:: Redes ::

- aplicación
- **transporte**
- **red**
- enlace
- física

Redes Privadas

David Villa <David.Villa@uclm.es> :: http://www.inf-cr.uclm.es/www/dvilla/

Contenidos

- Introducción
- Direccionamiento
- Redes Privadas Virtuales (VPN)
- Traducción de Dirección de Red (NAT)

Introducción

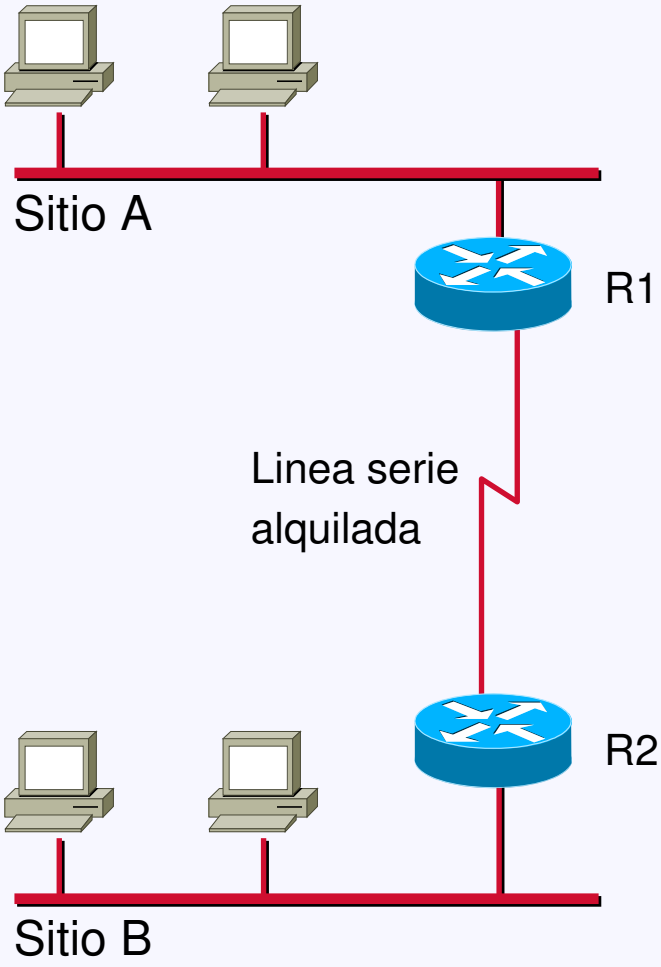
- **Red Privada:** Una red de computadores aislada de Internet.
- Una red privada se usa por una organización para gestionar el **acceso a recursos** compartidos por parte de sus empleados con un alto grado de **privacidad**.
- **Intranet:** Una red privada que conecta varios lugares y que utiliza la pila TCP/IP y los servicios típicos asociados.
- **Extranet:** Es similar a una Intranet pero algunos de los recursos de la red privada pueden ser accesibles para usuarios ajenos a la red previa autorización.

Direccionamiento para Redes Privadas

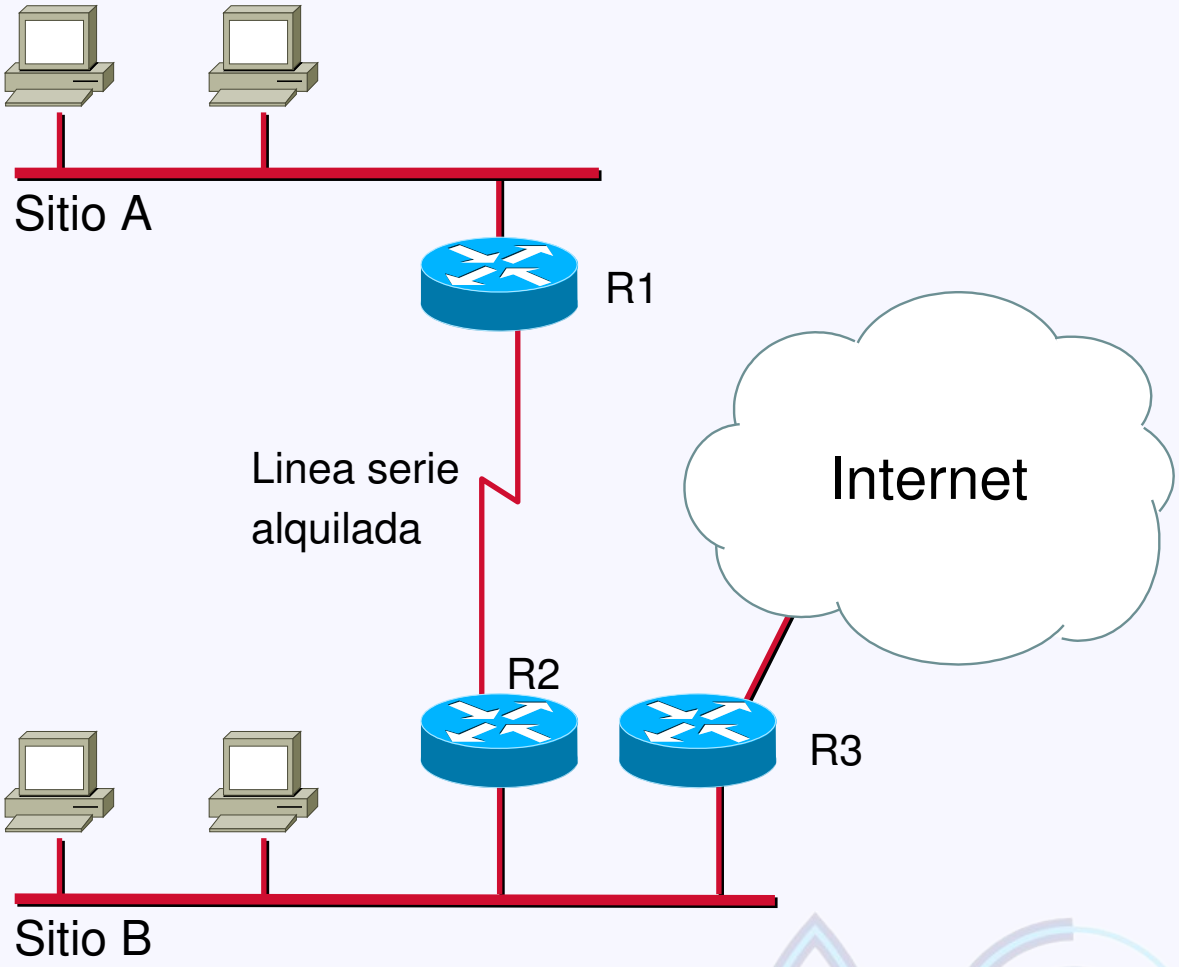
Tres posibilidades:

- Utilizar direccionamiento público otorgado por una entidad autorizada. Útil si la organización prevé conectarse a Internet en el futuro.
- Utilizar direccionamiento público no otorgado por una entidad. Plantea un grave problema si la red se conecta a Internet en el futuro.
- Utilizar los rangos de direccionamiento privado previstos para tal fin.
  - 10.0.0.0 - 10.255.255.255 /8 (16.777.216 hosts, 1 bloque)
  - 172.16.0.0 - 172.31.255.255 /12 (1.048.576 hosts, 16 bloques)
  - 192.168.0.0 - 192.168.255.255 /16 (65.536 hosts, 256 bloques)

Red Privada & Red Híbrida



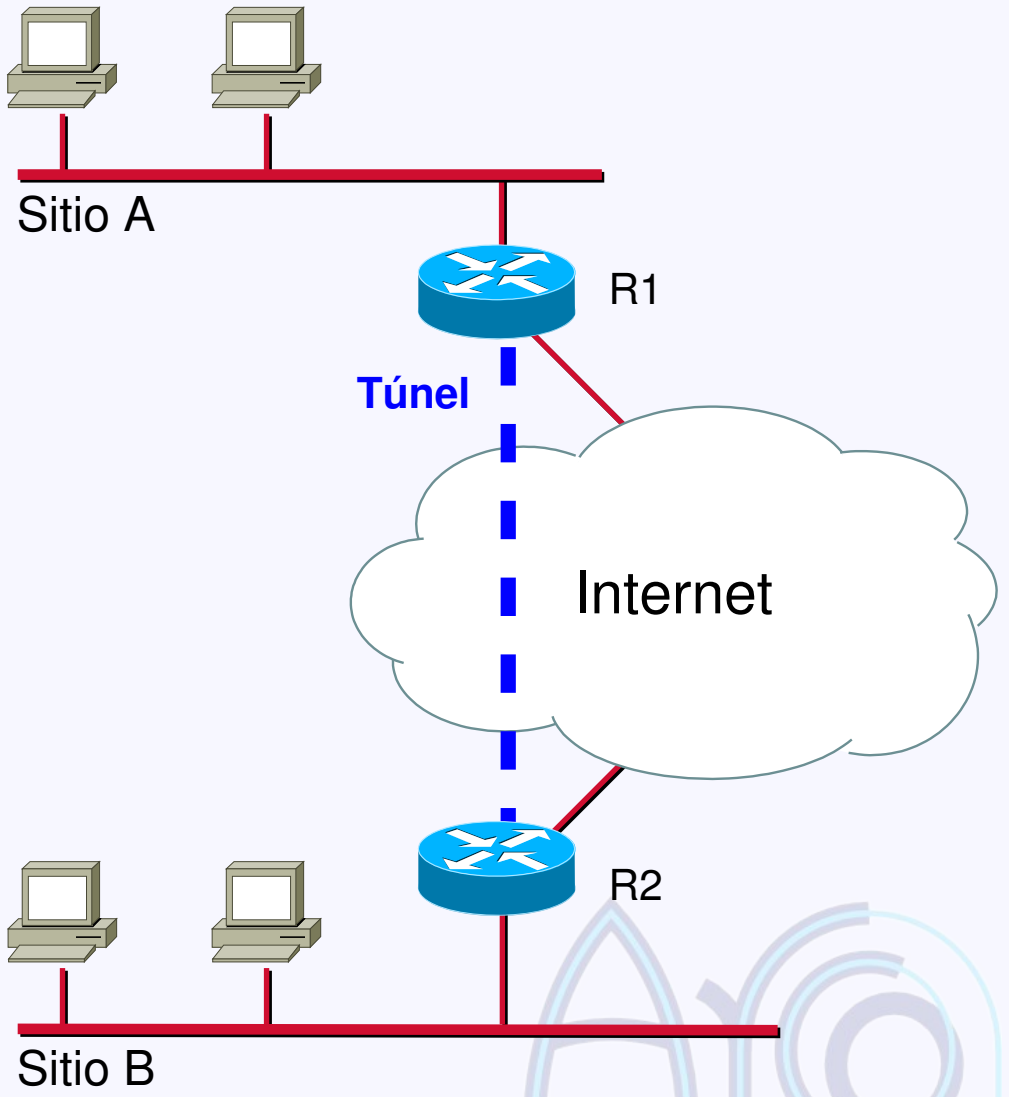
Red Privada



Red Híbrida: Es una red privada con conexión a Internet

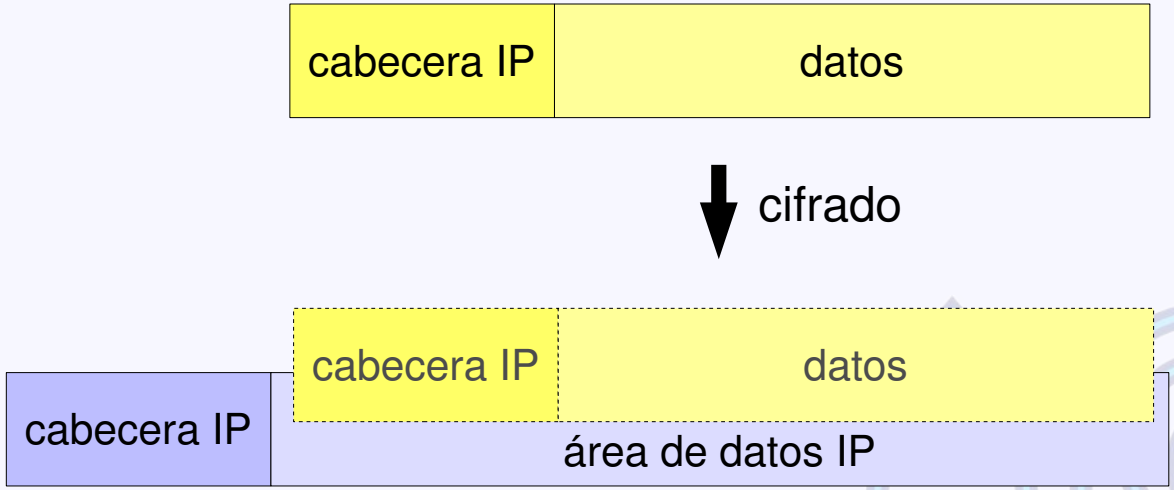
Red Privada Virtual :: VPN *(Virtual Private Network)*

- Es similar a red híbrida pero evitando el alto coste de líneas alquiladas para conectar los distintos lugares.
- Se utiliza Internet para la comunicación interna (por eso es virtualmente privada).
- El tráfico interno se cifra y se encapsula en un **túnel** hasta el lugar «interno» de destino.



Red Privada Virtual

- El **tráfico interior** (destinado a otros lugares) de la red privada se encapsula con IPSec. Puede usar AH *(Authentication Header)* y ESP *(Encapsulation Security Payload)*.
- Se cifra el datagrama completo (incluyendo la cabecera).
- El enrutador destino desencapsula el datagrama y lo enruta hacia el host en la red privada.



VPN de acceso :: acceso remoto a redes

- Conexión a demanda de usuarios externos (no pertenecientes a la red corporativa) utilizando redes IP.
- Dos alternativas:
  - Acceso de nodos externos utilizando Servidores de Acceso a la Red (NAS).
  - Acceso de nodos externos utilizando NAS de terceros.
- Las dos soluciones utilizan normalmente PPP para enviar paquetes IP al NAS.

NAS (*Network Access Server)*

El NAS se encarga de:

1. La interfaz con el medio físico.
2. Terminación lógica de la sesión LCP.
3. Autenticación PPP.
4. Agregación de canales según el protocolo Multilink PPP.
5. Terminación lógica de la sesión NCP.
6. Enrutamiento de paquetes a nivel de red.

Protocolo RADIUS *(Remote Access Dial-In User Service)*

RFC 2865

- Aspectos del acceso a redes (protocolos AAA)
  - Autenticación (Authentication).
  - Autorización (Authorization).
  - Contabilidad (Accounting).
- Características:
  - Modo cliente/servidor.
  - Seguridad: Las comunicaciones se autentican con una clave compartida (MD5).
  - Autenticación flexible: Varios mecanismos (PAP, CHAP)
  - Lista (atributo, valor): User-Name, User-Password, Framed-IP-Address, etc.

Túneles

- Un túnel IP es un encapsulamiento de paquetes IP en otro medio, simulando una conexión **punto a punto**.
- Ejemplos: IP sobre X25, IP sobre Frame-Relay, IP sobre ATM, IP multicast sobre IP, IP sobre IP, IPv6 sobre Ipv4.
- Implementación de IP sobre IP:
  1. Se encapsula el paquete IP original sobre otro paquete IP.
  2. Igual, pero se añaden cabeceras de información suplementarias.

Protocolo PPTP *(Point-to-Point Tunneling Protocol)*

RFC 2637

- Se utiliza para enviar paquetes PPP a través de una red IP.
- Las funciones de NAS y VPN están separadas.
- PPTP divide las funciones del NAS (explicadas antes)
  - El PAC *(PPTP Access Concentrator)* se encarga de las funciones 1 y 2.
  - El PNS *(PPTP Network Server)* se encarga de las funciones 4, 5 y 6.
  - La función 3 puede corresponder a uno u otro dependiendo de la implementación.

Protocolo PPTP

- Ventajas de separar las funciones del NAS:
  - Gestión más flexible de direcciones IP.
  - Permite utilizar redes de acceso IP para protocolos no IP.
- Usos
  - Se puede usar de forma obligatoria (y transparente) en el servidor de acceso.
  - El cliente lo puede utilizar de forma voluntaria siendo independiente del servidor de acceso.

Protocolo PPTP

- Hay dos componentes paralelos:
  - Una conexión de control entre cada PAC-PNS usando TCP.
  - Un túnel IP entre cada PAC-PNS que usa GRE *(Generic Routing Encapsulation)* para encapsular paquetes PPP de las sesiones de los usuarios.
- La conexión de control:
  - Se establece antes que el túnel. Es responsable del establecimiento, gestión y eliminación de las sesiones del túnel.
  - Con la conexión de control se pueden pedir llamadas salientes o autorizar llamadas entrantes.

Protocolo PPTP

- Proceso de Túnel PPTP:
  - Un túnel para cada par PNS-PAC.
  - El túnel transporta los mensajes PPP de todos los usuarios entre PNS-PAC.
  - El túnel se crea mediante el protocolo GRE (PPP sobre IP).
  - Un campo en la cabecera GRE permite distinguir las múltiples sesiones en el túnel.
  - La cabecera GRE dispone también de campos de secuencia y reconocimiento útiles para el control de flujo y congestión, y garantizar el orden de los mensajes PPP.

Protocolo PPTP :: Mensajes

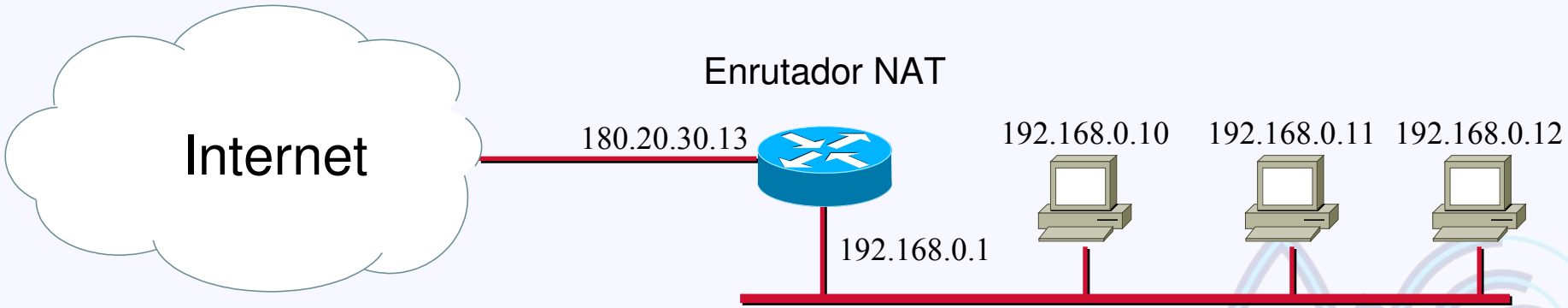
- Tipos de mensajes de control:
  - Start-Control-Connection-Request / Reply
  - Stop-Control-Connection-Request / Reply
  - Echo-Request / Reply
- Tipos de mensajes de gestión de llamadas:
  - Outgoing-Call-Request / Reply
  - Incoming-Call-Request / Reply
  - Incoming-Call-Connected
  - Call-Clear-Request
  - Call-Disconnect-Notify

Protocolo L2TP (Layer Two Tunneling Protocol)

- Es una combinación del protocolo L2F *(Layer Two Fordwarding)* de Cisco y PPTP. Tiene la misma funcionalidad que PPTP. Es más flexible pero también más complejo.
- L2TP permite encapsular mensajes PPP sobre cualquier red de forma transparente.
- Utiliza dos tipos de mensajes
  - **Control:** Para establecimiento, mantenimiento y eliminación de conexiones y túneles. Utilizan un canal de distribución seguro.
  - **Datos:** Se utilizan para encapsular mensajes PPP sobre el túnel. Su entrega no está garantizada.

Traducción de Dirección de Red (NAT)

- Permite que una red con direccionamiento privado pueda comunicarse con el exterior por medio de una o varias direcciones globales.
- El software NAT reside en el encaminador que tiene la única conexión hacia el exterior.



Traducción de Dirección de Red

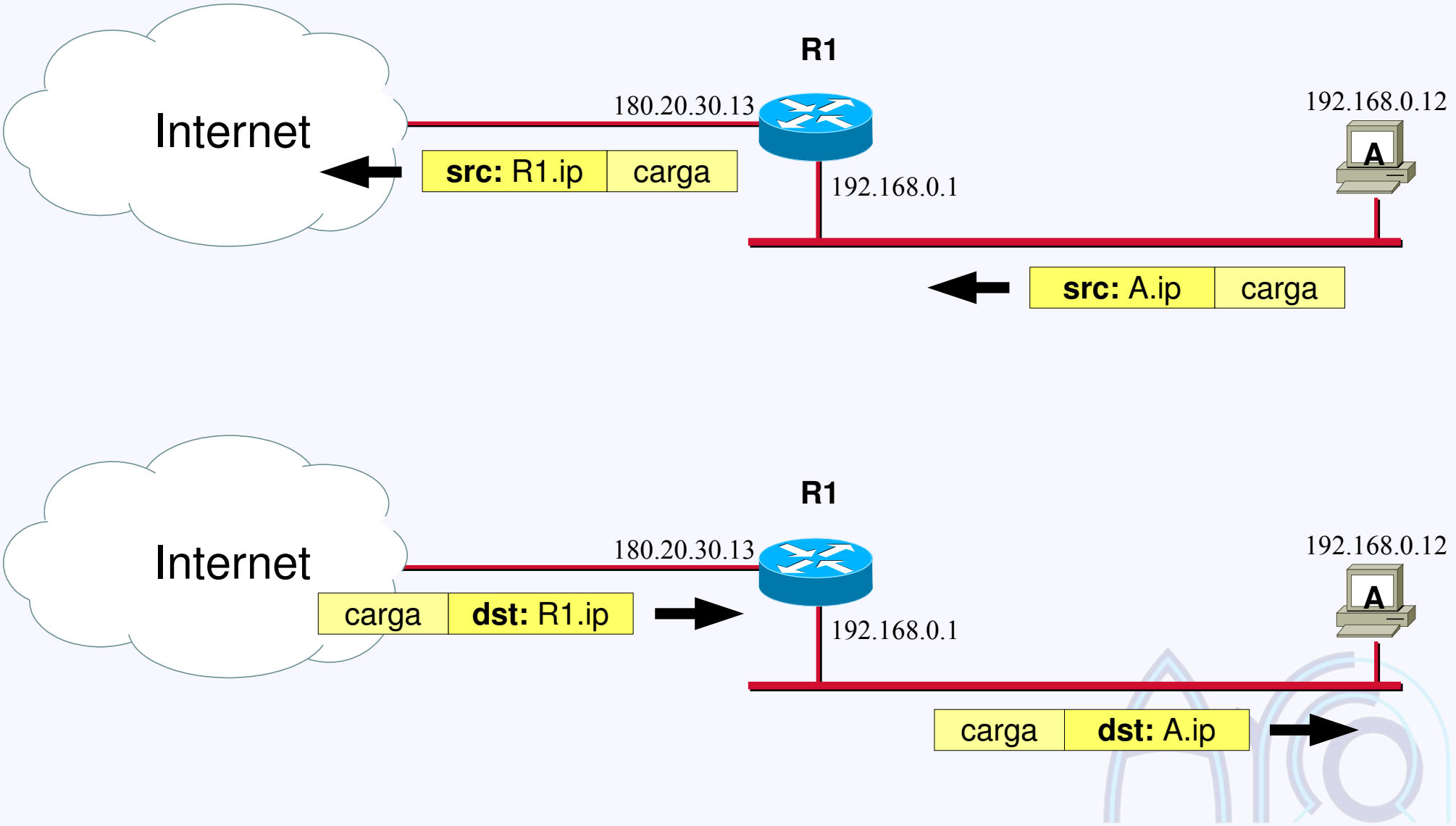


Tabla de Traducción de Direcciones

- Permite al enrutador saber cuál es el host local al que va dirigido un paquete procedente del exterior.
- Al enviar un paquete se apunta (dir. exterior, dir.origen). Al volver la respuesta se envía al host correspondiente.

- Problemas:
  - La comunicación no puede ser iniciada desde el exterior.
  - Un host local no puede acceder a más de un host exterior, al mismo tiempo.
  - Dos o más hosts locales no pueden acceder al mismo host externo, al mismo tiempo.

IP privada	IP externa
192.168.0.12	161.67.27.23
192.168.0.11	200.25.34.56

Tabla de traducción de un NAT básico

Tabla de Traducción de Direcciones

- Para resolver algunos de esos problemas se puede usar el puerto además de la dirección.
- En ese caso se llama NAPT *(Network Address Port Translation)*

IP privada	puerto privado	IP externa	Puerto externo	protocolo de transporte
192.168.0.12	32400	161.67.27.23	80	TCP
192.168.0.11	32750	161.67.27.23	80	TCP

- Problemas:
  - La comunicación no puede ser iniciada desde el exterior.
  - No funciona si en la respuesta, la dirección origen y el puerto destino coinciden para más de un host.

Tabla de Traducción de Direcciones (NAPT)