Clase XI

Interconexión de redes de datos (IRD101)

Agenda

- Listas de control de acceso. Parte II.
- NAT

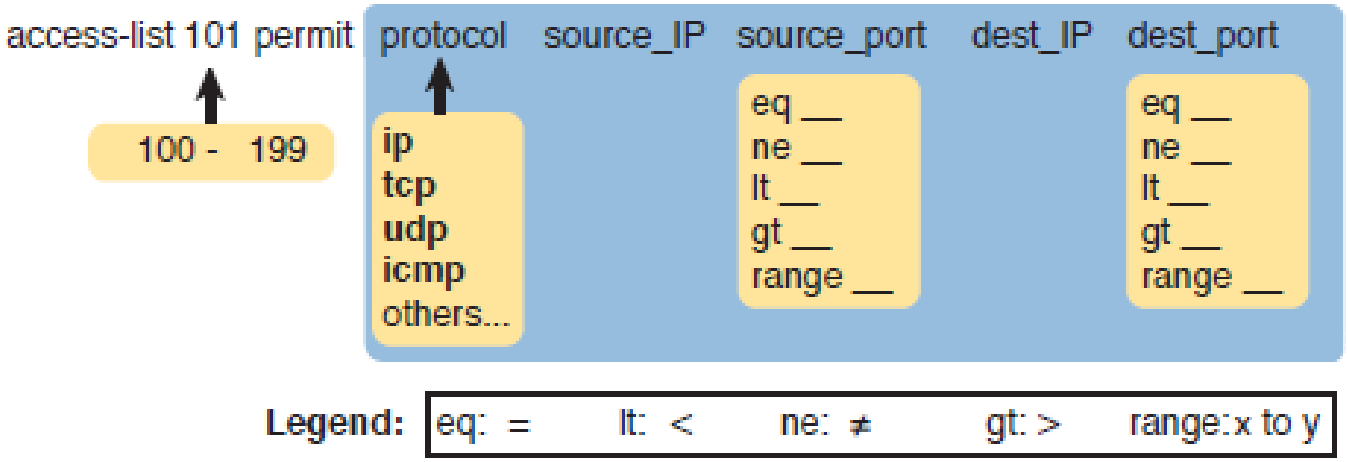
ACLs Extendidas Numeradas

Las ACLs extendidas numeradas tienen muchas similitudes comparadas con las ACLs estándar numeradas. Las ACLs extendidas numeradas también utilizan la lógica de la primera coincidencia, por esa razón el router deja de evaluar las condiciones cuando se encuentra la primera coincidencia.

Las ACLs extendidas numeradas difieren de las ACLs estándar debido a que los criterios de coincidencia del análisis del encabezado de paquete se amplían.

Una ACL extendida numerada puede examinar múltiples partes del encabezado del paquete, requiriendo que todos los parámetros del encabezado del paquete coincidan con la sentencia correspondiente de la ACL.

Sintaxis ACLs Extendidas Numeradas



access-list *access-list-number* {**deny|permit**} *protocol source source-wildcard [operator] source-protocol destination destination-wildcard [operator] destination-port*

ACLs Extendidas Numeradas

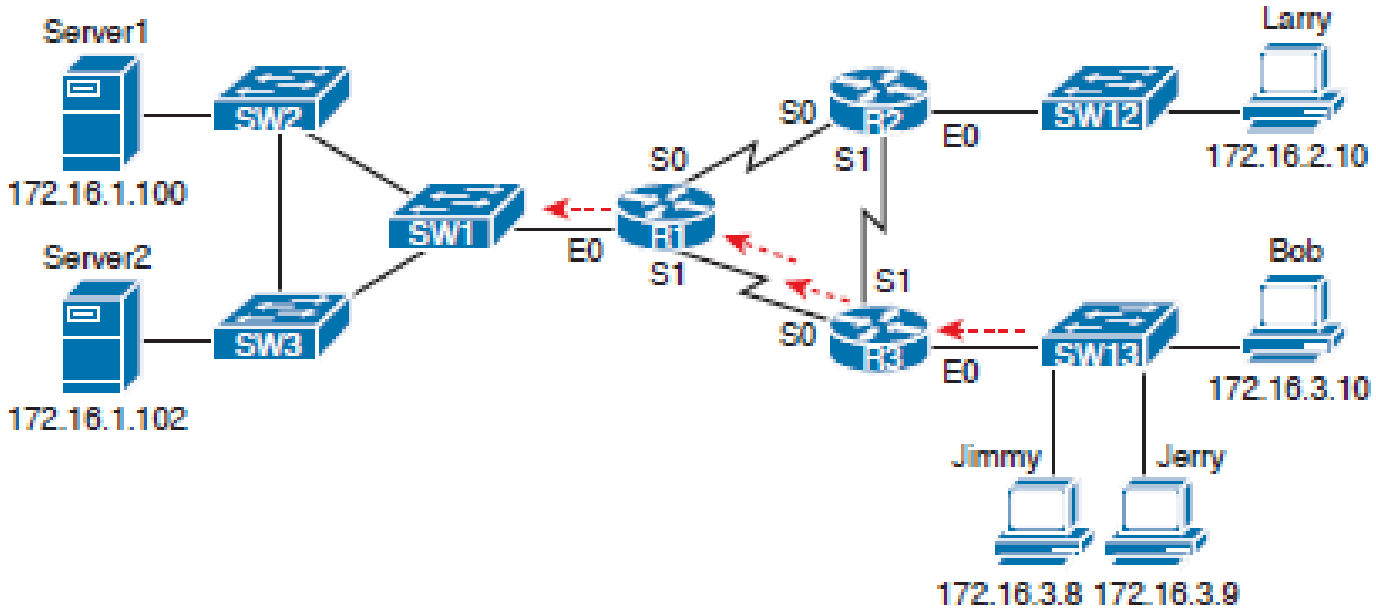
Sentencia ACL	Criterio de coincidencia
access-list 101 deny tcp any any	Cualquier paquete TCP
access-list 101 deny udp any any	Cualquier paquete UDP
access-list 101 deny icmp any any	Cualquier paquete ICMP
access-list 101 deny ip host 1.1.1.1 host 2.2.2.2	Todos los paquetes con origen 1.1.1.1 y con destino 2.2.2.2
access-list 101 deny udp 1.1.1.0 0.0.0.255 any	Todos los paquetes UDP originados desde la red 1.1.1.0/24 hacia cualquier destino.

ACLs Extendidas Numeradas

Sentencia ACL	Criterio de coincidencia
access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23	Paquetes de cualquier origen, con puertos de origen TCP mayores a 1023 y con IP de destino 10.1.1.1 con puerto destino TCP 23.
access-list 101 deny tcp any host 10.1.1.1 eq 23	Igual que el ejemplo anterior pero con cualquier puerto de origen TCP.
access-list 101 deny tcp any host 10.1.1.1 eq telnet	Igual que el ejemplo anterior pero utilizando la palabra reservada telnet en lugar del puerto de destino TCP 23.
access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any	Un paquete de origen perteneciente a la red 1.0.0.0/8, utilizando paquetes de origen de tipo UDP con puertos menores a 1023, hacia cualquier destino.

ACLs Extendidas Numeradas

Ejemplo # 1: Denegar el acceso de Bob hacia todos los servidores FTP y Larry al servidor Web



ACLs Extendidas Numeradas

Comandos aplicados en R1

```
interface Serial0
 ip address 172.16.12.1 255.255.255.0
 ip access-group 101 in
!
interface Serial1
 ip address 172.16.13.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 remark Stop Bob to FTP servers, and Larry to Server1 web
access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
```

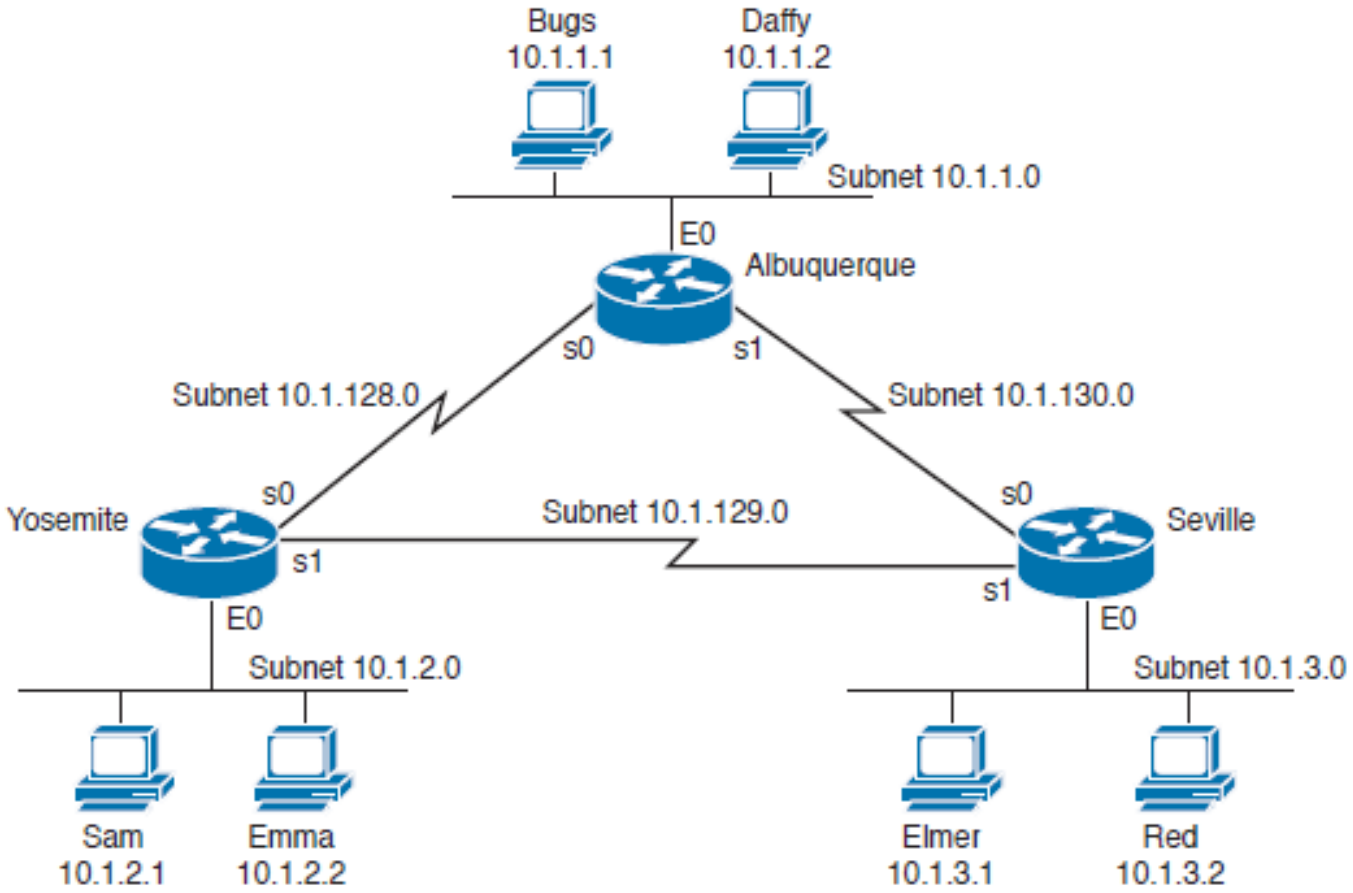
ACLs Extendidas Numeradas

Ejemplo # 2: Condiciones:

- Sam no tiene permitido el acceso a la subnet de Bugs o Daffy
- Los host en la LAN de Seville no tienen permitido el acceso a los hosts de la LAN de Yosemite.
- Cualquier otra comunicación es permitida.

ACLs Extendidas Numeradas

Topología



ACLs Extendidas Numeradas

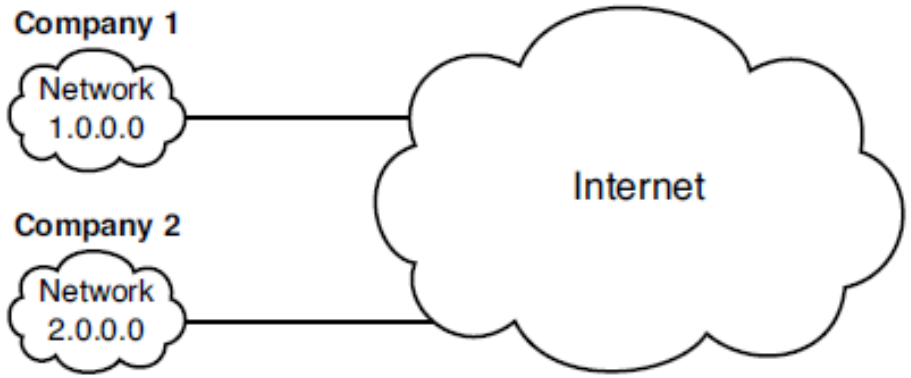
Configuraciones aplicadas en Yosemite.

```
interface ethernet 0
 ip access-group 110 in
!
access-list 110 deny ip host 10.1.2.1 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.1.2.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 110 permit ip any any
```

Redes Públicas

El diseño original de Internet requería que cualquier compañía que se conecte a Internet utilice una red IP pública registrada.

Este direccionamiento IP público registrado debería ser único a nivel global, esto garantiza que el enrutamiento en Internet se realice de forma óptima al evitar direcciones IP duplicadas.



Redes Públicas

El direccionamiento IP público puede ser:

- Estático.
- Dinámico.

También el direccionamiento IP público se encuentra asignado por regiones a nivel global y se encuentra gobernados por organismos internacionales como IANA (Internet Assigned Numbers Autority)

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Redes Privadas

El RFC 1918 presenta un set de segmentos de red como privados, por definición, estas redes privadas siguen las siguientes premisas:

- No serán asignadas a una organización como direccionamiento IP público.
- Pueden ser utilizadas por organizaciones que utilicen NAT (Network Address Translation) para enviar paquetes a través de Internet.
- Pueden ser utilizadas por organizaciones que nunca necesiten enviar paquetes hacia Internet.

Redes Privadas

El RFC 1918 define la siguiente lista para el direccionamiento IP privado.

Redes IP Privadas	Clase	Número de redes
10.0.0.0 hasta 10.255.255.255	A	1
172.16.0.0 hasta 172.31.255.255	B	16
192.168.0.0 hasta 192.168.255.255	C	256

NAT (Network Address Translation)

Es una herramienta que se encarga de cambiar o traducir direcciones IP cuando el tráfico pasa a través de un router. **PAT** es una extensión de NAT que permite que varias IPs internas utilicen una sola IP externa. Esto se consigue utilizando un identificador único por medio de un número de puerto en la IP externa para cada una de las IPs internas.

Las interfaces internas son las que pertenecen a la red privada y normalmente son del rango de la RFC 1918. No son enrutables en Internet y están clasificadas en dos tipos:

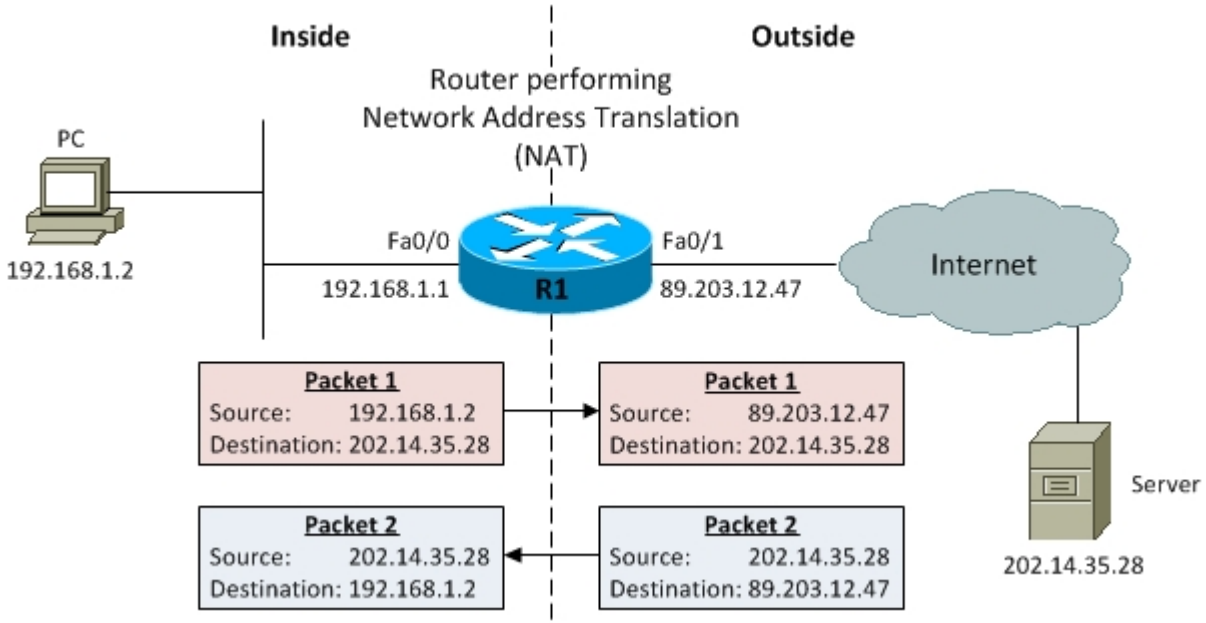
- **Interna Local:** IP asignada a un host en la red privada.
- **Interna Global:** Es como una IP privada; es vista desde la red pública.

NAT (Network Address Translation)

Las interfaces externas son las que existen en la red del proveedor o en Internet, dependiendo de la implementación pueden ser de la RFC 1918 o pueden ser direcciones de Internet enrutables. Están clasificadas en dos tipos:

- **Externa Local:** Es como la IP de un host interno; es vista en la red interna.
- **Externa Global:** IP asignada a un host externo.
- **Inside interface:** Es la interfaz del router conectada en el misma LAN que los hosts internos.
- **Outside interface:** Es la interfaz del router conectada a Internet.

NAT (Network Address Translation)



NAT Address Type	IP Address
Interna Local	192.168.1.2
Interna Global	89.203.12.47
Externa Local	202.14.35.28
Externa Global	202.14.35.28

Interface Type	ID
Inside	Fa0/0
Outside	Fa0/1

NAT (Network Address Translation)

Con la utilización de NAT es preciso que exista una dirección IP externa por cada IP interna que necesite ser traducida. Pero PAT se utilizan sockets o combinaciones de puerto y dirección IP interna, lo que permite tener hasta 65535 conexiones empleando una sola IP como dirección externa.

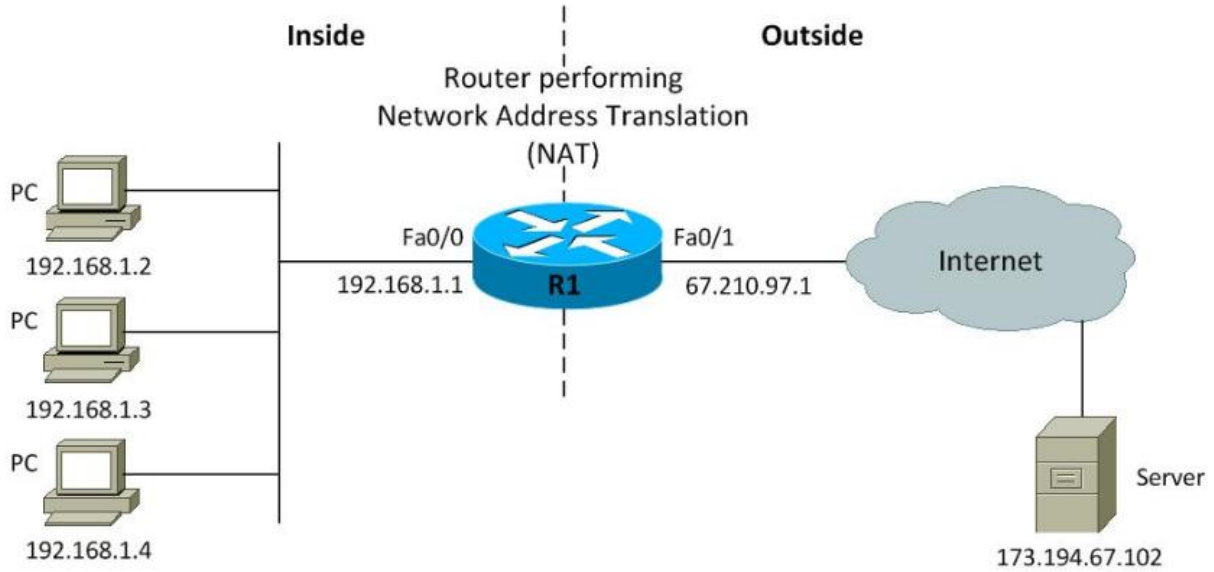
NAT Estático

Ejemplo de configuración:


```
ip nat inside source static 192.168.2.1 60.1.1.1
ip nat inside source static 192.168.2.2 60.1.1.2
ip nat inside source static 192.168.2.3 60.1.1.3
!
interface FastEthernet0/0
ip nat inside
!
interface Serial0/0
ip nat outside
```

NAT Dinámico

Ejemplo de configuración:



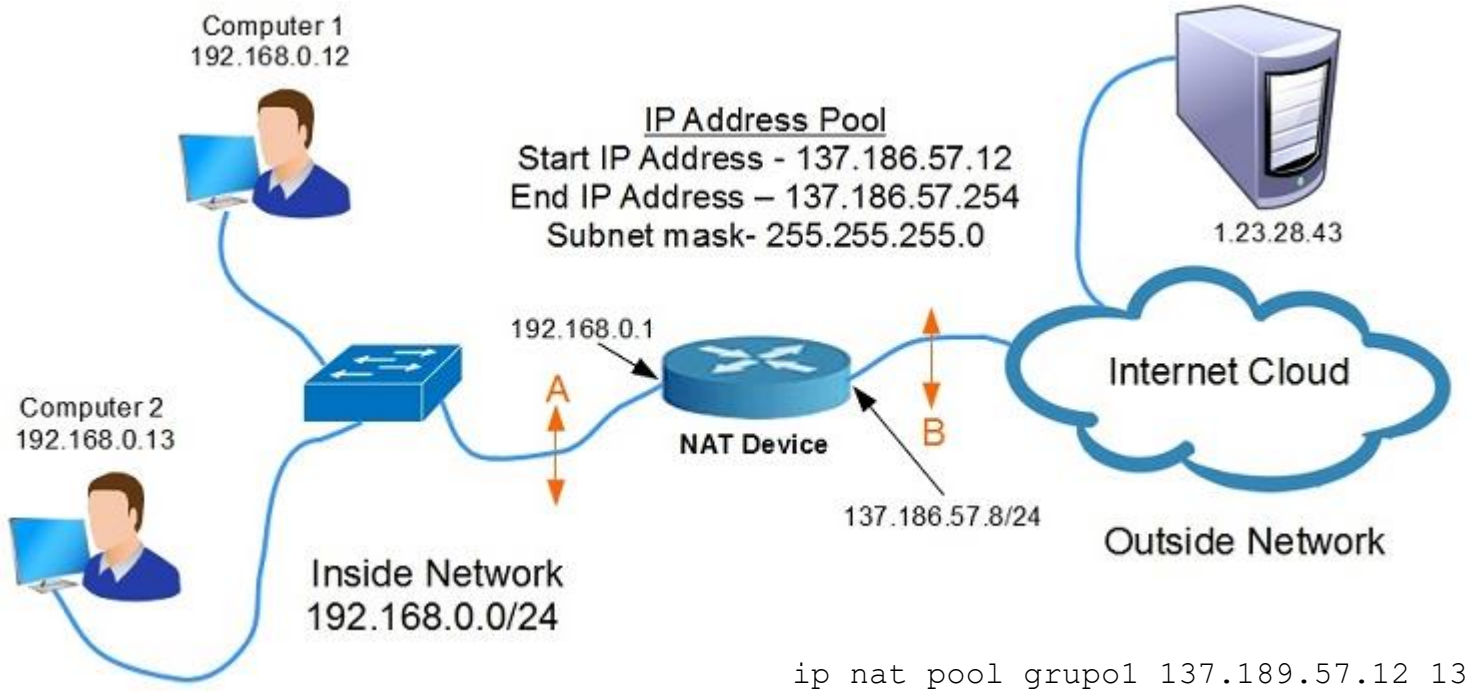
NAT Translation Table

Protocol	Inside Local IP : Port	Inside Global IP : Port
ICMP	192.168.1.2 : 18	67.210.97.1 : 18
ICMP	192.168.1.3 : 19	67.210.97.1 : 19
ICMP	192.168.1.4 : 20	67.210.97.1 : 20

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
interface FastEthernet0/1
ip address 67.210.97.1 255.255.255.0
ip nat outside
!
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet0/1
overload
```

NAT Dinámico (IP Pool)

Ejemplo de configuración:



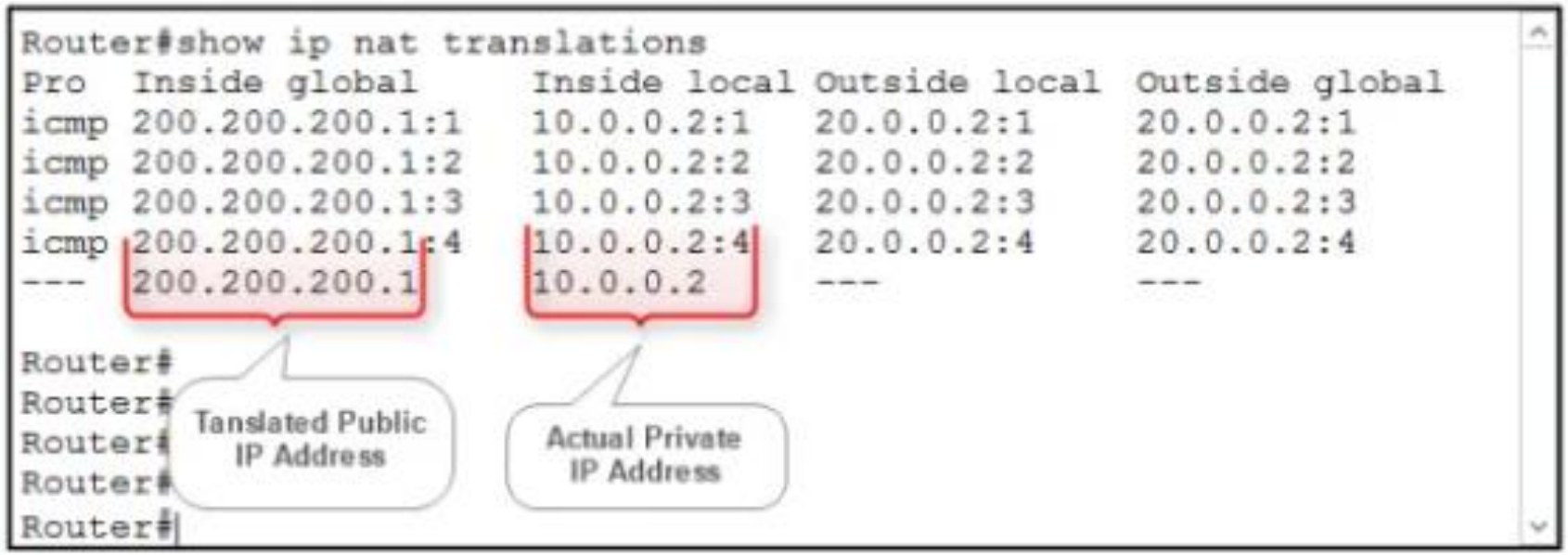

```
interface FastEthernet0/0
ip nat inside
!
interface Serial0/0
ip nat outside overload
```

```
ip nat pool grupo1 137.189.57.12 137.186.57.254 netmask 255.255.255.0
!
access-list 1 permit 192.168.0.0 0.0.0.255
ip nat inside source list 1 pool grupo1
```

Comandos de verificación

show ip nat translations

Se utiliza para verificar las entradas de traducción.



Comandos de verificación

show ip statistics

Verificar contadores y estadísticas de traducciones.

```
NAT# show ip nat statistics
Total active translations: 2 (2 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/0
Inside interfaces:
```

Comandos de resolución de problemas

```
clear ip nat translation *
clear ip nat translation inside 192.168.3.2
Clear ip nat translation outside 10.10.10.1
```

UNIVERSIDAD DON BOSCO

VITAM IMPENDERE VERO

EDUCACIÓN SUPERIOR CON ESTILO SALESIANO

AUTORIDAD DE AVIACIÓN CIVIL A.A.C. EL SALVADOR
Certificación del Técnico en Mantenimiento Aeronáutico
2016-2021

ACAAI
Agencia Centroamericana de Acreditación de Programas de Arquitectura y de Ingeniería

ISPO
INTERNATIONAL SOCIETY FOR PROSTHETICS AND ORTHOTICS
Acreditación Internacional en la carrera de Técnico en Ortesis y Prótesis
Presencial 2016-2021
A distancia 2018-2020

CdA
Comisión de Acreditación Calidad de la Educación Superior
UNIVERSIDAD DON BOSCO
ACREDITADA
2017 - 2022

Instituciones Salesianas de Educación Superior