Redes WAN

DHCP y NAT

Esteban De La Fuente Rubio
esteban@delaf.cl
LaTeX

Universidad Andrés Bello

27 abr 2011

Tabla de contenidos

1. DHCP
   - Funcionamiento
   - BOOTP
   - Configuración
2. NAT
   - Funcionamiento
   - Ventajas y desventajas
   - Configuración

DHCP

- Dynamic Host Configuration Protocol
- ¿Qué equipos utilizarán DHCP?
- Tarea primordial: asignar dirección IP.

Funcionamiento

Tipos de asignación:

- Dinámica: se elige una IP de un pool y se asigna al cliente.
- Estática: se tiene una relación IP-cliente mediante la dirección física del cliente.

Funcionamiento (2)

Pasos de la asignación:

- Descubrir: envio de DHCPDISCOVER buscando servidores DHCP.
- Ofrecer: el servidor busca una IP, crea entrada ARP y envia la oferta al cliente mediante DHCPOFFER.
- Solicitar: cliente envia DHCPREQUEST para dar origen al arrendamiento y renovar el arrendamiento.
- Acusar: servidor envia DHCPACK, igual que el DHCPOFFER pero con el tipo de mensaje distinto. Cliente hace busqueda ARP para la IP asignada, al no encontrar resultado la IP es válida.

Funcionamiento (3)

Otros envios entre cliente y servidor:

- DHCPNAK
- DHCPDECLINE
- DHCPRELEASE
- DHCPINFORM

Funcionamiento (4)

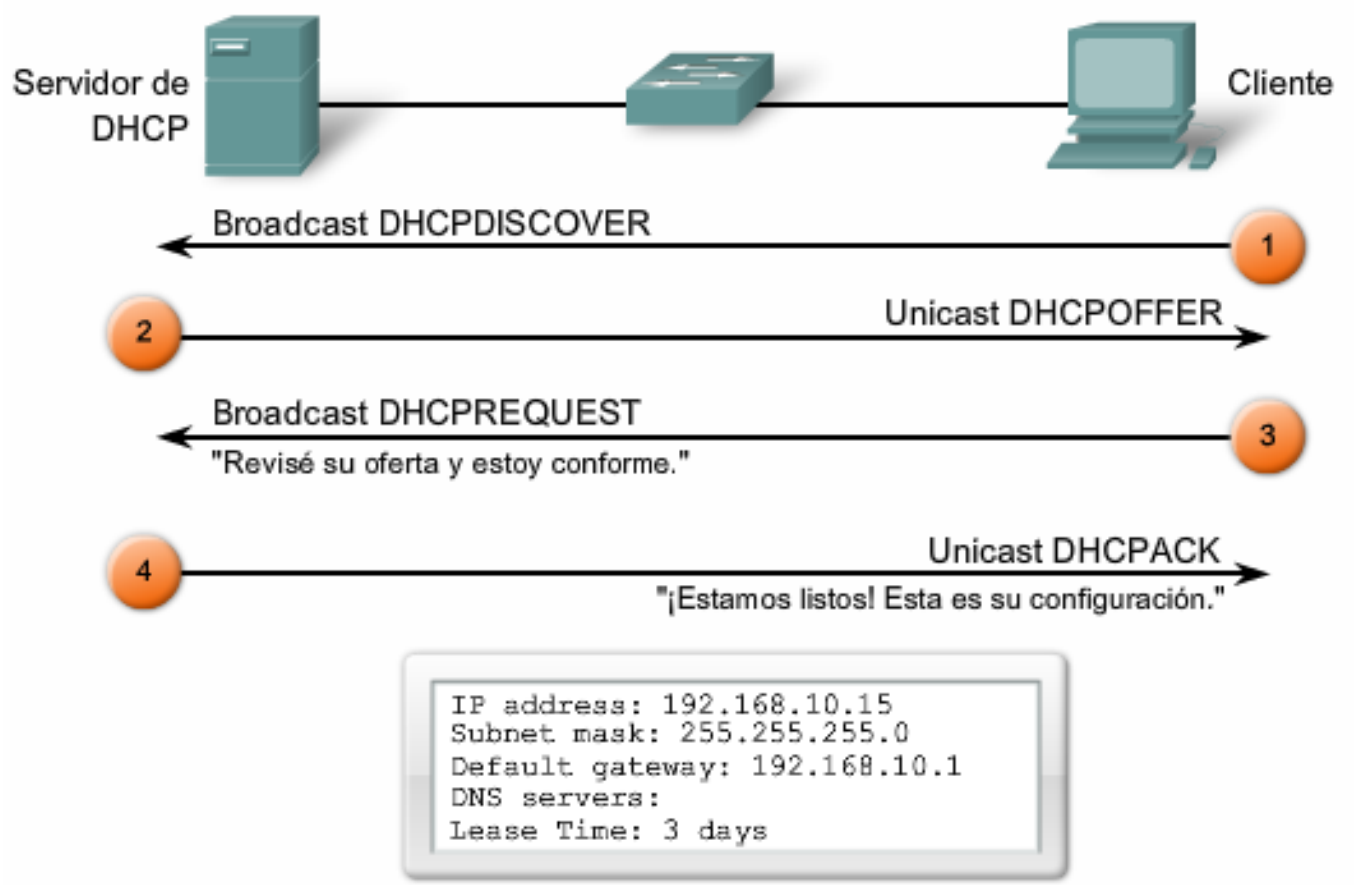

Figura: Funcionamiento DHCP

BOOTP

- Predecesor del protocolo DHCP.
- Utilizado en el arranque de la máquina, originalmente en máquinas sin disco.
- Utiliza puertos UDP 67 y 68 (al igual que DHCP).

BOOTP (2)

Diferencias entre DHCP y BOOTP:

- Diseñado para tener una configuración previa con la relación IP-cliente.
- BOOTP no utiliza arrendamiento, IP es fija y permanente para un cliente.
- DHCP proporciona parámetros adicionales (como el nombre de dominio).

Formato mensaje DHCP

Mismo formato que BOOTP por temas de compatibilidad, pero con un campo de opciones de DHCP.

- Código de operación: tipo de mensaje (1=solicitud, 2=respuesta).
- Tipo de hardware: tipo de hardware utilizado en la red (1=Ethernet, 15=Frame Relay, etc).
- Longitud de la dirección de hardware.
- Saltos: utilizado cuando hay DHCP relay.
- Identificador de transacción (generada por el cliente).
- Segundos: segundos transcurridos desde que el cliente comenzó a intentar adquirir o renovar un arrendamiento.

Formato mensaje DHCP (2)

- Señaladores: usado para el señalador de broadcast.
- Dirección IP del cliente.
- Dirección IP asignada.
- Dirección IP del servidor.
- Dirección IP del gateway: utilizado cuand hay DHCP relay.
- Dirección de hardware del cliente.
- Opciones DHCP.

Formato mensaje DHCP (3)

8	16	24	32
Código OP (1)	Tipo de hardware (1)	Longitud de dirección de hardware (1)	Saltos (1)
Identificador de transacción			
Segundos: 2 bytes		Señaladores: 2 bytes	
Dirección IP del cliente (CIADDR, Client IP Address): 4 bytes			
Su dirección IP (YIADDR, Your IP Address): 4 bytes			
Dirección IP de servidor (SIADDR, Server IP Address): 4 bytes			
Dirección IP del gateway (GIADDR, Gateway IP Address): 4 bytes			
Dirección de hardware del cliente (CHADDR, Client Hardware Address): 16 bytes			
Opciones DHCP: variable			

Figura: Formato mensaje

Formato mensaje DHCP (4)

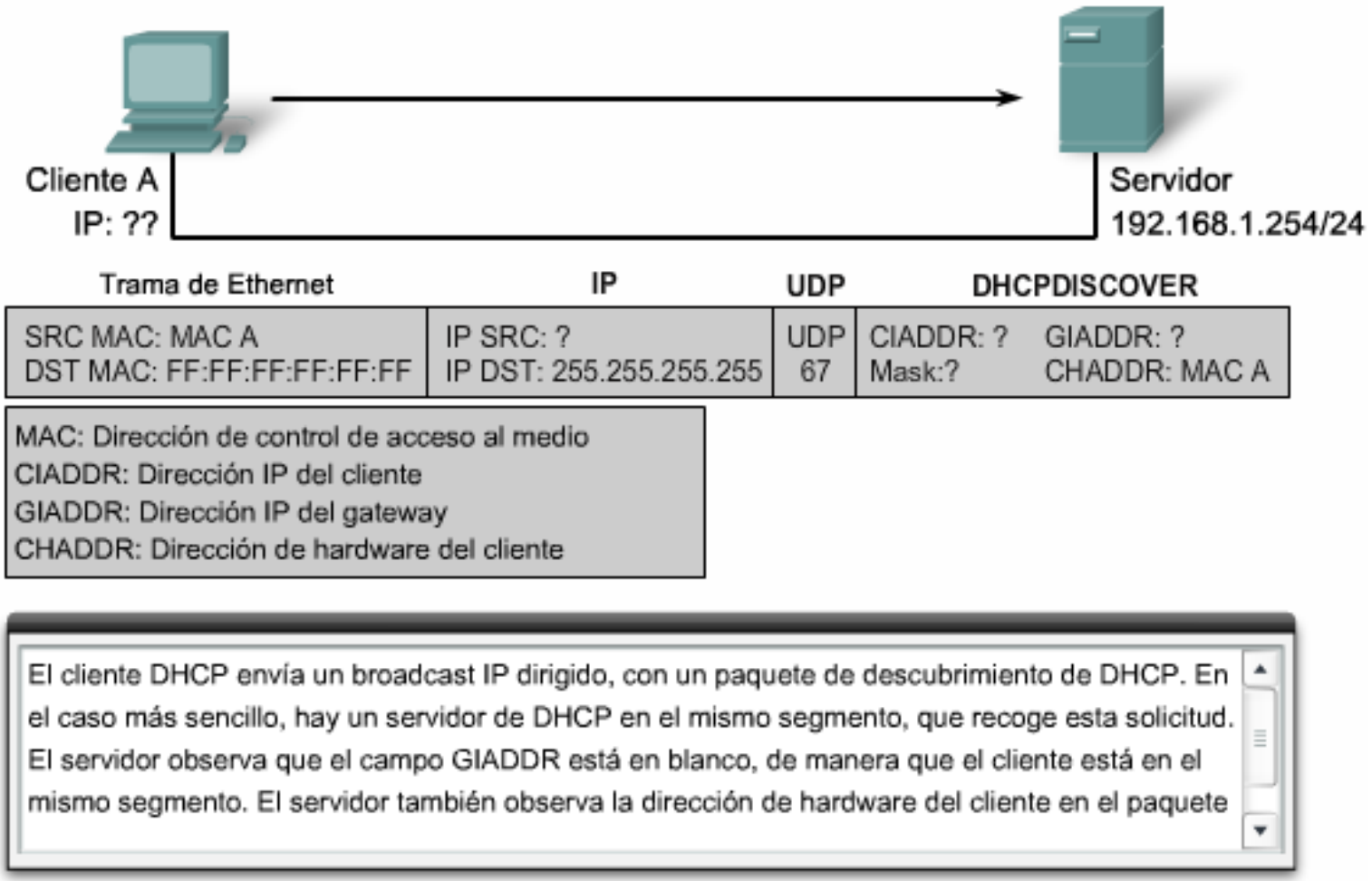

Figura: Descubrimiento

Formato mensaje DHCP (5)

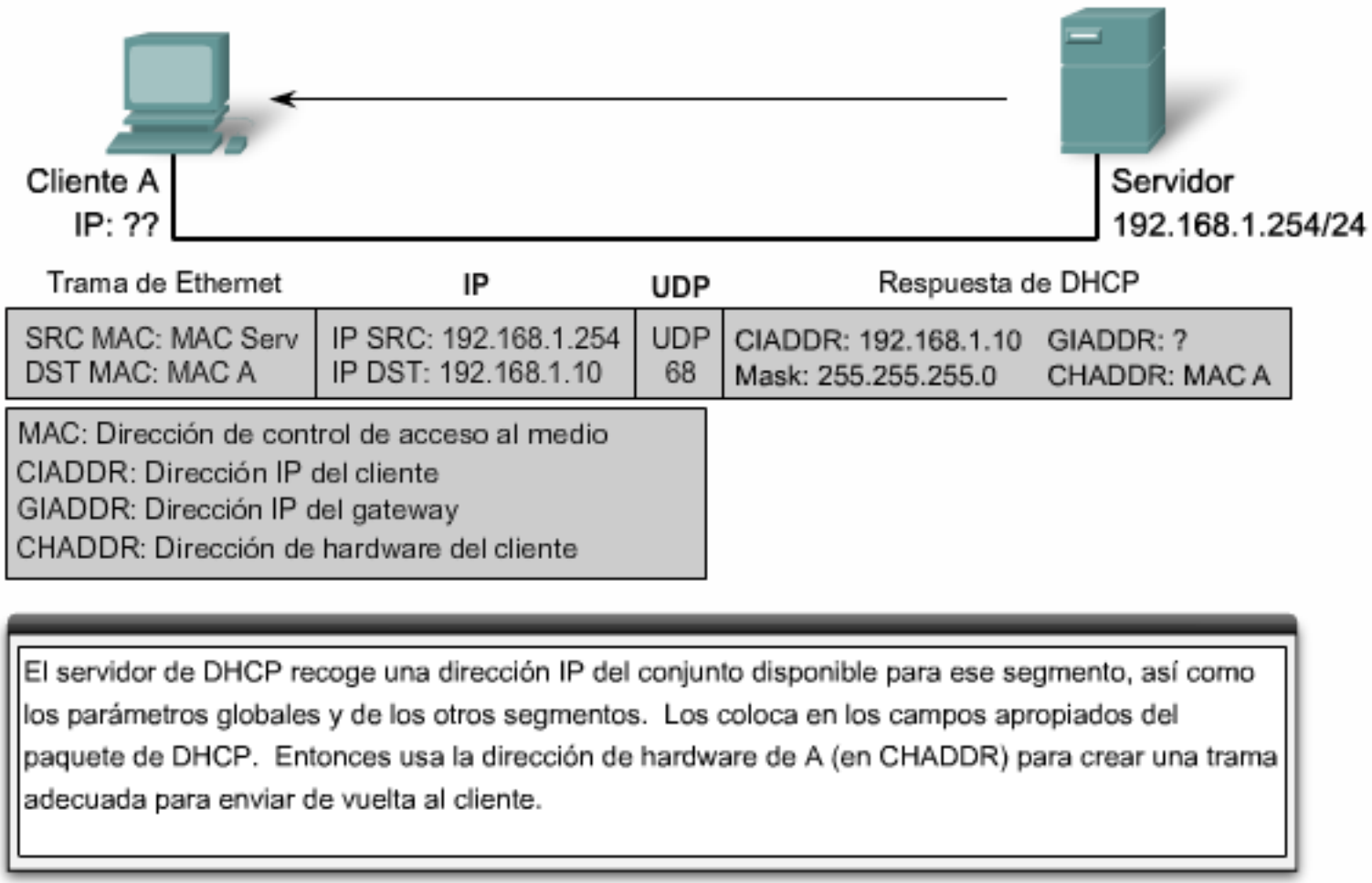

Figura: Oferta

A tener en cuenta

- No definir más de 3 DNS.
- Definir un tiempo de arrendamiento prudente según red.
- Colocar direcciones IP asociadas a direcciones físicas fuera del pool DHCP.
- Servidor DHCP servirá una red por interfaz física del servidor.

dhcp3-server

Instalación

```
# apt-get install dhcp3-server
```

Archivo de configuración /etc/dhcp3/dhcpd.conf

```
option domain-name "delaf.cl";
option domain-name-servers 172.16.1.1, 208.67.220.220;
max-lease-time 7200;
subnet 172.16.1.0 netmask 255.255.255.192 {
    range 172.16.1.40 172.16.1.62;
    option routers 172.16.1.1;
}
```

Direcciones IPs

Las direcciones IPs se clasifican en:

- Direcciones IPs públicas.
- Direcciones IPs privadas.

Direcciones IPs públicas

- Direcciones IPs públicas están registradas bajo alguno de los RIR (Regional Internet Registry). Estos asignan las IPs a los ISP.
- Organizaciones solicitan IPs a los ISP.
- IP pública solo puede ser asignada por quién haya solicitado una.
- IPs publican no deben utilizarce en redes privadas.
- Únicas en toda la red de internet.

Direcciones IPs públicas (2)

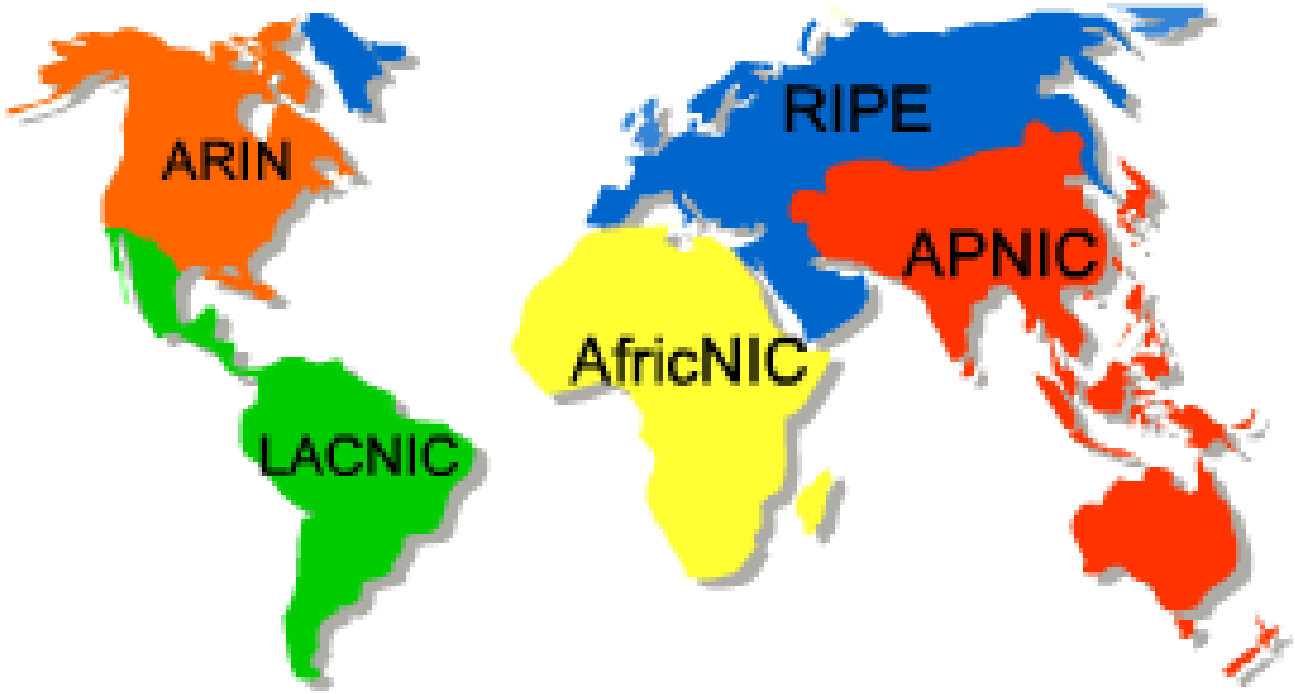

Figura: Zonas de cada RIR

Direcciones IPs privadas

- Menor cantidad que IPs públicas.
- 3 rangos definidos:
  - 10.0.0.0 a 10.255.255.255
  - 172.16.0.0 a 172.31.255.255
  - 192.168.0.0 a 192.168.255.255

NAT

- Direcciones IPs privadas permiten tener detrás de una única dirección pública muchos hosts conectados.
- Direcciones IPs privadas no son visibles en Internet.
- Se debe hacer un mapeo de dirección privada a dirección pública: NAT.
- NAT: network address translation.

NAT (2)

- Cuando un host envia paquetes fuera de la red NAT traduce la IP interna a una dirección externa.
- Para los usuarios externos, el tráfico que sale desde la IP del equipo que hace NAT pertenece toda a un mismo host.
- Principal uso para el ahorro de direcciones IPs públicas.
- Agrega privacidad y seguridad a la red.
- NAT operará generalmente en los equipos de borde.

NAT (3)

Conceptos de direcciones:

- Dirección local interna.
- Dirección global interna.
- Dirección global externa.
- Dirección local externa.

¿Cuando la dirección global externa es igual a la dirección local externa?

NAT (4)

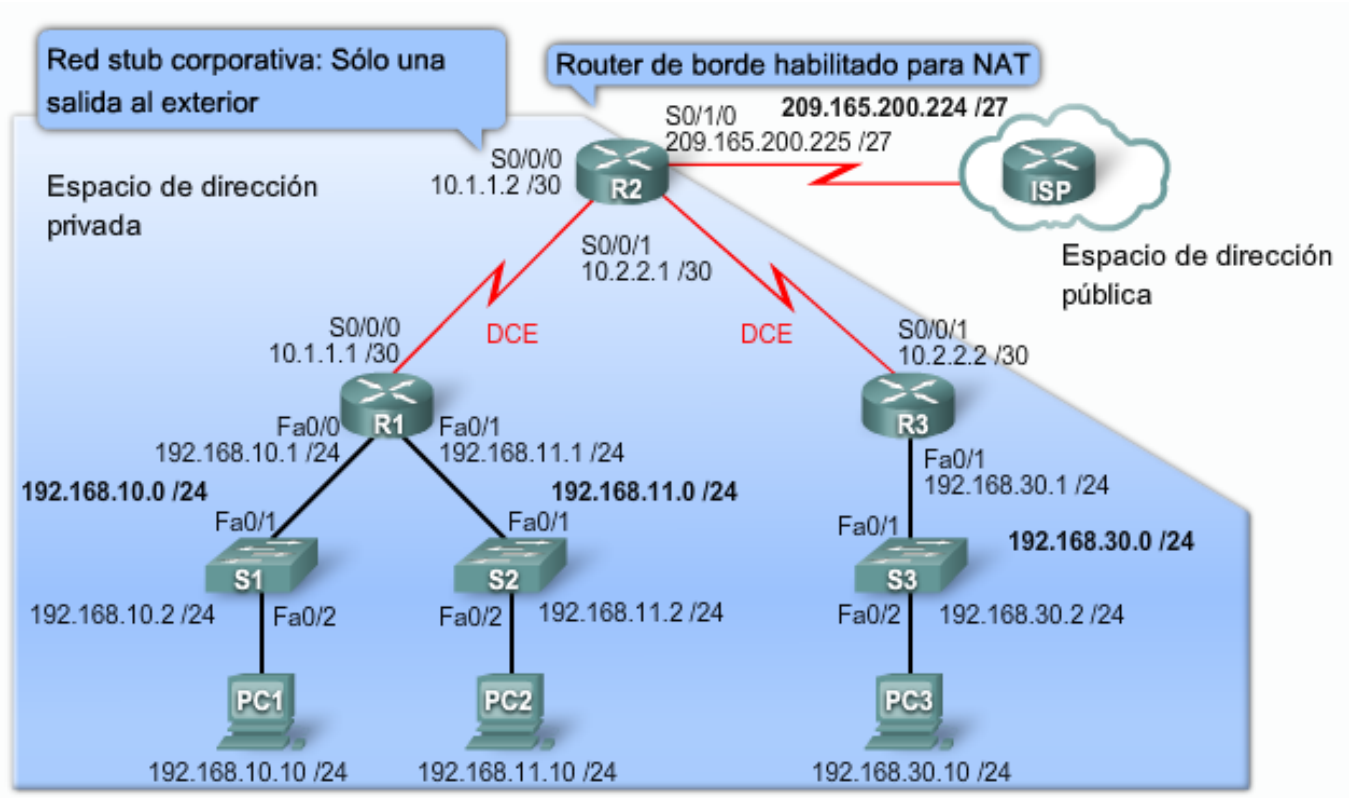

Figura: Red usando NAT

Pregunta

- ¿Es obligación utilizar IP pública para las direcciones externas del NAT?
- ¿Por qué?
- ¿De un ejemplo práctico de su justificación?

Funcionamiento

- Un host interno envia un paquete a la red externa.
- Router de borde cambia IP interna por IP externa.
- Se envia paquete y espera respuesta.
- Router recibe respuesta y según IP de destino externa envia la respuesta hacía el host en la red Interna.

Funcionamiento (2)

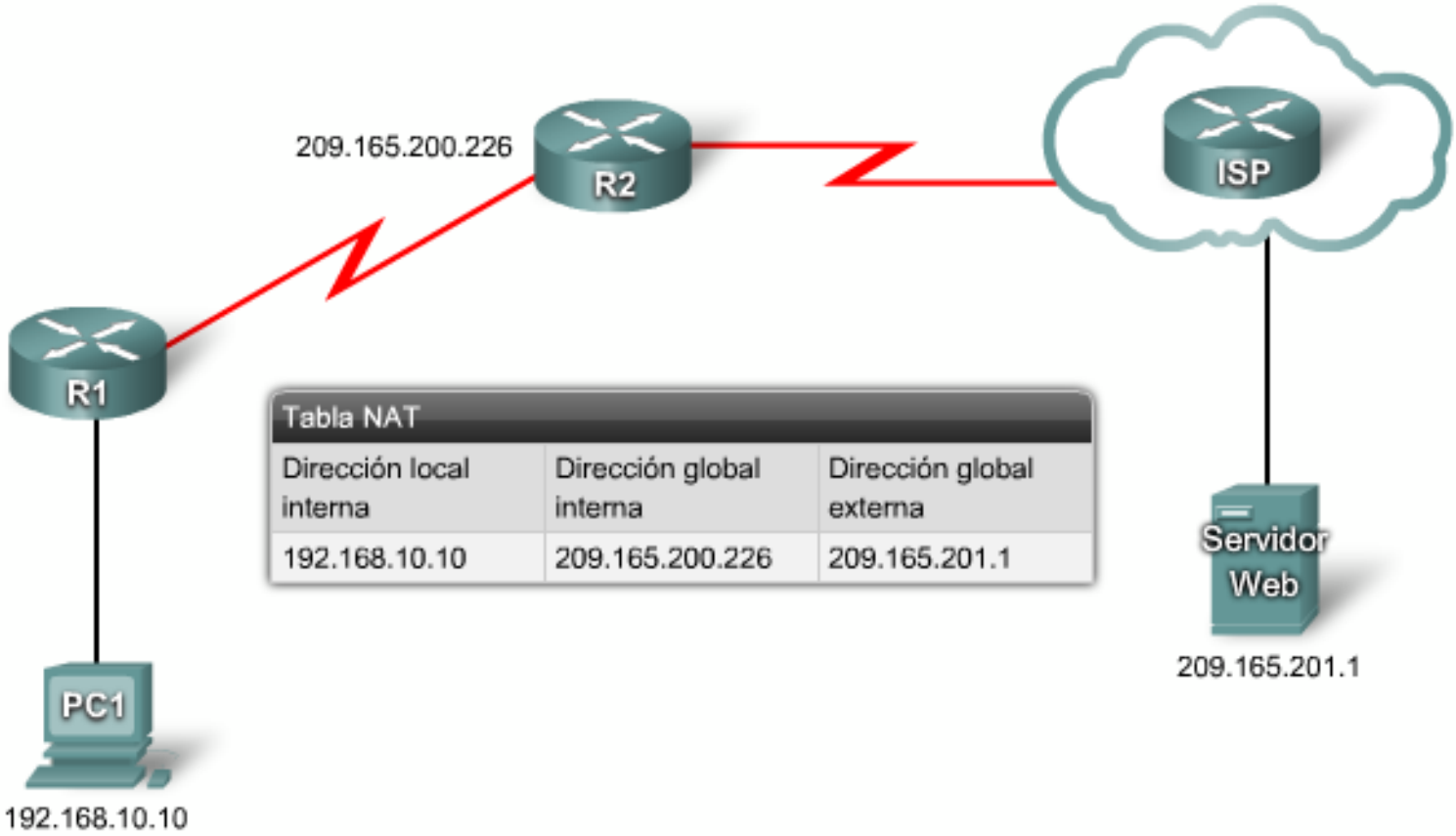

Figura: Funcionamiento de NAT

Funcionamiento (3)

Tipos de traducción:

- Dinámica: asigna un conjutno de direcciones públicas según orden de llegada.
- Estática. se realiza una asignación 1:1 (utilizada en servidores).

¿Qué pasa si hay más sesiones de usuarios abiertas que IPs externas disponibles?

Sobrecarga de NAT

- Sobrecarga de NAT o PAT (Port Address Translation) asigna varias direcciones IP privadas a una única dirección IP pública.
- Funcionamiento estándar de los router SOHO.
- ISP asigna IP al router y varios host pueden navegar por Internet de manera simultánea.
- Se hace una traducción utilizando IP y puerto de origen.
- Si el puerto ya fue ocupado por otro host en el equipo que hace NAT se utiliza el siguiente puerto libre.
- Si no hay más puertos disponibles se utiliza la siguiente dirección IP (de estar configurada).

Sobrecarga de NAT (2)

Diferencias entre NAT y la sobrecarga de NAT

- NAT traduce direcciones IP en una relación 1:1, PAT traduce IP y puertos (permitiendo que varios host usen la misma IP al mismo tiempo).
- PAT selecciona los puertos que ven los host de la red pública.
- NAT enruta los paquetes entrantes hasta el destino interno mediante la IP de origen entrante. Mediante PAT esto se realiza consultando por la relación IP puerto.

Reenvío de puertos

- Reenvío de puertos, tunneling o port forward consiste en reenviar una solicitud a un puerto de un host hacia otro host (y otro puerto).
- Permite a usuarios externos de la red llegar a un servicio que este situado en la red interna.
- NAT no permite iniciar solicitudes hacia un puerto específico hacia el interior (si hacia el exterior) he aquí la utilidad de este método.
- Evita tener una IP pública para cada servicio de la red interna.
- Ejemplo: servidor web en red interna sin IP pública en él.

Ventajas

- NAT hace posible que se requieran pocas direcciones externas para admitir muchos hosts internos.
- NAT aumenta la flexibilidad de las conexiones con la red pública.
- NAT proporciona uniformidad en los esquemas de direccionamiento internos de red.
- NAT proporciona seguridad de red.

Desventajas

- Menor rendimiento.
- Protocolos dependen de que los paquetes no sean modificados desde el origen al destino.
- También se pierde la capacidad de rastreo de extremo a extremo.
- El uso de NAT también complica el funcionamiento de los protocolos de tunneling, por ejemplo IPsec al modificar valores de los encabezados.
- Problemas con los servicios que requieren el inicio de conexiones TCP desde el exterior de la red.

Configuración mediante iptables

- Para la configuración y habilitación de nat se utilizará IPtables.
- Se definiran varias IPs en una sola interfaz de red.
- Mediante MASQUERADE se hará NAT *:1
- Mediante DNAT y SNAT se hará NAT 1:1
- Mediante DNAT se hará port forward.

Nota: revisar laboratorio 01.