Seguridad en Sistemas Informáticos

Seguridad del canal de comunicaciones

Redes privadas virtuales (VPN)

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

En clases anteriores...

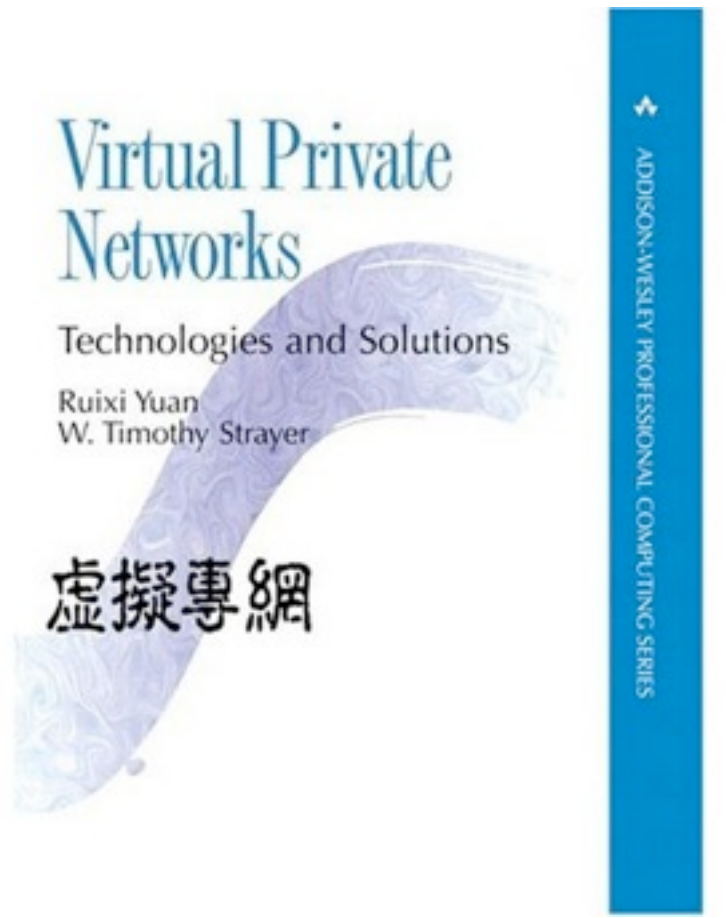
- La cadena de seguridad
  - Seguridad perimetral
- Sistemas de defensa
  - IDSs, honeypots...
- Criptografía

Hoy

- Asegurando el canal de comunicación
  - Introducción y conceptos básicos de VPNs

Bibliografía VPNs

- Virtual Private Networks
  by Ruixi Yuan, W. Timothy Strayer
  Addison Wesley, 2001



Seguridad en el canal

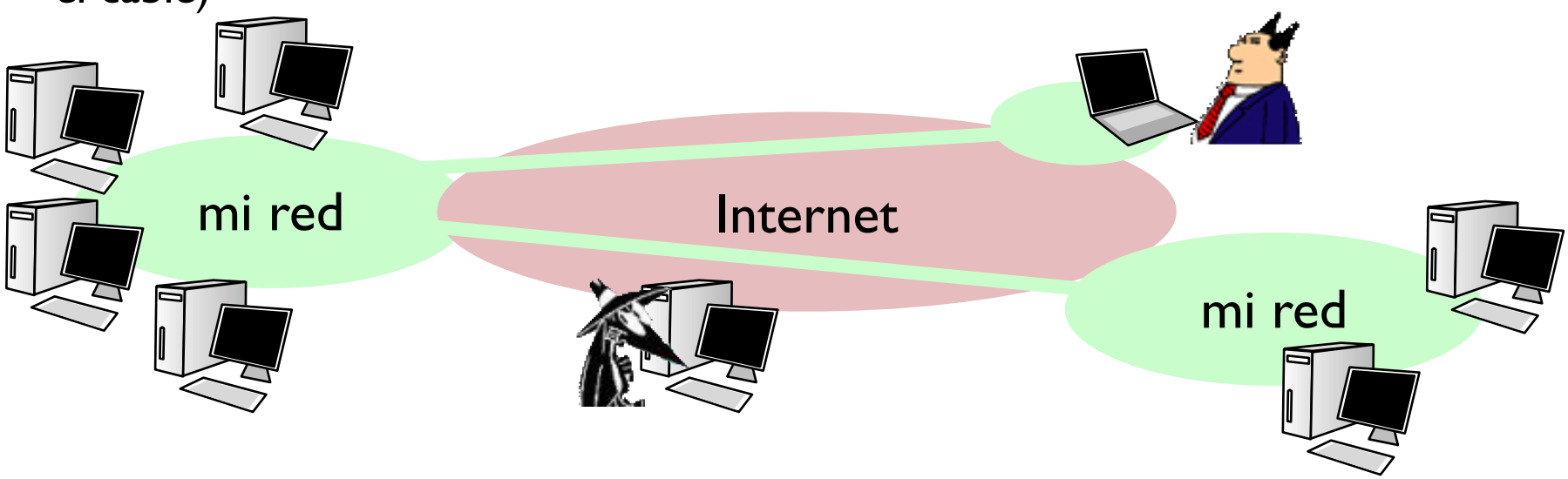
- En ocasiones queremos extender la red de una empresa más allá de los limites del edificio
  - Antiguamente se usaban lineas telefónicas alquiladas para unir routers en las sedes remotas y tener un enlace.

    (que se puede pinchar... o podemos fiarnos del operador)
  - Ahora surge la posibilidad de enviar esos paquetes a través de Internet

    Cobertura en cualquier parte (no hace falta tener preparada la linea alquilada)

    Ahorro (no hace falta pagar la linea alquilada)

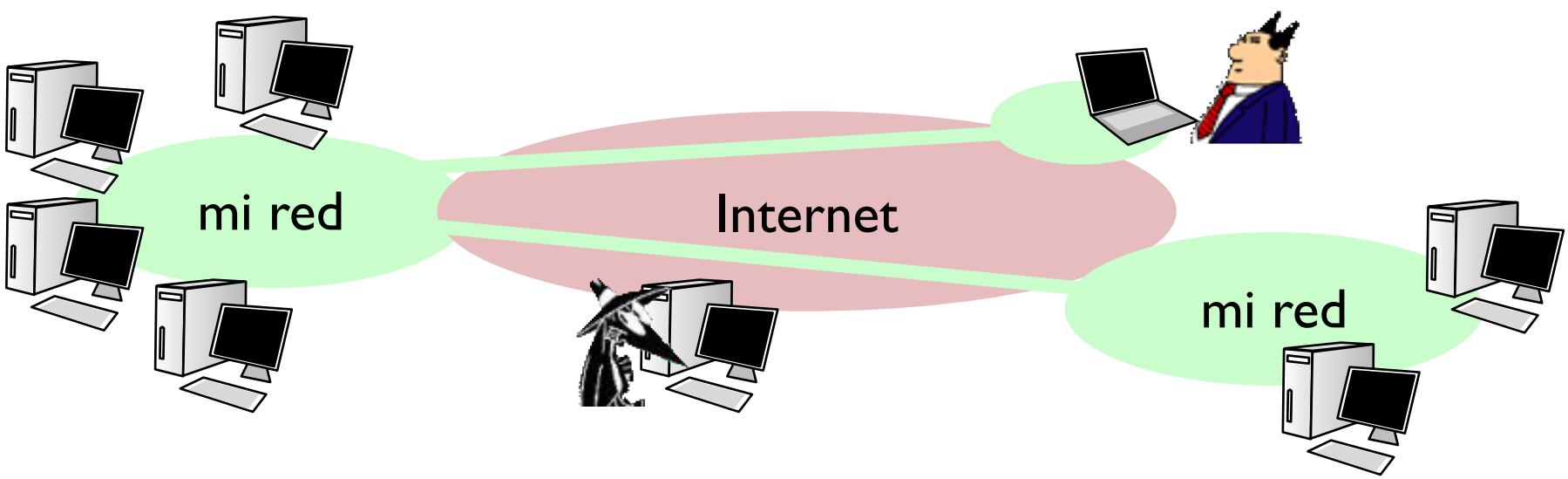
    Seguridad (podemos cifrar las comunicaciones y olvidarnos de si pinchan o no el cable)



Redes privadas virtuales (VPN)

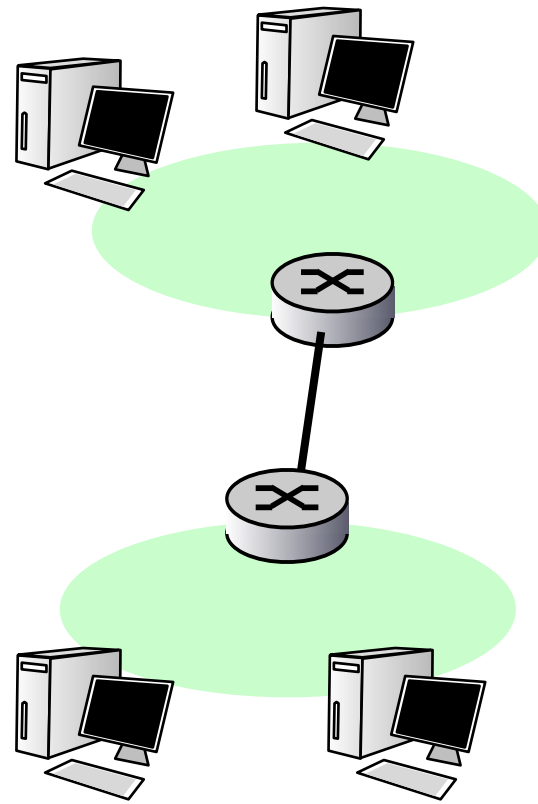
Dos cuestiones a resolver

- ¿Como hacemos para que las redes de diferentes sedes se comporten como si estuvieran en la misma red?
- ¿Como protegemos nuestras comunicaciones de los observadores?



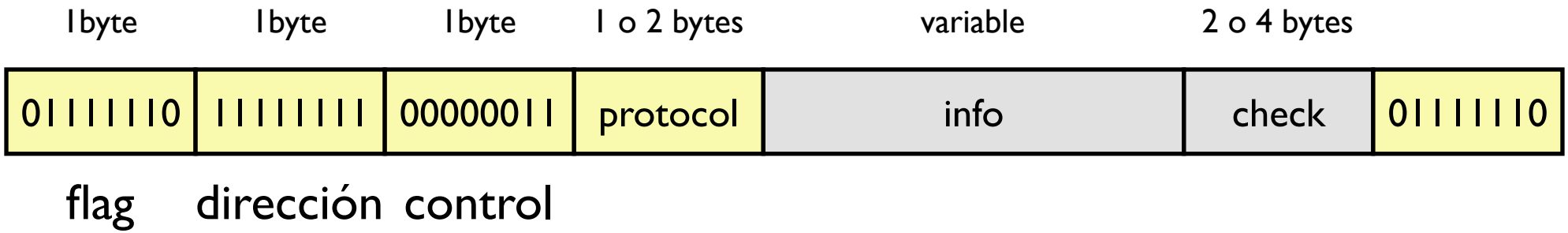
Enlace punto a punto

- Un emisor, un receptor. Más fácil que LAN.
  - No hay medio compartido que arbitrar
  - No hay necesidad de direccionamiento, sólo hablar con el otro extremo
  - Ejemplos:
    - Cable directo (RS-232 - RS-232)
    - Llamada telefónica
    - ...



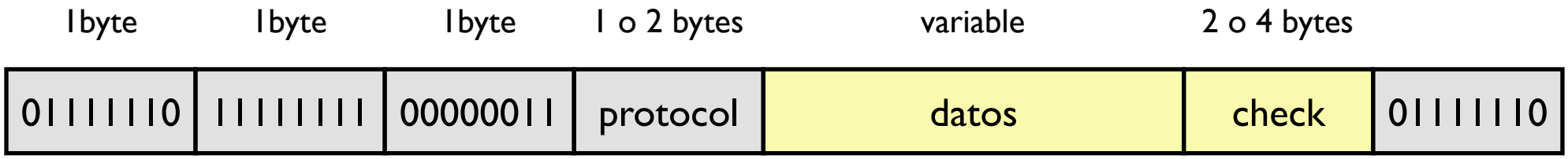
- Los protocolos de nivel de enlace punto a punto más populares:
  - PPP (point to point protocol)
  - HDLC (high-level data link control) (hubo un tiempo en el que el nivel de enlace era high level en la torre de protocolos...)

PPP: formato trama

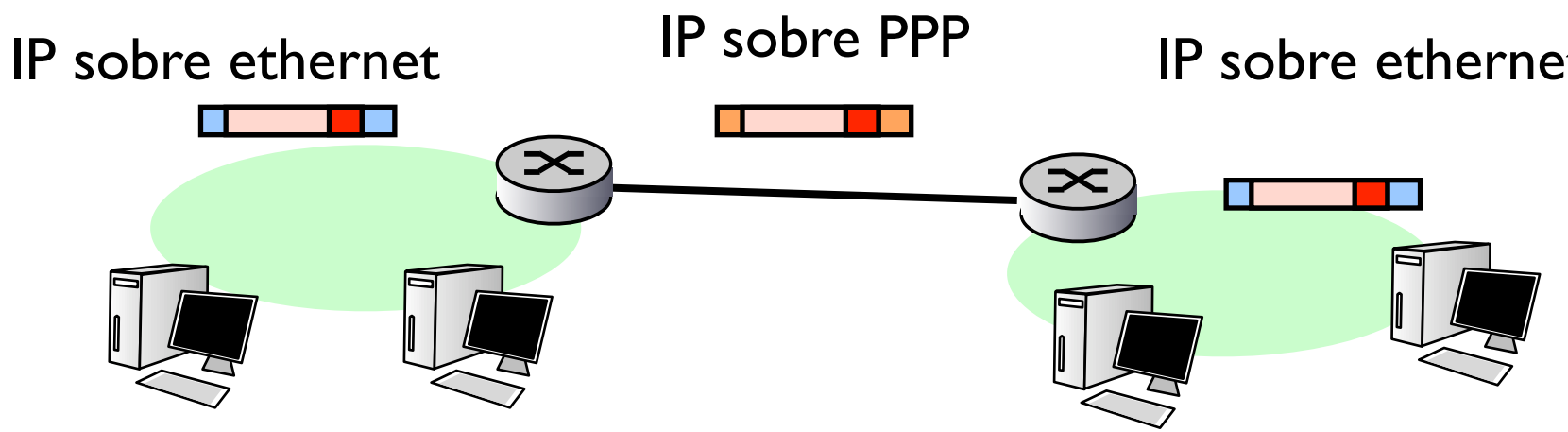


- delimitador: tramas delimitadas por 01111110
- dirección y control: no se usan
- protocol: protocolo transportado
  - IP
  - AppleTalk, Decnet
  - Protocolos propios de PPP IPCP (IP control protocol) y LCP (PPP link control protocol)
- Mucho más simple que ethernet

PPP: formato trama

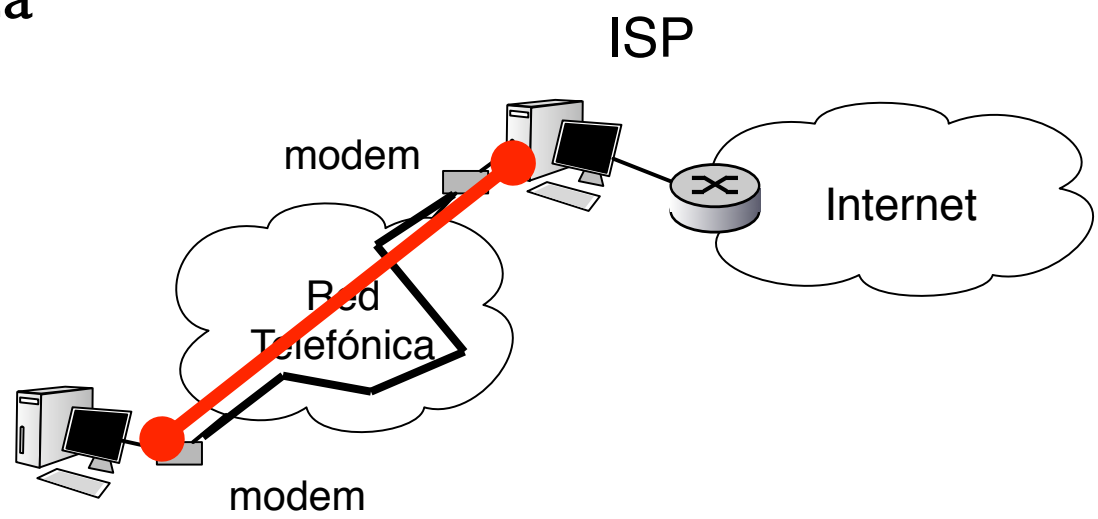


- datos transportados
- Checksum
- Encapsulando IP



Enlaces telefónicos

- Método más común de acceso a Internet hasta hace poco
  - Establecer una llamada telefónica entre un ordenador en casa del usuario y un ordenador del proveedor de internet
  - Una vez establecido el enlace, los dos ordenadores lanzan el protocolo PPP y establecen un enlace IP sobre la llamada telefónica



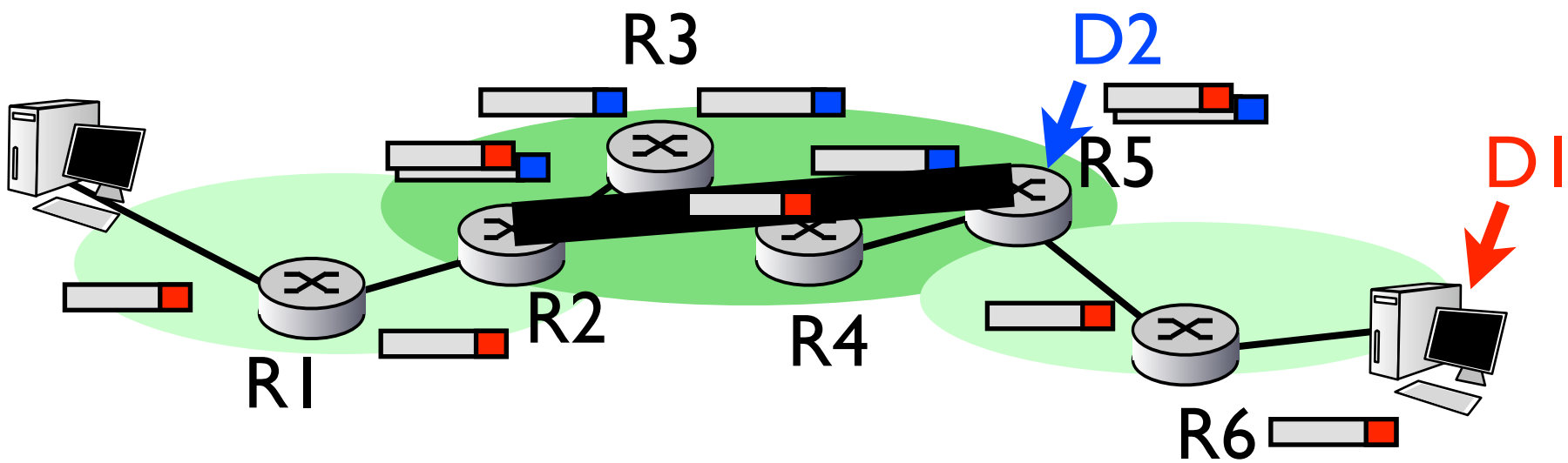
- Usamos una conexión de una red de comunicaciónes como enlace para Internet
- ¿Podemos hacer lo mismo transportando PPP sobre internet?

Tecnologías para VPNs

- Tuneling
- Autentificacion
- Control de acceso
- Seguridad de los datos (encriptación)

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

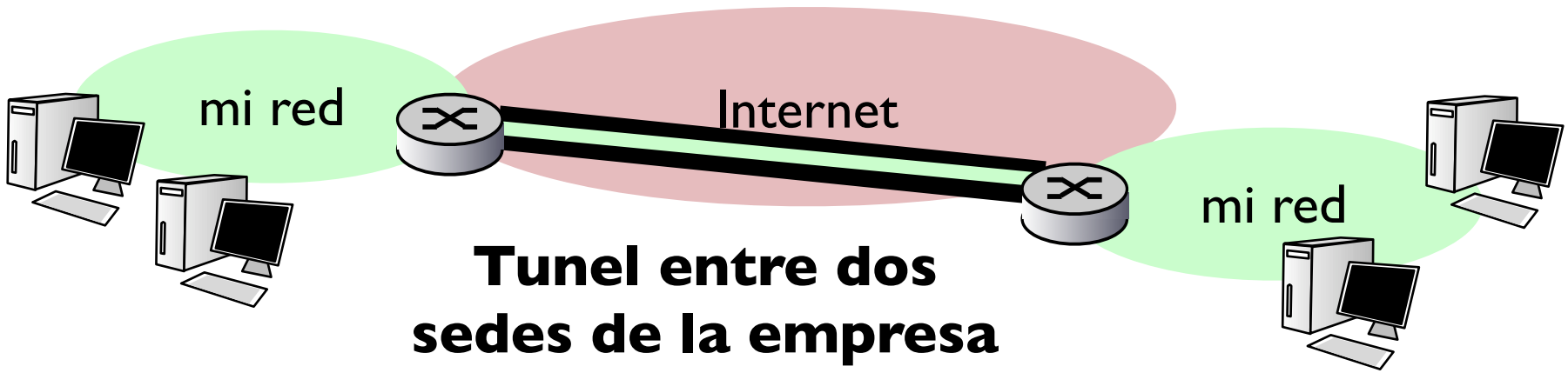


Túneles

- Se pueden hacer túneles a varios niveles pero los mas normales son
- Nivel 2: enlace
  - Una trama de nivel de enlace (PPP, Ethernet) se envía dentro de la unidad de datos (PDU) de otro protocolo que puede ser a su vez de nivel de enlace, red, transporte...
- Nivel 3: red
  - Una trama de nivel de red se envía dentro de la unidad de datos de otro protocolo
- Nivel 4: transporte
  - Una conexión redirigida a través de otra (via ssh)

Usos de los túneles

- Aplicar a todos los datos que van por el tunel un tratamiento común.
  - tratarlos con una misma calidad de servicio.
  - **encriptarlos** todos de la misma manera
- Enviar paquetes cuyas direcciones no tienen sentido en la red por la que se hace el tunel
  - enviar paquetes con direcciones privadas de nuestra red a través de Internet
- Enviar protocolos que no son tratados por la red por la que se ha hecho el tunel
  - IPX, AppleTalk, NetBIOS...



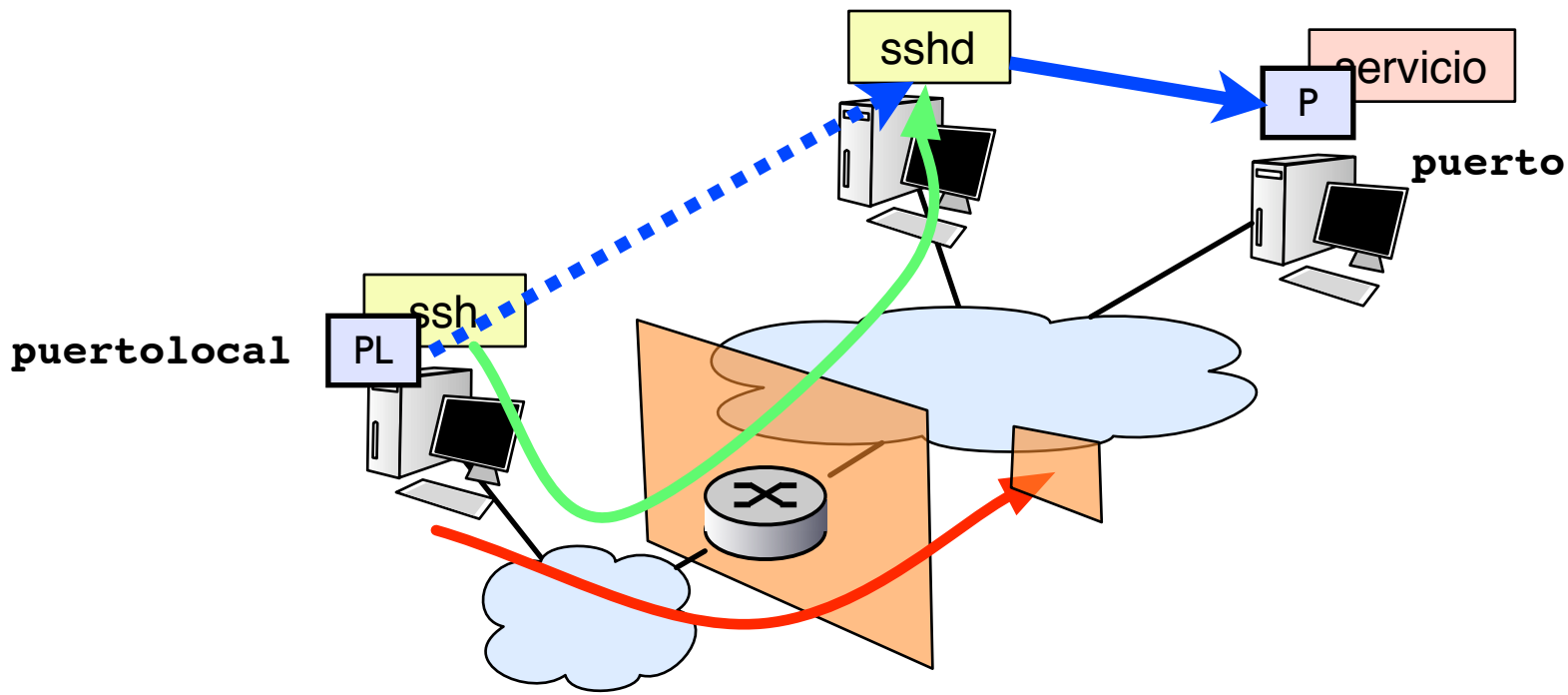
Ejemplo: Tuneles sobre SSH

Tunel de nivel de transporte sobre SSH

- Redireccionar un puerto local

```
$ ssh usuario@host -L puertolocal:destino:puerto
```

- Escenario con ssh permitido pero puerto P filtrado
  - Para el destino la conexion viene de H2



Tuneles sobre SSH

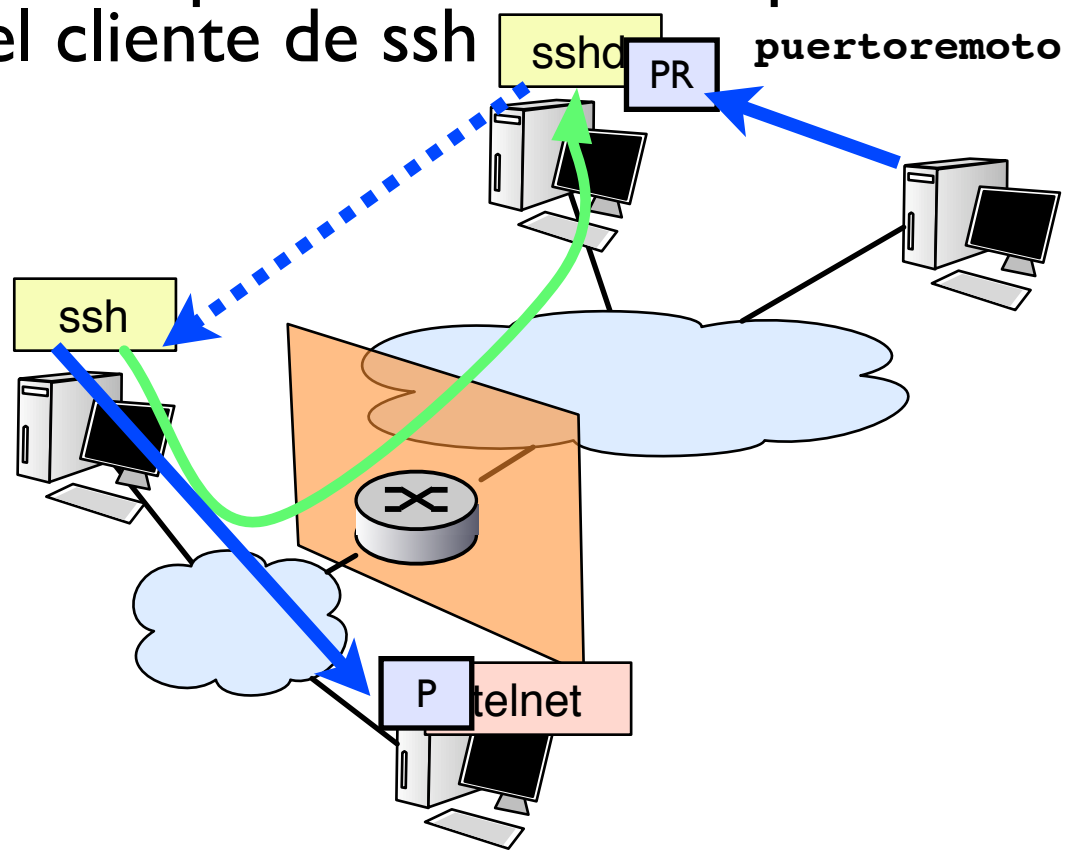
Tunel de nivel de transporte sobre SSH

- Redireccionar un puerto remoto

```
$ ssh usuario@host -R puertoremoto:destino:puerto
```

- Igual que en el caso anterior pero redirecciona puertos del servidor hacia la red del cliente de ssh

- Se puede usar SSH para proteger servicios clasicos



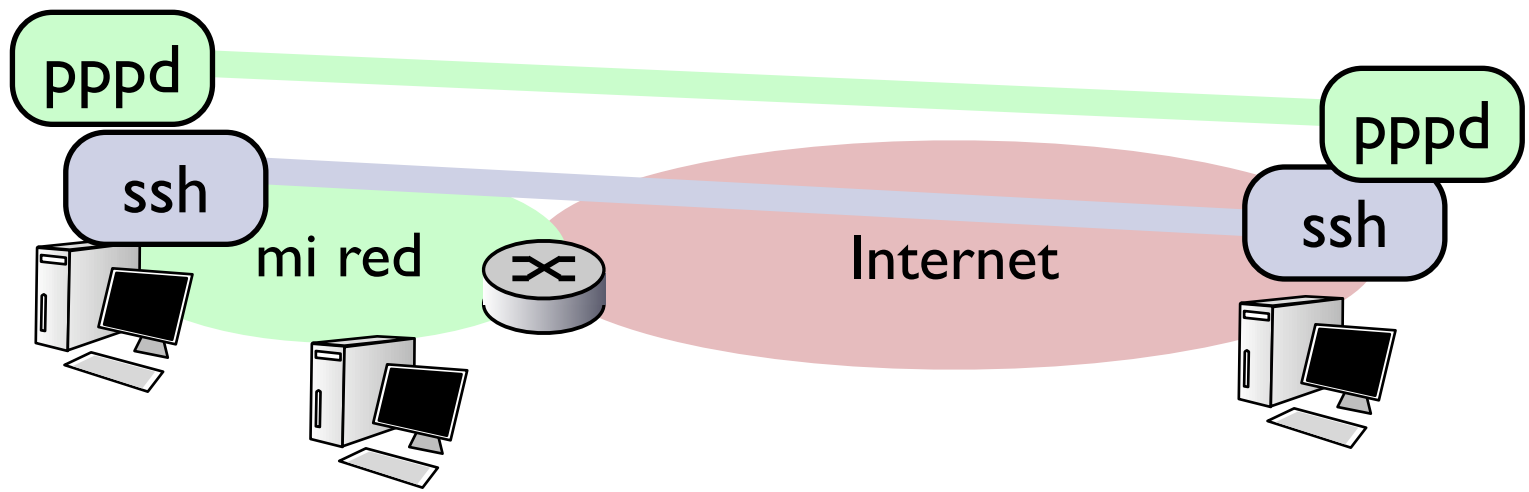
Ejemplos

Tuneles de nivel de enlace sobre ssh (PPP sobre ssh)

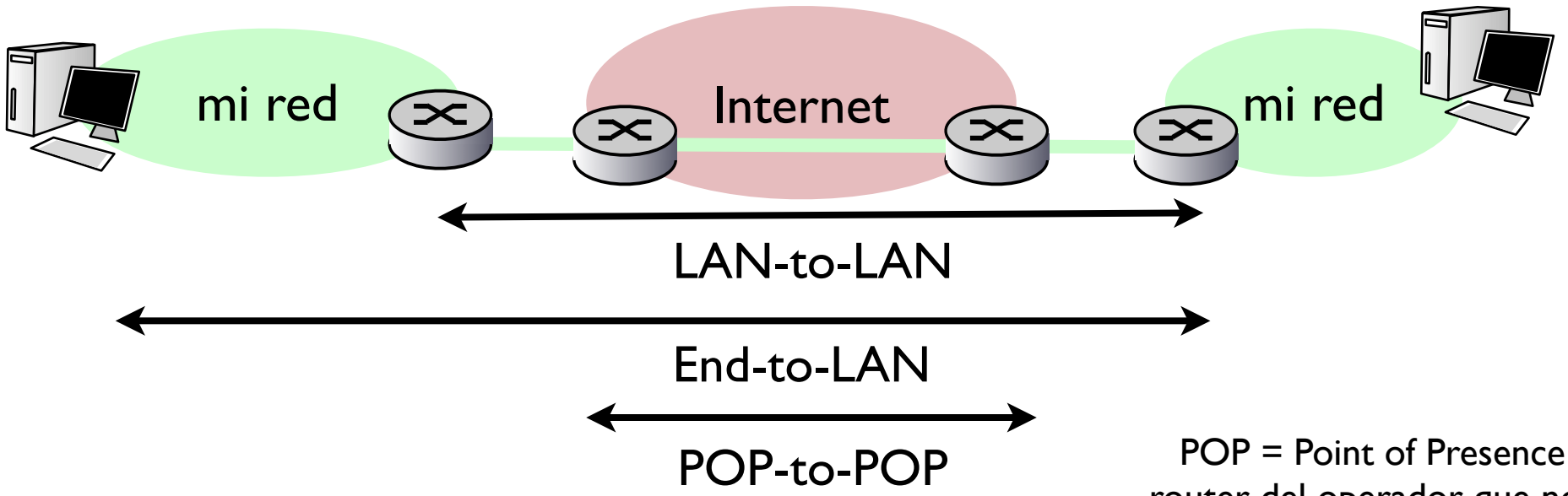
- Conexión ssh y un pppd en cada extremo

```
$ pppd pty "ssh usuario@host pppd"
```

- Puedo enviar paquetes IP a un PC de mi red que luego actue como router
  - Uso:VPN construida a mano con solo un servidor ssh y pppd
  - Uso : puerta de entrada a traves de cualquier firewall que soporte conexiones entrantes ssh



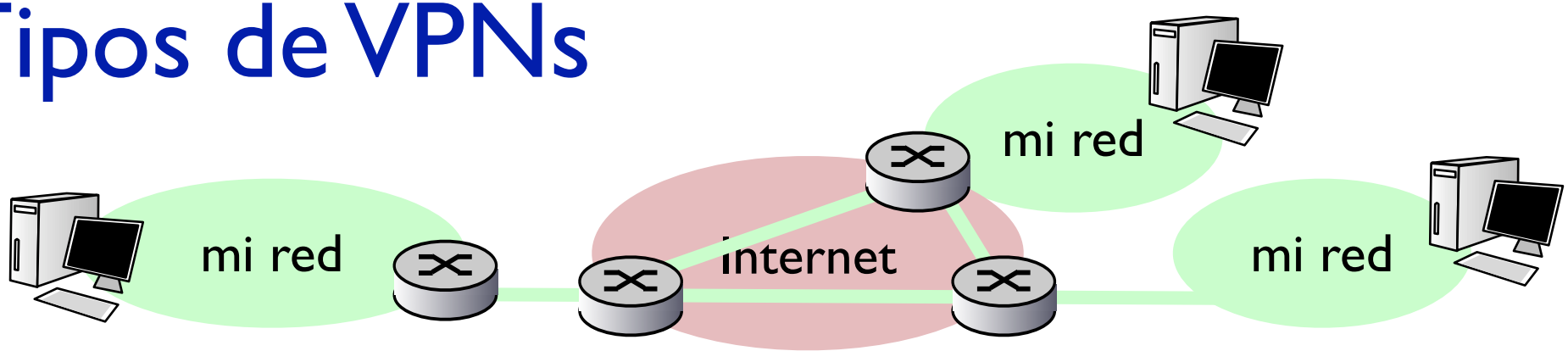
Arquitecturas de VPNs



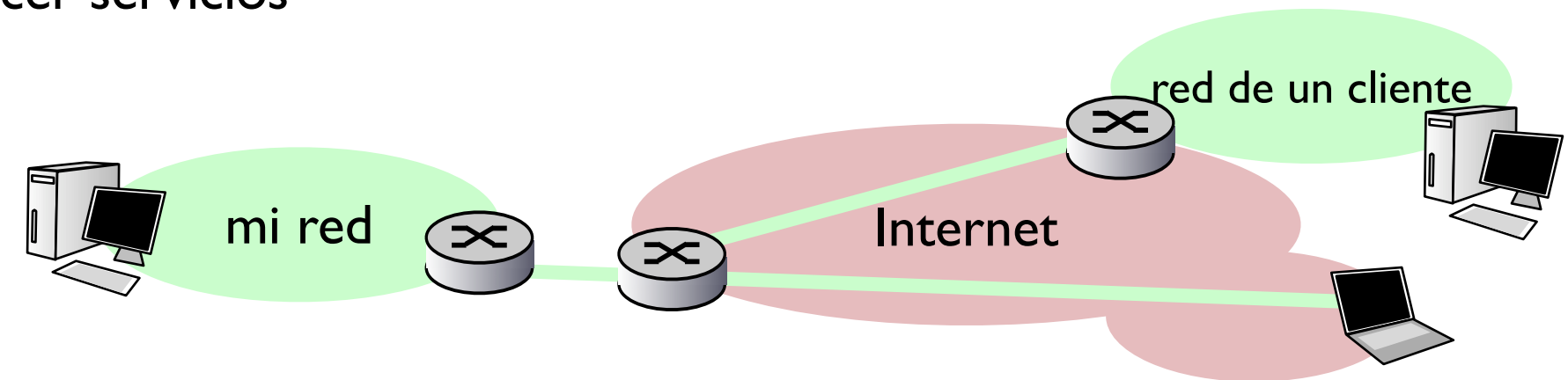
POP = Point of Presence
router del operador que nos vende el servicio de VPN

- Según las necesidades el tunel para la VPN puede realizarse desde un gateway (router) de la empresa o del proveedor y llegar hasta un gateway o bien llegar hasta el ordenador final
- Según quién realice el tunel tendremos diferente protección y diferente gestión de la red

Tipos de VPNs



- **Interna (Site-to-site)**: une dos o más redes internas como si fueran una sola red
- **Acceso**: permite el acceso de un cliente que esta en una red insegura. El tunel se hace desde el ordenador que accede
- **Extranet**: permite el acceso desde una red ajena a la empresa para ofrecer servicios



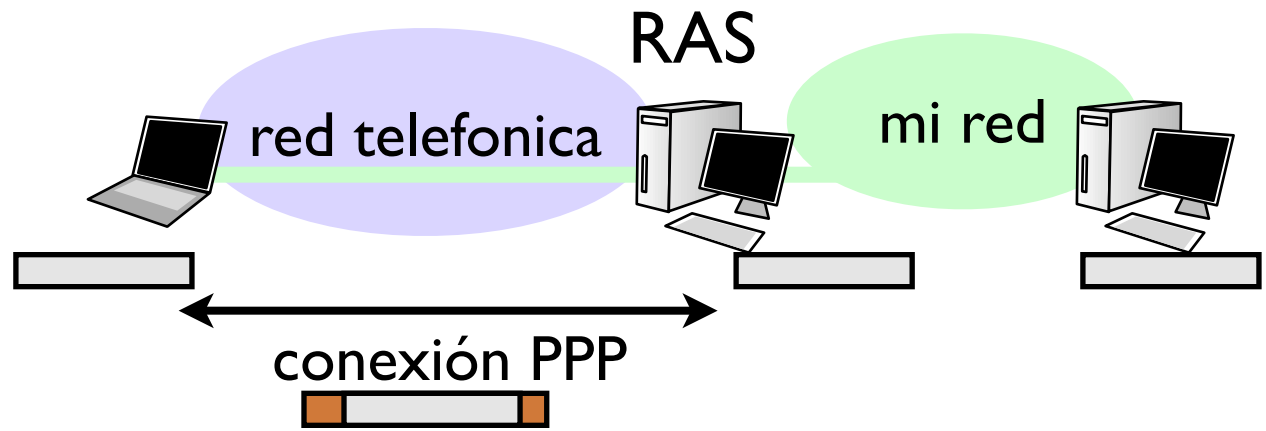
Protocolos de tuneling

- Permiten
  - Encapsular un protocolo dentro de otro para poder transportarlo sobre una infraestructura IP
  - Enrutar direcciones privadas a través de una red de direccionamiento publico
  - Proporcionar confidencialidad e integridad
- Layer 2: encapsulan tramas de nivel de enlace (PPP)
  - PPTP
  - L2TP
  - L2F
  - ssh
- Layer 3: enacpsulan tramas de nivel de red
  - IPSec
  - MPLS

Protocolos de tunel de nivel 2

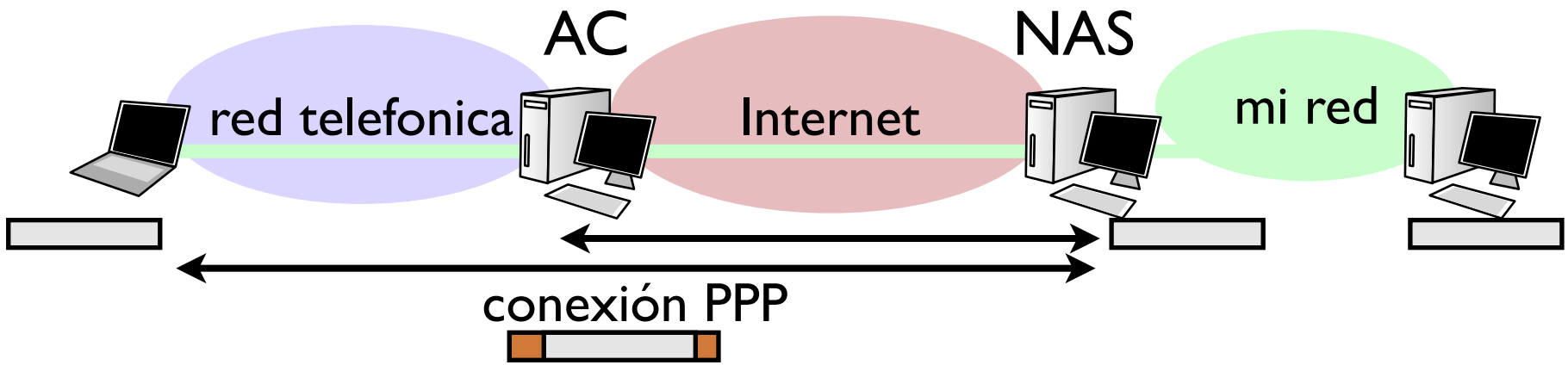
- Permiten reenviar tramas de nivel de enlace sobre un canal seguro
- El tunel se convierte en un enlace virtual

Antecedentes: acceso telefónico



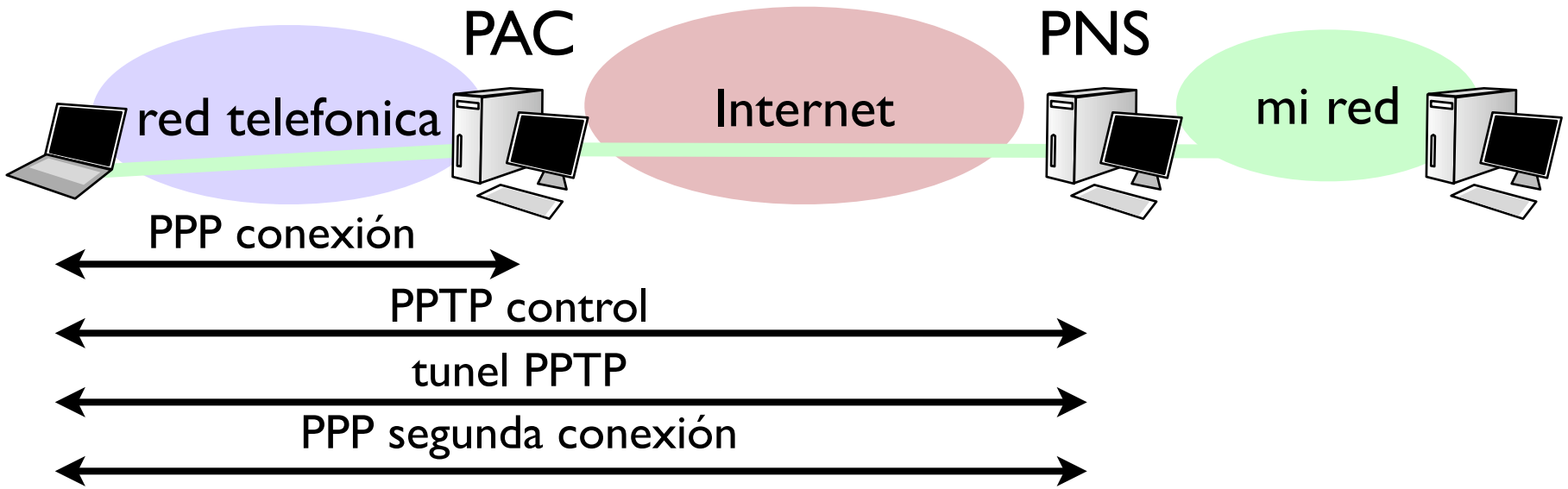
- RAS: remote access server
  - El ordenador remoto llama al RAS por telefono
  - Se establece un enlace PPP
  - Los paquetes se encapsulan dentro de tramas PPP
  - PPP proporciona también autentificación mediante su protocolo de establecimiento de enlace
  - Usuario y contraseña en el ordenador remoto
  - Base de datos de usuarios y contraseñas en el RAS
- Mejor organización proveedores de acceso a Internet ponen concentradores de acceso con bancos de modems (AC) y cada empresa hace la autentificación (NAS)

Antecedentes: acceso telefónico



- RAS: remote access server
  - El ordenador remoto llama al RAS por telefono
  - Se establece un enlace PPP
  - Los paquetes se encapsulan dentro de tramas PPP
  - PPP proporciona también autentificación mediante su protocolo de establecimiento de enlace
  - Usuario y contraseña en el ordenador remoto
  - Base de datos de usuarios y contraseñas en el RAS
- Mejor organización proveedores de acceso a Internet ponen concentradores de acceso con bancos de modems (AC) y cada empresa hace la autentificación (NAS)

PPTP



- PPTP: Point-to-Point Tunneling Protocol (Soportado por Microsoft)
  - PAC PPTP access concentrator y PNS PPTP Network Server
- Pasos

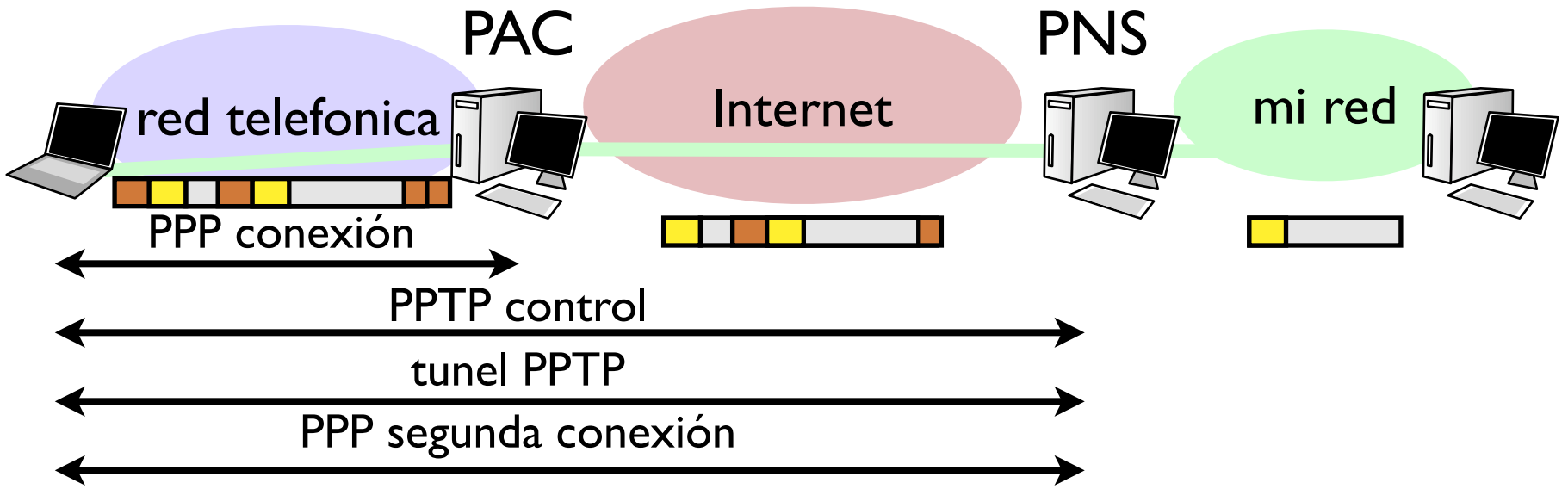
  1 Conexión PPP a traves del teléfono

  2 Canal de control PPTP sobre para autentificación

  3 PPP sobre PPTP

  4 IP sobre PPP

PPTP




IP con destino D


PPP con destino el PNS


IP con destino al PNS (dentro GRE y PPP)

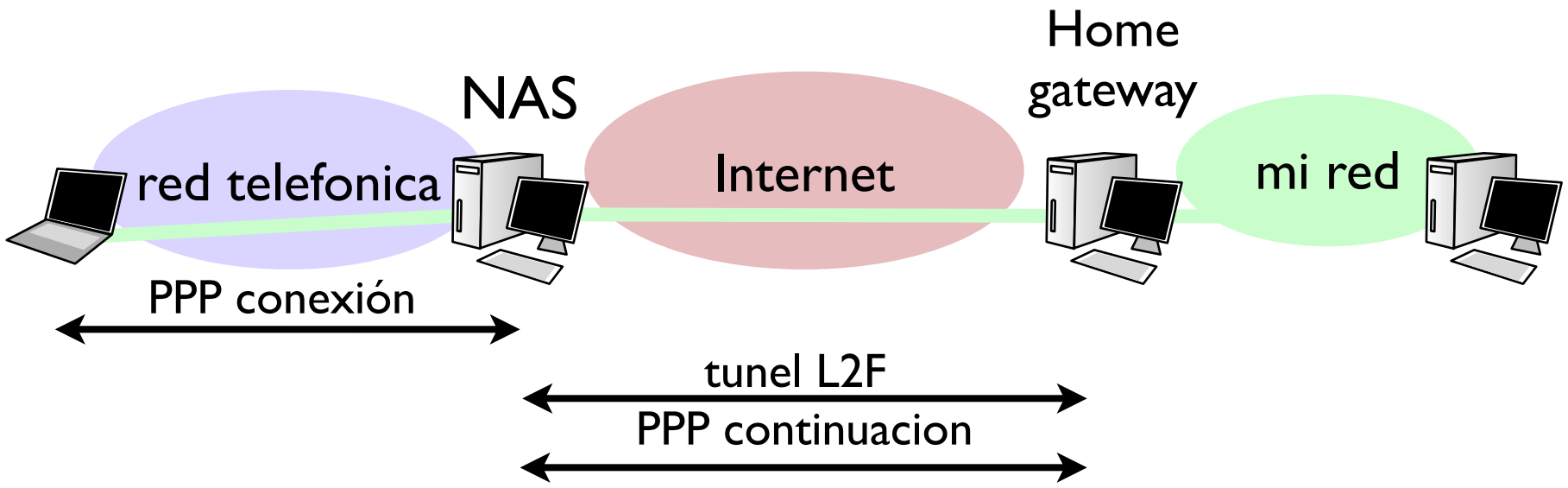

PPP con destino el PAC

- Aumenta el overhead...
- Hay que tener cuidado con la MTU (si enviamos paquetes grandes habrá fragmentación)

PPTP

- Problemas
  - Dificil de atravesar firewalls porque requiere una sesion de control (TCP puerto 1723) + flujos UDP con el tunel PPTP
  - La encriptación del tunel (MPPE) es cuestionable
- Ventajas
  - Facil de configurar
  - Muy extendido (por defecto en Windows)
- Autentificación sobre PPP
  - Con PAP, CHAP, EAP, MSCHAP...

L2F

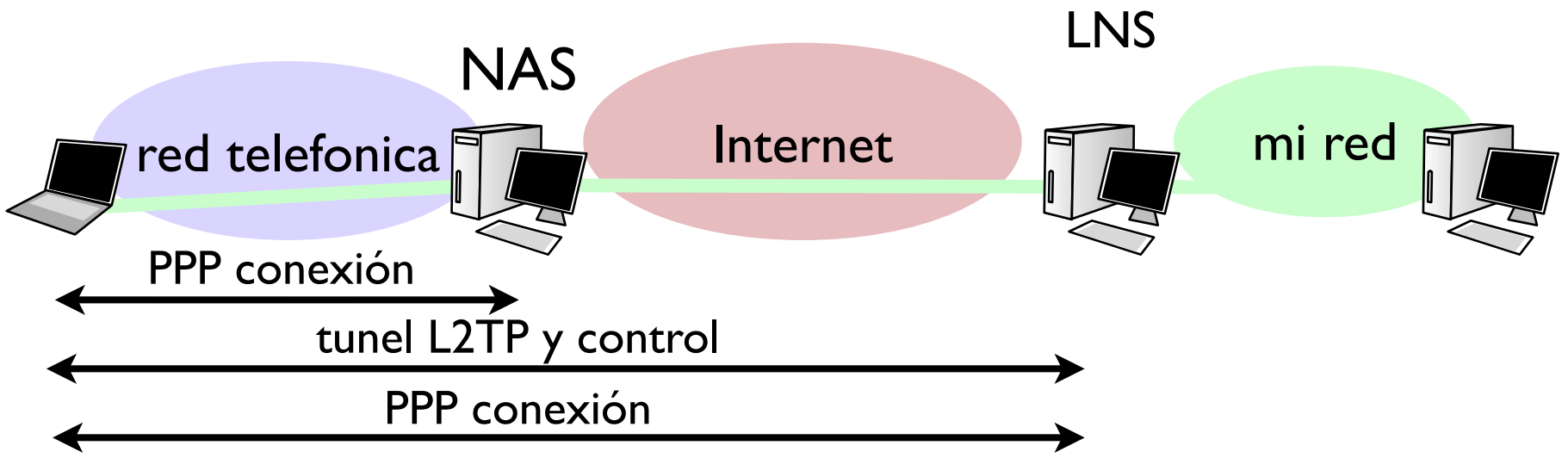


- L2F Layer 2 Forwarding protocol (soportado por Cisco)
  - Enlace PPP con el NAS
  - El NAS crea un un tunel L2F con el gateway de la red de destino
  - Los paquetes PPP se reenvían por ese tunel
  - Solo una autentificación PPP con el gateway
- Encapsulado más sencillo
- Soporta SLIP ademas de PPP
- Soporta autentificacion con RADIUS o TACACS

PPTP y L2F

- Autentificación basada en PPP y encriptación no se consideran muy fuertes
- Diferencias de filosofía
  - PPTP modo voluntario (el usuario crea los tuneles) MS
  - L2F modo compulsory (los routers crean los tuneles) Cisco
- El IETF hizo su propio estandar combinado lo mejor de los dos: L2TP (Layer 2 Tunneling Protocol)

L2TP



- No hay canal de control separado
- El tunel se hace con UDP en vez de GRE sobre IP
- Problemas
  - Sistemas de autentificación y encriptacion siguen siendo heredados de PPP y no son demasiado fiables

- Se usa normalmente sobre IPSec

Autentificación

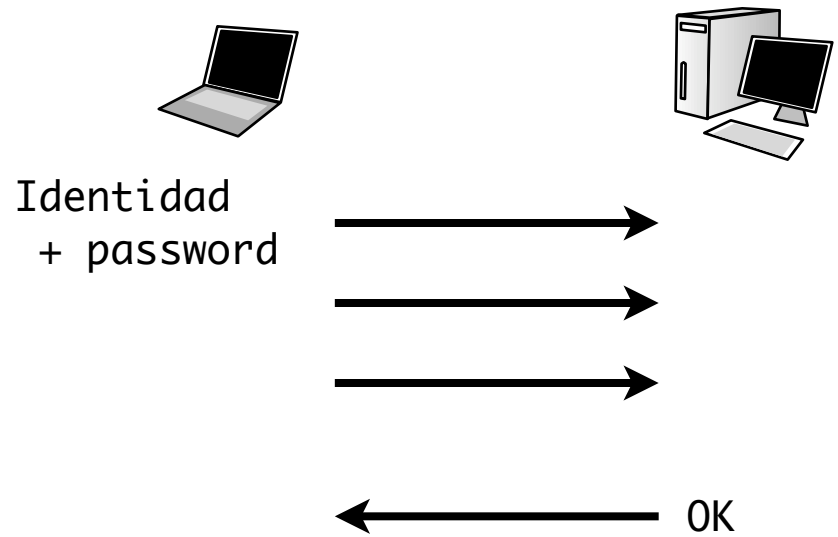
- En los sistemas de acceso remoto el usuario debe probar su identidad

- Protocolos de autentificación
  - Entre dos partes (Alice prueba su identidad a Bob mediante un secreto compartido o similar)
  - Con una tercera parte de confianza (Alice prueba su identidad a Bob con la ayuda de Trent del que Alice y Bob se fian)

PAP

- PAP: Password Authentication Protocol (RFC1334)
  - Se envia la identidad y contraseña en la petición

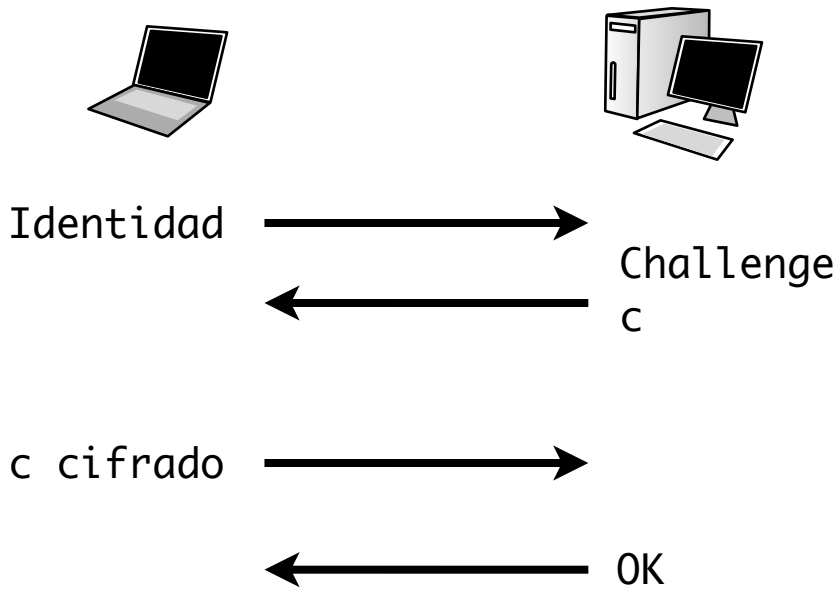
    (en ppp se hace varias veces porque va en el paquete de intento de establecimiento)
  - El servidor compara ese usuario y contraseña con su base de datos
  - Notifica del resultado



- Problemas
  - Contraseña sin cifrar
  - Mandar el hash no ayuda (por que?)
  - No se considera un método muy fuerte de autentificación pero se puede usar si la confidencialidad de los mensajes esta protegida a otro nivel (enlace serie o sobre cable telefonico: aceptable, dentro de PPTP, L2TP o L2F poco aceptable)

CHAP

- CHAP: Challenge Autentication Protocol (RFC1994)
  - Envío de un desafío (challenge) para encriptar
  - El cliente cifra el desafío y lo manda
  - El servidor lo cifra con la clave del usuario en la base de datos y comprueba si sale lo mismo
  - La clave nunca se envía
- Problemas
  - Obliga a que la clave se almacene en clientes y servidores sin cifrar
  - El challenge tiene que ser unico e impredecible, si no un atacante puede observar establecimientos y guardar challenges encriptados



EAP

- EAP: Extensible Authentication Protocol (RFC2284)
  - Durante el establecimiento del enlace PPP se elige autentificación EAP y se postpone la autentificacion
  - Protocolo genérico que soporta diferentes tipos de algoritmos de autentificación
- Problemas:
  - El atacante puede centrarse en el algoritmo más débil
- Algoritmos

  EAP-PSK, EAP-MD5,

  EAP-TLS, EAP-TTLS

  EAP-FAST, PEAP

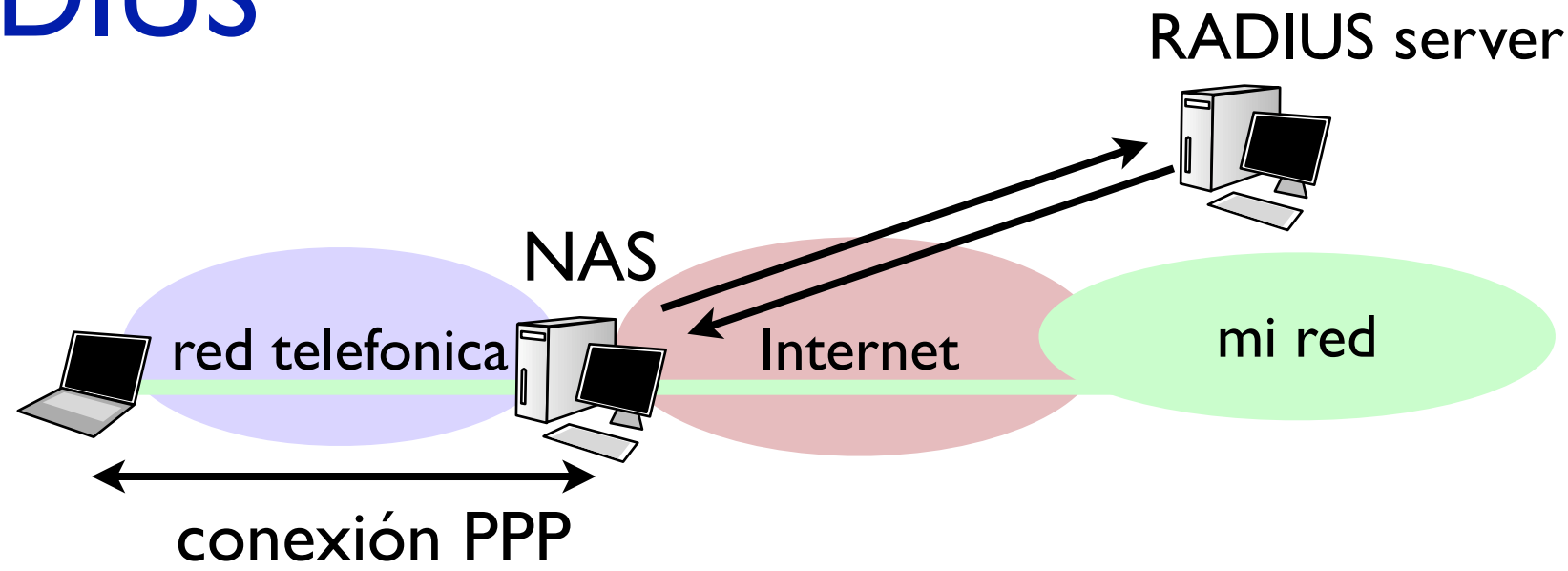
  ... (vease http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

Más sistemas de autentificación

- Passwords de un solo uso (S/KEY RFC1760, OTP RFC 1938)

  Cliente y servidor generan una lista de passwords de un solo uso
  - Que se genera a partir de la contraseña del cliente pero no puede invertirse
  - Cuando el servidor pide autentificación se le envía la siguiente password de la lista que nunca vuelve a utilizarse
- Sistemas basados en SmartCards para que el usuario no elija la contraseña sino que la genere la tarjeta con una CPU
- Kerberos (Autentificación basado en una tercera parte confiable)
  - El servidor de Kerberos comparte una clave secreta con los clientes y servidores y cuando es necesario genera tickets que permiten a un cliente autentificarse una vez en un servidor

RADIUS



- Remote Access Dial In User Service (RFC2138)
  - El usuario establece enlace PPP y hace autentificación
  - El NAS construye una peticion de autentificación y la envía por UDP al servidor RADIUS
  - El servidor RADIUS la valida y envía respuesta
  - En la respuesta envía parámetros de configuración y de filtrado para el acceso
  - Se notifica al servidor is el usuario desconecta para que pueda tarificar

AAA

- RADIUS es un protocolo de Autentificación Autorization and Acounting (AAA)
  - Muy utilizado, tanto por modem telefónico como en sistemas de inalámbricos
  - Permite arquitectura distribuida con varios servidores RADIUS para resistencia a que caiga uno de ellos
  - Permite que un proveedor centralice el servidor RADIUS en un proxy que reenvíe las peticiones de autentificación a diferentes servidores de RADIUS de clientes (nombres de usuario de tipo usuario@miempresa.com)
- Otros sistemas de AAA
  - TACACS, TACACS+ (Terminal Access Controller Access-Control System) de Cisco

Protocolos de tunel de nivel 3

- Permiten reenviar paquetes de nivel 3 de forma segura
- El tunel es transparente y no se puede distinguir de un envío sobre IP

IPsec

- Conjunto de protocolos del IETF para asegurar las comunicaciones de IP
  - Se puede usar sobre IPv4 aunque está diseñado para IPv6
- Referencias
  - Arquitectura IPsec (RFC2401)
  - Protocolo AH Autentication Header (RFC2402)
  - Protocolo ESP Encapsulating Security Payload (RFC2406)
  - Gestion e intercambio de claves

    Internet Security Asociation and Key Management ISAKMP (RFC 2408)

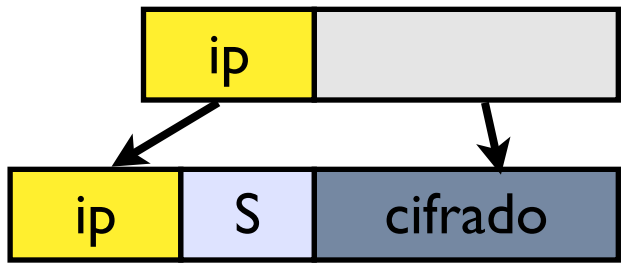
    Internet Key Exchange protocol IKE (RFC 2409)
- Usa encriptación y protocolos criptográficos de intercambio de claves muy estudiados.
- Soporta múltiples protocolos/cifradores que se negocian en el establecimiento de la VPN

IPsec tuneles

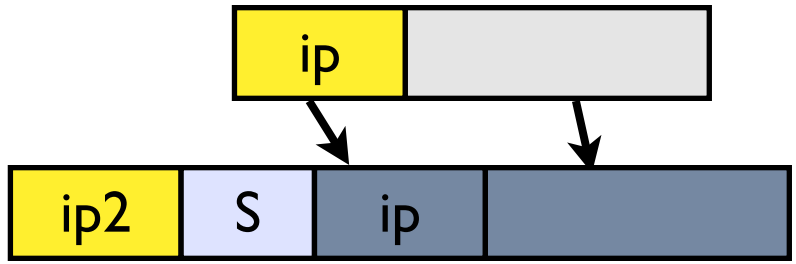
Dos modos de encapsulación

- **Modo transporte**
  - Mantiene cabecera IP y añade cabecera de seguridad
  - Solo vale si el tunel es para comunicar Host-to-host
- **Modo tunel**
  - Nueva cabecera IP con destino entre gateways
  - El paquete orginal se transporta entero

Modo transporte



Modo tunel



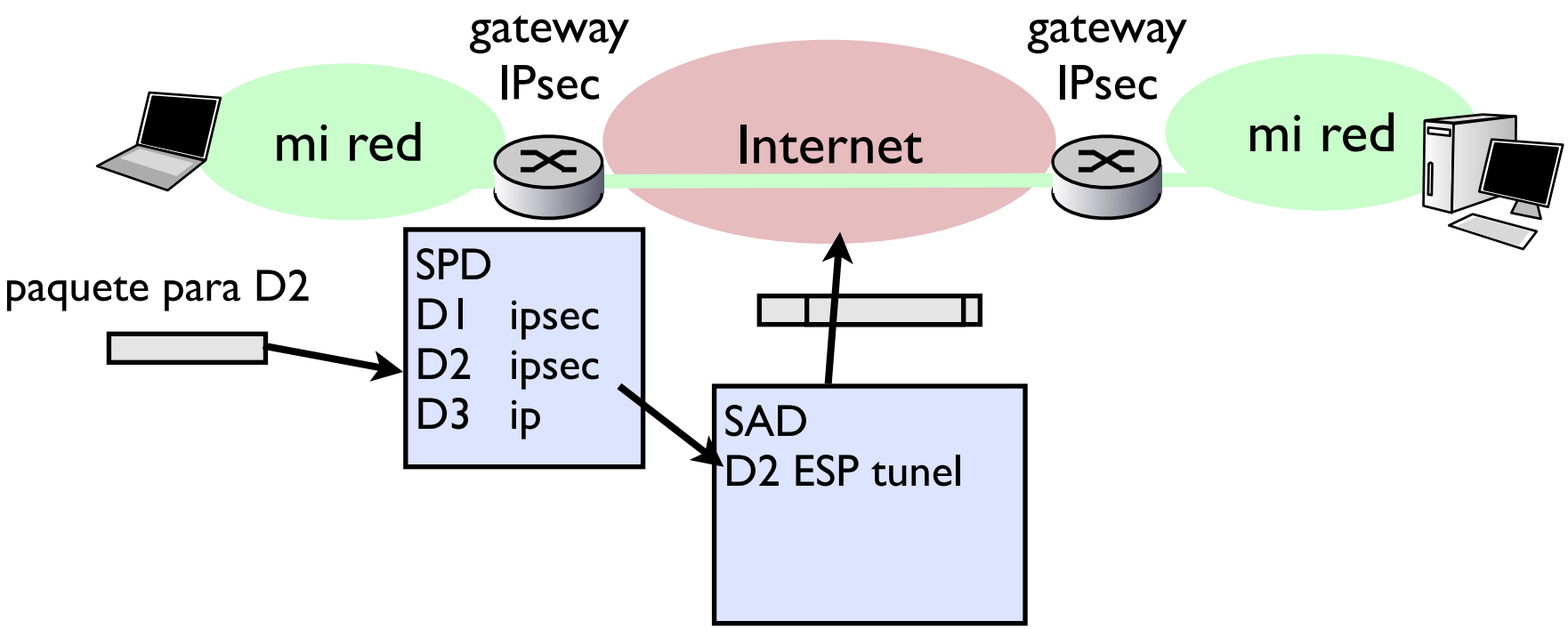
- Dos protocolos para transportar datos seguros dentro de IP
  - **AH** (proto=51) Autentication Header

    Permite garantizar autentificación e integridad del paquete
  - **ESP** (proto=50) Encapsulating Security Payload

    Permite garantizar autentificación e integridad asi como encriptar

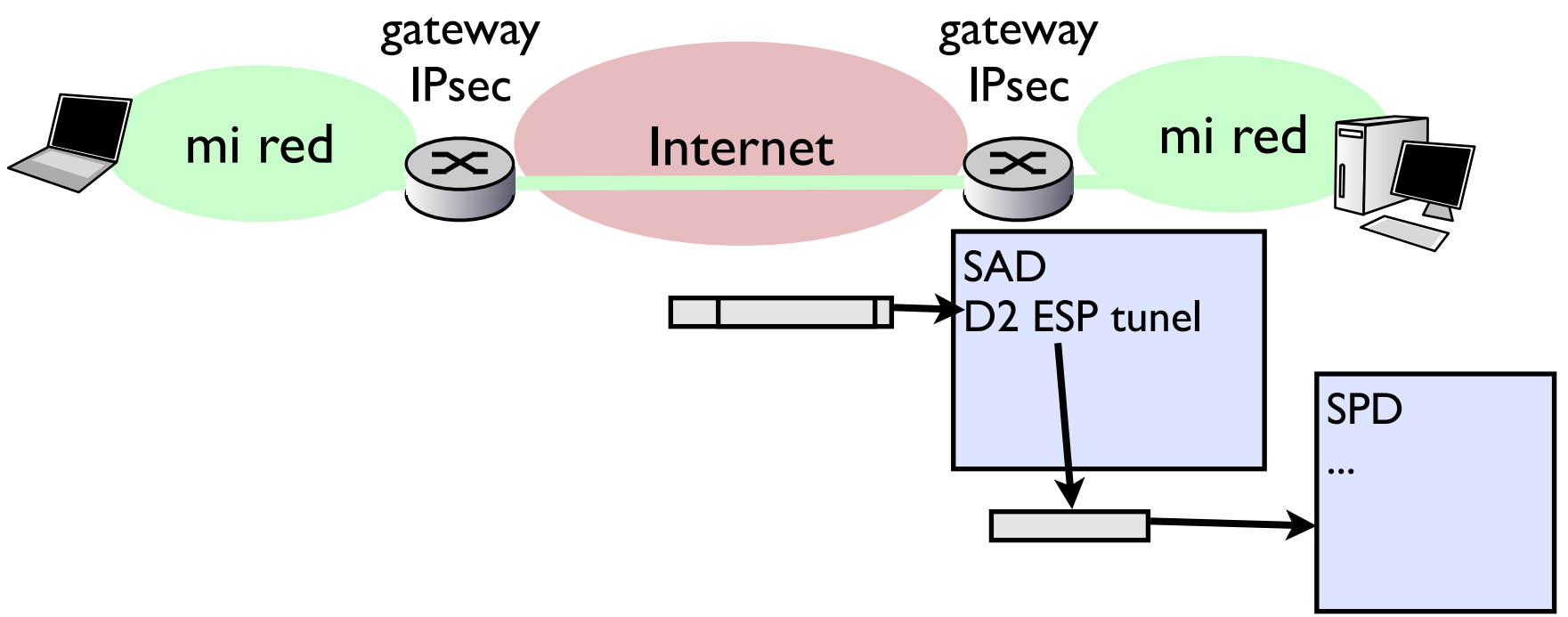
IPsec

- Configuración de túneles mediante dos bases de datos de Politicas (SPD) y Asociaciones de Seguridad (SAD)
  - Al enviar un paquete la tabla de politicas de seguridad nos dice si debe ser enviado por un tunel IPsec o sobre IP (reglas sobre IPs y puertos)
  - La base de datos de asociaciones de seguridad contiene los tuneles establecidos y sus claves y demás estado criptográfico



IPsec

- Al recibir un paquete IPsec (ESP o AH) la tabla de Asociaciones de Seguridad es consultada para descifrar el paquete y extraer su contenido
- Una vez recuperado el paquete IP original se consulta la tabla de politicas para saber si reenviarlo o aplicarle nuevas reglas de filtrado (por ejemplo solo aceptar ciertos puertos TCP o UDP sobre el tunel)



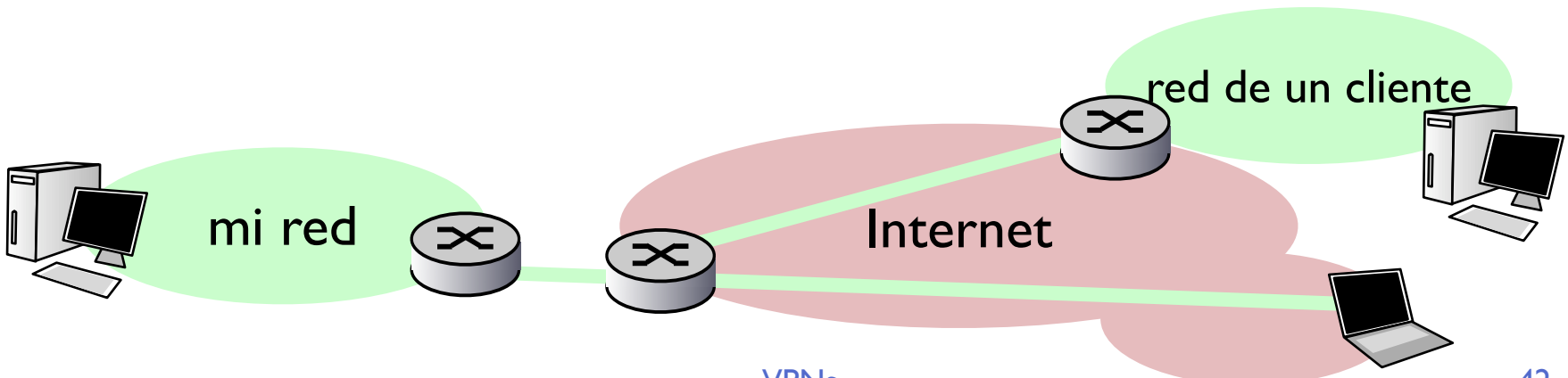
IPsec manejo de claves

- Las asociaciones de seguridad y sus claves necesarias
  - Pueden ser establecidas manualmente por un administrador
  - Pueden ser generadas y negociadas automáticamente por los extremos del tunel. Protocolo IKE para intercambio de claves entre dos extremos (RFC 2409). Usa UDP y puerto 500
  - Las claves se pueden negociar basándose en técnicas de secreto compartido (indicando la misma contraseña en ambos extremos del tunel) o bien configurando certificados (X.509) con capacidad de generación de claves privada/publicas o Diffie-Hellman
  - En la negociación de claves va incluida la autentificación de los extremos que establecen el tunel

Usando IPsec

- Mediante Gateways/routers que soporten IPsec puedo configurar conexiones VPN de tipo
- **LAN-to-LAN o Host-to-LAN**:
  - Hay que usar IPsec en modo tunel para que el paquete viaje hasta el gateway extremo del tunel y una vez extraido se utilice la dirección destino para direccionar hosts en la subred
- **Host-to-Host**:
  - Se puede usar el modo transporte de IPsec para proteger servicios entre un host y otro
  - Esto se puede usar para proteger una conexión PPP y tener asi un enlace directo a un router de la empresa protegido por IPsec

    Los equipos VPN suelen soportar L2TP sobre IPsec



Conclusiones

- Asegurando el canal de comunicaciones para establecer redes seguras a través de redes de comunicación inseguras
- Túneles de nivel 2 que permiten establecer enlaces virtuales
  - Y de paso autentificar y tarificar al que establece el enlace (AAA). Usados en el acceso telefónico a ISPs y empresas
  - Muy usados pero con problemas de seguridad (protocolos de protección no del todo seguros)
- Túneles de nivel 3 que permiten establecer comunicaciones muy seguras sobre IP.
  - Algún día serán el estandar
  - Aún son más difíciles de configurar/no tan extendidas
- Próxima clase:
  - Un caso particular de redes de acceso con problemas de seguridad

    Redes inalámbricas (WiFi) 802.11