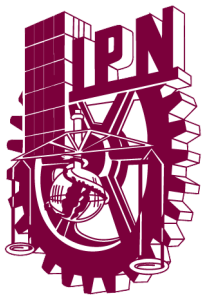


INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Actividad 12: Configuración básica de DHCP y NAT

NOMBRES:

- MACÍAS CASTILLO JOSUÉ
- OCHOA MONROY JOSÉ LUIS

GRUPO: 4CV3

UNIDAD DE APRENDIZAJE: ADMINISTRACIÓN DE SERVICIOS EN RED

PERIODO: 20-21/1

FECHA: 04 DE DICIEMBRE DEL 2020

INTRODUCCIÓN

DHCP

Algunos servicios de red se caracterizan por tener clientes efímeros; es decir, los clientes solamente consumirán el servicio durante una cantidad de tiempo relativamente pequeña, para luego desconectarse. Para evitar que este tipo de clientes agote las direcciones IP disponibles, se hace uso del Protocolo de Configuración Dinámica de Hosts (DHCP por sus siglas en inglés).

De acuerco con (ITESA, s.f.), "DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica." Esto resulta especialmente benéfico para un servicio como el mencionado arriba, o cuando los equipos terminales representan un porcentaje muy elevado de la composición de la infraestructura de red. Utilizando DHCP, los administradores ahorran tiempo al no tener la necesidad de asignar una dirección IP específica a cada host (lo cual, además de tardado, incluso podría no ser posible), y también se ofrece (indirectamente) una reutilización de direcciones IP cuando los hosts se conectan de manera temporal a la red ya que, al desconectarse, la dirección IP que estaban utilizando puede asignarse de manera automatizada a otro cliente.

"Un servidor de DHCPv4 dedicado es escalable y relativamente fácil de administrar. Sin embargo, en una sucursal pequeña o ubicación SOHO, se puede configurar un router Cisco para proporcionar servicios DHCPv4 sin necesidad de un servidor dedicado." (ITESA, s.f.).

El DHCP puede implementarse simplemente para comunicarle a un dispositivo la dirección IP estática (establecida por el administrador) que lo identificará dentro de una red, o también para asignarle de manera automática y permanente una dirección a un dispositivo. Aunado a esto, existe una opción aún más poderosa (y utilizada) que consiste en "asignar o arrendar dinámicamente una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección. Cuando caduca el arrendamiento, el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma." (ITESA, s.f.).

NAT

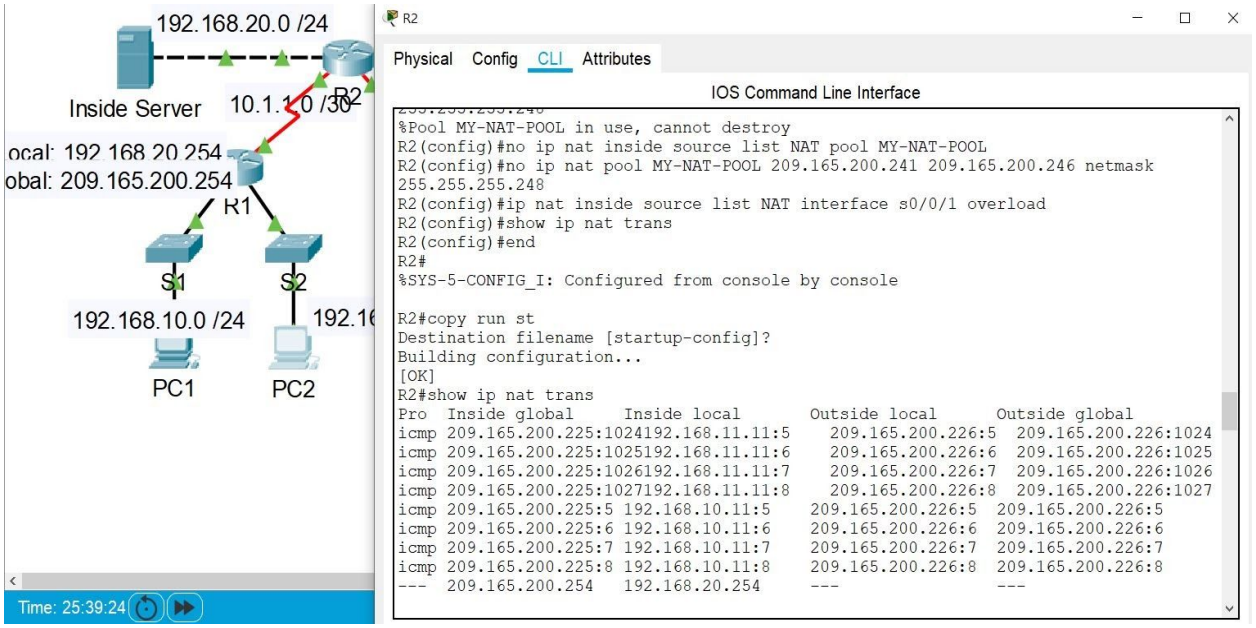
Como sabemos, el protocolo IP permite identificar a cada dispositivo dentro de una infraestructura de red. Al igual que con nuestra identidad personal, existe un riesgo cuando una identidad cibernética se encuentra al alcance de cualquier dispositivo de red.

Por otro lado, en (ITESA, s.f.) se menciona que existe un máximo teórico de 4300 millones de direcciones públicas en IPv4. Aunque parece una cantidad bastante grande, resulta escasa para la enorme y creciente cantidad de agentes digitales actualmente.

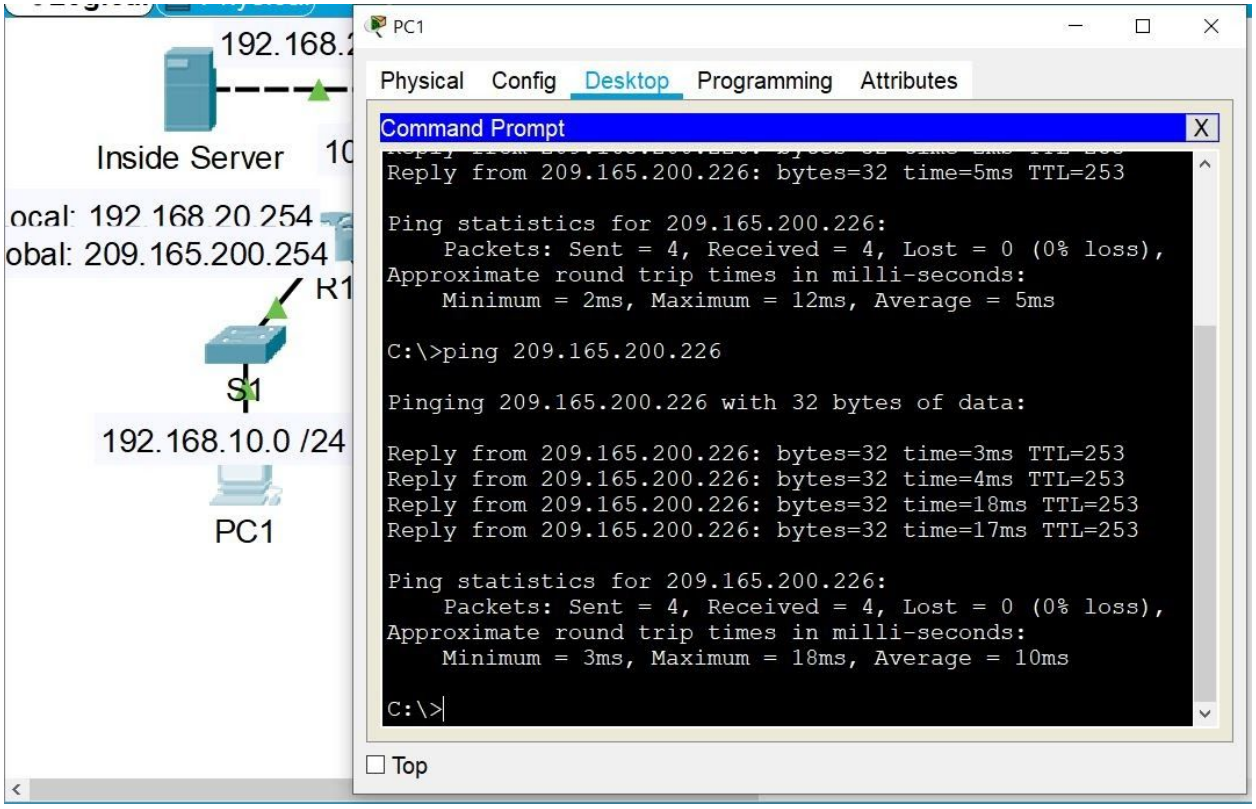
Con el objetivo de resolver ambos problemas, el IETF implementó la Traducción de Direcciones de Red (NAT, por sus siglas en inglés) junto con el establecimiento de direcciones IPv4 privadas. Esta traducción consiste en asignar direcciones privadas a cada dispositivo de una infraestructura de red de manera interna; cuando se requiere utilizar un servicio al que se accede por medio de la Internet, un router de la infraestructura interna se configura como una “frontera” que traduce cada dirección privada de un dispositivo interno en una dirección IP que forma parte del espacio público de la Internet. Por medio de NAT se resuelven los dos problemas mencionados anteriormente: existe una protección de la identidad de los dispositivos internos y se ralentiza el agotamiento de las direcciones públicas de IPv4.

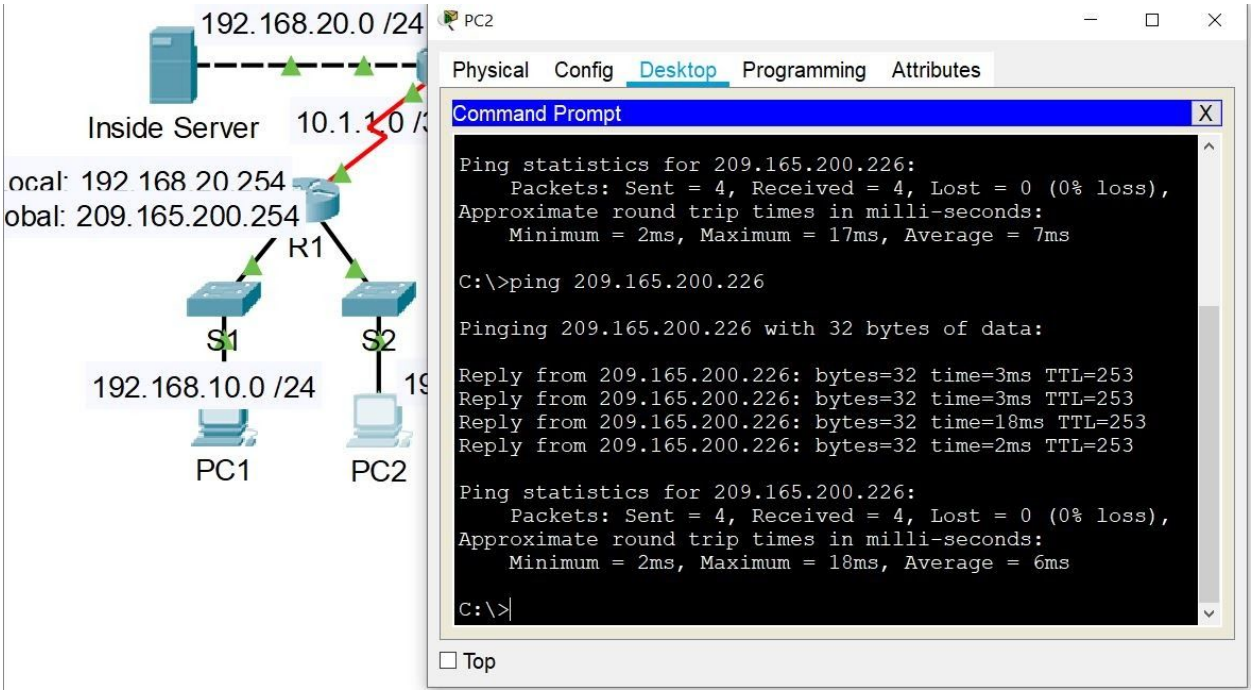
SOLUCIÓN DE LA ACTIVIDAD

Después de concluir con las actividades solicitadas por la práctica, el router R2 cumple con su función como frontera de NAT, y su funcionamiento puede apreciarse en la siguiente captura:



Como podemos observar, se utilizó la misma dirección IP pública para cada paquete enviado por ambos hosts. Lo que difiere en cada transacción es el número de puerto asignado a la dirección IP pública. A continuación se muestran los pings realizados al router ISP desde PC1 y PC2.





Por último, se incluye la configuración en ejecución de cada router en la topología, para verificar el cumplimiento de los requisitos de la actividad.

R1

```
R1#show run
Building configuration...

Current configuration : 1431 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
enable password cisco
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.11.1 192.168.11.10
!
ip dhcp pool R1Fa0
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
```

```
 dns-server 192.168.11.5
ip dhcp pool R1Fa1
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 192.168.11.5
!
ip cef
no ipv6 cef
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip classless
!
```

```
ip flow-export version 9
!
no cdp run
!
banner motd ^CSolo acceso autorizado!^C
!
line con 0
 password class
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password class
 logging synchronous
 login
line vty 5 15
 password class
 logging synchronous
 login
!
end
```

R2

```
R2#show run
Building configuration...

Current configuration : 1399 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
enable password cisco
!
ip cef
no ipv6 cef
!
no ip domain-lookup
!
```

```
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
!
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
ip nat inside source list NAT interface Serial0/0/1 overload
ip nat inside source static 192.168.20.254 209.165.200.254
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip flow-export version 9
!
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip 192.168.11.0 0.0.0.255 any
```

```
!
no cdp run
!
banner motd ^CSolo acceso autorizado!^C
!
line con 0
 password class
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password class
 logging synchronous
 login
line vty 5 15
 password class
 logging synchronous
 login
!
end
```

ISP

```
ISP#show run
Building configuration...

Current configuration : 975 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
enable password cisco
!
ip cef
no ipv6 cef
!
no ip domain-lookup
!
spanning-tree mode pvst
```

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
ip flow-export version 9
!
no cdp run
!
banner motd ^CSolo acceso autorizado!^C
!
line con 0
 password class
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password class
 logging synchronous
```

```
 login
line vty 5 15
 password class
 logging synchronous
 login
!
end
```

CONCLUSIONES

MACÍAS CASTILLO JOSUÉ

En esta práctica se vuelve a retomar la asignación dinámica de direcciones IP con ayuda del protocolo DHCP, se nos pidió configurar un servidor DHCP en este caso en un router de los 3 que aparecen en la topología, también nos pidió configurar el NAT de forma estática y dinámica e incluso se utilizo lo de la actividad anterior de una NAT overload que ya habíamos realizado con anterioridad, con esta práctica se puede ver como poco a poco todo lo que se ha realizado en el semestre se está uniendo en un solo proyecto.

OCHOA MONROY JOSÉ LUIS

En esta práctica, implementamos dos procedimientos de red que se encuentran presentes para resolver, cada uno, problemas determinados. Por un lado, con DHCP se asignan de manera temporal y automática direcciones IP para dispositivos que solamente estarán presentes en la infraestructura de red por un corto periodo, así podemos ofrecer el servicio de red a más clientes con la reutilización de direcciones. Además, NAT se implementa para proteger la identidad de los dispositivos internos de la infraestructura y para evitar que las direcciones IPv4 públicas se agoten rápidamente. Si se utiliza el DHCP en una infraestructura de red, entonces se vuelve inviable la NAT de forma estática, porque no contamos con la certeza de qué direcciones serán asignadas en un determinado momento y sería necesario mapear manualmente cada dirección posible. Aunque existe la NAT dinámica, el pool de direcciones públicas puede

llegar a volverse escaso para infraestructuras que brindan servicio a una gran cantidad de clientes de manera simultánea. Es por ello que finalmente optamos por implementar PAT, ya que cada dirección IP pública disponible en el pool puede utilizarse asignando un número de puerto distinto para cada usuario. De esta manera, es posible ofrecer una infraestructura con alta disponibilidad y con protección de las direcciones privadas que cada dispositivo posee dentro de la misma.

REFERENCIAS

- ITESA, Cisco Networking Academy. (s.f.). *Funcionamiento de DHCPv4*. Recuperado el 28 de noviembre de 2020, de: https://www.itesa.edu.mx/netacad/switching/course/module10/index.html#10.1.1.1
- ITESA, Cisco Networking Academy. (s.f.). *Funcionamiento de NAT*. Recuperado el 28 de noviembre de 2020, de: https://www.itesa.edu.mx/netacad/switching/course/module11/index.html#11.0.1.1