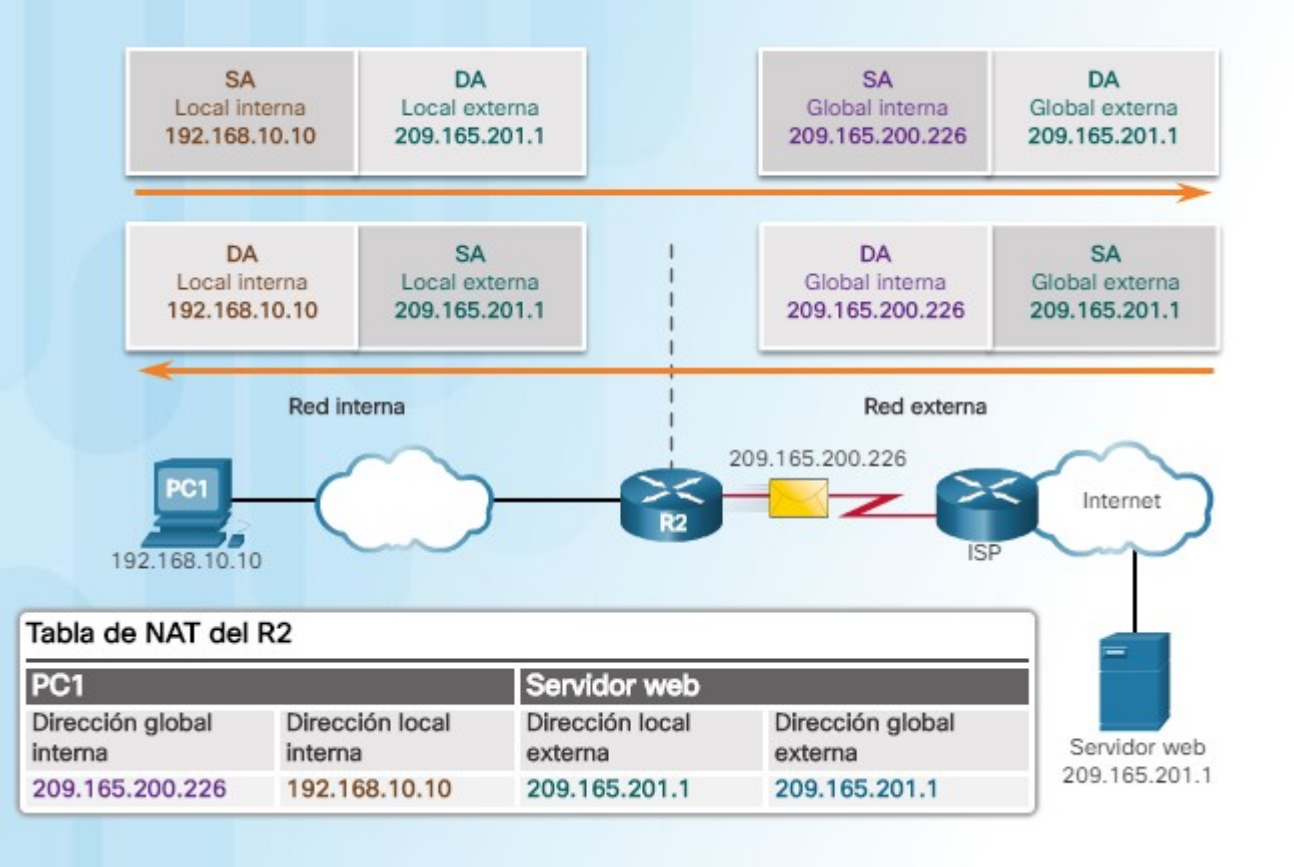
Capitulo 9. NAT(Traducción de dirección de red)

Concepto.

Permite que los dispositivos de una red que utilizan IPs privadas puedan salir a una red pública(Internet)/privada(Xunta) substituyendo la IP fuente(privada) por una IP pública(o de otra red privada) antes de mandar el paquete a la red pública(o privada). Se aplica en los routers de frontera. Cuando las respuestas regresan se realiza el proceso contrario, pero en este caso con la IP de destino.

Terminología de NAT

Siempre se aplica desde la perspectiva del dispositivo con la dirección traducida.



1. Dirección **local interna(inside local)**: la dirección de origen vista desde el interior de la red. En la ilustración, la dirección IPv4 192.168.10.10
2. Dirección **global interna(inside global)**: la dirección de origen vista desde la red externa. En el ejemplo es la IP externa del router de la empresa: 209.165.200.226
3. **Dirección global externa(outside global):** la dirección del destino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en Internet. Por ejemplo, se puede llegar al servidor web en la dirección IPv4 209.165.201.1. Por lo general, las direcciones externas globales y locales son iguales.

4. **Dirección local externa:** la dirección del destino vista desde la red interna. En este ejemplo, la PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrrutable del destino.

Tipos de NAT

NAT **estático**: A cada IP privada le corresponde una IP pública. Se utiliza para permitir el acceso desde el exterior a un servicio interno(instalado en un equipo interno). Se necesita una IP pública por cada servicio interno al que queremos acceder.

Redireccionamiento de puertos: A cada puerto externo le corresponde una IP y un puerto interno. Se utiliza para permitir el acceso desde el exterior a un servicio interno(instalado en un equipo interno). Pero aquí, al hacer NAT, además de cambiar la IP de destino(la interna) también cambiamos el puerto de destino interno. Podemos acceder a varios servicios internos(en el mismo o distintos servidores) con una única IP pública usando distintos puertos externos.

NAT dinámico: Se utiliza para que las redes internas puedan salir al exterior cuando disponemos de un grupo de IPs públicas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas. Si un dispositivo quiere salir cuando todas las direcciones del pool están siendo usadas por otros dispositivos verá denegada su petición.

PAT(NAT dinámico con sobrecarga): Con NAT dinámico los segmentos salen al exterior con el mismo puerto de origen que puso el equipo que origino la comunicación. Cuando hai sobrecarga el router cambia dicho puerto(si el router ya lo tiene ocupado) por el siguiente que tenga libre. Es igual que NAT dinámico, pero por cada dirección en el pool se pueden usar los 65,536 puertos de origen para asociar el paquete con el equipo interno que origino la comunicación. Sin embargo, la cantidad de direcciones internas a las que se puede asignar una única dirección IPv4 es aproximadamente 4000.

PAT de dirección única: los hosts internos pueden compartir una única dirección IPv4 pública(la que tiene configurada la interfaz especificada) para todas las comunicaciones externas.

Configurar NAT

1. Si es necesario, crear ACL que permita las direcciones que se deben traducir. Puede ser estándar o extendida, numerada o nombrada. Debe ser con **permit** y no olvidarse de que tiene una **denegación implícita**.

2. Si es necesario, crear pool de IPs públicas(Define un grupo de direcciones globales que se deben usar para la traducción):
   ip nat pool *"nombre pool"* "P.U.B.L inicial" "P.U.B.L final" **netmask** "M.A.S.K"

3. Dependiendo del objetivo, establecer la traducción según alguno de los siguientes tipos de NAT:

ip nat inside source	**static**		*"P.R.I.V"*		*"P.U.B.L"*			**NAT estático**
ip nat inside source	**static**	**tcp/udp**	*"P.R.I.V"*	*"Puerto Priv".*	*"P.U.B.L"*	*"Puerto públ"*	**[extendable]**	**Redireccionamiento de puertos**
ip nat inside source	**list**	*"ACL"*	**pool**	*"nombre pool"*				**NAT dinámico**
ip nat inside source	**list**	*"ACL"*	**pool**	*"nombre pool"*	**overload**			**PAT. NAT dinámico con sobrecarga**
ip nat inside source	**list**	*"ACL"*	**interface**	"ID int."	**overload**			**PAT de dirección única(Masquerade)**

[extendable] se aplica de forma automática. Permite poder redireccionar más de un puerto en el mismo router(es decir poder poner más de un comando de este tipo).

4. Especificar cual es la interfaz conectada al exterior(outside) e interior(inside)

   interface g0/0

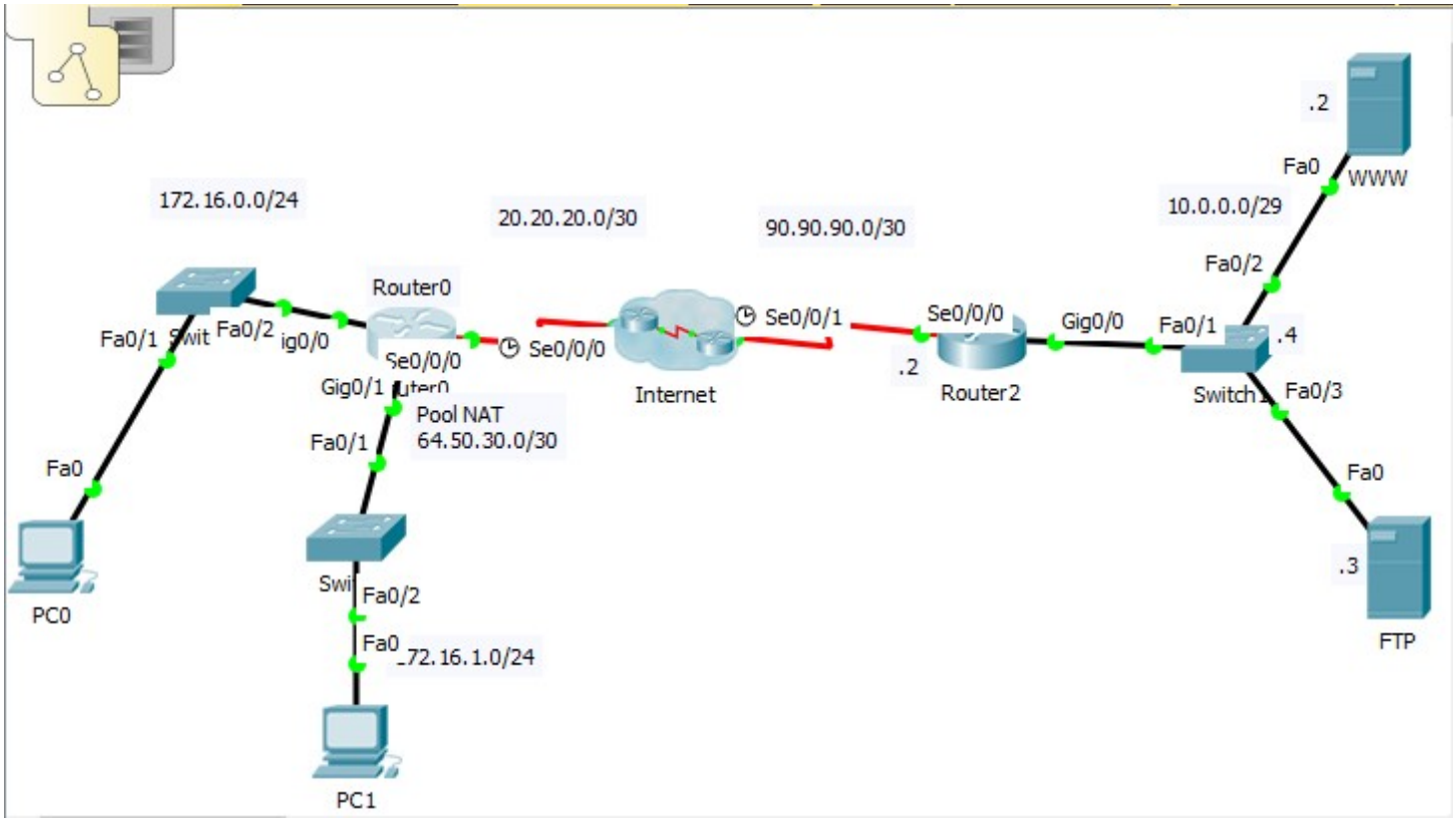
   ip nat inside

   interface s0/0/0

   ip nat outside

Ejemplos:

Basándonos en la imagen:



NAT estático(Para que el servicio FTP sea accesible desde el exterior):

Router2(config)# ip nat inside source static 10.0.0.3 90.90.90.2
interface Serial0/0/0
ip nat outside
interface GigabitEthernet0/0
ip nat inside

Redireccionamiento de puerto(Para que el servicio www y la administración del Switch1 sea accesible desde el exterior):

Router2(config)# ip nat inside source static tcp 10.0.0.2 80 90.90.90.2 10000
Router2(config)# ip nat inside source static tcp 10.0.0.4 23 90.90.90.2 1023

NAT dinámico(todos los equipos de la red 172.16.1.0/24 puedan salir a Internet):

Router1(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router1(config)# ip nat pool PUBLICAS 64.50.30.0 64.50.30.3 netmask 255.255.255.252
Router1(config)# ip nat inside source list 1 pool PUBLICAS
interface g0/1
ip nat inside
interface s0/0/0
ip nat outside

PAT. NAT dinámico con sobrecarga(todos los equipos de la red 172.16.1.0/24 puedan salir a Internet) igual que el anterior pero con sobrecarga:

Router1(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router1(config)# ip nat pool PUBLICAS 64.50.30.0 64.50.30.3 netmask 255.255.255.252
Router1(config)# ip nat inside source list 1 pool PUBLICAS overload
interface g0/1
ip nat inside
interface s0/0/0
ip nat outside

PAT de dirección única(Masquerade)(todos los equipos de la red 172.16.1.0/24 puedan salir a Internet)

Router1(config)# access-list 1 permit 172.16.0.0 0.0.0.255
Router1(config)# ip access-list extended INTERNET_PARA_TODOS
permit ip 172.16.0.0 0.0.0.255 any
Router1(config)# ip nat inside source list INTERNET_PARA_TODOS interface Serial0/0/0 overload
interface g0/0
ip nat inside

Verificar NAT

show ip nat translations

show ip nat statistics

clear ip nat statistics

clear ip nat translation *

debug ip nat

debug ip nat detailed

Cuando decodifique el resultado de este comando, observe los significados de los siguientes símbolos y valores:

•*** (asterisco):** el asterisco junto a NAT indica que la traducción se realiza en la ruta de switching rápido. Al primer paquete en una conversación siempre se aplica el switching de procesos, que es más lento. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido.

•**S=** - Este símbolo hace referencia a la dirección IPv4 de origen.

•**a.b.c.d--→w.x.y.z:** este valor indica que la dirección de origen a.b.c.d se traduce a w.x.y.z.

•**d=** - Este símbolo hace referencia a la dirección IPv4 de destino.

•**[xxxx]** - El valor entre corchetes es el número de identificación IPv4. Esta información puede ser útil para la depuración, ya que habilita la correlación con otros seguimientos de paquetes realizados por los analizadores de protocolos.

Ventajas de NAT

1. NAT conserva el esquema de direccionamiento(público) legalmente registrado al permitir la privatización de las intranets(Hogares, empresas). No derrocha IPs públicas. Utilizando NAT con sobrecarga, una IP pública por cada intranet.
2. Flexibilidad de las conexiones a la red pública. Podemos contratar varios proveedores y tener conexión de respaldo o balanceo de carga.
3. Podemos cambiar de ISP sin necesidad de modificar direccionamiento interno.
4. Proporciona seguridad. Ocultar las direcciones IPv4 de los equipos internos a las redes externas.

Desventajas de NAT

1. Se deteriora el rendimiento. Retardo y tiempo de proceso
2. Se deteriora la funcionalidad de extremo a extremo.
3. Se reduce el seguimiento IP de extremo a extremo.
4. El tunneling se torna más complicado
5. El de la conectividad TCP puede interumpirse. Ejemplo “FTP activo”(El servidor no puede iniciar el canal de datos hacia un equipo que este en una red que utilice NAT.