Network Address Translation (NAT)

Carlos Vicente
cvicente@ns.uoregon.edu

NAT: Necesidad

- Escasez de direcciones IP reales
  - Esta idea es aún debatible, pero…
  - El hecho de que Internet empezó en E.E.U.U significó una repartición desbalanceada
- Dificultad en obtener bloques
  - Necesidad de NICs regionales
    - Ver LACNIC:
      - http://www.lacnic.net

NAT: Necesidad

- Seguridad
  - Los bloques RFC-1918 no son 'enrutados'
    - Los routers suelen bloquear cualquier paquete con estas direcciones en origen o destino
    - Ningún AS debe publicar estos bloques
  - Se enmascara la topología de la red interna
- Gestión
  - Protegerse de los cambios de bloques del ISP

RFC 1918

- Asigna varios bloques para uso interno y privado

  10.0.0.0 - 10.255.255.255 (10/8 prefix)

  172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

  192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

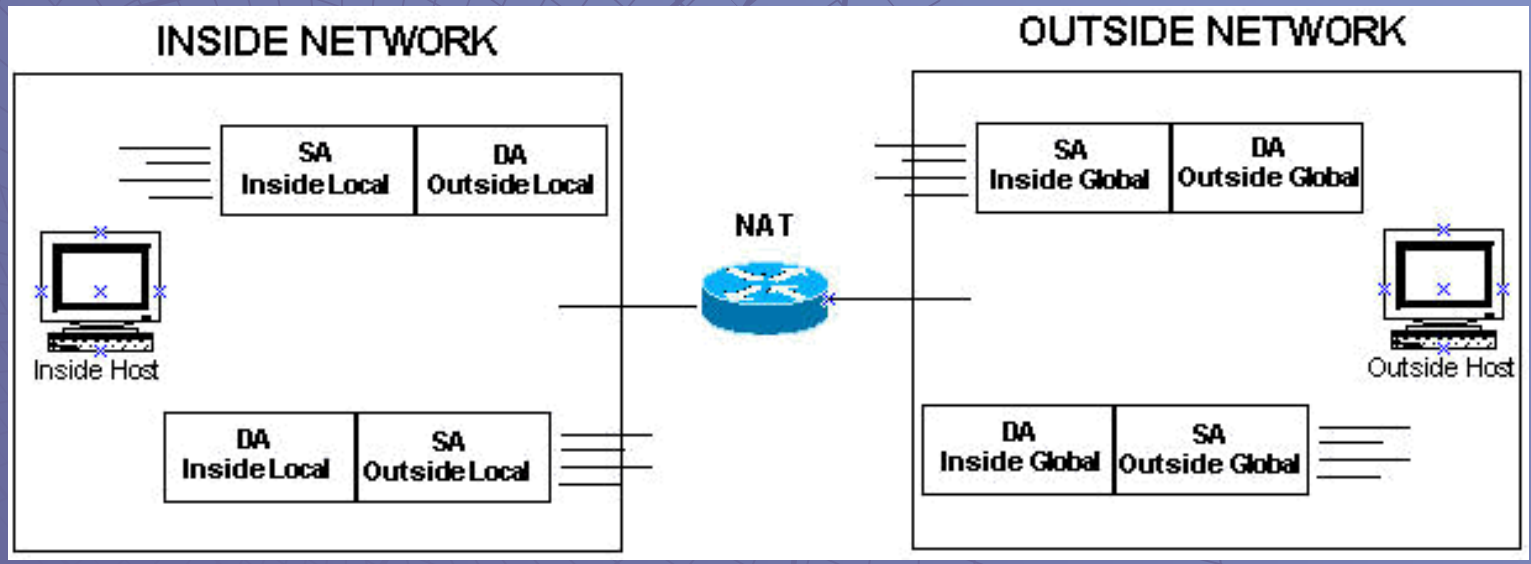
- ¿Consecuencias de usar o no usar estos bloques?

Funcionamiento

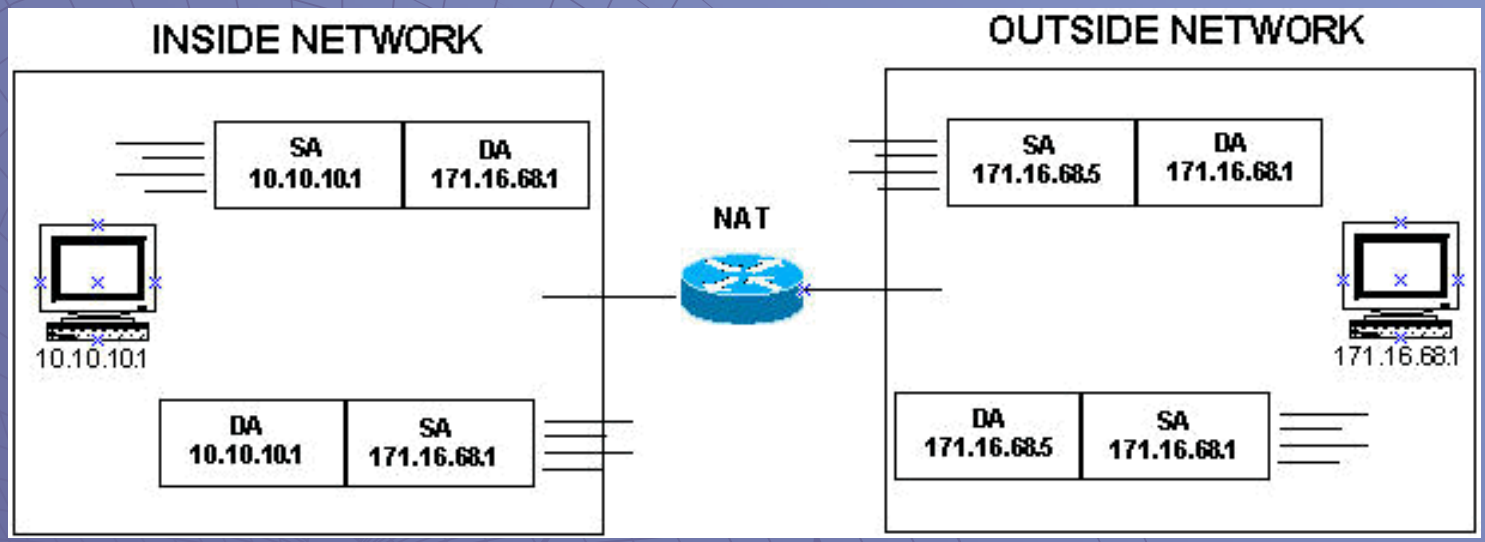
- NAT básico
  - Una sola dirección pública
    - El router recibe el paquete y cambia la dirección origen (O) con la dirección pública (P) y reenvía el paquete al destino (D)
    - Inserta una entrada en su tabla dinámica
      - D -> O
    - Recibe el paquete de vuelta, busca la dirección remota en su tabla (D), cambia la dirección destino (P) por la original (O)

Terminología (Cisco)

- Inside Local, Inside Global
- Outside Local, Outside Global



Terminología (Cisco)



Funcionamiento

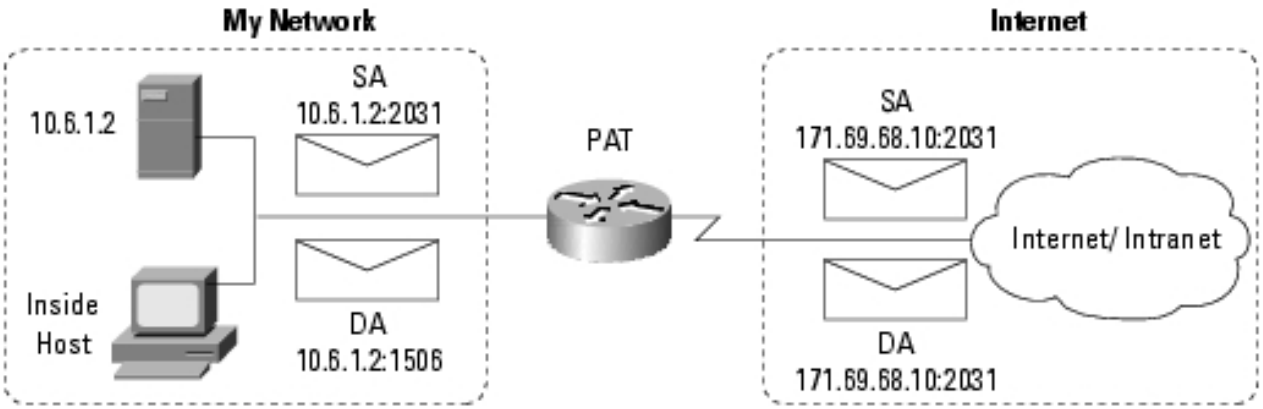
- Problema:
  - Qué pasa si dos máquinas locales acceden a la misma máquina remota simultáneamente?
    - La tabla contendrá
      - D -> O_1
      - D -> O_2
    - A quién le devuelvo el paquete?

NAT múltiple

- Utiliza un rango de direcciones públicas para traducir
  - Cada nuevo paquete saliente con dirección origen O_1, 0_2…,O_n es traducido en P_1, P_2…,P_n etc
- Permite que *n* máquinas internas accedan a un mismo servidor simultáneamente

NAPT/PAT

- NAPT = Network Address Port Translation
- Otra solución es agregar más información a la tabla
  - Traducir también los números de puerto origen y destino



Port Address Translations (PAT) extends NAT form "1 to 1"
to "many-to-1"by associating the source port with each flow

NAPT/PAT

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80

PAT (Port Address Translation) includes ports in addition to IP address
Many-to-one translation
Maps multiple IP addresses to 1 or a few IP addresses
Unique source port number identifies each session
Conserves registered IP addresses
Also called NAPT in IEFTF documents

- NAT múltiple y NAPT se pueden combinar
  - Cisco utiliza el comando 'overload', con el que el router utiliza otra dirección del rango sólo si ha mapeado todos los puertos de la primera dirección en su tabla

NAT/PAT estático

- Se configura una relación fija entre una dirección privada y una pública
  - Generalmente sólo es necesario cuando se quiere proveer un servicio desde la red interna
  - Los puertos no tienen que coincidir necesariamente
    - Ej: 192.168.0.5:80 -> 203.132.165.9:8080
- Los firewalls suelen usar esta técnica

Limitaciones

- Protocolos que incluyen direcciones IP y números de puerto en su campo de datos
  - ICMP (Destination Unreachable)
  - FTP (incluye dirección y puerto del cliente para conexión de datos)
  - H.323, SIP (videoconferencia, VOIP)
  - RealAudio
  - SNMP en algunos casos
  - X-Windows
- Las nuevas implementaciones resuelven algunos de éstos
  - El router tiene que inspeccionar el contenido del paquete IP (más carga de procesamiento)

Problemas con cifrado

- TCP header checksum
  - Direcciones IP en su pseudo-cabecera
    - Calcula un checksum de ésta
  - Como las direcciones cambian, el checksum tiene que ser recalculado
- Qué pasa si está cifrado?
  - Caso SSH/SSL vs. IPSEC end-to-end

Consideraciones

- Decisión de usar NAT debe tomar en cuenta la relación costo/beneficio
  - Qué tanto pesan las ventajas obtenidas en comparación con
    - Complejidad
    - Incapacidad para proveer ciertos servicios
    - Gestión más difícil
    - Descontento de usuarios

Más información

- Documentos IETF (www.ietf.org)
  - RFC-1918: Address Allocation for Private Internets
  - RFC-1631:The IP Network Address Translator (NAT)
  - RFC-2993: Architectural Implications of NAT
  - RFC-3027: Protocol Complications with the IP Network Address Translator
- The Trouble with NAT, Internet Protocol Journal (Cisco)
  - http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac182/about_cisco_ipj_archive_article09186a00800c83ec.html