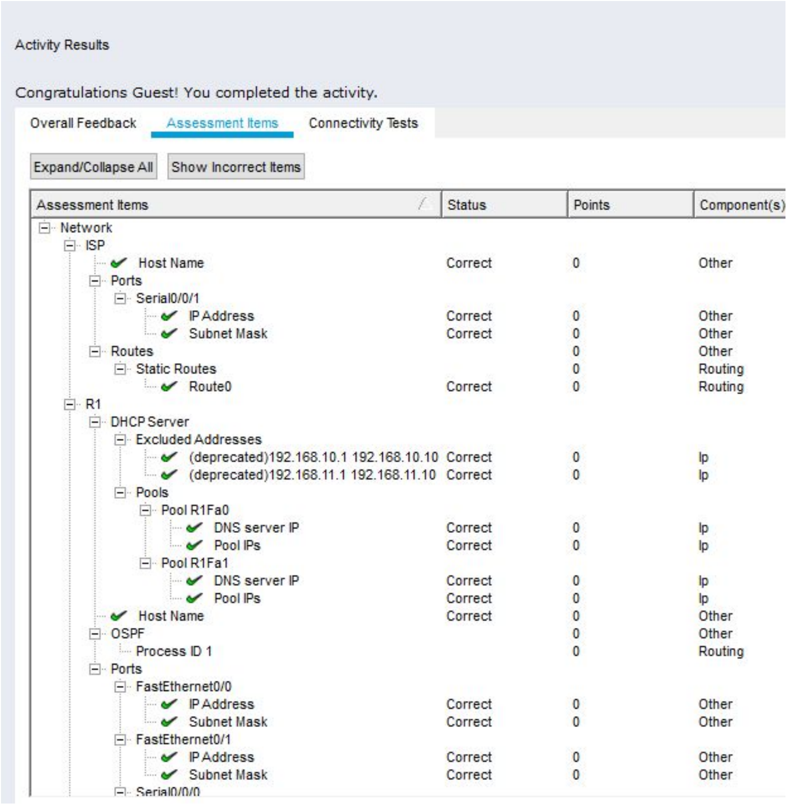
```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Step 3: Verify the configuration.

Ping ISP from PC1 and PC2. Then use the **show ip nat translations** command on R2 to verify NAT.

```
R2#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp    209.165.200.225:3    192.168.10.11:3               209.165.200.226:3
209.165.200.226:3
icmp    209.165.200.225:1024192.168.11.11:3               209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                 ---
```

Note: In the previous task, you could have added the keyword **overload** to the **ip nat inside source list NAT pool MY-NAT-POOL**command to allow for more than six concurrent users.



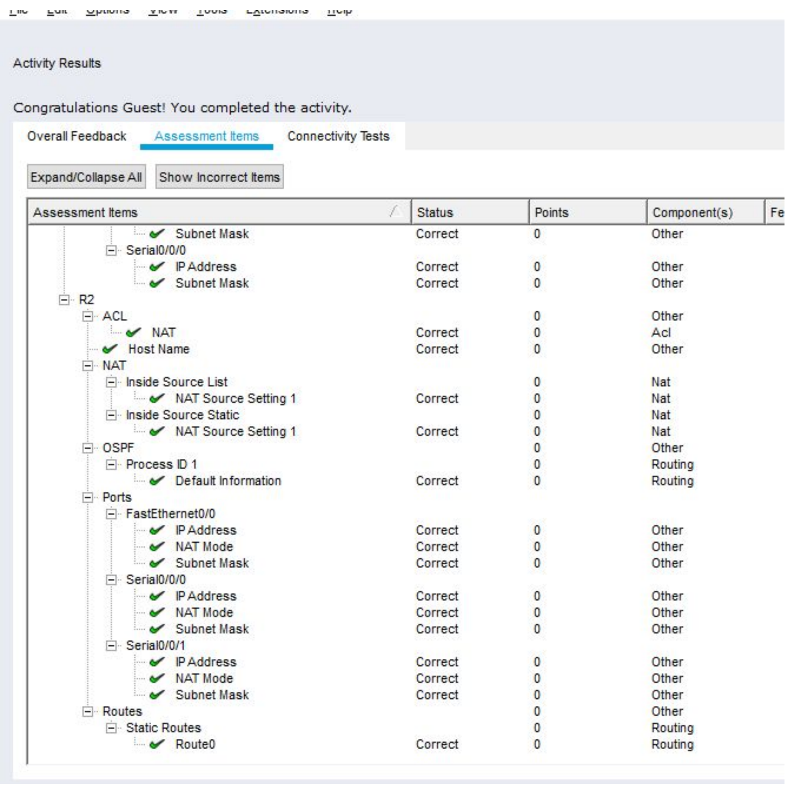
Activity Results

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)
Network			
ISP			
✓ Host Name	Correct	0	Other
Ports			
Serial0/0/1			
✓ IP Address	Correct	0	Other
✓ Subnet Mask	Correct	0	Other
Routes		0	Other
Static Routes		0	Routing
✓ Route0	Correct	0	Routing
R1			
DHCP Server			
Excluded Addresses			
✓ (deprecated)192.168.10.1 192.168.10.10	Correct	0	Ip
✓ (deprecated)192.168.11.1 192.168.11.10	Correct	0	Ip
Pools			
Pool R1Fa0			
✓ DNS server IP	Correct	0	Ip
✓ Pool IPs	Correct	0	Ip
Pool R1Fa1			
✓ DNS server IP	Correct	0	Ip
✓ Pool IPs	Correct	0	Ip
✓ Host Name	Correct	0	Other
OSPF		0	Other
Process ID 1		0	Routing
Ports			
FastEthernet0/0			
✓ IP Address	Correct	0	Other
✓ Subnet Mask	Correct	0	Other
FastEthernet0/1			
✓ IP Address	Correct	0	Other
✓ Subnet Mask	Correct	0	Other
Serial0/0/0			

Cajiga Gutiérrez Edgar Uriel 4CV3

Zepeda Flores Alejandro de Jesús



Activity Results

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Fe
✓ Subnet Mask	Correct	0	Other	
Serial0/0/0				
✓ IP Address	Correct	0	Other	
✓ Subnet Mask	Correct	0	Other	
R2				
ACL		0	Other	
✓ NAT	Correct	0	Acl	
✓ Host Name	Correct	0	Other	
NAT				
Inside Source List		0	Nat	
✓ NAT Source Setting 1	Correct	0	Nat	
Inside Source Static		0	Nat	
✓ NAT Source Setting 1	Correct	0	Nat	
OSPF		0	Other	
Process ID 1		0	Routing	
✓ Default Information	Correct	0	Routing	
Ports				
FastEthernet0/0				
✓ IP Address	Correct	0	Other	
✓ NAT Mode	Correct	0	Other	
✓ Subnet Mask	Correct	0	Other	
Serial0/0/0				
✓ IP Address	Correct	0	Other	
✓ NAT Mode	Correct	0	Other	
✓ Subnet Mask	Correct	0	Other	
Serial0/0/1				
✓ IP Address	Correct	0	Other	
✓ NAT Mode	Correct	0	Other	
✓ Subnet Mask	Correct	0	Other	
Routes		0	Other	
Static Routes		0	Routing	
✓ Route0	Correct	0	Routing	

Conclusiones:

Cajiga Gutiérrez Edgar Uriel

En esta práctica tuvimos la oportunidad de combinar dos configuraciones muy útiles, que son la DHCP y la NAT. Para conseguir estas configuraciones tuvimos asignar las configuraciones básicas para cada router, dentro de estas configuraciones retomamos OSPF, además de agregar utilidades como contraseña y asignación de IP 's para los puertos correspondientes. Ya teniendo las configuraciones básicas pudimos pasar a configurar la DHCP y la NAT, dentro de la configuración DHCP, tuvimos que dejar fuera un par de IP 's antes de crear el pool de direcciones para evitar que estas fueran tomadas para ser asignadas, y como ya sabemos las direcciones son asignadas dinámicamente facilitando la configuración de las diferentes máquinas dentro de la red. Por el lado de la configuración NAT es muy útil ya que al enviar paquetes desde redes diferentes estas pueden ser compatibles ya que el protocolo las convierte en tiempo real y con esto se consigue que los paquetes lleguen a su destino.

Zepeda Flores Alejandro de Jesús

La implementación de esta práctica nos permitió configurar automáticamente los parámetros de configuración ip en los host de una red mediante DHCP además de la importancia de este, ya que, sin un servidor DHCP, sería necesario establecer todas las IP a mano para cada dispositivo. De igual manera, se pueden indicar IP’s para que el DHCP no las considere y no las asigne, para así tenerlas reservadas. Respecto a NAT, tiene gran utilidad ya que no sólo intenta traducir el tráfico de red de varias maneras, sino que también, puede servir para desviar el tráfico de un firewall a otra máquina.

Bibliografía

[1] Jiménez, J. (2020, 31 julio). *Qué es NAT y cómo actúa en nuestra red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

[2] 1&1 IONOS Inc. (2020, 3 diciembre). *Qué es el DHCP y cómo funciona*. IONOS Digitalguide. https://www.ionos.mx/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona