VPNs,Túneles,NATs, Firewalls

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

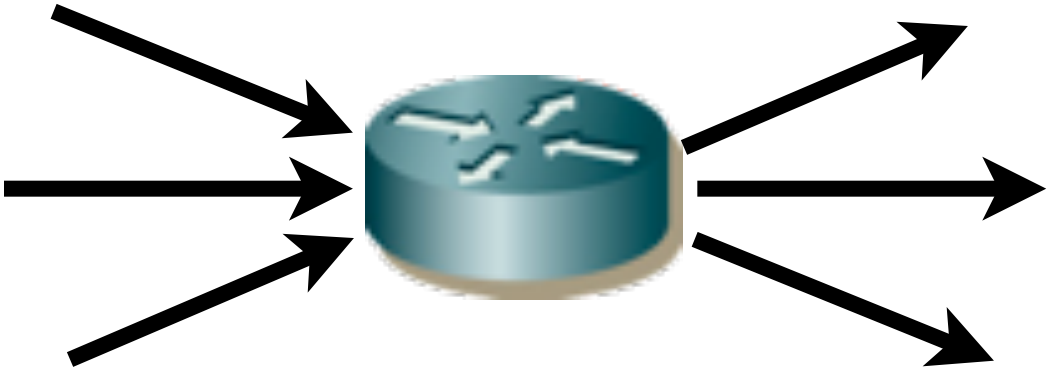
Redes
4º Ingeniería Informática

Hoy...

1. **Introducción a las redes**
2. Tecnologías para redes de área local
3. Conmutación de circuitos
4. Tecnologías para redes de área extensa y última milla
5. Encaminamiento
6. Arquitectura de conmutadores de paquetes
7. Control de acceso al medio
8. Transporte extremo a extremo

Router / Nivel 3 / Red

- Reenviar datagramas
  Según la dirección de destino
  El resto es cosa de los extremos de la red



Router / Nivel 3 / Red

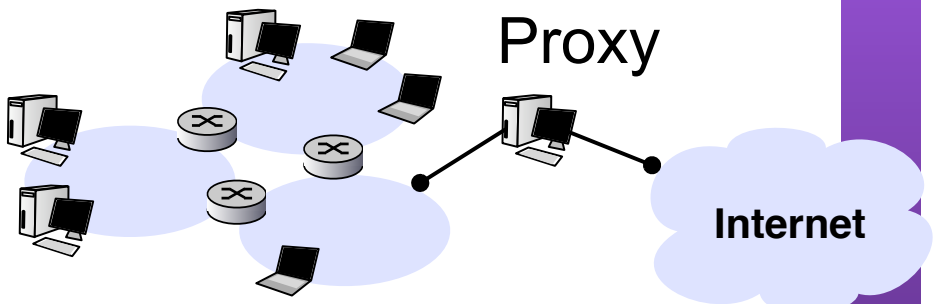
- Pero poco a poco las cosas se han ido complicnado...
- Veamos algunos casos mas complicados del nivel de red...
  - Intranets y redes privadas...
  - ... NATs
  - VPNs y virtualización de enlace...
  - ...Tuneles
  - Mezclando todo

Intranets

- Intranet
  - Construir una red con protocolos TCP/IP
  - Aislada físicamente de Internet
  - Direccionamiento sin tener en cuenta el de Internet
  - Usar y configurar nuestros propios servidores raiz de DNS
  - Algoritmos de enrutamiento que queramos
- Red de tipo Internet pero aislada
  - Puede ser una opción para algunas empresas
  - Por seguridad
- Y si luego quiero conectarla a Internet?
- Y si quiero conectarla a Internet de forma limitada?

Conectando Intranets a Internet

- A nivel de aplicación: Proxies
  - Un host multihomed puede estar a la vez en la Intranet y en Internet
  - La aplicaciones se pueden configurar para realizar servicios usando Inet a través del proxy (ej navegadores web piden las paginas al proxy)

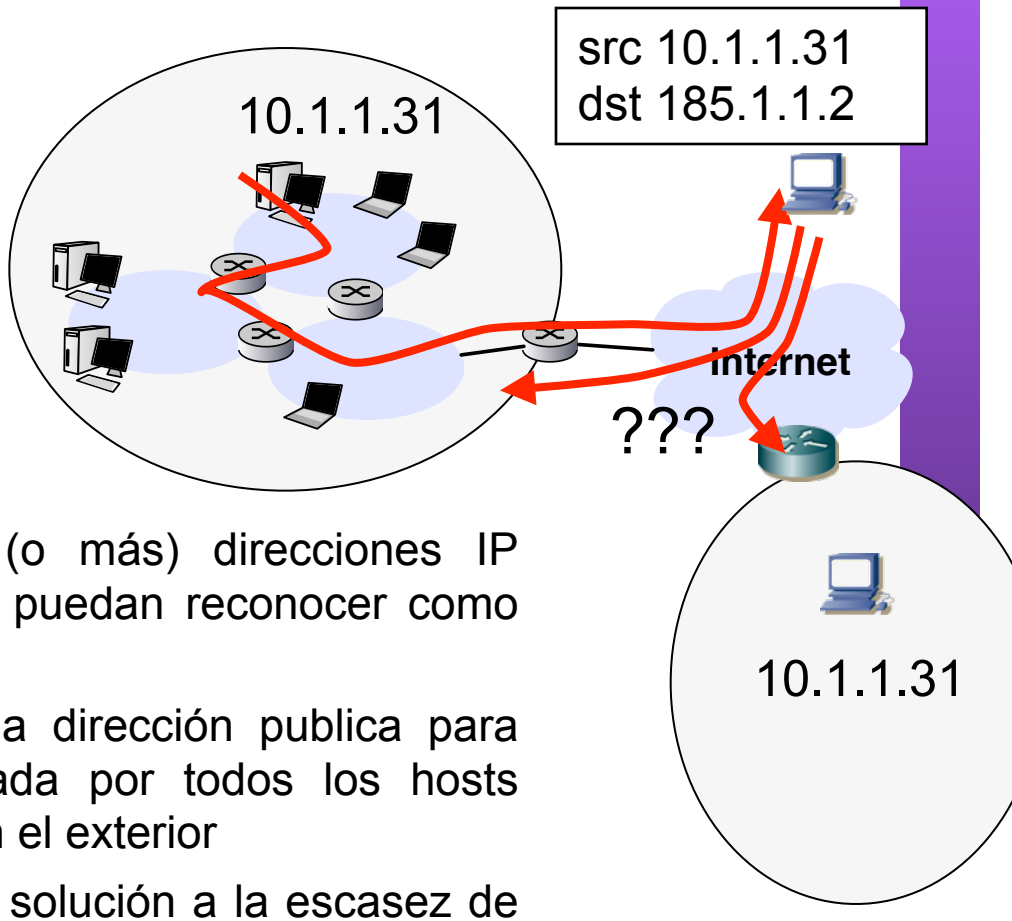


- A nivel de red
  - Problema de colisión en el direccionamiento
  - Para eso están los rangos de direcciones IP de usos privados

    10/8,172.16/12, 192.168/16, 169.254/16

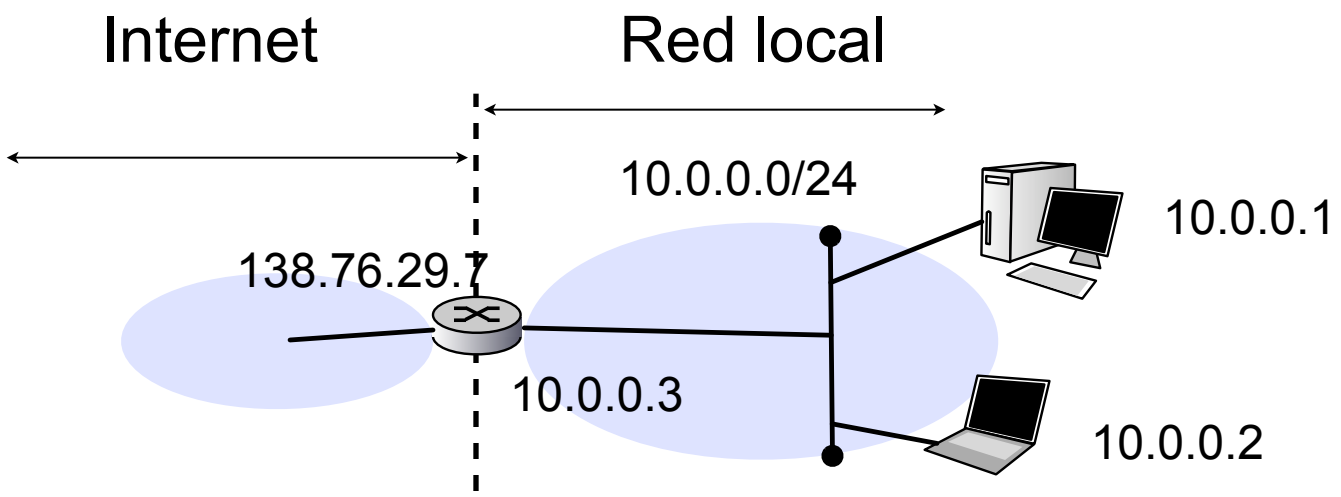
Conectando Intranets a Internet

- A nivel de red
  - El direccionamiento privado no es suficiente
  - Los host de Internet no pueden comunicarse con IPs privadas (que estaran en más de una Intranet)
  - Es necesario conseguir una (o más) direcciones IP publicas que los host externos puedan reconocer como direcciones de Internet
  - Se puede usar desde una sola dirección publica para toda la Intranet que será usada por todos los hosts internos que se comuniquen con el exterior
  - Esto representaba también una solución a la escasez de direcciones IP



NAT (Network address translation)

- Traducción de direcciones de red
  - Aparece para permitir a varios ordenadores compartir una unica IP
  - Los ordenadores internos usan un rango de direcciones privadas
  - Todos los paquetes que salen hacia internet llevan la misma IP origen
    - El problema es como dirigir los paquetes de respuesta que llegan al router
    - Se utilizaran los puertos



NAT: router

- Funciones de un router con NAT
  - Datagramas salientes de la red

    reemplazar (dirIP, puerto) origen por (dirIPexterna, nuevoPuerto)
  - Mantener una tabla de (dirIP,puerto) reemplazados
  - Datagramas entrantes

    reemplazar (dirIPexterna, puerto) destino por los que correspondan en la tabla

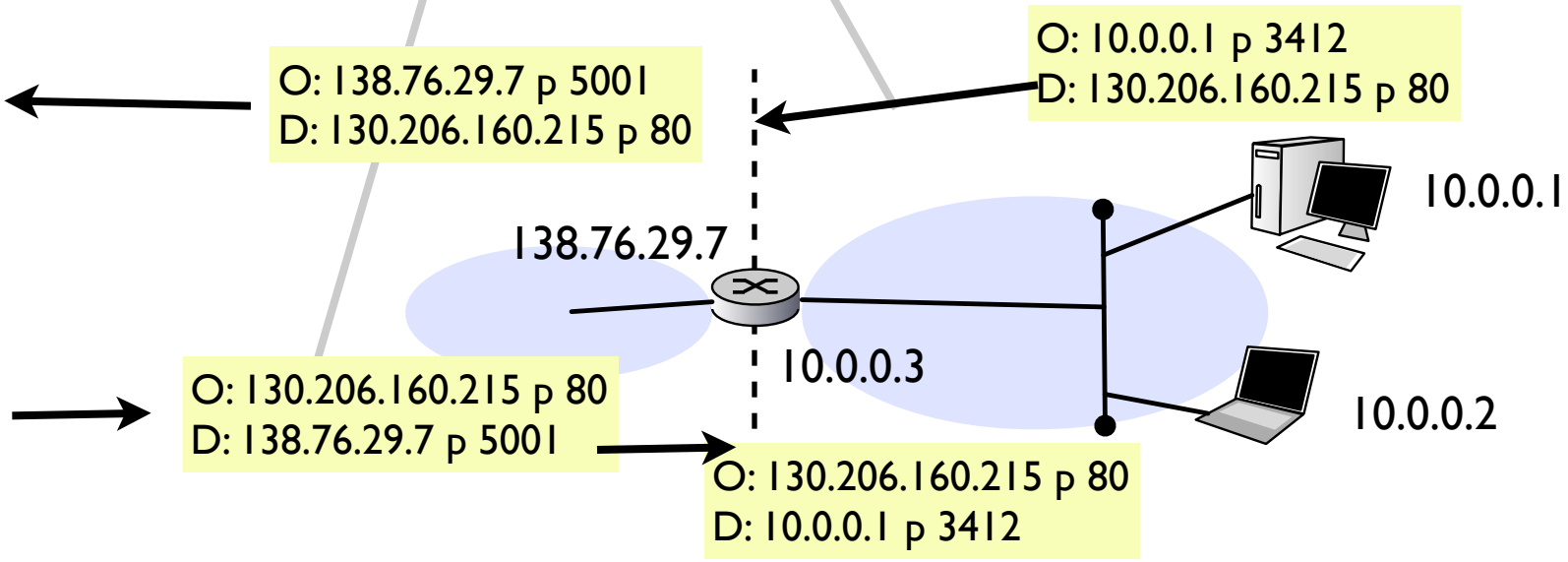
    descartar los (dirIPexterna, puerto) destino que no estén en la tabla
  - Normalmente se permite también asignar (dirIPexterna, puerto) a (dirIPinterna, puertointernos) determinados

    PortForwarding

NAT: ejemplo

Tabla de NAT

Red externa	Red interna
138.76.29.7 p 5001	10.0.0.1 p 3412



NAT: Ventajas

- Desde el exterior la red externa usa una única IP
  - Más fácil de conseguir del ISP
  - Podemos cambiar las direcciones internas sin avisar al exterior
  - Podemos cambiar de ISP sin reconfigurar la red interna
  - Los dispositivos internos **NO son accesibles desde fuera** (clientes pero no servidores)
    - Más **complejidad** para algunas aplicaciones
      Esto es un coste que estropea las ventajas
    - Es una ventaja para la seguridad
      Los dispositivos no son direccionables desde fuera

NAT: Problemas

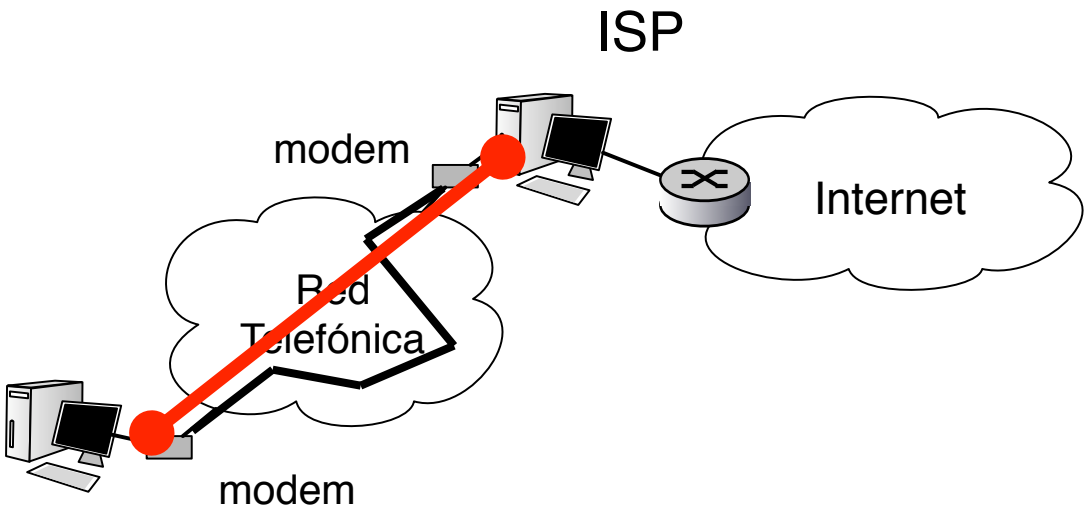
- Número de conexiones limitadas
  - puerto origen 16 bits: 65000 conexiones

    o limitación debido al espacio necesario para la tabla
- Problemas de NAT
  - Dispositivo de RED que usa información de nivel de TRANSPORTE

    Los routers no deberían manejar información de nivel de transporte
  - contrario a la filosofia extremo-a-extremo (app no conoce el puerto de su aplicacion peer, app no conoce su propia dirección IP)
    - Las aplicaciones deben tenerlo en cuenta
    - Importante en aplicaciones peer-2-peer, el NAT solo se puede atravesar a iniciativa de un cliente en la red local
  - Dificulta el desarrollo de aplicaciones peer-2-peer
  - La escasez de direcciones debería resolverse con IPv6

Virtualización de enlaces

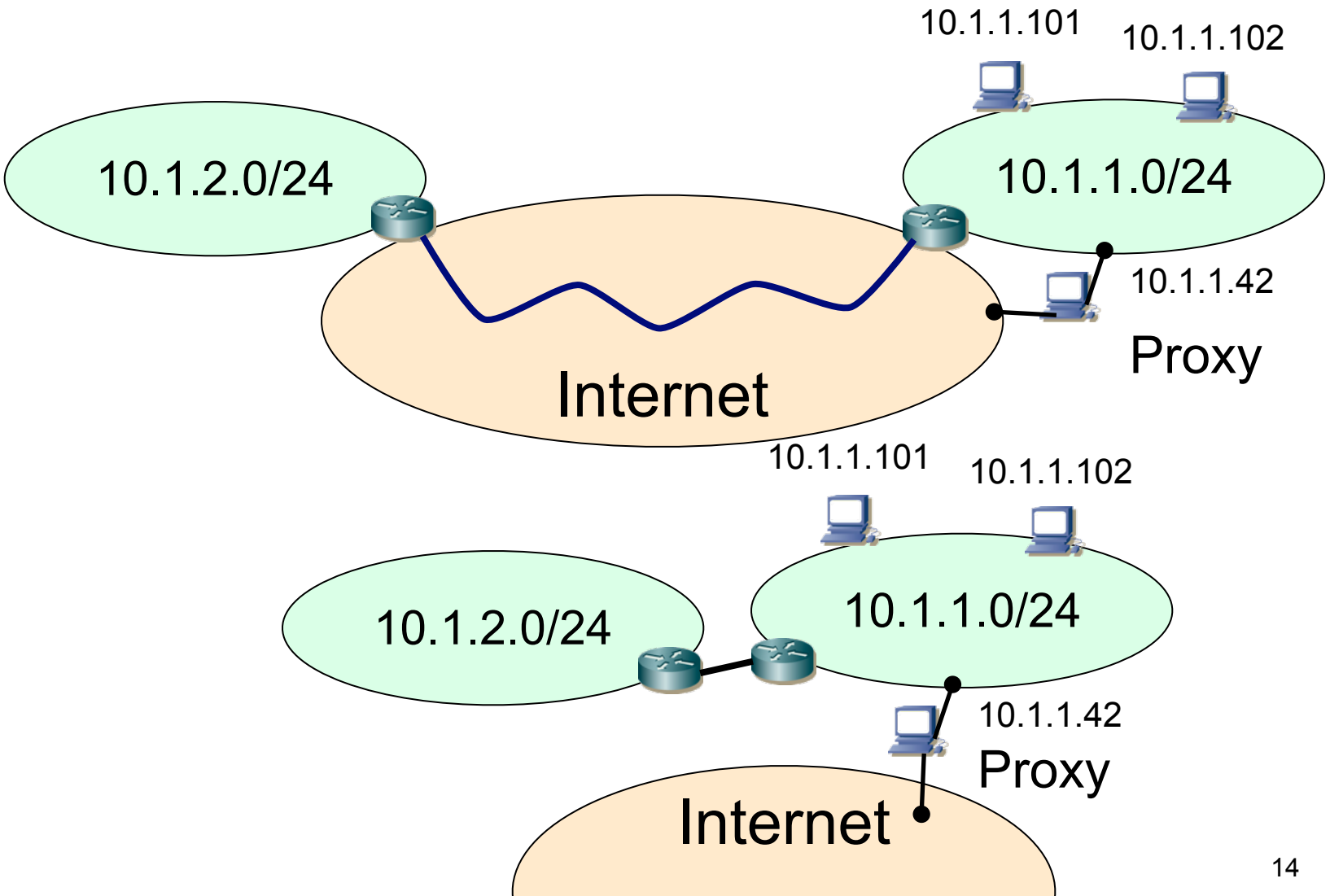
- Uniendo redes privadas a través de otra red
- Enlaces virtuales sobre una red subyacente
- Ejemplos conocidos:
  - Acceso telefónico a Internet



  - Podemos hacer lo mismo para unir redes

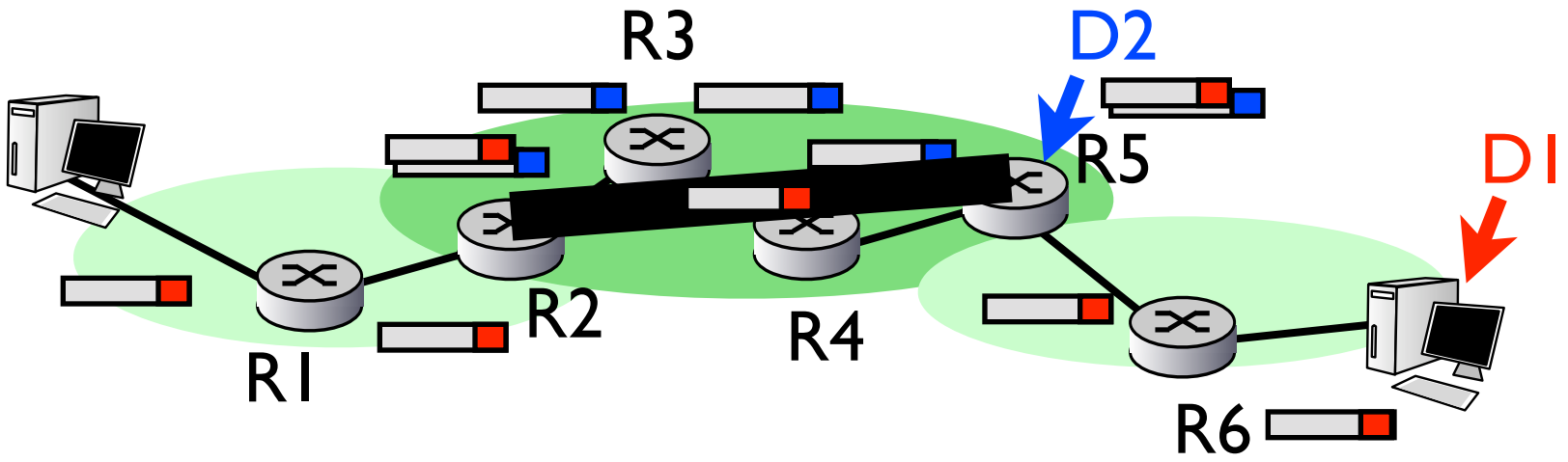
VPNs de tipo enlace

- VPNs para unir redes privadas



Túneles

- Al transportar un paquete en una red de ordenadores este es encaminado siguiendo la dirección de destino del paquete (D1)
- Si un router intermedio R2 encapsula el paquete que va a D1 dentro de un nuevo paquete que va a R5 (D2) los routers R3 y R4 encaminarán ese paquete a hacia R5 sin saber el destino final del paquete
- Se dice que el paquete ha sido enviado a través de un tunel R2-R5
- Los routers intermedios actuan como un nivel de enlace punto a punto entre R2 y R5
- El paquete puede ir encapsulado dentro de un paquete IP (IP over IP), UDP o de una conexión TCP o cualquier protocolo que sirva para que R2 envíe datos a R5



Protocolos de tunel

- IP in IP (protocol=4) RFC 2003
- GRE (protocol=47) RFCs 1701,2784

- PPP
- PPTP, L2F, L2TP

- MPLS
- ATM

Firewalls

- Elemento de nivel 3 (router, ip_forwarding=1)
- Aplica reglas para filtrar
  - Incluso accediendo a información de transporte

- Tipos:
  - Filtro de paquetes:
    Reglas por cada paquete, sin estado
  - Inspección de estados
    Reglas con estado, sigue la conexión TCP

Resumiendo...

- Direcciones privadas e Intranets
- NATs para llegar a Internet
- VPNs/tuneles para extenderlas sobre Internet
- Firewalls para filtrar

Transición IPv4 - IPv6

- Dificil hacer la transición a un nuevo protocolo de red
  - La transición de los protocolos originales de ARPAnat a TCP/IP llevo 1 año en los primeros tiempos de Internet (1982-1983 ver RFC801)

    Hoy ya no se puede poner un dia para actualizar todos los routers
- 2 propuestas (RFC-2893)
  - **Dual-stack**

    Todos los host que implementen IPv6 tienen tambien IPv4

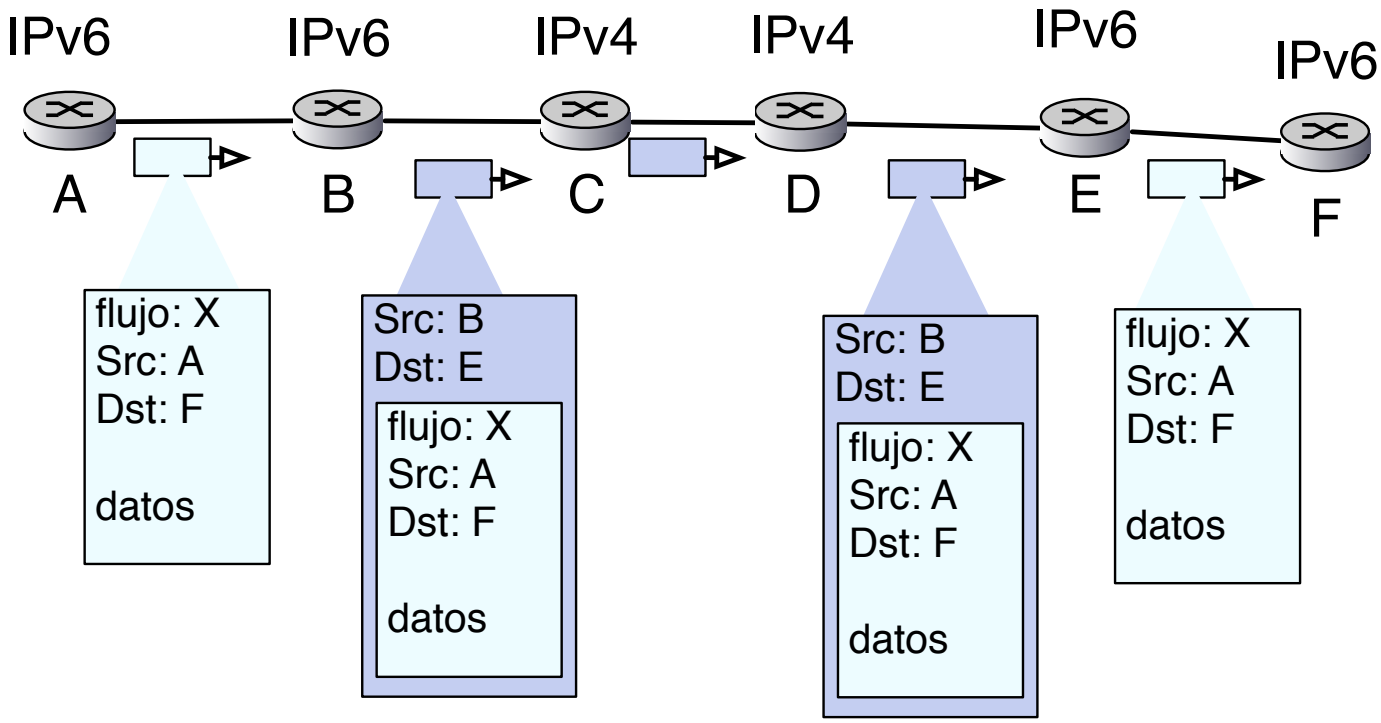
    Según con quien se comuniquen usan uno u otro (DNS devuelve direcciones v4 o v6)
  - **Tunneling**

    Islas IPv6 conectadas por zonas IPv4

    Paquetes IPv6 encapsulados en paquetes IPv4

Transición IPv4 - IPv6

- Tuneles sobre IPv4



Conclusiones

- En la realidad el modelo de nivel 3 que sólo reenvía datagramas según la dirección de destino tiene muchas excepciones
- Entender que es y principios básicos
  - NAT
  - Túneles/VPNs
  - Firewalls