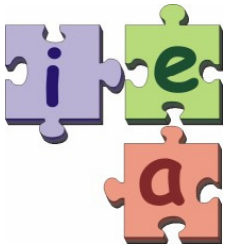
Sistemas de Transporte de Datos (9186)
Ingeniería en Informática (plan 2001)

Práctica 1. Introducción a Redes y a TCP/IP sobre Tecnología Ethernet

Curso: 2008-2009



Juan Antonio Corrales Ramón

Francisco Andrés Candelas Herías

Santiago Puente Méndez

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

Departament de Física, Enginyeria de Sistemes i Teoria del Senyal
Departamento de Física, Ingeniería de Sistemas y Teoría de la Señal

Listas de Control de Acceso (ACL)

• Las ACL son un mecanismo para clasificar los paquetes que circulan a través de un router.

• Una ACL está formada por un grupo de declaraciones que permiten ("permit") o deniegan ("deny") paquetes.

• Se pueden aplicar a: interfaces, políticas QoS, traducciones NAT…

• Las reglas ACL se verifican en **orden descendente**. Colocar las más restrictivas primero.

• Existe un **deny any any** implícito al final de la ACL.

Rango del identificador	
1 – 99	**Lista IP estándar** (IP Orig)
100 – 199	**Lista IP extendida** (IP Orig/Dest; Puerto Orig/Dest)
200 – 299	Lista de acceso por campo "type-code"
700 – 799	Lista LAN con direcciones de 48-bit MAC
1100 – 1199	Lista LAN extendida con direcciones de 48-bit MAC
1300 – 1999	Lista IP estándar (rango expandido)
2000 – 2699	Lista IP extendida (rango expandido)

Listas de Control de Acceso (ACL)

- **Sintaxis ACL**

access-list acl_num {**deny**|**permit**} protocolo

IP_origen [wildcard_origen] [operador puerto_origen]

IP_destino [wildcard_destino] [operador puerto_dest]

Protocolo: **ip** | **icmp** | **udp** | **tcp**

Wildcard: Complementario en binario de la máscara de red.
Mask: 255.255.0.0 → Wildcard: 0.0.255.255

Operador: **eq** (igual) | **lt** (menor) | **gt** (mayor)

- **Ejemplo ACL**

access-list 101 remark Criterios para marcar precedencia 1

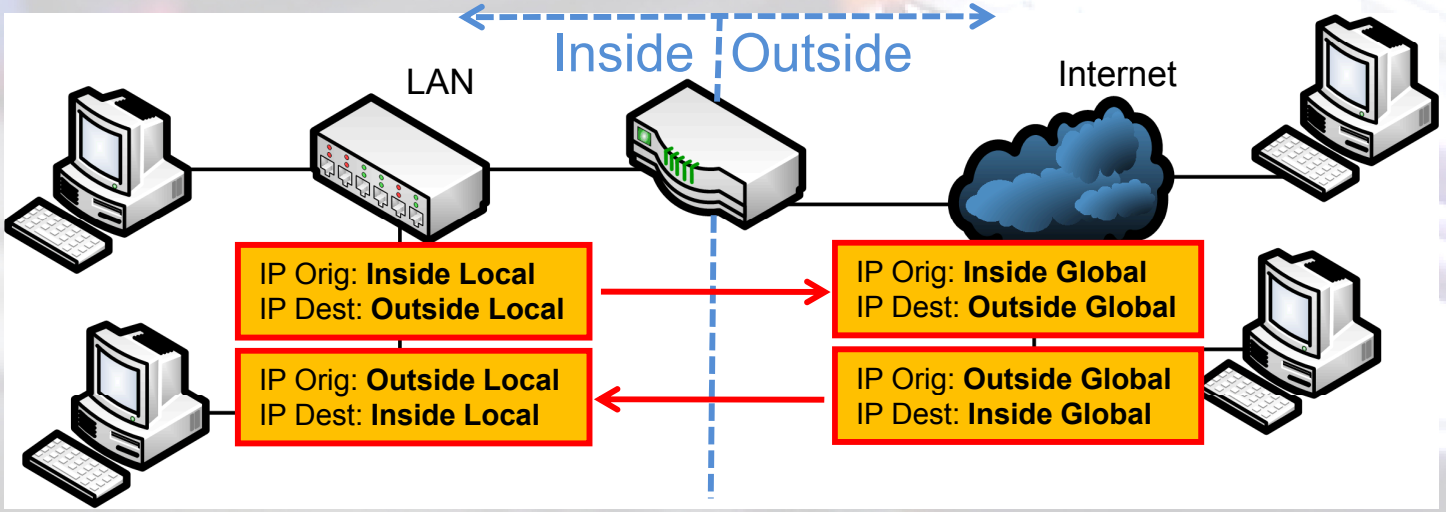
access-list 101 permit ip host 193.145.232.131 host 10.1.3.3

access-list 101 deny udp any 10.1.0.0 0.0.255.255 eq 80

access-list 101 permit ip host 193.145.232.132 host 10.1.2.2

Traducción de direcciones con NAT y PAT

- **NAT:** Cambia las direcciones IP de los paquetes (NAT básico) y los puertos TCP/UDP (PAT, overloading NAT).
- **Objetivo:** Equipos de una red privada, con direccionamiento privado, acceden a una red externa con otro direccionamiento.

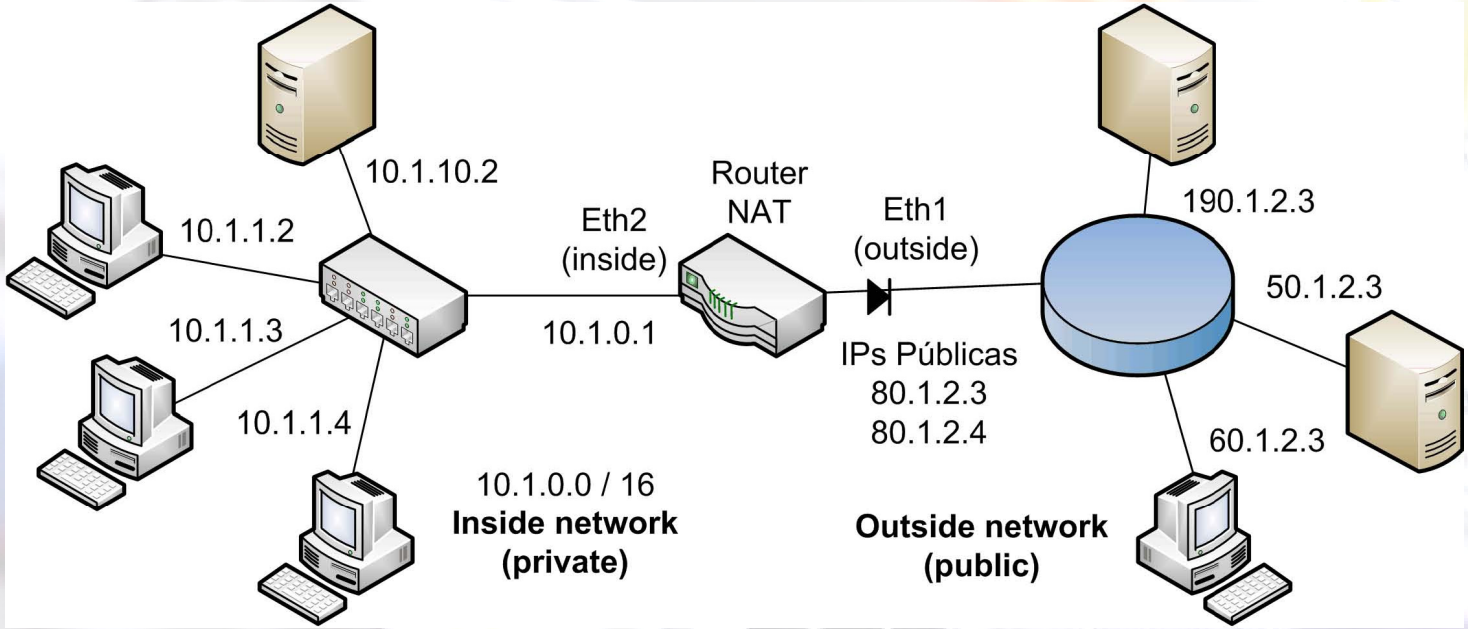


- **2 redes:** inside (interior) y outside (exterior).
- **4 direccionamientos:** inside local/global, outside local/global.
- **NAT Estático:** Cada dirección/puerto siempre se traduce igual.
- **NAT Dinámico:** Se dispone de un conjunto (pool) de direcciones.

Pasos para configuración NAT

- Definir interfaces NAT inside y outside.
- Definir objetivos que se pretenden conseguir con NAT:
  - Permitir a usuarios internos acceder a internet.
  - Permitir a usuarios de internet acceder a servicios internos.
  - Permitir redirigir tráfico TCP a otro puerto TCP.
  - Permitir que se comuniquen redes con direcciones solapadas.
- Configurar NAT para cumplir los requisitos establecidos:
  - NAT estático.
  - NAT dinámico (conjunto de direcciones: pool).
  - PAT / Overloading NAT (múltiples IP → 1 IP con múltiples puertos).
  - Una combinación de los anteriores.
- Verificar el funcionamiento de NAT:
  - Analizador de tráfico (WireShark, tcpdump…)
  - Comando “show ip nat translations” para ver tabla NAT.

Traducción de direcciones internas



NAT Dinámico: Todas las máquinas 10.1.0.0/16 deben salir a través de dos direcciones IP públicas 80.1.2.3/4 mediante el uso de PAT (overload).

Paquete Red Interior	Paquete Red Exterior
origen: IP 10.1.1.2, puerto 1000 destino: IP 190.1.2.3, puerto 53	origen: IP 80.1.2.3, puerto 1000 destino: IP 190.1.2.3, puerto 53
origen: IP 10.1.1.3, puerto 2000 destino: IP 50.1.2.3, puerto 80	origen: IP 80.1.2.4, puerto 2000 destino: IP 50.1.2.3, puerto 80
origen: IP 10.1.1.4, puerto 1000 destino: IP 50.1.2.3, puerto 80	origen: IP 80.1.2.3, puerto 1001 destino: IP 50.1.2.3, puerto 80

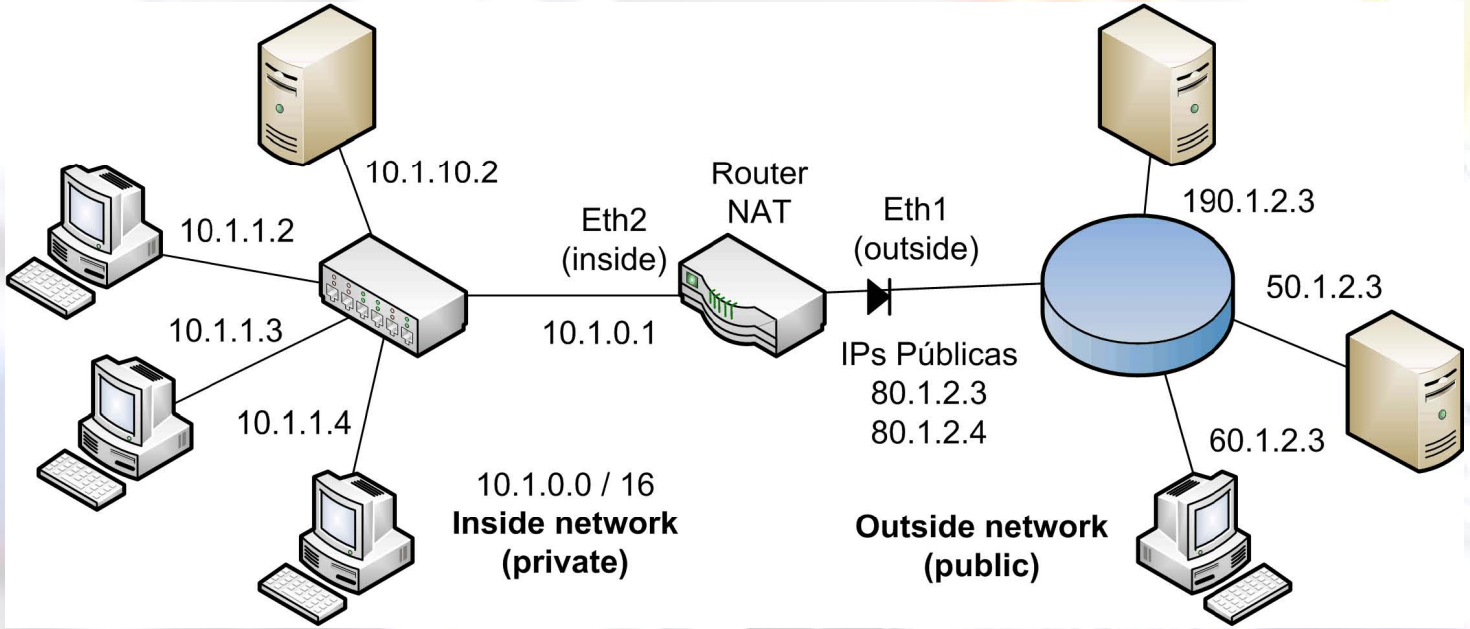
```
interface Eth2
  ip address 10.1.0.1 255.255.0.0
  ip nat inside

interface Eth1
  ip address 80.1.2.3
  ip address 80.1.2.4 secondary
  ip nat outside

ip nat inside source interface Eth1 overload
```

inside global

Traducción de direcciones internas



NAT según ACL: Al definir una traducción NAT se puede asociar a una lista ACL para que sólo se aplique la traducción a los paquetes que la cumplan.

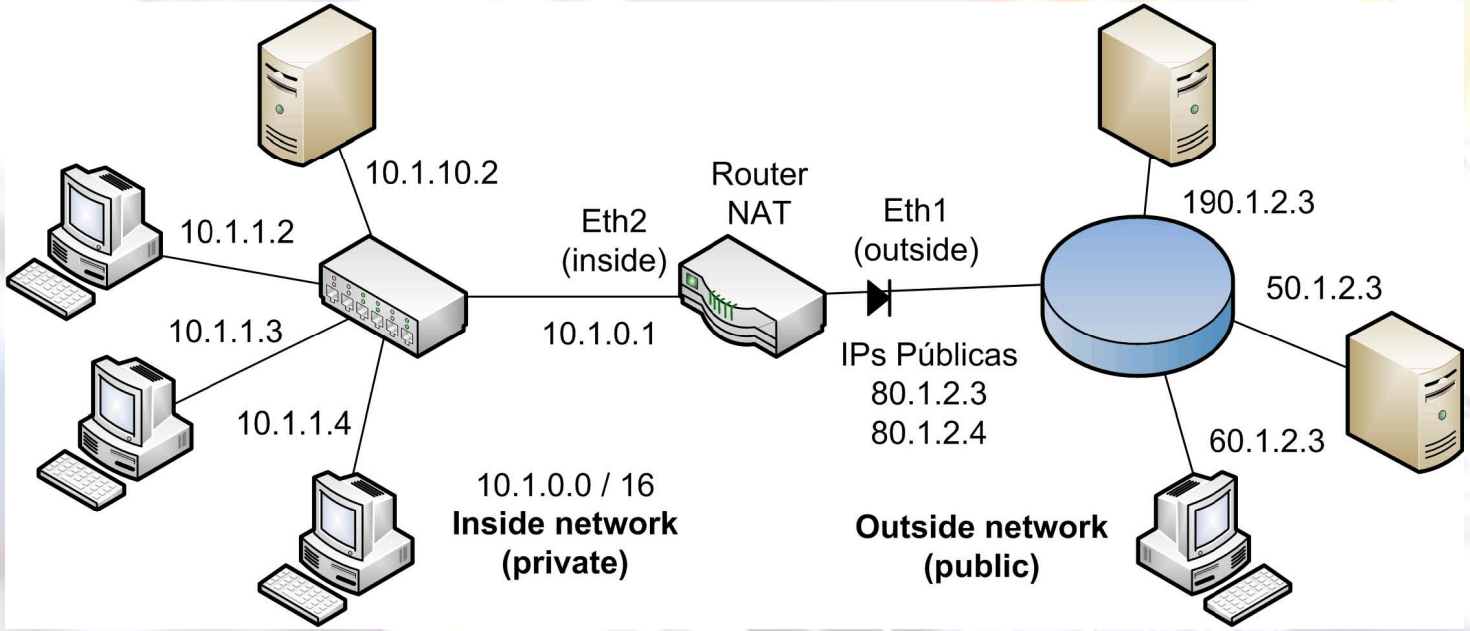
- ACL asociada directamente a un comando NAT:

ip nat inside source **list 106** interface Eth1 overload
access-list 106 deny IP any 172.25.30.0 0.0.0.255
access-list 106 permit any any

- ACL asociada a un comando NAT a través de un "route-map":

ip nat inside source **route-map permitidos** interface Eth1 overload
access-list 100 permit 10.2.0.0 0.0.255.255 any
access-list 100 permit 10.1.0.0 0.0.255.255 any
route-map permitidos permit 10
match ip address 1000

Traducción de direcciones internas



NAT Estático: Los servidores de la red privada siempre tienen que ser accesibles con las mismas IPs desde fuera.

Paquete Red Exterior	Paquete Red Interior
origen: IP X1.X1.X1.X1, puerto Y1 destino: IP 80.1.2.3, puerto 80	origen: IP X1.X1.X1.X1, puerto Y1 destino: IP 10.1.10.2, puerto 80
origen: IP X2.X2.X2.X2, puerto Y2 destino: IP 80.1.2.3, puerto 8080	origen: IP X2.X2.X2.X2, puerto Y2 destino: IP 10.1.1.3, puerto 80
origen: IP X3.X3.X3.X3, puerto Y3 destino: IP 80.1.2.3, puerto 21	origen: IP X3.X3.X3.X3, puerto Y3 destino: IP 10.1.1.4, puerto 21

Inside local

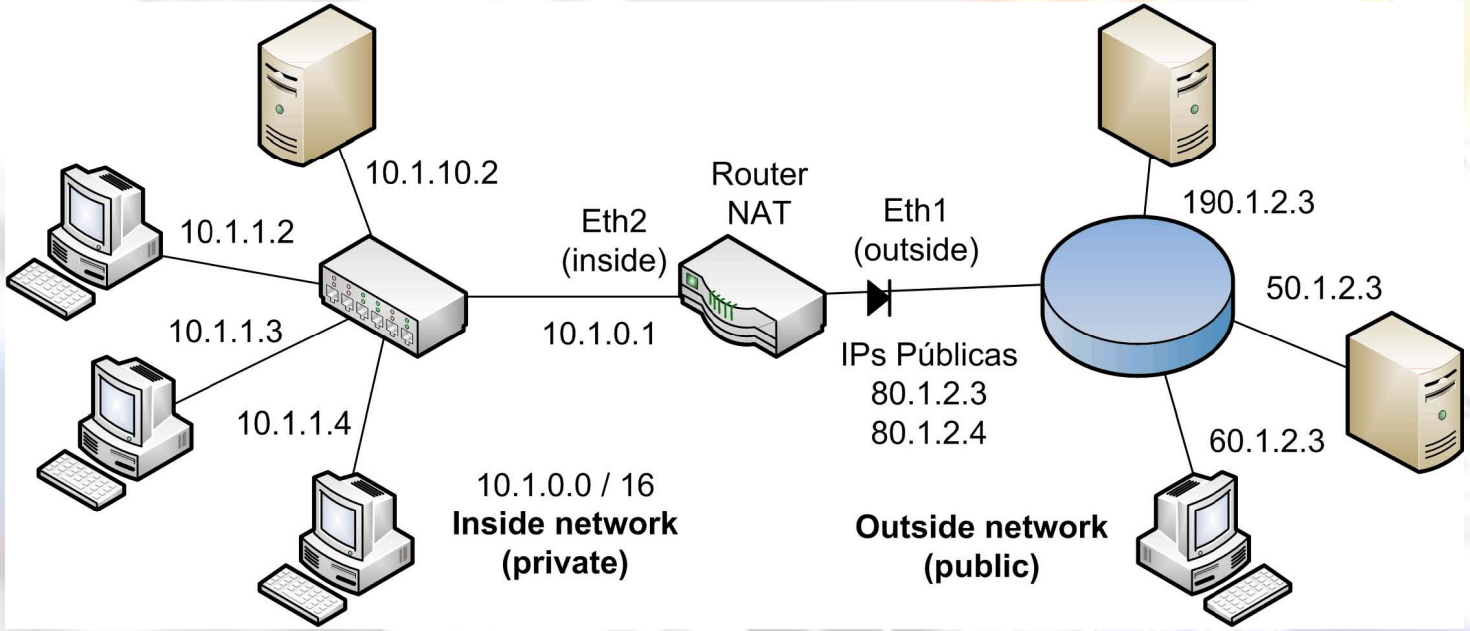
ip nat inside source static tcp 10.1.10.2 80 → interface Eth1 80

Inside global

ip nat inside source static tcp 10.1.1.3 80 → interface Eth1 8080

ip nat inside source static tcp 10.1.1.4 21 → interface Eth1 21

Traducción de direcciones externas



NAT Estático: Los equipos de la red interna pueden acceder a los servicios de un equipo externo como si estuviera en la red interna.

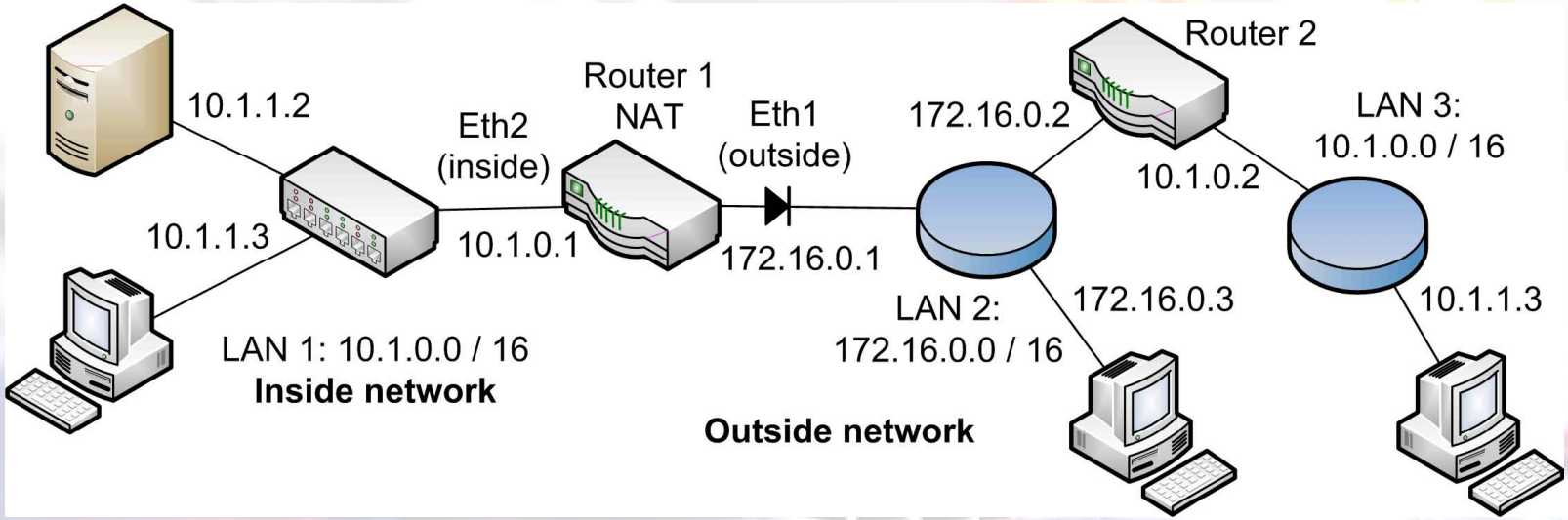
Paquete Red Interior	Paquete Red Exterior
origen: IP 10.1.1.4, puerto 1010 **destino: IP 10.10.10.5, puerto 80**	origen: 80.1.2.3, puerto 1010 **destino: 190.1.2.3, puerto 80**

outside global: 190.1.2.3 — outside local: 10.10.10.5

ip nat outside source static 190.1.2.3 10.10.10.5

• Sería también necesaria la traducción inside para direccionar los equipos internos mediante la IP pública 80.1.2.3:
ip nat inside source interface Eth1 overload

Traducción de direcciones externas



NAT Dinámico: Permitir que equipos externos (LAN 3) con el mismo rango de direcciones que los equipos internos accedan a la red interna (LAN 1).

Paquete Red Exterior	Paquete Red Interior
origen: IP 10.1.1.3, puerto 1010 destino: IP 172.16.0.1, puerto 80	**origen: 10.55.0.1, puerto 1010** destino: 10.1.1.2, puerto 80

ip nat pool ip-nuevas 10.55.0.1 10.55.255.254 netmask 255.255.0.0
access-list 1 permit 10.1.0.0 0.0.255.255
ip nat outside source list 1 pool ips-nuevas

• Sería necesario también una traducción inside estática para direccionar el servidor 10.1.1.2 con la IP pública 172.16.0.1:

ip nat inside source static tcp 10.1.1.2 80 interface Eth1 80

Resumen funcionamiento NAT

- Cuando un paquete viaja del exterior (outside) al interior (inside):
  - 1º Traducción NAT ⟶ 2º Encaminamiento IP
- Cuando un paquete viaja del interior (inside) al exterior (outside):
  - 1º Encaminamiento IP ⟶ 2º Traducción NAT
- La siguiente tabla indica la dirección del paquete IP que es traducida según el comando de definición NAT utilizado:

Comando	Acción
ip nat inside source static	• Traduce la IP origen de los paquetes interior → exterior • Traduce la IP destino de los paquetes exterior → interior
ip nat outside source static	• Traduce la IP origen de los paquetes exterior → interior • Traduce la IP destino de los paquetes interior → exterior

- Las definiciones NAT estáticas tienen **una entrada fija** en la tabla NAT y permiten iniciar la conexión tanto a equipos internos como externos.
- Las definiciones NAT dinámicas **generan una entrada** en la tabla NAT sólo cuando se inicia una conexión desde el lado correspondiente a la definición. Por lo tanto, no se puede iniciar conexión desde el otro lado.

Enrutamiento dinámico RIP

• Los **protocolos de enrutamiento dinámico** permiten que los routers describan y administren las rutas necesarias para crear sus tablas de encaminamiento dinámicamente.

• **RIP** (Routing Information Protocol) es un protocolo de enrutamiento dinámico:

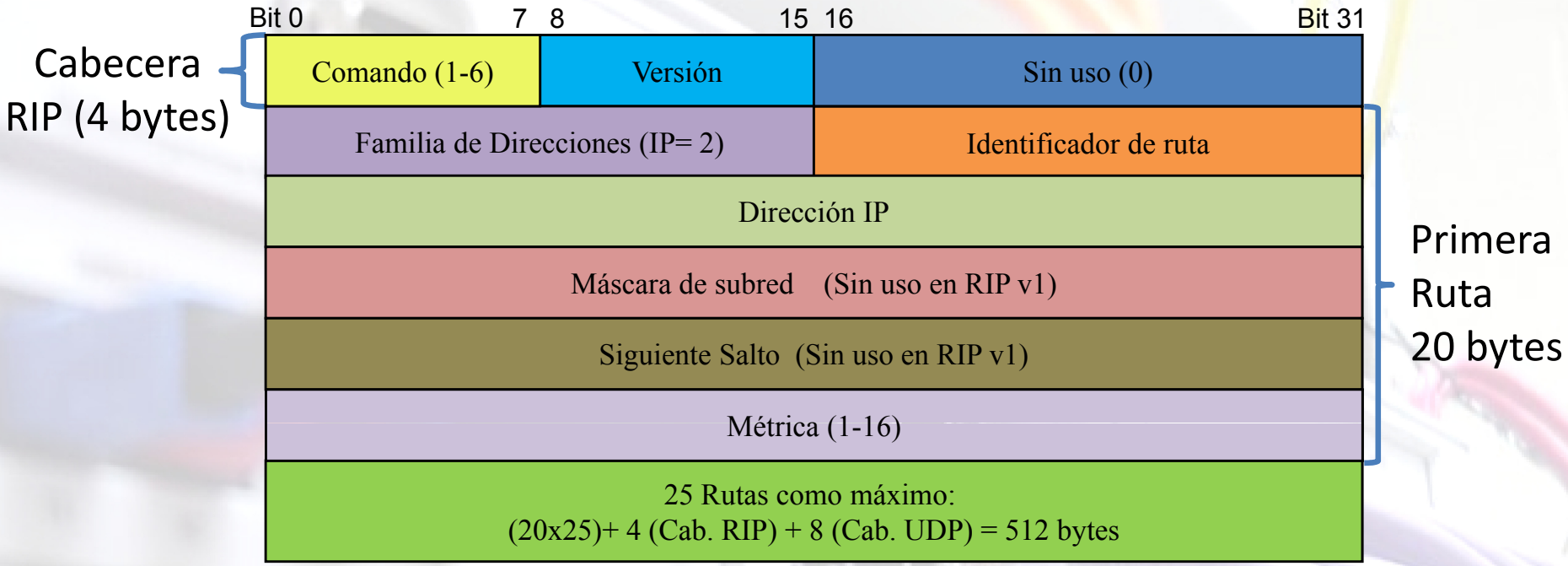
➢ Los mensajes RIP son transportados por **datagramas UDP** dirigidos al puerto 520. Son enviados a la dirección de multicast MAC: 01:00:5E:**00:00:09** / IP: 224.**0.0.9.**

➢ Es un protocolo de **vector de distancias**: Emplea el número de saltos a un destino (métrica) para determinar la ruta óptima a un destino. No analiza el ancho de banda.

➢ El nº máximo de saltos es 15. Cualquier ruta con 16 saltos, se considera inalcanzable.

➢ Usaremos **RIP v.2**, que incluye mejoras respecto a RIP v.1.

Mensajes RIP



- Existen dos tipos de mensajes:
  - **Petición (Comando=1):** Son enviados por un router que ha sido recientemente iniciado. Solicita información de encaminamiento a los routers vecinos.
  - **Respuesta (Comando= 2):**
    - Mensajes ordinarios: Se envían de manera periódica (cada 30 segundos).
    - Mensajes enviados como respuesta a un mensaje de petición.
- Un router actualizará su tabla de rutas al recibir un mensaje de respuesta RIP:
  - Si aparece una **ruta nueva** que no conoce.
  - Si la nueva puerta de enlace permite alcanzar el destino en **menos saltos.**
- Cada ruta generada con RIP tiene un temporizador que la elimina si no se actualiza.

Enrutamiento dinámico EIGRP

• **EIGRP** (Enhanced Interior Gateway Routing Protocol) es un protocolo de enrutamiento dinámico de "vector de distancia" pero con características de "estado de enlace". Es una mejora de IGRP.

• Utiliza tres tablas para su funcionamiento:

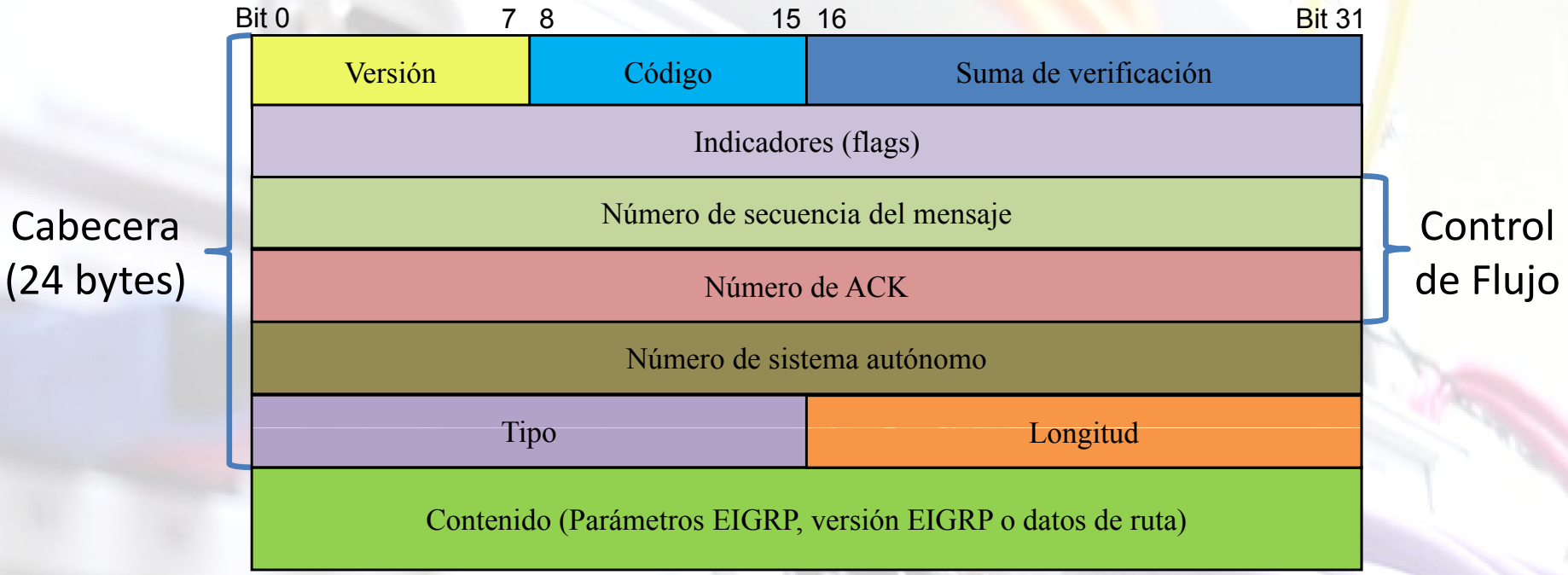
- **Tabla de vecinos:** EIGRP mantiene actualizada una tabla de routers adyacentes mediante mensajes **Hello** enviados a la IP multicast 224.0.0.10.

- **Tabla de topología:** Es una base de datos de las rutas informadas por los vecinos y sus métricas obtenidas mediante el algoritmo DUAL.

    - Para cada par destino-vecino, se almacena la métrica indicada por el vecino (Advertised Distance) y la métrica total (incluyendo el coste del enlace con dicho vecino).

- **Tabla de encaminamiento:** Se obtiene a partir de la tabla de topología, seleccionando la ruta con menor métrica (Feasible Distance) para cada destino.

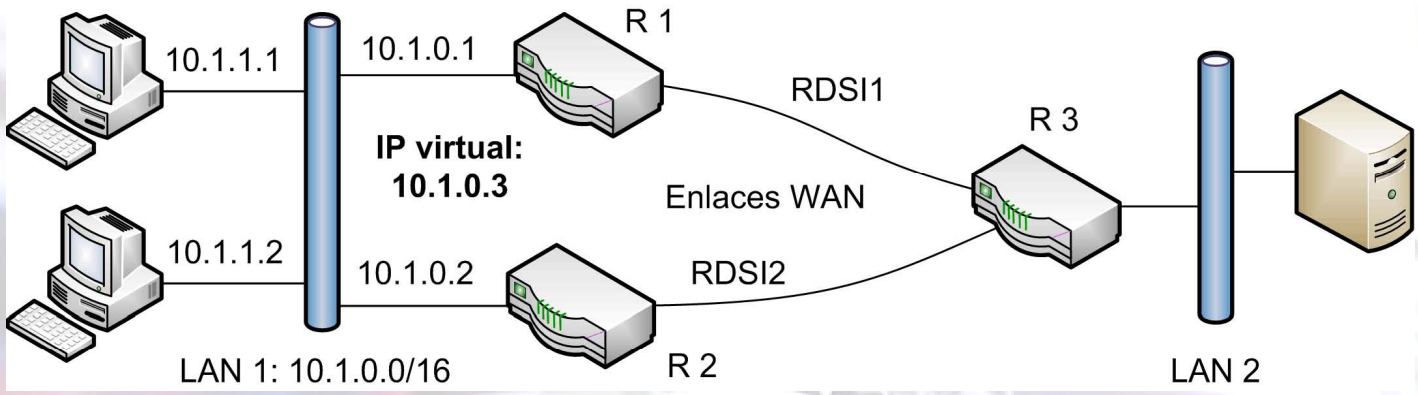
Mensajes EIGRP



- Existen cinco tipos de mensajes:
  - **Update (cod. 1):** Envía sólo rutas que cambian a los routers vecinos.
  - **Query (cod. 3):** Solicita posibles rutas para llegar a un destino.
  - **Reply (cod. 4):** Respuesta a mensaje Query con información sobre rutas.
  - **Hello (cod. 5):** Descubrimiento de vecinos. No necesita ACK.
  - **Acknowlegment (cod. 5):** Confirmación de la recepción de otros mensajes.

Routers redundantes con HSRP

• **HSRP** (Host Standby Routing Protocol) es un protocolo de Cisco que permite definir routers redundantes para crear una topología de red tolerante a fallos.



• HSRP genera un **router virtual** que tiene una IP dentro de la red y una MAC de la forma 00:00:0C:AC:XX. El router con mayor prioridad será el **router activo** que ejecuta las funciones del virtual. Si falla, el **router en espera** ("standby") con mayor prioridad del grupo HSRP (nº grupo = XX) ocupará su puesto.

• HSRP utiliza tres tipos de mensajes que son enviados entre los routers:

- **Hello** (Saludo): Mensajes multicast (224.0.0.2) con información de estado.
- **Coup** (Asalto): Router en espera se transforma en activo al pasar "hold time".
- **Resign** (Renuncia): Router activo indica que va a dejar de ser activo porque se va a apagar o porque ha recibido un hello de otro router con mayor prioridad.

Topología L24