UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

Xarxes de Computadors

Lab 4
Laboratorio de ACLs y NAT con Cisco IOS

José Suárez-Varela

jsuarezv@ac.upc.edu

Conceptos básicos

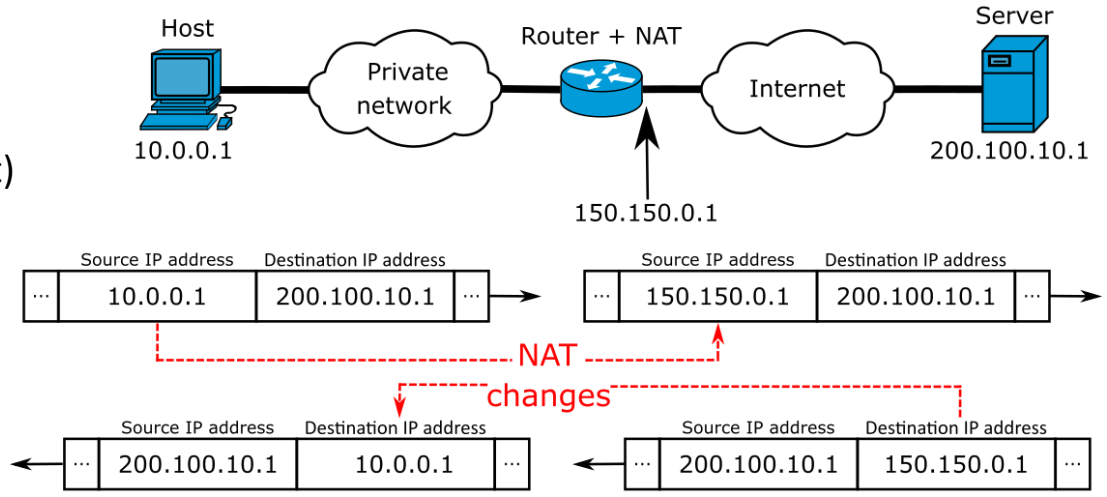
NAT (Network Address Translation):

- **Uso típico → Traducción de IPs de pública a privada (y viceversa)**

Tipos:

- **NAT estático** → Traducción fija (e.g., servidores con IP fija)
- **NAT dinámico o por puertos (PAT)** → Traducción temporal
  Según IPs públicas disponibles
  (e.g., permitir acceso a Internet)

PAT → Reutilizar IP pública para varias IPs privadas



Nomenclatura Cisco IOS:

- **Dirección "local"** → IP en la red local (típicamente privada)
- **Dirección "global"** → IP en la red externa (típicamente pública)

Conceptos básicos

ACLs (Access Lists):

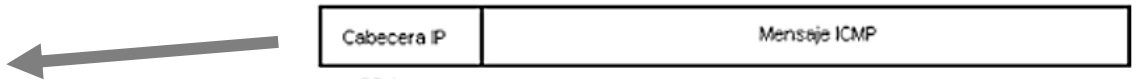
- **ACLs para TCP/IP** → Filtrado por IPs y puertos (UDP ó TCP)
- Cada Interfaz puede tener una ACL de entrada y otra de salida (ACL in/out)
- ACL → Secuencia de instrucciones (match + acción)
- Se ejecuta la primera acción que haga "match" (importa el orden!)

Por ejemplo no es lo mismo estas dos líneas de una ACL:

- Si el paquete es icmp recházalo
- Si el paquete es ip acéptalo

que la secuencia:

- Si el paquete es ip acéptalo
- Si el paquete es icmp recházalo



Conceptos básicos

ACLs (Access Lists):

- **La última regla (por defecto) es rechazarlo TODO!**

Dentro de las listas de acceso TCP/IP hay dos tipos de ACLs

- Listas de acceso IP estándar (1-99) → Sólo *source* IPs
- Listas de acceso IP extendidas (100-199) → Src-dst IPs + IP proto + src-dst ports (puertos sólo para TCP/UDP)

- En lugar de máscaras se usan *wildcads* (notación inversa):

Mask=255.255.255.0 → *wildcard* = 0.0.0.255

Wildcard = 0.0.0.0 → *"host"*

Wildcard = 255.255.255.255 → "any"

Comandos básicos

- NAT estático:

  R# *configure terminal*

  R(config)# *ip nat inside source static <local-ip> <global-ip>* → Para una sóla IP

  ----- ó ----

  R(config)# *ip nat inside source static network <local-net> <global-net> <mask>* → Rango de IPs (red); mismo # de IPs (misma máscara)

  R(config)# interface <if_name> → *Interfaz de red local (privada)!*

  R(config-if)# ip nat inside

  R(config-if)# exit

  R(config)# interface <if_name2> → Interfaz de red global (pública)!

  R(config-if)# ip nat outside

Comandos básicos

- NAT dinámico ó PAT:

R# *configure terminal*

R(config)# *ip nat pool <name> <start-ip> <end-ip> {netmask <mask> | prefix-length <prefix-length>}* → Se define el conjunto de IPs públicas*

(config)# *access-list <acl#> permit <IP_src> <wildcard>* → ACL para identificar a los host (IPs privadas) a los que se aplica NAT

R(config)# *ip nat inside source list <acl#> pool <name> [overload]* → *Opción overload* solo para PAT (en lugar de dinámico)*

R(config)# *interface <if_name>* → Interfaz de red local (privada)!

R(config-if)# *ip nat inside*

R(config-if)# *exit*

R(config)# *interface <if_name2>* → Interfaz de red global (pública)!

R(config-if)# *ip nat outside*

***Si no hay un conjunto de IPs públicas (pool), se puede usar directamente la IP de la interfaz externa:**

R(config)# ip nat inside source list <#acl> ***interface <if_name>*** *overload*

Comandos básicos

- ACL standard:

  R# *configure terminal*

  R(config)# *access-list <acl#> {deny|permit} {@IPsource WildcardMask | host @IPsource | any}*

  ... → *(Secuencia de reglas;* ***Nota: la última es "access-list acl# deny any" por defecto****)*

  R(config)# *interface <if_name>*

  R(config-if)# *ip access-group <acl#> {in|out}* → *(in = tráfico de entrada; out = tráfico de salida)*

- ACL extendida:

  R# *configure terminal*

  R(config)# *access-list <acl#> {deny|permit} <protocol> {@IPsource WildcardMask | host @IPsource | any} [operador port_source] {@IPdest WildcardMask | host @IPdest | any} [operador port_dest] [established]* → ***"Operador" = {lt,gt,eq,neq} (para puertos)***

  ... → *(Secuencia de reglas;* ***Nota: la última es "access-list acl# deny ip any any" por defecto****)*

  R(config)# *interface <if_name>*

  R(config-if)# *ip access-group <acl#> {in|out}* → *(in = tráfico de entrada; out = tráfico de salida)*

Comandos básicos

- Comandos de consulta de estado y debugging:

ACLs:

R# *show ip interface <if_name>* → Muestra si hay una ACL en la interfaz indicada

R# *show access-lists* → ACLs definidas

NAT:

R# show ip nat translations → Comprobar configuración NAT

R# debug ip nat → Ver traducciones realizadas en tiempo real; (**R# no debug ip nat** → para detenerlo)

R# clear ip nat translation * → Borra traducciones en la tabla NAT (**No borra la configuración NAT!**)

Genérico:

R# *show ip interface brief* → Comprobar asignación de IPs y estado interfaces

R# *show running-config* → Comprobar configuración general en el router

Realización práctica

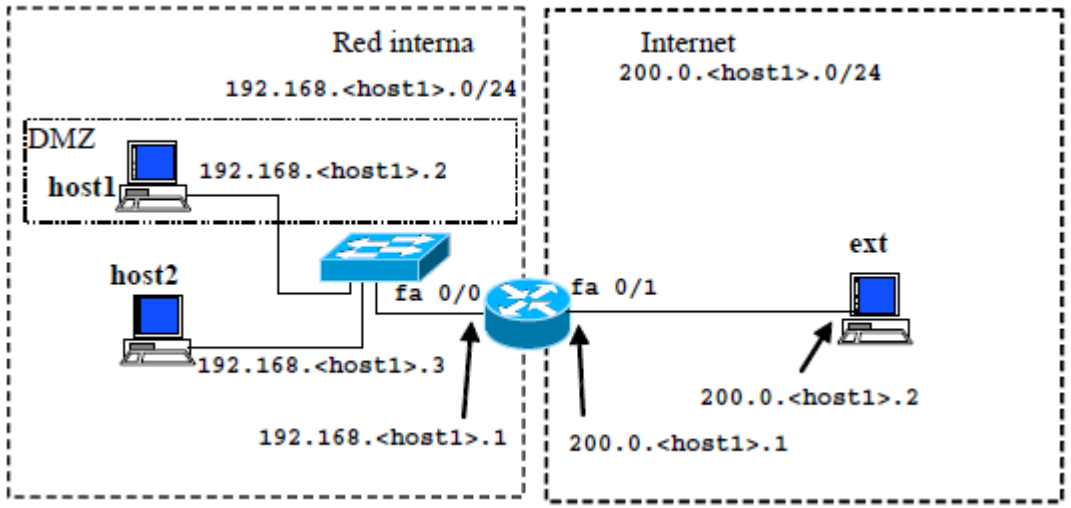
Pasos a seguir

1) Montar esquema de red (routers 1841 con interfaz serie WIC-1T; Switches 2950-24)
2) Configurar IPs y gateway en PCs (menu "config")
3) Configurar IPs en routers
4) Configuración de NAT y ACLs

Nota: Ficheros Packet Tracer con práctica resuelta en el Racó FIB (parte NAT y parte ACLs)

Realización práctica

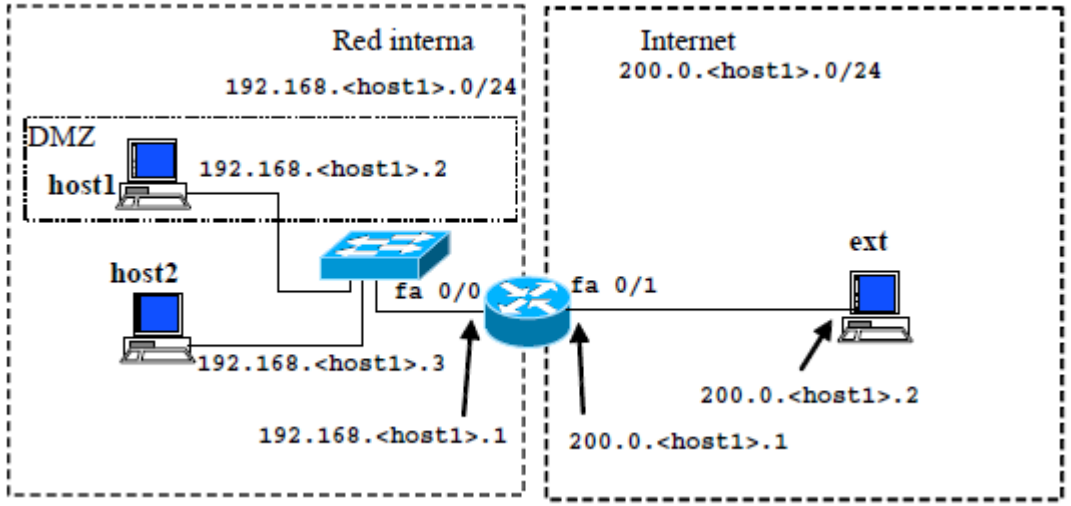
Parte 1: NAT



- No añadir gateway por defecto en PC "ext"! → Representa un host genérico de Internet
- Conectividad *host1/2-ext* → *# ping <IP_dest>*
- *No debe haber conectividad directa entre ext y hosts de la red interna*

Realización práctica

Parte 1: NAT



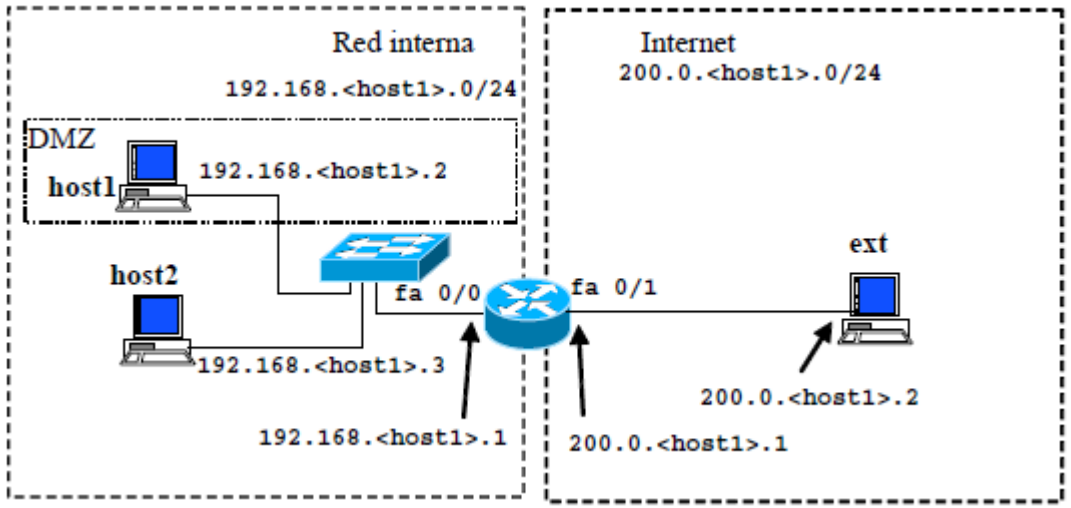
- *Acceso de red interna a Ext:*

  *PAT en la interfaz fa0/1! (**no IP pool**) → **R(config)#** ip nat inside source list <acl#> interface <if_name> overload*

- *Wildcard* → Notación inversa de la máscara!
- *R# show ip nat translations → Ver tabla dinámica de traducciones*

Realización práctica

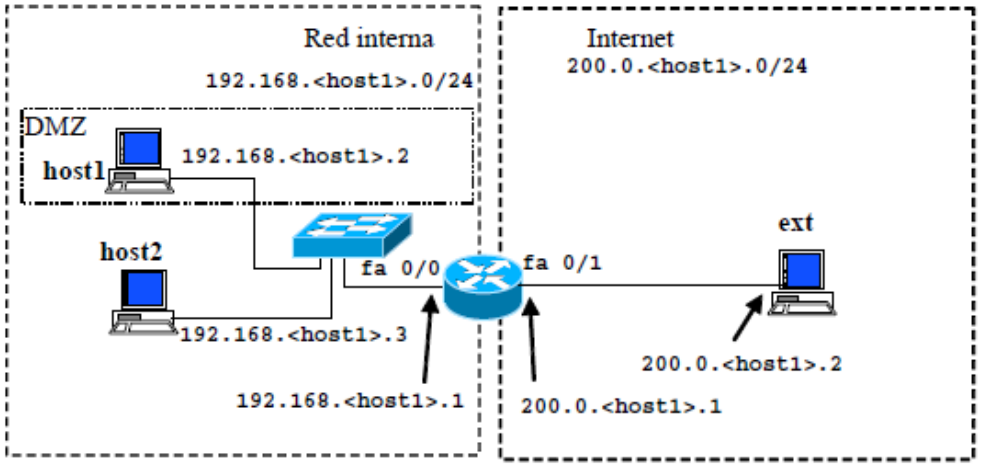
Parte 1: NAT



- NAT estático → Acceso desde "ext" a host1 (mediante IP pública router)
- Comprobar conectividad ext-host1 → **ext: #ping 200.0.<host1>.1** (IP pública fija asignada a host1)
- *R# debug ip nat* → Ver traducciones en tempo real (**R# no debug ip nat** → Para detener)

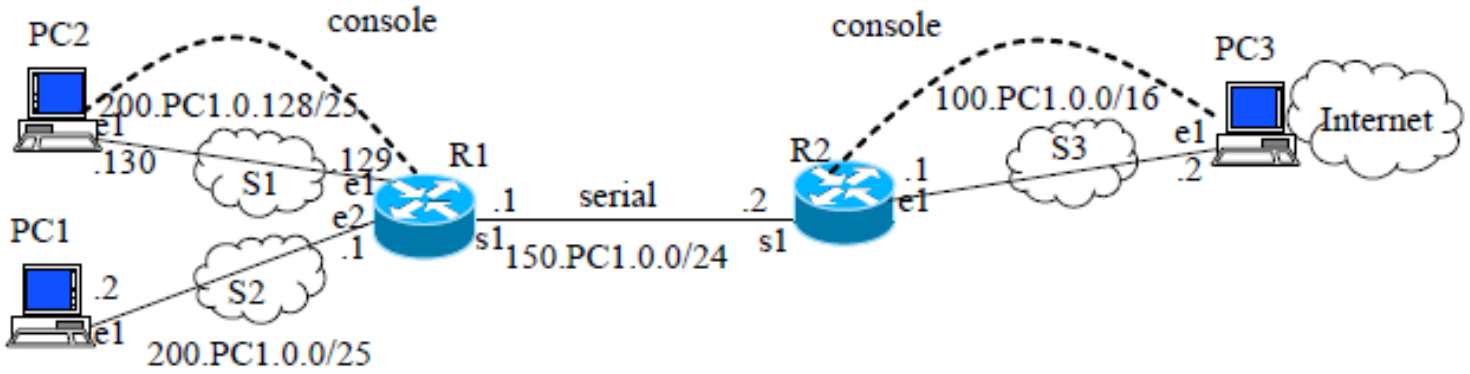
Realización práctica

Parte 2: ACLs



- Configurar servidores FTP y HTTP → Demo YouTube (https://youtu.be/AmFrNCyvJB8)
- Sólo *host2* puede acceder a Internet → Configurar ACL en fa0/0 "in" (con la IP privada de *host2*)
- **Punto 5 del cuaderno de prácticas** → *Host1* no puede contestar *ping* a "ext"
- **Punto 6** → En lugar de SSH y Telnet, usar HTTP (puerto 80) y FTP (puertos 20 y 21) respectivamente

Repaso práctica 3



- Problema "Count to infinity"
- *Split horizon*
- *Poison reverse* y *Triggered updates* → Se anuncian inmediatamente gateways no accesibles (métrica RIP infinita)
- Cisco incrementa en 1 la métrica de sus tablas al enviar mensaje RIP (RFC-2453)

  Ej: RIP "metric 2" → "[120/1]" en tabla de encaminamiento

Dudas / preguntas?

Contacto:

José Suárez-Varela
jsuarezv@ac.upc.edu

Minicontrol

- Herramienta WebTest:

  # su

  # root

  # udhcpc -i e0

- **User y password (DNI sin letra)**
- 4 preguntas tipo test (multirrespuesta **o respuesta única**)
- No se puede volver atrás
- No se penalizan respuestas erróneas
- Se puede usar cuaderno de prácticas y calculadora
- Quitar móviles de encima de la mesa