CEU

4 Capa de red II

4.2 *Internetworking*

RdE 2014-2015

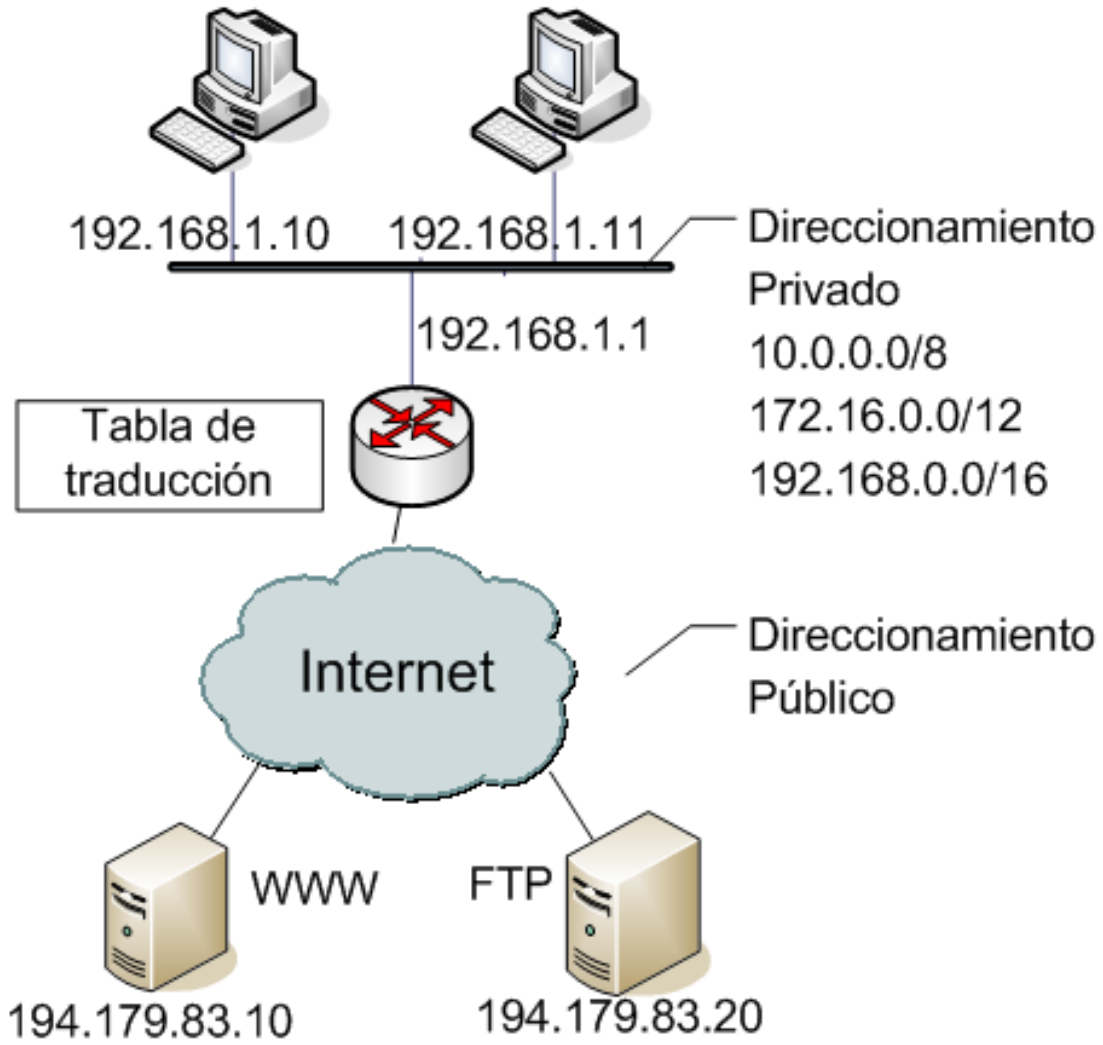
4 Guión del Tema 4

- 4 CAPA de RED II:
  - 4.1 Calidad de servicio.
  - **4.2 Internetworking.**
  - 4.3 IPv6.

4.2 NAT Network Address Translation

- **NAT** es una técnica de paso de tráfico a través de un *router* que implica la reescritura de la dirección IP origen y/o destino, y normalmente también de los puertos origen y o destino.
- La reescritura de direcciones y puertos implica el recálculo de *checksum* en el caso TCP y UDP.
- Utilidad:
  - ❑ Permitir a múltiples sistemas de una Red Privada, acceder a Internet usando una sola dirección pública.
  - ❑ Posibilitar la conexión de interredes cuyo direccionamiento se solapa.
- Existe el mito de que permite un mayor nivel de seguridad.

4.2 Uso de NAT


192.168.1.10
192.168.1.11
Direccionamiento
Privado
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
192.168.1.1
Tabla de
traducción
Internet
Direccionamiento
Público
WWW
FTP
194.179.83.10
194.179.83.20

4.2 NAT Beneficios e Inconvenientes

- Beneficios:
  - NAT permite reducir el problema del escaso número de **direcciones IP públicas**, válidas en Internet. Con este sistema una dirección se sobrecarga con varias direcciones en paralelo.
  - NAT proporciona una forma sencilla de configurar **equipos finales**. Las redes remotas pueden ser siempre la misma.
- Inconvenientes
  - La **conectividad no es realmente extremo a extremo**. Servicios que requieren la iniciación de conexiones TCP desde fuera de la red, o protocolos sin mantenimiento de estado que usan UDP. Para esto es necesario que el router "colabore" con *Application Level Gateway* ALG.
  - Los **protocolos tunelados**, p.e IPSec, se complican con NAT, ya que estos protocolos utilizan en comprobaciones de integridad valores modificados por NAT. Para solventarlo *NAT Traversal*.

4.2 Tipos de NAT

- Existen dos tipos básicos de NAT, según los campos:
  - **NAT básico**. Sólo cambio de direcciones IP.
  - **NAPT**, *Network Address Port Translation*. Involucra la traslación de direcciones y puertos.
- Si se involucra la dirección fuente, SNAT. Si se involucra la dirección, DNAT. Pueden ser aplicados simultáneamente.
- Existen dos tipos de NAT, según la temporalidad:
  - **Estático**. La tabla de conversión de dirección y puertos se carga al arrancar, y el tráfico no la modifica. Bidireccional.
  - **Dinámico**. La tabla se construye y se modifica en función del tráfico. Las direcciones y puertos se reusan. Requiere mantener en el NAT información de estado. Normalmente es unidireccional.

4.2 Tipos de NAT

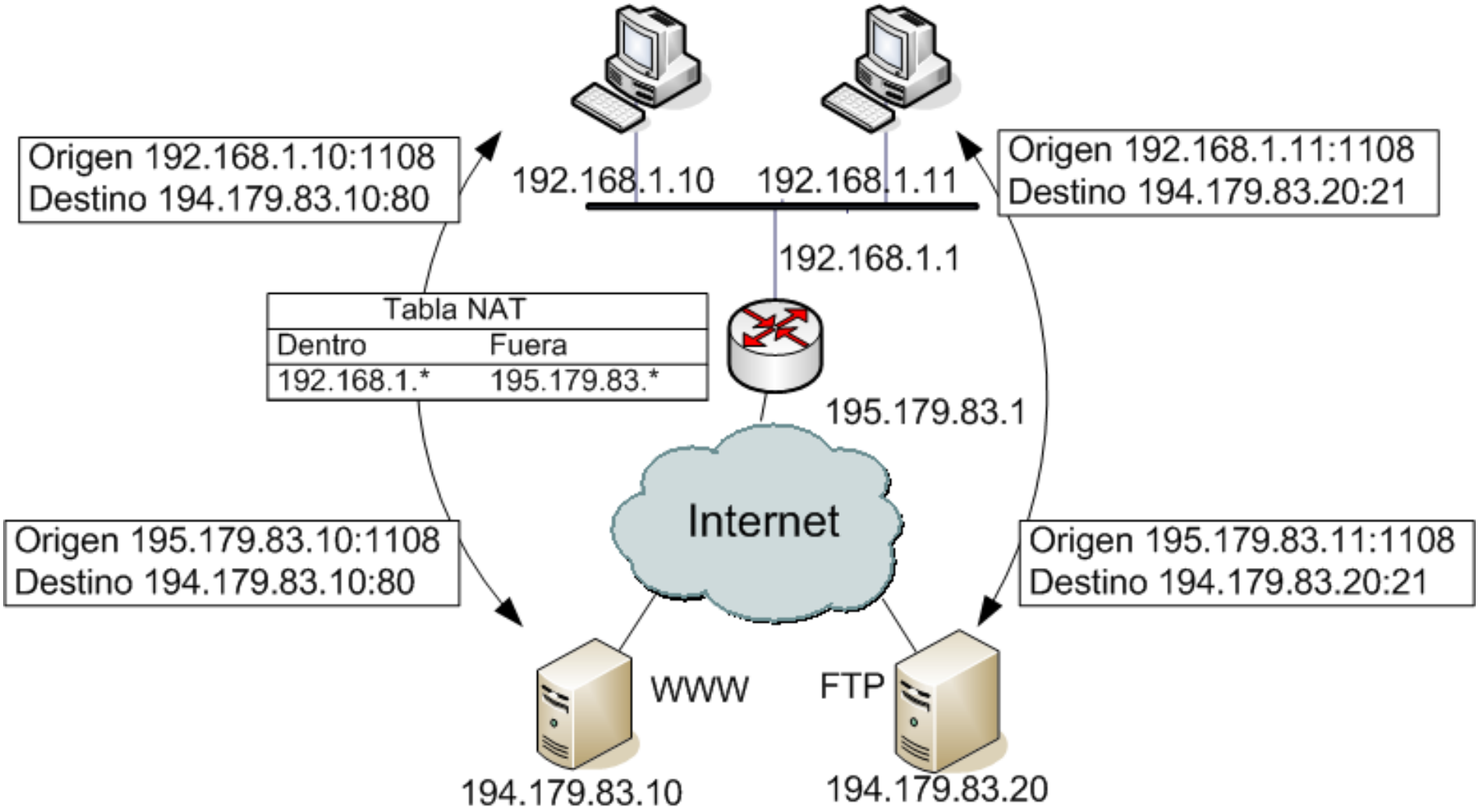
	Estático (bidireccional)	Dinámico (unidireccional)
NAT Básico	El número de direcciones públicas ha de ser igual al de privadas. **NAT Estático.**	El número de direcciones públicas puede ser menor que el de privadas, pero ha de ser suficiente para el número de ordenadores conectados simultáneamente. **NAT Dinámico.**
NAPT	En conexiones entrantes permite asociar a una misma dirección diferentes servidores, eligiendo por el número de puerto. **Port Forwarding.**	Una sola dirección pública permite la conexión de miles de ordenadores (64k) multiplexando por el número de puerto. **Overloading o PAT**.

4.2 Formas de trabajo Cisco

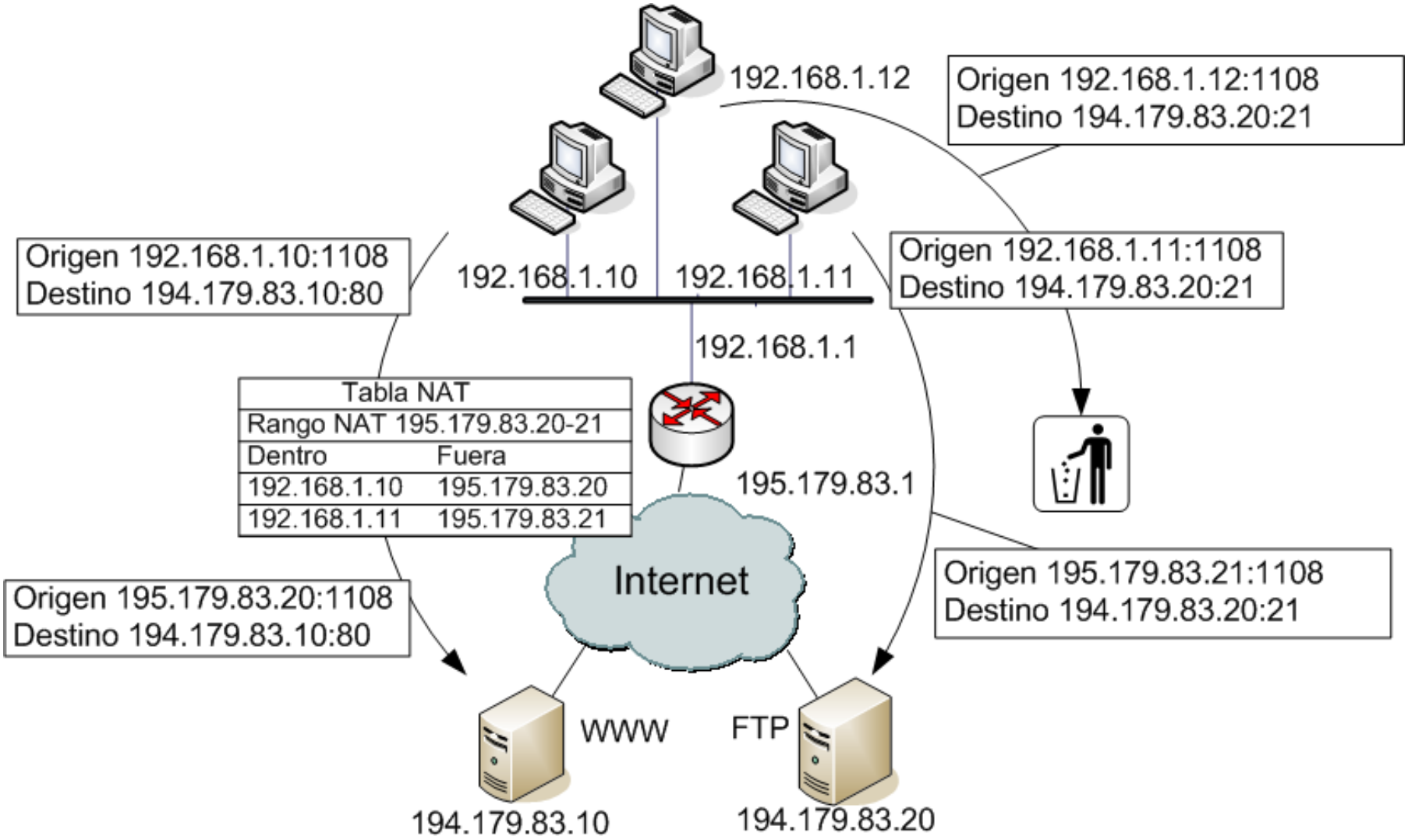
Formas de trabajo en NAT:

- **NAT estático**. Se traslada una dirección no registrada a una dirección registrada una a una. Útil cuando se precisa acceder desde Internet a una dirección interna.
- **NAT Dinámico**. Se traslada una dirección no registrada a una dirección registrada de un grupo de direcciones o pool. Establece un mapeo uno a uno entre direcciones no registradas y registradas. Depende de la disponibilidad de direcciones en el pool.
- **Overloading o PAT**. Es una forma de NAT dinámico en la que se traslada múltiples direcciones no registradas en una sola dirección registrada.
- **Overlapping**. Las direcciones internas coinciden con direcciones registradas. El *router* debe mantener una tabla de *lookup*, donde reemplace las direcciones repetidas internas por direcciones válidas.

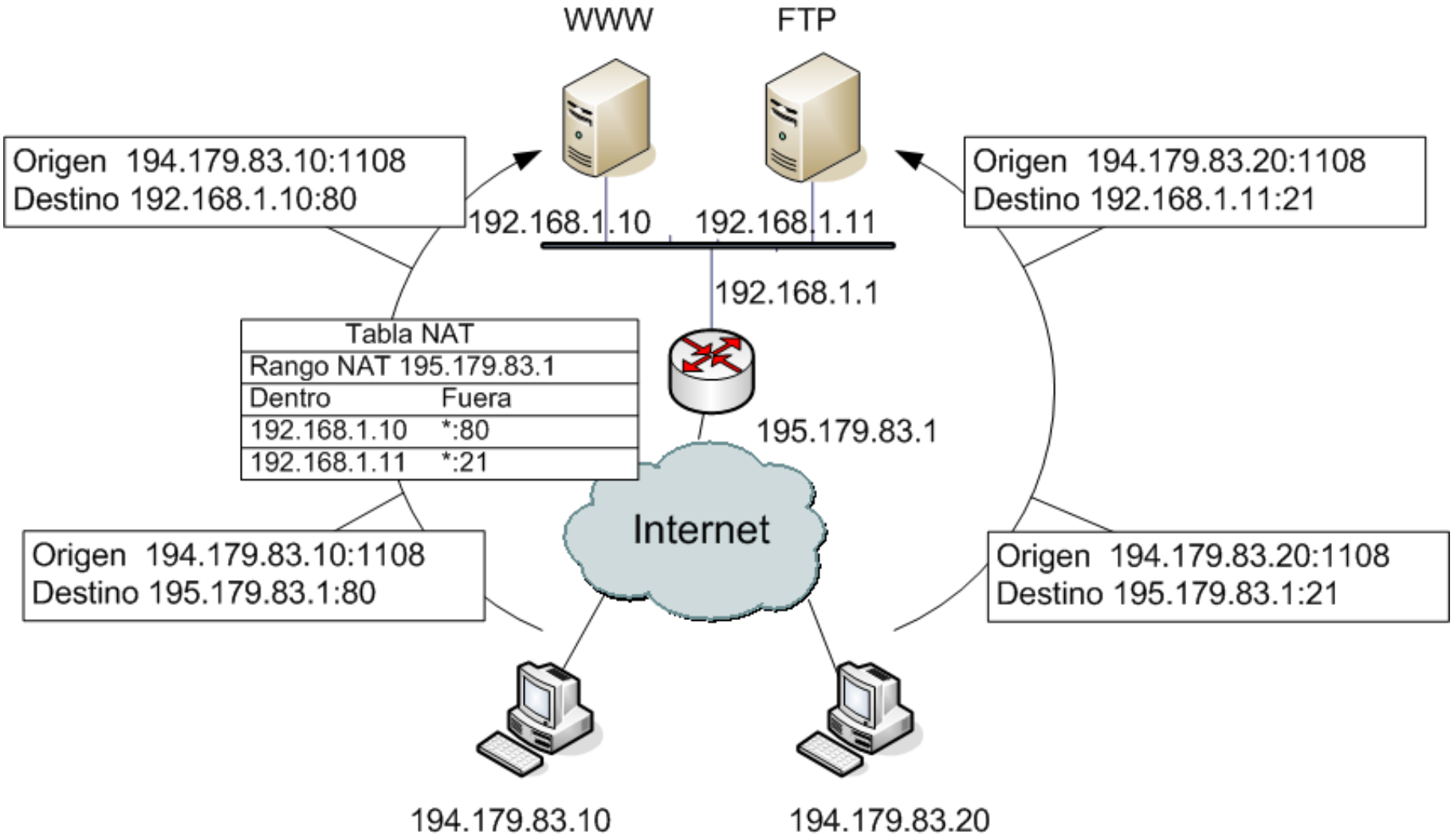
4.2 NAT Básico Estático



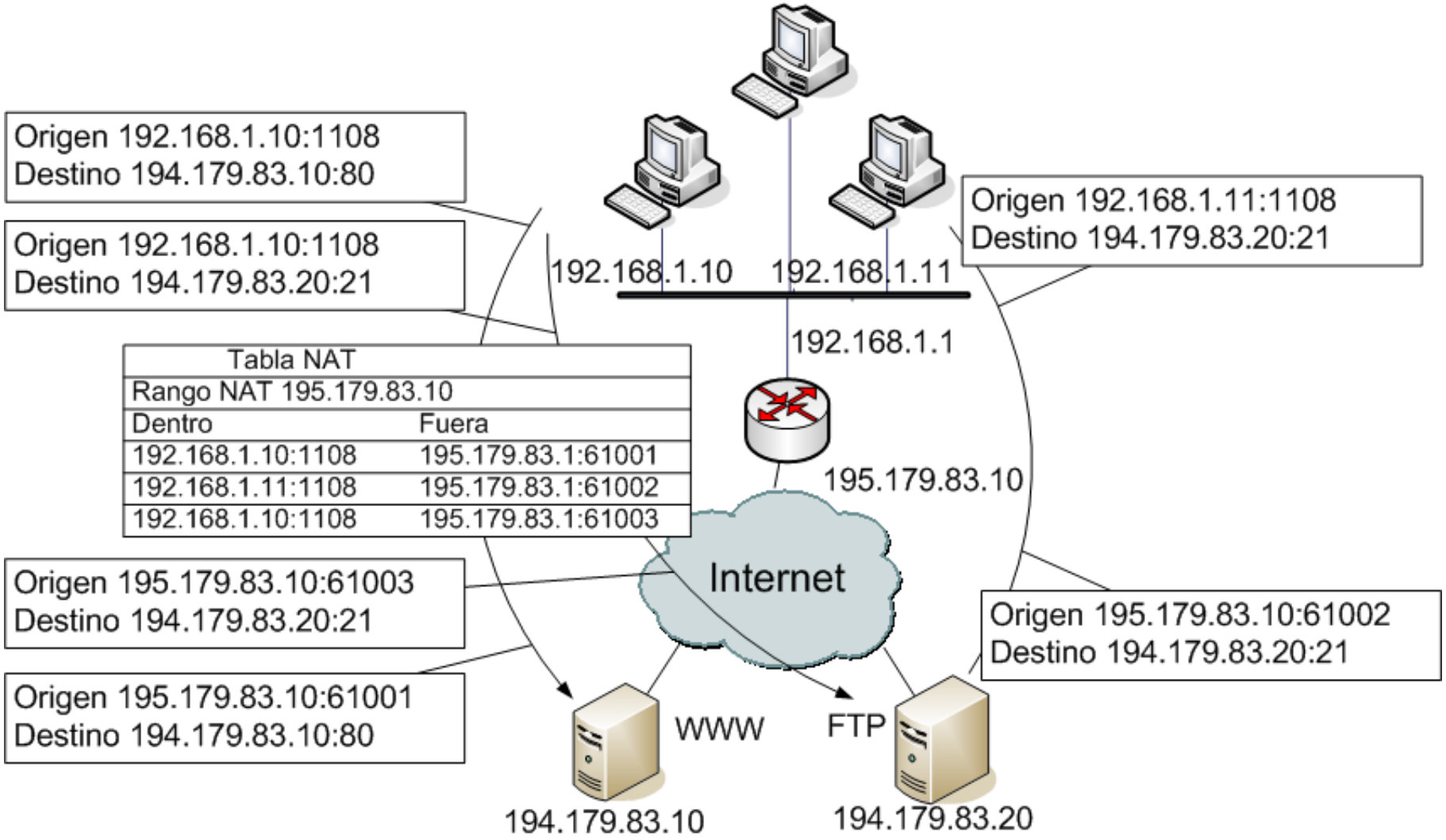
4.2 NAT Básico Dinámico



4.2 NAPT Dinámico o *Port Forwarding*



4.2 NAPT Dinámico o *Overloading* o PAT



4.2 Ejemplo de Tabla de NAT

Tabla NAT del router Zyxel P660R-T1

Comando ip nat iface wanif0

Slot	Prot	Internal-IP :Port Out	IP :Port External	IP :Port	Idle
4	UDP	192.168.200.253:64493	78.36.169.5 :12353	58.100.49.114 :43234	2
11	TCP	192.168.200.253:2798	78.36.169.5 :10013	194.186.55.21 :443	12
12	TCP	192.168.200.253:1901	78.36.169.5 :10062	205.188.8.121 :5190	1
15	TCP	192.168.200.253:1080	78.36.169.5 :10015	194.186.55.20 :2041	12
17	TCP	192.168.200.253:4800	78.36.169.5 :10021	194.186.55.21 :2041	10
18	TCP	192.168.200.253:2891	78.36.169.5 :10392	85.21.168.87 :13423	70

4.2 NAT y soporte de protocolos

IP transporta otros protocolos. NAT debe tener en cuenta el protocolo.

- **IP**. Cambios en direcciones origen y/o destino, y recalcular el *checksum*
- **TCP y UDP**. Recálculo del *checksum* que aparece en la pseudocabecera. Cambio de puertos origen y/o destino NAPT.
- **ICMP**. Cambio de las direcciones IP de la parte de datos.
- **SNMP**. Cambio de las direcciones IP transportadas.
- **IPSec**. Debe cumplir unos requisitos para que funcione a través de dispositivos. RFC 3715.

Los protocolos soportan un dispositivo que haga NAT. No se soporta dos dispositivos que hagan NAT.

4.2 NAT *Traversal*

- **NAT *Traversal***. Conjunto de técnicas para establecer y mantener sesiones a través de NAT. Técnicas muy variadas.
- Se clasifican en función su relación con NAT:
  - ❑ Técnicas basadas en el **comportamiento** de NAT, por ejemplo:
    - *Simple Traversal of UDP over NAT*, STUN.
    - *Traversal Using Relay* NAT, TURN.
  - ❑ Técnicas basadas en **control** de NAT: por ejemplo:
    - SOCKS.
    - *Application Level Gateway*, ALG.
- NAT viola el principio básico de conectividad extremo a extremo, propiciado por el IAB. IPv6 elimina la necesidad de NAT.

4.2 ALG Application Level Gateway

ALG. Application Level Gateway. Componente de los equipos que hacen NAT. Ofrece funciones extendidas que permiten el funcionamiento de NAT y ciertos protocolos:

- Uso de puertos efímeros para ciertas aplicaciones cliente para conectarse a servidores con puertos bien conocidos.
- Conversión de elementos de la capa de red dentro de la carga de pago de la aplicación.
- Reconocimiento de comandos específicos, ofreciendo controles de seguridad.
- Sincronización entre múltiples sesiones de datos de la aplicación. Por ejemplo FTP, separa una sesión para el intercambio de datos y control. La sesión de control debe mantenerse aunque venza su *timeout*.
- Revisión en profundidad de los paquetes, entendiendo los campos del protocolo.

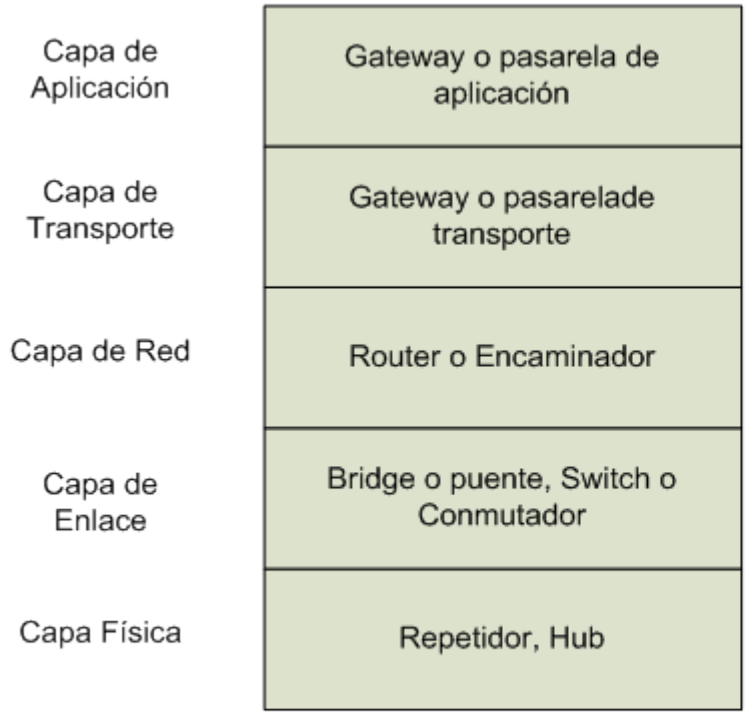
ALG: SIP, MGCP, H.323, FTP, RSTP. Similar a un servidor *proxy*.

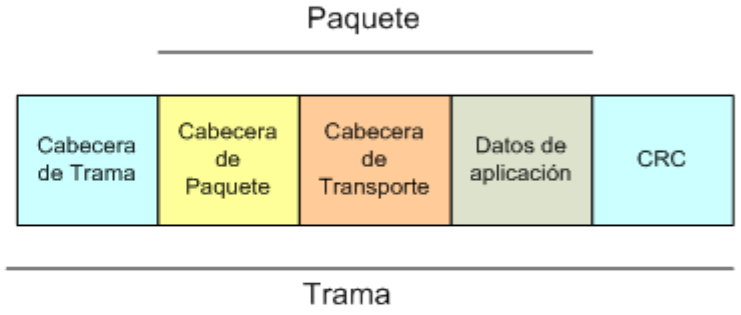
CEU

4 Capa de red II

4.2 *Internetworking (2/2)*

4.2 Elementos de red





(a) Dispositivos y Arquitectura de protocolos

(b) Estructura del paquete

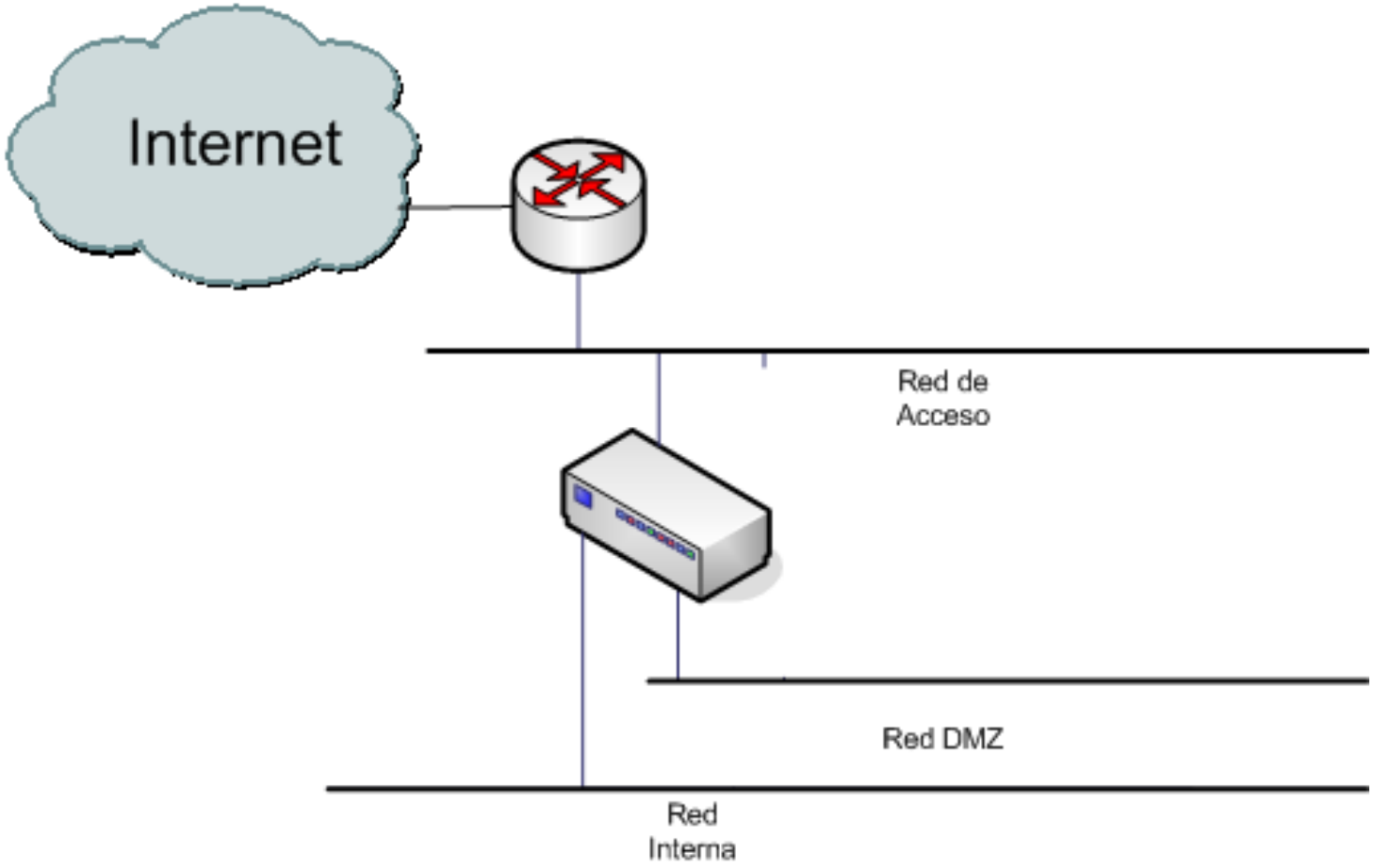
4.2 *Firewall*

- ***Firewall* o Cortafuegos**. Es una colección integrada de medidas diseñadas para prevenir el acceso no autorizado de acceso electrónico a un sistema de ordenadores en red.
- También es un dispositivo configurado para permitir, denegar, cifrar, descrifrar, o *proxificar* todo el tráfico de ordenadores entre diferentes dominios de seguridad, basado en un conjunto de reglas u otros criterios.
- Se implementan en *software*, o en *hardware* o en ambos. El *firewall* examina cada paquete y bloquea aquellos que no cumplen los requisitos de seguridad.

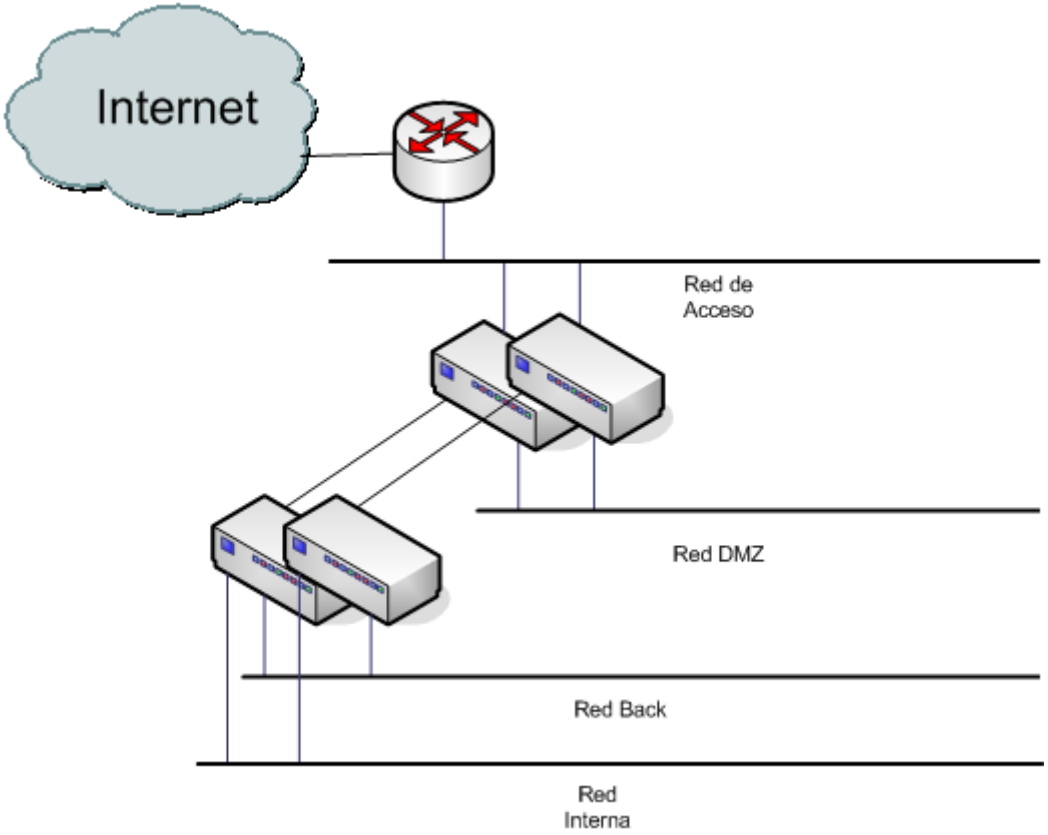
4.2 *Firewall* o Cortafuegos

- Existen varias técnicas de *Firewall* o cortafuegos:
  - **Filtrado de paquetes**. Se inspecciona cada paquete, permitiendo o denegando en función de las reglas de usuario. Es efectivo y transparente, pero difícil de configurar. Susceptible de IP Spoofing. Denegado por defecto.
  - ***Application Gateway***. Ya comentado. Consumidor de recursos.
  - ***Circuit Level gateway***. Mecanismos de seguridad cuando la conexión TCP o UDP se establece. Una vez establecida la conversación continua.
  - **Servidor *Proxy*.** Intercepta todos los mensajes de entrada y salida, interponiéndose en las conexiones. Oculta de forma efectiva las direcciones reales de la red.
- A menudo hacen la función de NAT.

4.2 Integración básica



4.2 Integración avanzada de firewall



En la red DMZ se sitúan los sistemas a los y desde los que se accede a Internet. De forma separada, protegidos por *firewall* diferentes, se sitúan las redes de *back* (datos), y las redes internas.

4.2 Historia

- **1ª generación**. 1988. Filtros de paquetes. Filtrado paquete a paquete a partir de reglas de acceso. No tiene en cuenta flujos.
- **2ª generación**. 1991. *Firewall* de estado, *Stateful Firewall. Inspection*. Tiene en cuenta que paquetes forman parte de una conexión admitida.
- **3ª generación**. 1993. *Application Layer Firewall*. El *firewall* entiende ciertas aplicaciones y protocolos.
- **Futuro desarrollo**. Integración de dispositivos tipo IPS (*Intrusion-Prevention Systems*). Mejora de los sistemas de gestión.

4.2 *Proxy*

- Un **servidor *proxy***, un sistema o programa, actúa en nombre de clientes en sus peticiones de recursos a otros servidores.
- Proceso:
  - Cliente solicita el recurso, página *web*, vídeo, fichero, al *proxy*.
  - El *proxy* evalúa la petición de acuerdo a sus reglas de filtrado.
  - El *proxy* hace la solicitud, si cumple las reglas, al servidor en nombre del cliente (incluyendo la resolución DNS). En algunos casos, la información puede haber sido solicita y el *proxy* la tiene guardada, función de *Cache*.
- Objetivos:
  - **Anonimación**. Las máquinas clientes no se conectan directamente. Seguridad.
  - **Aceleración**. Mejorar la respuesta de acceso a recursos.
  - **Acceso a Internet**. Grandes organizaciones no disponen de IP suficientes. Alternativa a NAT. Punto de control legal.

4.2 Funciones

- **Cache**. El servidor proxy puede guardar los contenidos a los que se va accediendo (PUSH) o precargar (PULL) contenidos. Primer tipo de servidores Proxy. HTTP 1.0 y posteriores, permiten especificar en la cabecera donde se declara el contenido *cacheable* (*static*), *timeout* de expiración (*expiry*), validación por fecha (*if-modified since*).
- **Web Proxy**. Servidor proxy enfocado a tráfico http. Usado desde entornos empresariales hasta hogares.
- **Antivirus**. Se integran dentro del sistema Proxy o a través del protocolo ICAP (*Internet Content Adaptation Protocol*, RFC 3507). Se inspeccionan los contenidos para evitar virus o malware.
- **Autenticación**. En entornos empresariales cada usuario debe autenticarse para acceder a contenidos en Internet.
- **Autorización**. **Filtrado de contenidos**. Asociado a la autenticación, permite acceso a contenidos en función del perfil o usuario. Integrado en el sistema proxy o a través de ICAP en un sistema externo.
- **Registro**. Asociado a la autenticación, por restricciones legales debe quedar registro de los accesos realizados.
- **Anonimación**. La dirección IP con la que se navega es la del Sistema proxy.
- ***Proxy* Transparente**. Es un *proxy* que no modifica las peticiones y respuestas, salvo las necesarias para autenticación y registro si se requiere.

4.2 Otras cuestiones

- **Circunvectores**. Existe software que permite saltar el control de los proxy. Normalmente es a su vez un *proxy* server o un software de túnel a través de HTTP. Por ejemplo elgoog en China.
  - ❑ Basado en proxy: Proxify, CGIProxy.
  - ❑ Basado en túneles: Ultrasurf, Freegate

- ***Proxys* públicos**. Usados para anonimación. Riesgo de compromiso de información personal. Actividades delictivas. Habitualmente bloqueados para acceso a ciertos sitios. Listas negras.

4.2 *Session Border Controller*

- ***Session Border Controller***. Es un dispositivo utilizado en redes de VoIP para realizar un control intermedio de la señalización, el flujo, y la terminación de la llamada. Habitualmente se utiliza para interconectar redes separadas a través de *Firewall* y/o NAT.
- Se usan por parte de las empresas para interconectar su red de ToIP con Internet. Ofrecen punto de intercepción legal.
- Implementa protocolos de señalización, H.323, SIP, MGCP, y de flujo, RTP.
- Controversia. Se argumenta que no son necesarios utilizando técnicas de NAT *Traversal*.
- En nuevas arquitecturas de redes, IMS (IP *Multimedia Subsystem*) o 3GPP (3rd *Generation Partnership Project*), aparece como un elemento de la arquitectura.

4.2 Túneles

- **Túnel**. Permite transportar un protocolo a través de otro.

- Ejemplos:
  - Mbone. Túneles *multicast* sobre redes *unicast*.
  - 6bone. Túneles IPv6 sobre redes IPv4.

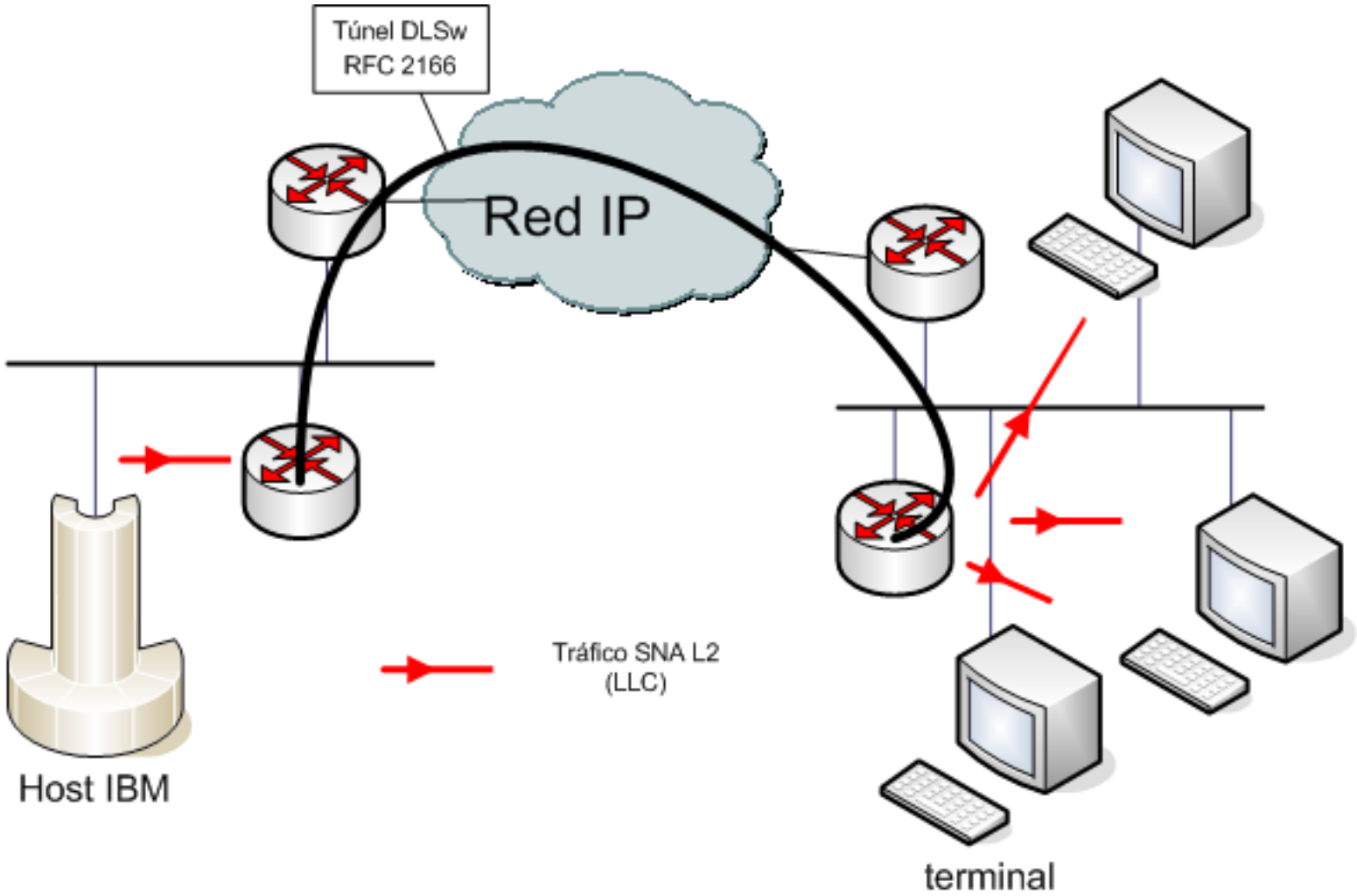
- Uso:
  - Permiten crear redes privadas virtuales o VPN.
  - Permiten a crear extensiones de redes de nivel 2, útil para protocolos no enrutables (SNA, X25).

4.2 Túneles Clasificación

Existen varios tipos de túneles:

- **Basados en datagramas**
  - GRE (Generic Routing Encapsulation). RFC 2890.
  - IP in IP. RFC 2003.
  - L2TP (Layer2 Tunneling Protocol). V3 en RFC 3931.
  - PPTP (Point-to-Point Tunneling Protocol). RFC 2661.
  - IPSec Modo Túnel.
  - MPLS (Multi-Protocol Label Switching), GTP (GRPS Tunneling Protocol), PPPoE (Point to Point Protocol over Ethernet), PPPoA (ídem ATM), XOT (X.25 over TCP), IPv6 tunneling, DLSw (SNA over IP), IEEE 802.1Q.
- **Basados en flujo:**
  - SSH.
  - SOCKS.

4.2 Ejemplo de Túnel



4.2 VPN

- **VPN, *Virtual Private Network***. Consiste en utilizar redes públicas para simular una red privada o en los operadores ofrecer a sus clientes redes separadas e independientes sobre la misma infraestructura (MPLS).
- El direccionamiento es independiente al de la red pública.
- Suele tener requisitos de cifrado. IPSec o SSL.
- Se basa en la creación de túneles entre los sitios que se quiere comunicar.
  - ❑ *Site-to-site*. Conexión de redes entre sitios.
  - ❑ *Client-to-site*. Conexión de clientes PC a un sitio central, teletrabajo.

4.2 MTU

- **MTU, Maximun Transmission Unit**. En general es el máximo tamaño de PDU que un protocolo puede enviar. Está asociado al interfaz de comunicaciones y/o fijado por el estándar de comunicaciones (p.e. ethernet).
- MTU grandes mejoran la eficiencia del protocolo, pero deben lidiar con los errores y enlaces lentos.

Medio	MTU (bytes)	Notas
Internet (RFC879)	Al menos 576	Normalmente más grande. Se usa PMTU.
Ethernet v2 (RFC 1191)	1500	Normalmente IP sobre ethernet usa v2.
Ethernet 802.3 (RFC 1191)	1492	
Ethernet Jumboframes	1500-9000	Depende del fabricante. Debe ser la misma.
802.11	2272	
802.5	4464	
FFDI (RFC 1191)	4500	

4.2 PMTUD

- **PMTUD, Path MTU Discovery**, RFC 1191. Se basa en el envío de datagramas al destino con el bit DF=1, de modo que los *router* intermedios comuniquen la MTU.
- Actualmente es poco práctico debido a que los mensajes ICMP (*Destination Unreachable: datagram too big*) se bloquean, por motivos de seguridad.
- Como técnica alternativa existe el uso de MSS, *Maximum Segment Size*, en TCP.

4.2 Bibliografía

[1] Tanenbaum, A. S., Computer Networks, Pearson 2003, apartado 5.5 y 5.6.

[2] Comer, D. E., TCPIP Principio Básicos, Protocolos y Arquitectura, 3ª Ed Prentice Hall 1995. Capítulo 16.

[3] RFC 1631 The IP Network Address Translator.

[4] Geoff Huston, APNIC , Anatomy: A Look Inside Network Address Translators, The Internet Protocol Journal - Volume 7, Number 3