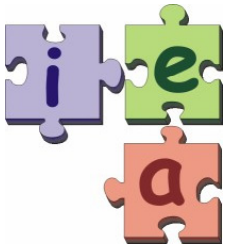
Sistemas de Transporte de Datos (9186)
Ingeniería en Informática (plan 2001)

Práctica 2. Túneles y VPNs

Curso: 2008-2009



Juan Antonio Corrales Ramón

Francisco Andrés Candelas Herías

Santiago Puente Méndez

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

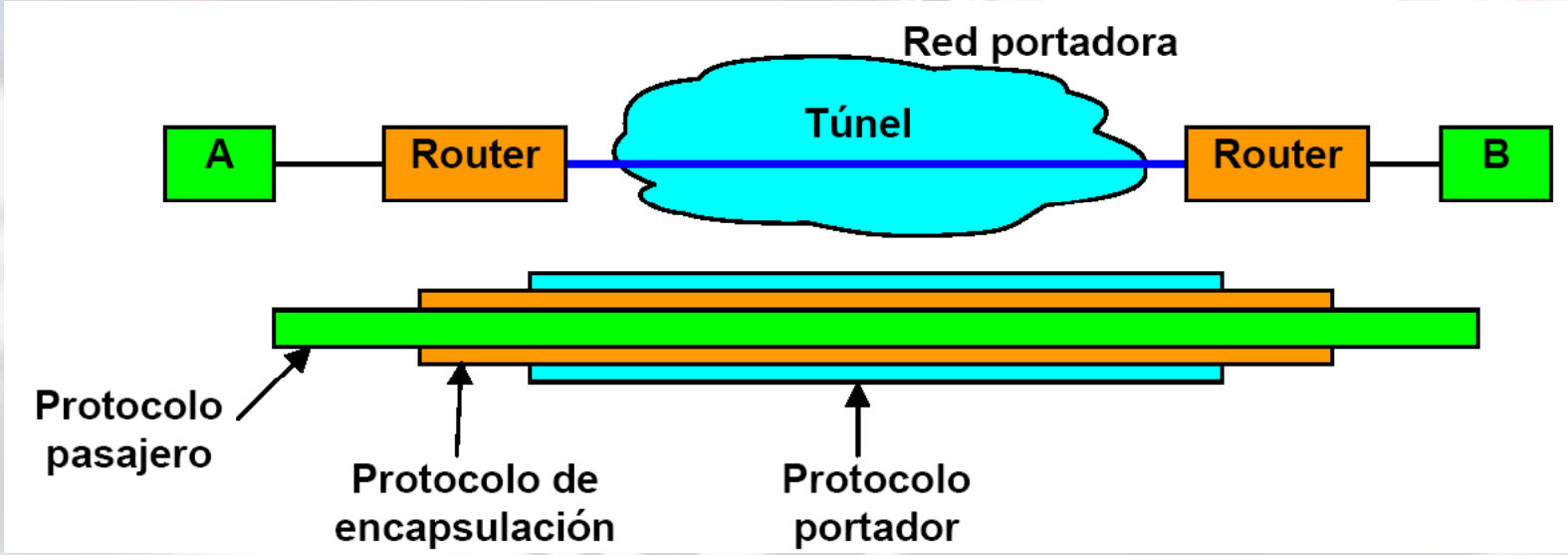
Universitat d'Alacant
Universidad de Alicante

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

Interconexión de Redes mediante Túneles

• **Tunneling**: Técnica para **encapsular** paquetes de un protocolo (**pasajero**) dentro de otro protocolo (**portador**).

• Se puede utilizar un protocolo adicional (**de encapsulación**) para gestionar el túnel.



• Se utiliza para poder enviar un paquete por una red portadora que usa diferente direccionamiento o no es compatible con el protocolo pasajero.

Túneles de nivel 3 (de red)

- **Tunel de nivel 3:** El protocolo pasajero es de nivel 3 (de red).
  - **Pasajero:** Protocolo de red (IP, IPX, Apple-Talk…).
  - **Portador:** Protocolo de red (IP generalmente).
  - **Encapsulación:** GRE, IPSec.
- La encapsulación es realizada por routers que soportan esta técnica:
  - Los routers en los extremos del túnel tienen una **interfaz virtual**:

```
interface Tunnel0          (en c1720)
 ip unnumbered Serial0
 tunnel source FastEthernet0
 tunnel destination 10.4.2.1
 tunnel mode ipip
```

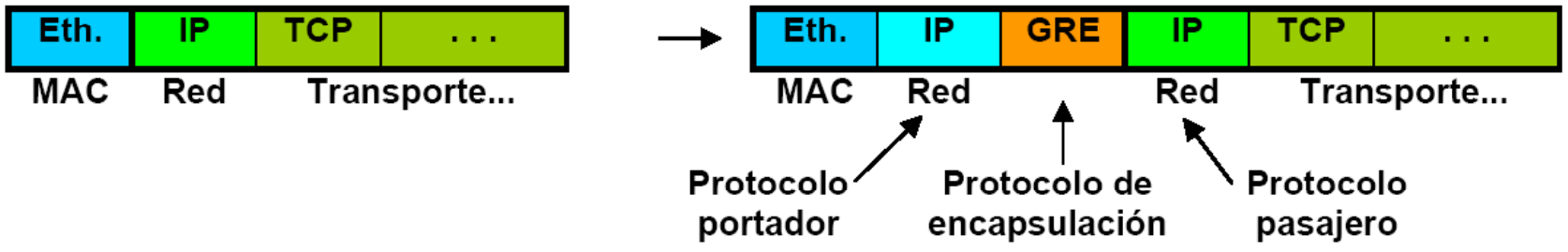
  - La **tabla de rutas** del router de cada extremo del túnel tiene una entrada para dicha interfaz virtual:

10.5.2.2/32 is directly connected, **Tunnel0** *(en c1720)*

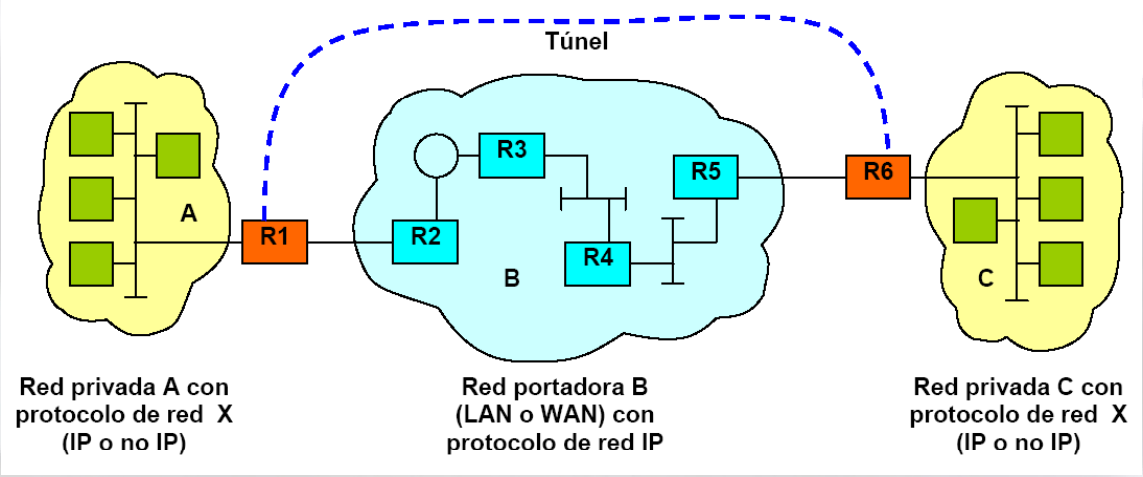
- El túnel puede ser **unidireccional** (si sólo se define la interfaz del túnel y las rutas en el router origen) o **bidireccional** (si se definen en los dos routers de los extremos del túnel).

Túneles de nivel 3 (de red)

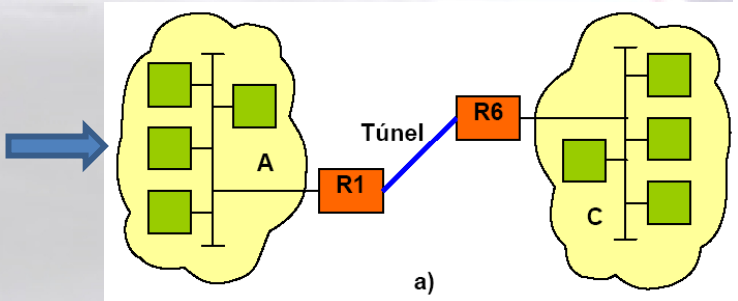
• El router origen del túnel añadirá a cada paquete pasajero (*payload*) las cabeceras del portador y/o de encapsulación. El pasajero será fragmentado antes de ser encapsulado si es necesario.



• El **campo TTL** de la cabecera IP del paquete pasajero no es modificado una vez encapsulado. Hay sólo 1 salto para el pasajero.



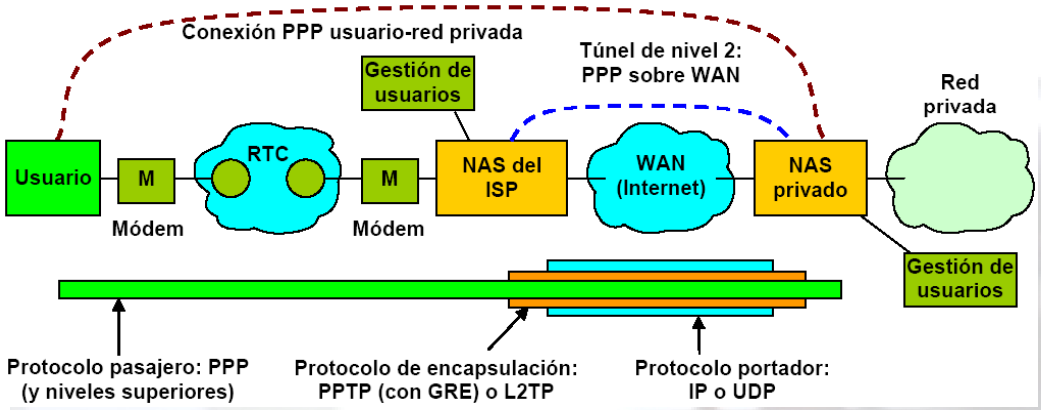
El túnel tiene 5 saltos para el portador B



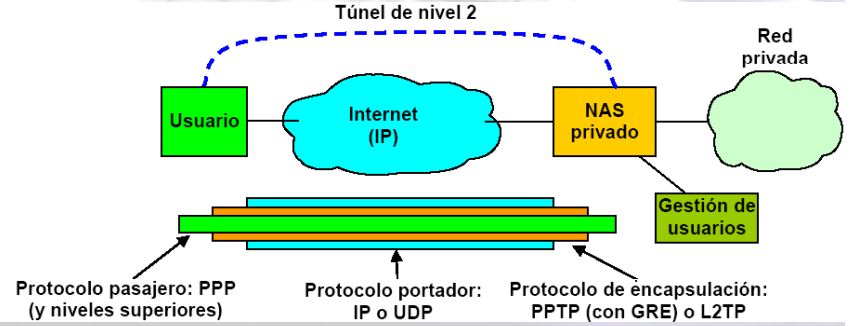
Tiene 1 salto para el pasajero X

Túneles de nivel 2 (de enlace)

- **Tunel de nivel 2:** El protocolo pasajero es de nivel 2 (de enlace).
  - **Pasajero:** Protocolo de enlace punto a punto (PPP, HDLC…).
  - **Portador:** Protocolo de red (IP…) o enlace (Frame Relay…).
  - **Encapsulación:** GRE, L2TP, IPSec.
- Permiten la **conexión de usuarios remotos** a una red privada: **VPN** (Virtual Private Network) o **VPDN** (Virtual Private Dial-up Network).
- Dos modelos de VPN según su administrador: usuario o ISP.



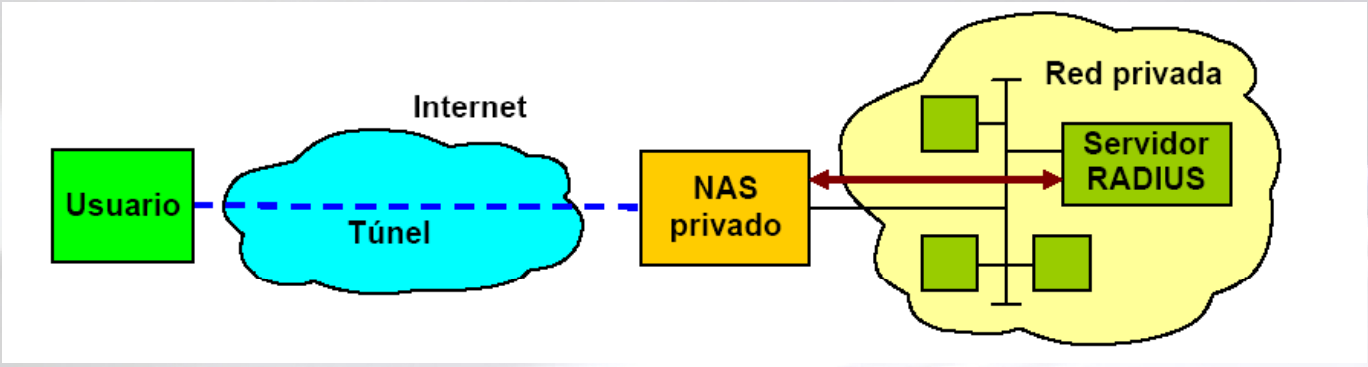
VPN entre ISP y NAS privado



VPN entre usuario y NAS privado

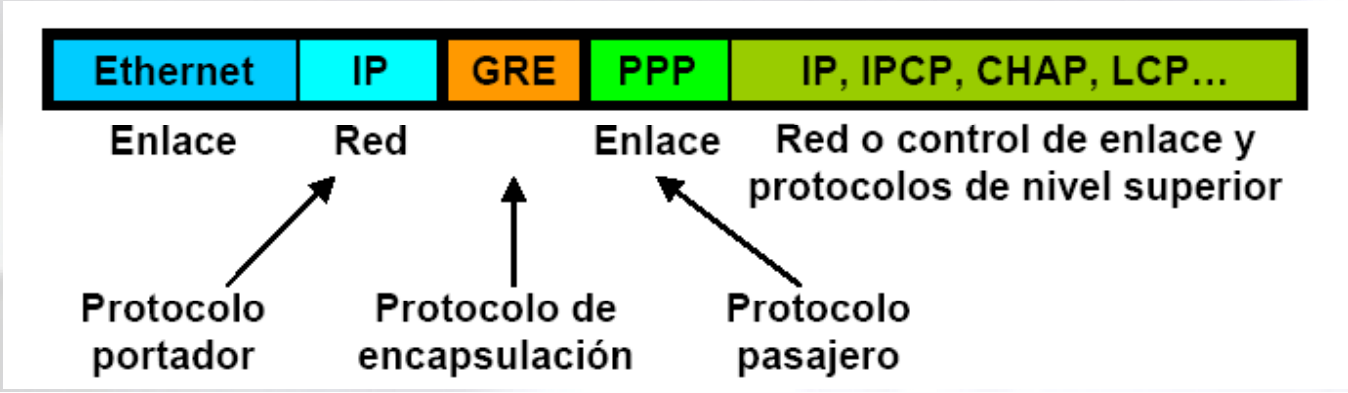
Autentificación y Gestión de Usuarios

- Necesidad de **seguridad** para el acceso a redes privadas con VPNs:
  - **Authentication:** Validar usuarios.
  - **Authorization:** Permitir a usuarios acceder a recursos.
  - **Accounting:** Base de datos sobre usuarios-recursos.
- Servidor **RADIUS** es la solución más extendida:
  - Atiende los puertos **UDP 1645** (authentication) y **1646** (accounting).
  - Mensaje **Access-Request** (NAS→ RADIUS) para validar nuevo usuario.
  - Mensaje **Access-Accept** (RADIUS → NAS) para aceptar usuario y enviar los parámetros del perfil del usuario (dirección IP, máscara, MTU…).
  - Mensaje **Access-Reject** (RADIUS → NAS) si el usuario no está en la BD.
  - Mensaje **Accounting-Request** (NAS → RADIUS) / **Response** (RADIUS → NAS) para gestionar contabilidad de usuarios.

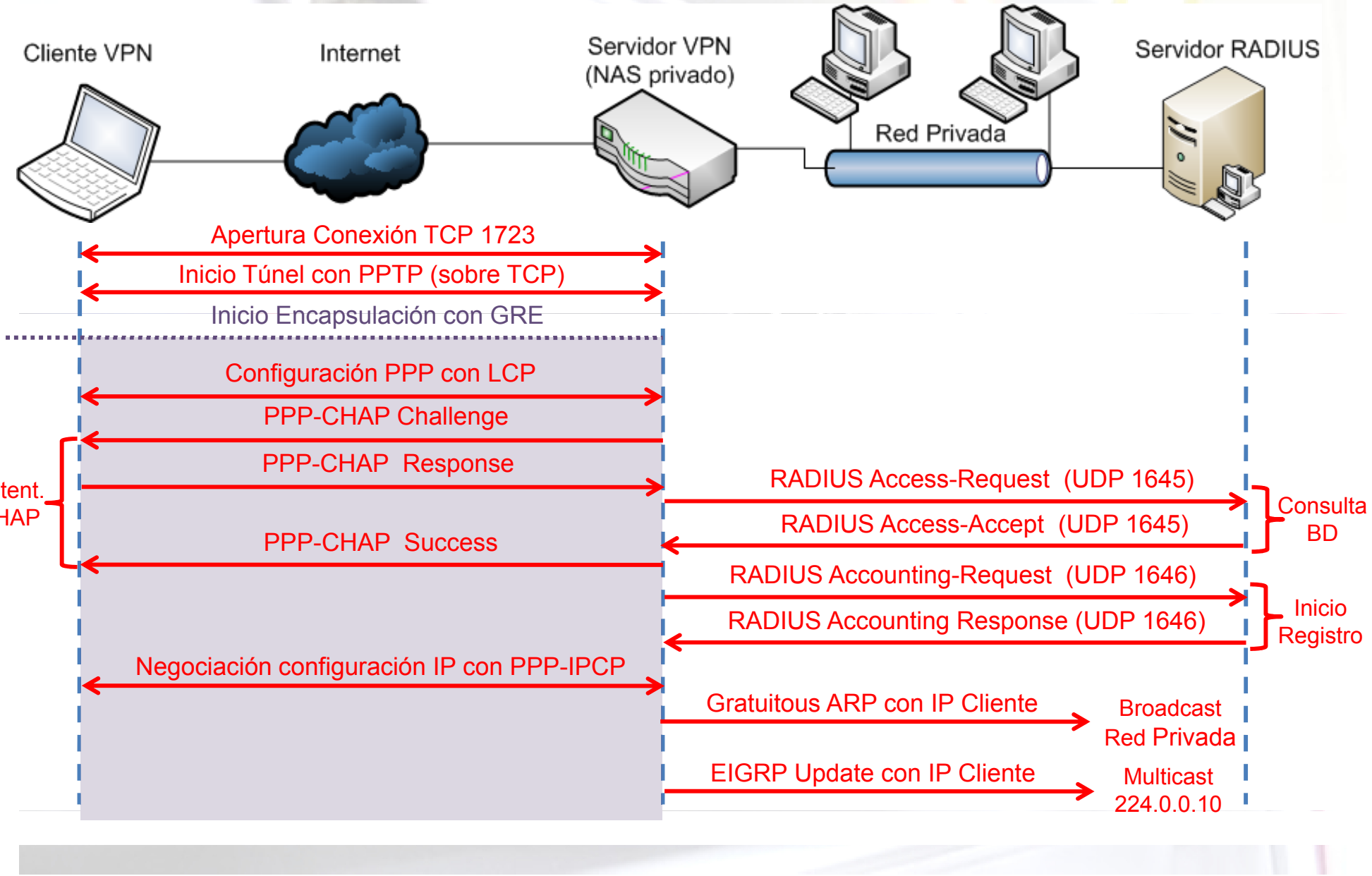


VPNs con PPTP

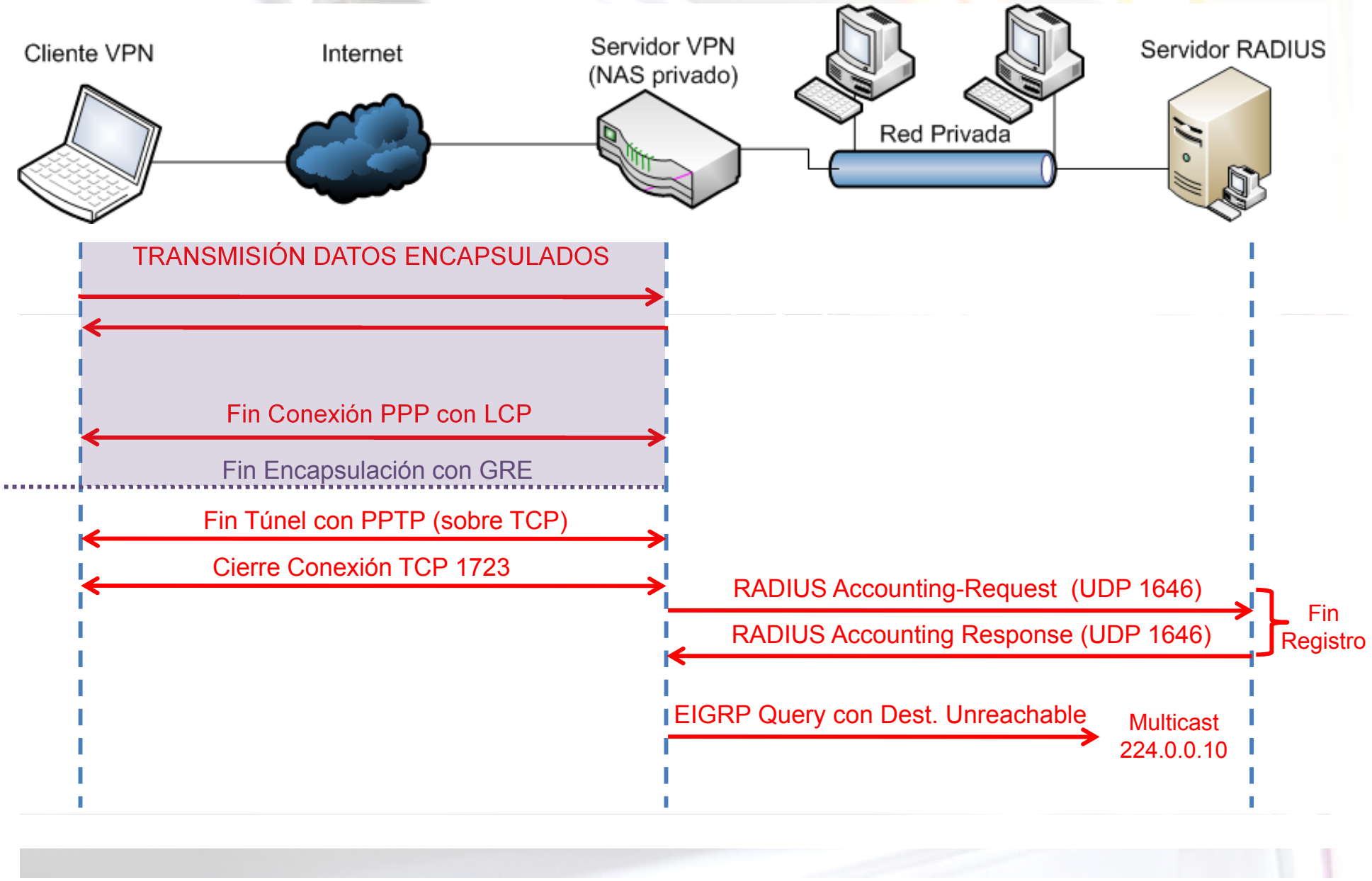
- **PPTP:** Protocolo que utiliza una conexión TCP (puerto 1723) para iniciar una VPN.
- Las VPNs con PPTP utilizan generalmente los siguientes protocolos:
  - **PPP** como protocolo de enlace pasajero:
    - **LCP** para establecer parámetros de la conexión PPP.
    - **PPP-CHAP**, PAP o MS-CHAP para autentificación.
    - **IPCP** o NCP para configurar los protocolos de red (IP).
  - **GRE** como protocolo de encapsulación.
  - **IP** como protocolo portador.



Apertura de una VPN PPTP

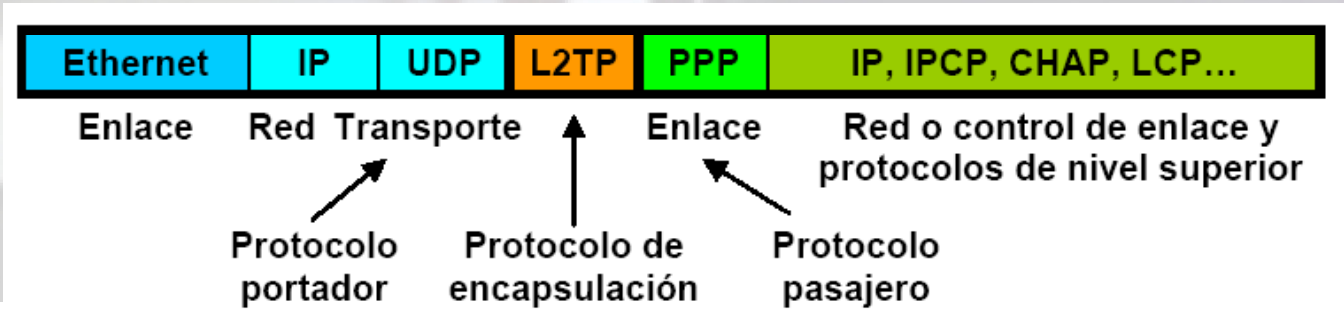


Cierre de una VPN PPTP



VPNs con L2TP

- **L2TP** es un protocolo para crear VPNs más robusto que PPTP.
- Las VPNs con L2TP utilizan generalmente los siguientes protocolos:
  - **PPP** como protocolo de enlace pasajero:
    - **LCP** para establecer parámetros de la conexión PPP.
    - **PPP-CHAP**, PAP o MS-CHAP para autentificación.
    - **PPP-CCP** para negociar compresión y cifrado de PPP.
    - **IPCP** o NCP para configurar los protocolos de red (IP).
  - **L2TP** como protocolo en encapsulación. Se utilizan mensajes L2TP para abrir y cerrar el túnel.
  - **UDP** (puerto 1701) como protocolo portador.



Topología L24