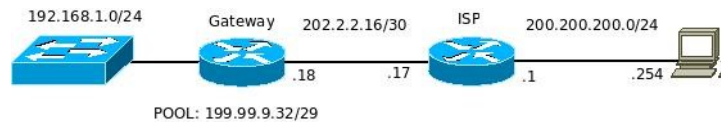


Actividad 1. Un ISP ha asignado a una empresa la dirección IP pública 199.99.9.32/29. Internamente, la LAN de la empresa utiliza la red 192.168.1.0/24. Se desea implementar NAT dinámico en el router de la empresa para poder salir hacia el exterior. La ip pública del gateway de la empresa será 202.2.2.18/30, y la ip del ISP será 202.2.2.17/30.

NOTA: El enrutamiento se realizará entre el ISP y el router gateway de la empresa mediante una ruta estática entre el ISP y el router de gateway y una ruta por defecto entre el router de gateway y el ISP.

Objetivo: Desde la LAN se debe poder acceder a una máquina en internet (al otro lado del ISP).



Sol: Asignar ips, y rutas.

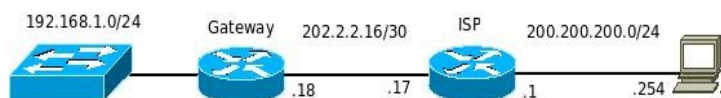
```
Gateway(config)# ip nat pool PUB-LAN 199.99.9.33 199.99.9.38 netmask 255.255.255.248
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)# ip nat inside source list 1 pool PUB-LAN
Gateway(config)# int ser 2/0
Gateway(config-if)# ip nat outside
Gateway(config-if)# int fa 0/0
Gateway(config-if)# ip nat inside
```

¿Qué pasa cuando hay más ip's privadas que públicas (en el pool)? ¿Pueden salir todos?

Actividad 2. Un ISP ha asignado a una empresa la dirección IP pública 202.2.2.18/30. Internamente, la LAN de la empresa utiliza la red 192.168.1.0/24. Se desea implementar NAT dinámico con sobrecarga (Nat overload, o PAT) en el router de la empresa para poder salir hacia el exterior. La ip del ISP será 202.2.2.17/30.

NOTA: El enrutamiento se realizará entre el ISP y el router del gateway de la empresa. Se utilizará una ruta estática entre el ISP y el router de gateway y una ruta por defecto entre el router de gateway y el ISP.

Objetivo: Desde la LAN se debe poder acceder a una máquina en internet (al otro lado del ISP).



Sol: Configurar ips y rutas.

```
Gateway(config)# access-list 1 permit 192.168.1.0 255.255.255.0
Gateway(config)# ip nat inside source list 1 interface serial 2/0 overload
Gateway(config)# int ser 2/0
Gateway(config-if)# ip nat outside
Gateway(config-if)# int fa 0/0
Gateway(config-if)# ip nat inside
```

Actividad 3. Un ISP ha asignado a una empresa la dirección IP pública 199.99.9.32/30. La empresa requiere poner en funcionamiento de manera inmediata un servidor web accesible desde el exterior. Se ha decidido implementar NAT estático. El servidor web tiene la ip privada 172.16.0.2/28 y se asociará con la ip pública 199.99.9.33.

NOTA: El enrutamiento se realizará entre el ISP y el router del gateway de la empresa. Se utilizará una ruta estática entre el ISP y el router de gateway y una ruta por defecto entre el router de gateway y el ISP.

Objetivo: Desde Internet (al otro lado del ISP), una máquina deberá acceder al servidor web de la empresa.

Sol: configurar ips y rutas.

```
Gateway(config)# ip nat inside source static 172.16.0.2 199.99.9.33
```

```
Gageway(config)# int ser 2/0
```

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

```
Gageway(config-if)# int fa 0/0
```

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

Actividad 4. Un ISP ha asignado a una empresa la dirección IP pública 199.99.9.32/28. Esto es equivalente a 14 direcciones IP públicas. Como la empresa tiene la necesidad interna de más de 14 direcciones, el responsable del departamento de Administración de Sistemas ha decidido implementar NAT.

Las direcciones 199.99.9.33 – 199.99.9.36 para la asignación estática y 199.99.9.37 – 199.99.9.46 para la asignación dinámica. Inicialmente se empleará una topología sin DMZ, de modo que los servidores estarán dentro de la LAN.

Las direcciones 199.99.9.33 y 199.99.9.34 se emplearán para direccionar a los servidores web de la empresa, con ip 192.168.1.2 y 192.168.1.3 mediante NAT estático (inicialmente la empresa solo empleará estas ips para asignación estática, reservando el resto para más adelante). Los PC's de la red local, de ip 192.168.1.0/24, emplearán el pool de direcciones 199.99.9.37-199.99.9.46 empleando NAT dinámico **con sobrecarga**.

NOTA: El enrutamiento se realizará entre el ISP y el router del gateway de la empresa. Se utilizará una ruta estática entre el ISP y el router de gateway y una ruta por defecto entre el router de gateway y el ISP. La conexión del ISP a la Internet se representará con una dirección de loopback en el router del ISP.

Objetivo 1: Desde Internet (al otro lado del ISP) se debe poder acceder a los servidores web.

Objetivo 2: Desde la LAN se debe poder acceder a Internet.

Sol: Configurar ips y rutas

```
gateway(config)# ip nat inside source static 192.168.1.2 199.99.9.33
```

```
gateway(config)# ip nat inside source static 192.168.1.3 199.99.9.34
```

```
gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

```
gateway(config)# ip nat pool acceso-publico 199.99.9.37 199.99.9.46 netmask 255.255.255.240
```

```
gateway(config)# ip nat inside source list 1 pool acceso-publico overload
```

```
Gageway(config)# int ser 2/0
```

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

```
Gageway(config-if)# int fa 0/0
```

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

Actividad 5. Configurar un router para que haga *port forwarding del puerto 80 hacia un web server local*. El router tiene la ip pública 202.2.2.18/30, y el web server tiene la ip 172.16.0.2/24. El pc externo desde el que cargaremos la página web tendrá la ip 202.2.2.17/30. Se debe comprobar que ningún paquete que se dirija a un puerto diferente al 80 llega a entrar en la red.

```
Router(config)# ip nat inside source static tcp 172.16.0.2 80 202.2.2.1 80
```

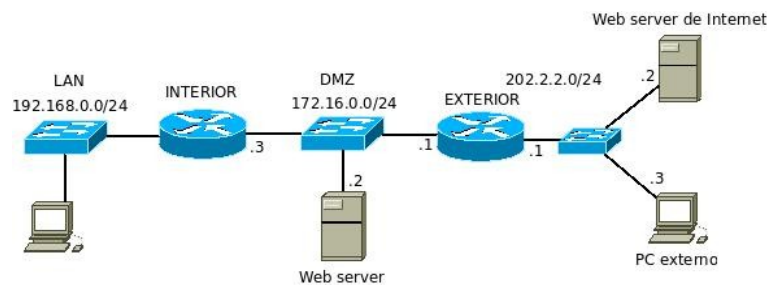
```
Gageway(config)# int fa 1/0
```

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

```
Gageway(config-if)# int fa 0/0
```

Gateway(config-if)# ip nat inside

Actividad 6. Una empresa dispone de una topología como la siguiente, consistente en una DMZ y una red local.



El router llamado “Exterior” es propiedad del ISP y proporciona unas reglas de filtrado muy básicas. El router llamado “Interior”, es propiedad de la empresa, y debe implementar las principales políticas de seguridad.

La DMZ tiene el rango de red 172.16.0.0/24. En la DMZ hay un servidor web, cuya ip es 172.16.0.2. Este servidor debe ser accesible desde Internet. Por otro lado, la LAN tiene el rango de red 192.168.1.0/24. Los usuarios de la LAN pueden salir hacia el exterior y solo podrán utilizar el servicio web, ya sea del servidor de la DMZ o de Internet. Los paquetes que entren hacia la LAN solo pueden formar parte de conexiones que se establecieron previamente desde la LAN.

Las políticas que implementa cada router son las siguientes:

Router exterior:

- Nat con sobrecarga (PAT) para que los paquetes procedentes de la LAN puedan salir hacia el exterior.
- PAT (redireccionamiento de puertos) para que al atacar al puerto TCP 80 del router se redirija al puerto 80 del servidor web de la DMZ.

Router interior:

- Permitir paquetes entrantes solo si pertenecen a una conexión preestablecida.
- Permitir paquetes salientes solo si se dirigen a un puerto 80.

Objetivo 1: desde la LAN se llega al web server de la DMZ y al web server de Internet.

Objetivo 2: Desde un PC en internet se llega al web server de la DMZ de la compañía.

```
exterior(config)# access-list 1 permit 192.168.1.0 0.0.0.255
exterior(config)# ip nat inside source list 1 interface fa 1/0 overload
exterior(config)# ip nat inside source static tcp 172.16.0.2 80 202.2.2.1 80
exterior(config)# int fa 1/0
exterior(config-if)# ip nat outside
exterior(config-if)# int fa 0/0
exterior(config-if)# ip nat inside
```

```
interior(config)# access-list 100 permit tcp any 192.168.1.0 0.0.0.255 established
interior(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
interior(config)# int fa 1/0
interior(config)# ip access-group 100 in
interior(config)# int fa 0/0
interior(config)# ip access-group 101 in
```