Sistemas de Transporte de Datos

Ingeniería Informática (9186)

Manual de la Práctica 2:

Túneles y Redes Virtuales Privadas

Francisco Andrés Candelas Herías

Santiago Puente Méndez

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

Universitat d'Alacant

Universidad de Alicante

Práctica 2. Túneles y Redes Virtuales Privadas

1. Objetivos

Para la interconexión de las redes de datos no sólo se utiliza el encaminamiento de paquetes con tablas y protocolos de enrutamiento. Los routers también pueden realizar otras funciones de encaminamiento más avanzadas, y que juegan un papel muy importante en las redes de datos actuales. El objetivo principal de esta práctica será conocer los fundamentos y aplicaciones de las técnicas de túneles: la interconexión entre dos equipos mediante un túnel y las Redes Privadas Virtuales (VPN). Además, se analizarán aspectos de la gestión de usuarios, y la actualización de rutas en VPN con encaminamiento dinámico.

2. Conocimientos básicos

2.1. Interconexión de redes mediante túneles

2.1.1. ¿Qué es un túnel?

La comunicación a través de un túnel (*tunneling*), es una técnica para encapsular paquetes de un protocolo cualquiera, llamado **pasajero**, dentro de otro protocolo determinado, llamado **portador**, en una conexión entre dos equipos remotos (ver **Figura 1**). Además, se puede utilizar un protocolo de **encapsulación**, situado entre los dos anteriores. El protocolo pasajero es el protocolo que usan los equipos remotos para comunicarse, y que se quiere encapsular para poder enviarlo por una red portadora que usa un esquema diferente de direccionamiento o que no puede soportar el protocolo pasajero. El protocolo portador es el protocolo que utiliza la red portadora, y cuyos paquetes llevan dentro los de pasajero. Finalmente, el protocolo de encapsulación sirve básicamente para informar de que los paquetes pertenecen a un túnel y de qué protocolo pasajero se está usando en aplicaciones que admiten múltiples protocolos pasajeros.

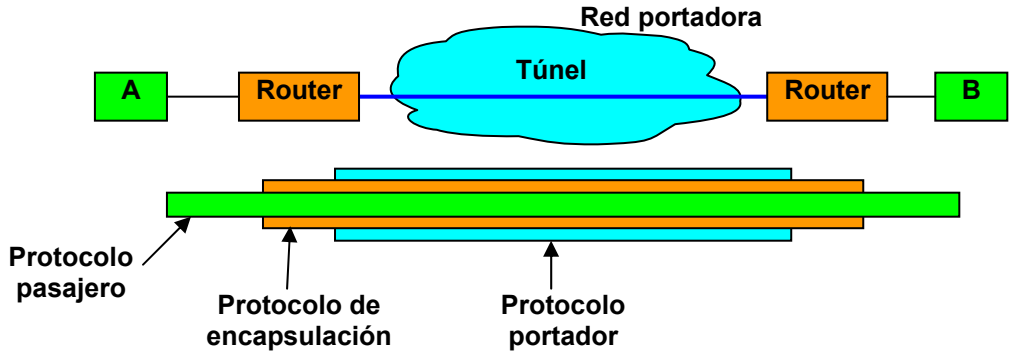

Figura 1. Esquema general de un túnel entre dos equipos.

A lo largo de los últimos años, distintos fabricantes de equipos y de software han propuesto y utilizado diferentes técnicas de túneles y protocolos de encapsulación, muchas de ellas propietarias, lo que significa que requieren de determinados equipos, software o sistemas operativos para funcionar.

Los protocolos concretos utilizados en un túnel, y los niveles a que trabajan éstos dentro de la arquitectura de red, dependen de cada aplicación, y por ello se han planteado muchas técnicas de encapsulación. Para aplicaciones de interconexión de redes y equipos remotos, la mayoría de los túneles consideran protocolos pasajeros de nivel de enlace (como PPP o Ethernet) o de nivel de red (IP, Apple-Talk, IPX...) que se envían sobre un protocolo portador de enlace, red o transporte (PPP, *Frame Relay*, IP, TCP, UDP...).

2.1.2. Túneles de nivel 3 (de red)

Se puede hablar de encapsulación de nivel 3 o de red cuando el protocolo pasajero es de nivel 3. Los protocolos habituales que se emplean en este caso son los siguientes:

- **Pasajero** (o *passenger protocol*). Puede ser un protocolo de red como IP, IPX, NetBeui, Apple-Talk, etc., con todo el contenido de sus correspondientes niveles superiores.
- **Portador** (o *transport protocol*). Habitualmente es un protocolo de red como IP.
- **Enscapsulación** (o *carrier protocol*). Aunque también es posible implementar un túnel de nivel 3 sin este protocolo, existes diferentes opciones, como por ejemplo:
  - **GRE** (*Generic Route Encapsulación*). Funciona con diferentes protocolos pasajeros. Fué promovido inicialmente por Cisco Systems, pero su uso se ha extendido mucho.
  - **IPSec** (*Internet Protocol Security*). Este protocolo es un estándar del IETF (*Internet Engineering Task Force*) que trabaja sobre IPv4 e IPv6, y ofrece varias técnicas para seguridad en la transmisión de datos. Permite enviar el contenido del pasajero de forma segura, con autenticación, autorización y cifrado.
  - **EON**. Estándar para transportar como pasajero el protocolo CLNP (protocolo estándar del nivel de red de la arquitectura OSI) sobre redes IP.
  - **Cayman**. Para usar el protocolo de red Apple-Talk (Apple) sobre el portador IP.

Este tipo de encapsulación se suele utilizar para interconectar entre sí las redes privadas remotas de una compañía determinada a través de redes públicas como Internet. Es habitual usar un protocolo de encapsulación como IPSec, que permita cifrar el contenido del protocolo portador, lo cual, junto con otras medidas de seguridad, ofrece un túnel seguro a través de una red pública insegura.

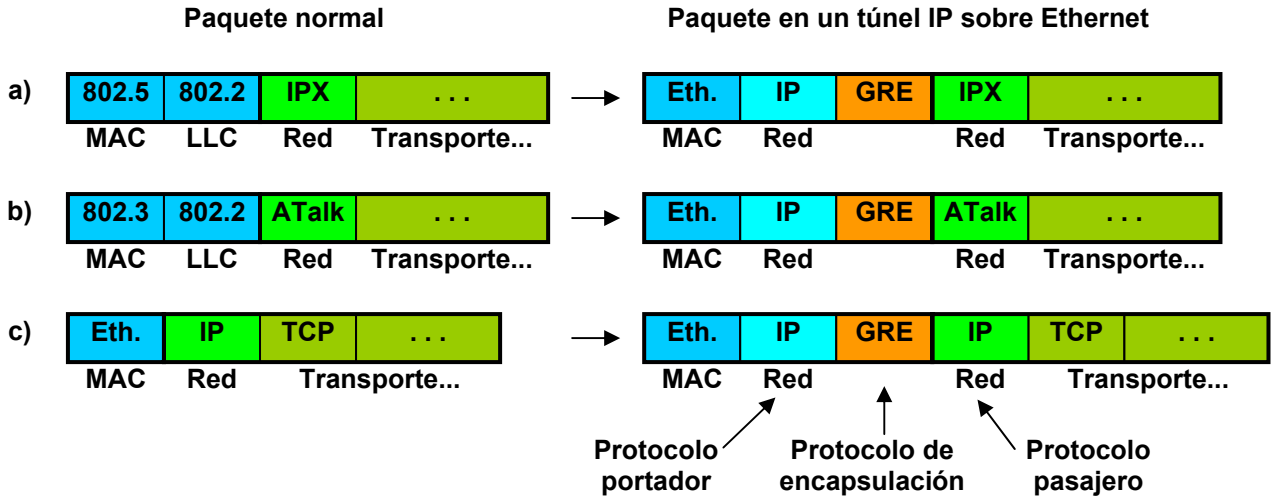

Figura 2. Ejemplos de encapsulación de nivel 3 en un túnel IP.

La **Figura 2** muestra un ejemplo de como quedarían diferentes paquetes normales procedentes de distintas redes al aplicarles una encapsulación de nivel 3. La opción **a)** representa la encapsulación de un paquete IPX de Novell que viaja por una LAN IEEE 802.5 (Token-Ring), la opción **b)** representa la encapsulación de un paquete Apple-Talk de Apple que viaja sobre una LAN IEEE 802.3 (Ethernet), y, finalmente, la opción **c)** representa la encapsulación de un paquete IP que viaja sobre una red Ethernet para IP. Los tres se encapsulan sobre paquetes IP que viajan por una red Ethernet para IP usando el protocolo de encapsulación GRE. De esta forma, los tres paquetes, de distintas características, se pueden enviar por una misma LAN.

La encapsulación es realizada por un router que soporta esta técnica, para enviar encapsulados los paquetes del protocolo pasajero a otro router, que realizará el proceso de "desencapsulación", es decir, obtendrá el paquete pasajero original. Al enlace que existe entre los dos *routers* se le conoce como túnel. Un túnel suele ser bidireccional, pero también se puede configurar un túnel para transmitir en un solo sentido. Para configurar el túnel es necesario definir una dirección para cada uno de sus extremos. Estas direcciones no tienen por que ser de la misma red, ya que el túnel no es un enlace físico punto a punto como el empleado en un enlace con SLIP o PPP. Además, para que los paquetes del protocolo portador se encaminen por las redes deseadas, es necesario configurar adecuadamente las tablas de encaminamiento de los equipos que atraviesa el túnel. Una vez configurado el túnel en un *router*, este queda disponible como una interfaz más de ese *router* (por ejemplo *Tunnel1*), por la que se puede encaminar los paquetes a los destinos deseados configurando adecuadamente la tabla de encaminamiento.

El contenido de la PDU del protocolo GRE es bastante simple. Consta de dos campos, uno de indicadores y otro de identificador de protocolo. El primero indica cosas como la versión de GRE empleada, y el segundo identifica el protocolo pasajero utilizado. Por ejemplo, IP se identifica como pasajero con el valor 800H.

Supóngase ahora que se quieren conectar dos redes privadas **A** y **C** (típicamente LANs) en las que se utiliza un protocolo de red **X** (que puede ser diferente de IP) y los correspondientes niveles superiores de su arquitectura a través de otra red portadora B (que puede ser una LAN, una interconexión de éstas, o una WAN), la cual sólo admite el protocolo IP en el nivel de red. El uso de *tunneling* es la solución más adecuada para esta situación. Para ello se utilizan dos *routers*, denominados **R1** y **R6**, que conectan cada red privada con la red portadora, tal y como muestra la **Figura 3**.

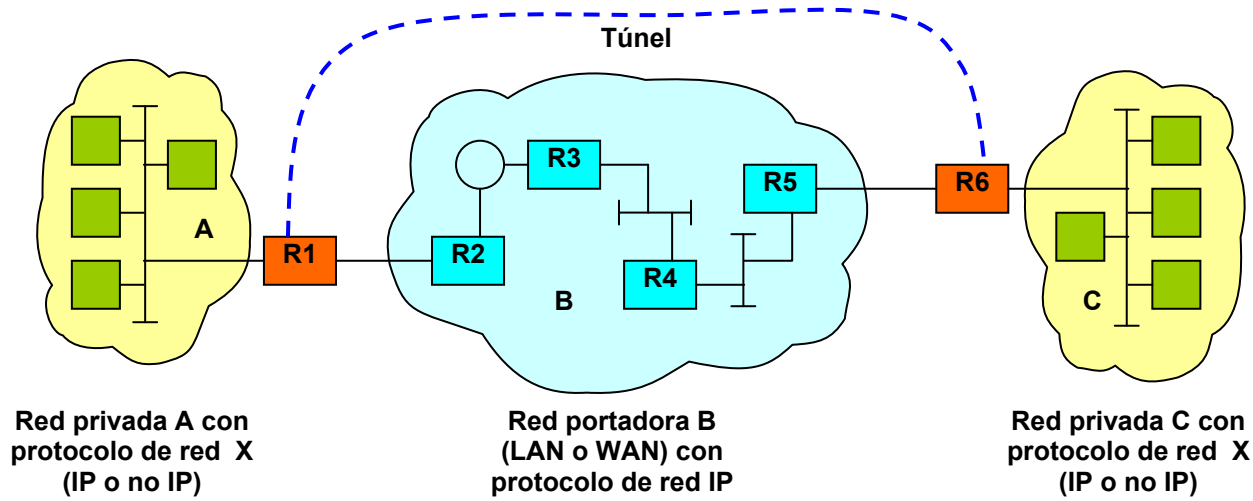

Figura 3. Ejemplo de interconexión de dos redes mediante un túnel.

R1 y **R6** deben soportar la misma técnica de *tunneling*, y es conveniente que sean del mismo fabricante u de una misma asociación de fabricantes por motivos de compatibilidad. Estos *routers* se encargan de hacer que los paquetes con protocolo *X*, que deben ir de la red **A** a la **C**, o viceversa, viajen encapsulados sobre paquetes IP a través de toda la red portadora **B**, pasando por los *routers* **R2** a **R5**, de forma similar a los casos reflejados en la **Figura 2**.

Hay que tener en cuenta que la técnica de *tunneling* es gestionada por **R1** y **R6** de forma totalmente transparente a los equipos de las redes **A** y **C**. Para estas redes privadas, sus paquetes del protocolo X dan un salto directo entre **R1** y **R6**, ya que viajan como datos del protocolo portador IP a lo largo de la red **B** y no se altera su contenido. Las redes privadas **A** y **C** quedan conectadas aparentemente de forma directa a través del túnel, como representa el esquema de la **Figura 4**-a. Este salto directo aparente tiene una consecuencia importante; para el protocolo **X** los paquetes que viajan entre ellas dan 1 salto, aunque realmente realizan 5 saltos al pasar por la red **B**. Incluso se podrían configurar los *routers* **R1** y **R6** de forma que el salto entre ambos no se tenido en cuenta (Figura 4-b).

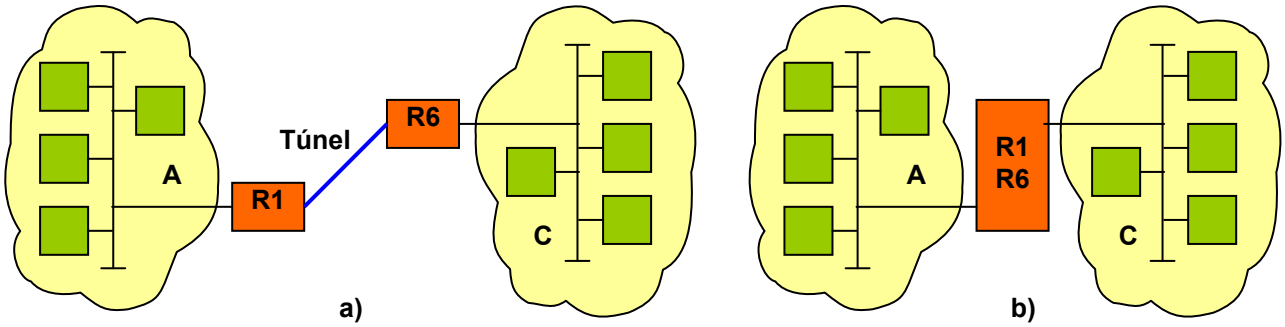

Figura 4. Efecto de la interconexión de dos redes mediante un túnel.

2.1.3. Túneles de nivel 2 (de enlace)

Cuando el protocolo pasajero es de nivel de enlace, se suele hablar de encapsulación de nivel 2. Los protocolos habituales que se emplean en este caso son los siguientes:

- **Pasajero**. Protocolo de enlace y punto a punto, habitualmente PPP (*Point to Point Protocol*) u otro derivado de HDLC, con todo el contenido de los niveles superiores.
- **Portador**. Típicamente es el protocolo de red IP, pero puede ser un protocolo de enlace como *Frame Relay*, otros protocolos de red como X.25, de nivel superior como TCP o UDP, o protocolos de ATM.
- **Enscapsulación**. Este protocolo está presente siempre en túneles a nivel 2, y depende del tipo de túnel empleado.

La encapsulación de nivel 2 se utiliza principalmente en la conexión de usuarios remotos con una red privada de una empresa, de forma que puedan trabajar con los recursos de esa red privada como si estuviesen en ella, incluso con el direccionamiento de red interno y privado. A esta estructura se le denomina VPN (*Virtual Private Network*) o VPDN (*Virtual Private Dial-up Network*). Actualmente destacan dos estándares independientes que definen el funcionamiento completo de túneles de nivel 2 para VPN:

- **PPTP** (*Point-to-Point Tunneling Protocol*). Fue creado por un consorcio de empresas (PPTP Forum), entre las que estaban US Robotics, Microsoft, 3COM, Ascend y ECI Telematics. Aunque esta opción se usa cada día menos por su falta de

seguridad, será estudiada con detalle en la práctica por qué es sencilla, y emplea el mismo principio de funcionamiento que L2TP.

– **L2TP** (*Layer 2 Tunneling Protocol*). Es un producto más reciente creado por el PPTP Forum y Cisco Systems, y normalizado por el IETF (Internet Engineering Task Force). Con él se trata de solventar los problemas de seguridad de PPTP. Incluso puede ofrecer un túnel cifrado utilizando IPSec. Está soportado en los S.O. actuales (M.S. Windows desde Windows 2000 y últimas versiones de Linux).

Independientemente del estándar utilizado, se pueden considerar dos modelos básicos de VPN según el túnel lo gestione el usuario o el ISP (proveedor de servicios de Internet), los cuales se describen a continuación.

La **Figura 5** representa el primer modelo para una VPN. Habitualmente, la empresa no se preocupa de la conexión mediante módems con los usuarios a través de la red telefónica conmutada (RTC), y esta función se contrata a un ISP. El usuario se comunica con el ISP mediante un acceso telefónico, ADSL o cable-módem y un protocolo de enlace punto a punto como PPP, mientras que el ISP se comunica con el router de la empresa que gestiona las VPN (servidor de túneles) mediante una arquitectura WAN (que puede ser Internet). Tanto el router del ISP que le conecta con Internet como el router de la empresa se conocen como NAS (Network Access Server), y para distinguirlos denominaremos NAS privado al segundo. Para conseguir una conexión directa a nivel de enlace entre el usuario y el NAS privado salvando la red WAN, se encapsula PPP sobre el protocolo correspondiente de la red WAN (que pude ser IP). De este modo, el usuario no debe preocuparse por el túnel, y no requiere disponer de un S.O. concreto que soporte determinada técnica de túnel. En contraste, se requiere un ISP que ofrezca este tipo de servicio, el cual debe ser contratado por la empresa.

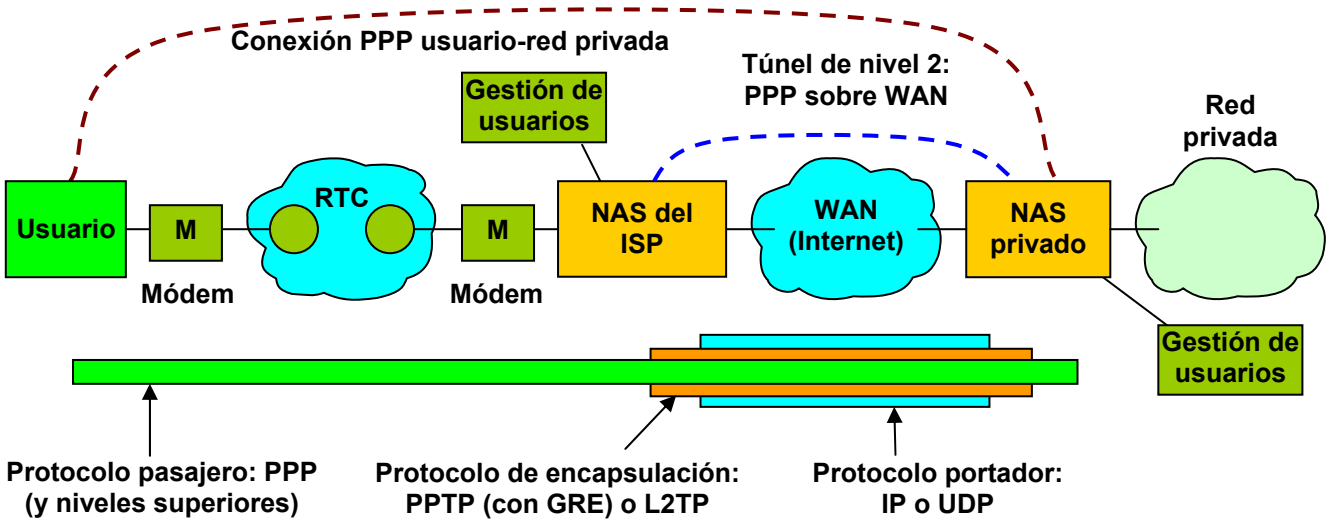

Figura 5. Ejemplo de un túnel de nivel 2 entre el ISP y el NAS privado.

Además, es habitual disponer de un sistema de autentificación y gestión de usuarios, para lograr que sólo usuarios de confianza registrados puedan usar la VPN. Este sistema puede estar controlado por el NAS del ISP o por el NAS privado, o de forma coordinada por ambos. Sobre este aspecto se profundizará más en el apartado 2.1.4.

El otro modelo de VPN se basa en que es el mismo usuario el que establece el túnel desde su equipo con el NAS privado, tal y como muestra la **Figura 6**. En este caso no se requiere un servicio especial por parte del ISP, si éste existe, pero, en cambio, el usuario

requiere disponer en su equipo de un S.O. o de un software cliente compatible con el tipo de túnel utilizado, sea PPTP o L2TP. Este esquema, que será el estudiado en la práctica, se describirá mejor en los siguientes apartados. Este segundo modelo también se suele utilizar un sistema de gestión y autentificación de usuarios como en el caso anterior.

Una vez se ha establecido el túnel de nivel 2, el usuario puede utilizar el mismo nivel de red y direccionamiento que existe en la red privada, como si estuviera presente en ella.

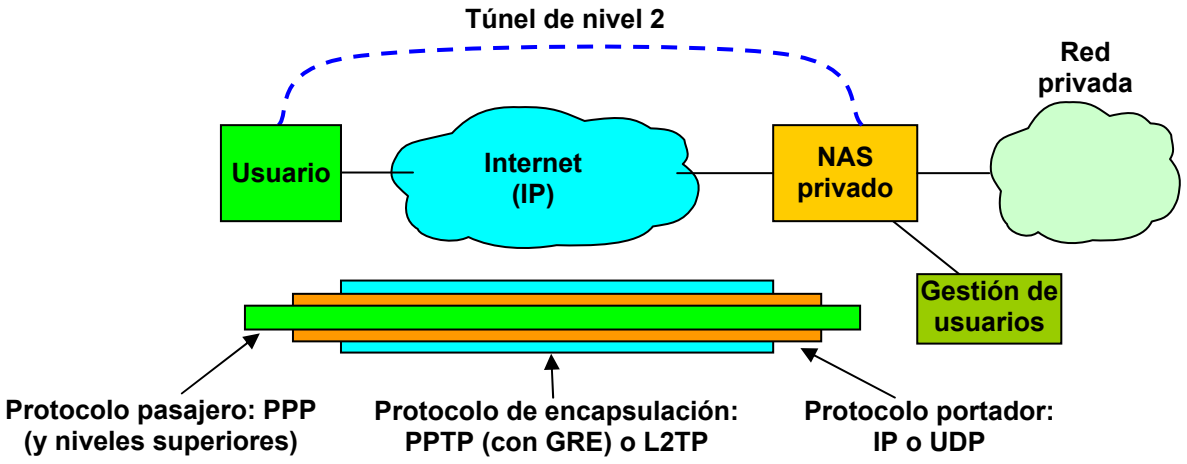

Figura 6. Ejemplo de un túnel de nivel 2 directo entre usuario y el NAS privado

Un tema de gran actualidad es la aplicación de las VPN a equipos de usuario móviles, como ordenadores portátiles o PCs de bolsillo, sustituyendo la RTC por redes inalámbricas de datos (WLANs, Bluetooth…) o de telefonía móvil (GSM, GPRS). Sin embargo, para poder sacar un buen partido a las VPN es conveniente disponer de accesos con suficiente ancho de banda, ya que el habitualmente equipo del usuario usará servicios típicos de una LAN tras establecer la VPN.

2.1.4. Autentificación y gestión de usuarios

Es evidente la necesidad de medidas de seguridad dentro de las redes de datos, y en especial en los accesos a recursos privados de una empresa con VPN a través de redes públicas inseguras. Además de los procedimientos de cifrado, resulta muy importante tener en cuenta medidas de verificación y gestión de usuarios, o lo que se conoce como AAA: *Authentication, Authorization and Accounting*.

La autentificación se refiere a validar los usuarios que deben usar el sistema y a asegurar que son quienes dicen ser, la autorización controla que sólo determinados usuarios podrán acceder a determinados recursos del sistema, con ciertas requisitos establecidos, y la contabilidad se refiere a disponer de una base de datos donde se almacene información sobre los usuarios que han utilizado los recursos del sistema. Esta información de contabilidad se puede componer del número de bytes transmitidos, la hora y fecha de conexión, el tiempo de uso, el tipo de acceso, el origen del acceso, etc.

Una de las soluciones más extendidas es disponer de un equipo Unix o MS. Windows con un servidor RADIUS (*Remote Authentication Dial In User Service*) dentro de la red privada según muestra la **Figura 7**. RADIUS es un software cliente-servidor de gestión de usuarios original de Livingston Enterprises, que se ha extendido mucho por varios motivos: fué normalizado por el IETF en 1996 (RFC 2058), hay versiones para muchas plataformas

(como Linux o MS. Windows), hay versiones de libre distribución (alguna GNU), y es escalable y aplicable a muchas situaciones.

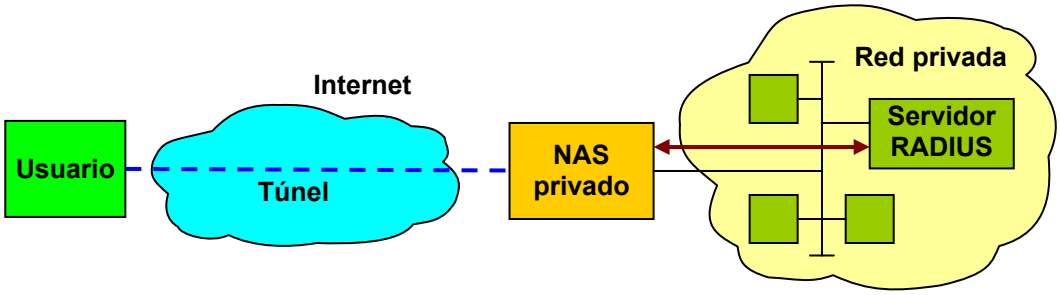

Figura 7. Disposición de un servidor RADIUS.

RADIUS emplea un programa servidor (en Unix/Linux es un demonio llamado *radiusd*) que se apoya en **UDP** y atiende los puertos **1645** para autentificación y **1646** para contabilidad. En el caso de VPN, sus clientes son los NAS que atienden las VPN, tanto los privados como los de los ISP en caso de que estos también gestionen los usuarios. Para esto, RADIUS soporta un modo *proxy*, de forma que cuando el servidor que atiende a los *routers* del ISP no encuentra información de un usuario, puede buscar esa información realizando peticiones a otros servidores, incluidos servidores privados. RADIUS gestiona una base de datos con los usuarios y los *routers* clientes, que puede estar implementada como archivos de texto fáciles de editar y comprender, como archivos compilados indexado, o en bases de datos comunes como MySQL. La primera opción no es recomendable cuando hay muchos usuarios.

Cuando un NAS recibe una petición de establecimiento de un túnel desde un usuario, con un nombre y una contraseña cifrada, este envía un mensaje **Access-request** al puerto 1645 del servidor RADIUS para verificar si el usuario es válido. Este mensaje incluye información como el nombre del usuario, su contraseña (cifrada) y la IP del NAS. El servidor comprueba su base de datos, y si el usuario tiene un perfil asociado, devuelve al NAS un mensaje **Access-accept** con los atributos de configuración del perfil. Al recibir ese mensaje, el NAS comprueba que se cumplen otras condiciones para el usuario dadas por los atributos (origen, tipo de acceso,...), y de ser así configura entonces el acceso del usuario según la información recibida (protocolo, direcciones, nuevas rutas...), y continúa la sesión de trabajo con el túnel. Si el usuario no existe o no es válido, RADIUS envía la respuesta **Access-reject** al NAS, y se cancela el túnel.

Por otra parte, el NAS puede enviar información de contabilidad al servidor con mensajes **Account-request** al puerto 1646. El servidor responde con mensajes **Account-response**, y almacena esa información del usuario.

Los atributos de un perfil de usuario son básicamente pares *nombre de atributo - valor*. Existe una lista de atributos estándar (del IETF), además de las extensiones propias que utiliza cada fabricante de equipos para redes de datos. También se puede definir atributos personalizados. Algunas de las características que se pueden establecer con los atributos son:

- Nombre y contraseña.
- Direcciones o números de teléfono desde los que se puede establecer la sesión.
- Tipo de conexión que debe utilizar el usuario (RTC, RDSI, *Frame Relay*...).
- Llamada a cobro revertido (permite que sea la empresa la que pague la conexión).
- Programa a ejecutar cuando el usuario se conecta. Muy útil para acciones especiales con usuarios sospechosos: por ejemplo, enviar un SMS al móvil del administrador.

- Tiempo máximo que puede durar la sesión, y tiempo máximo sin uso de la sesión, tras los cuales se cierra el túnel automáticamente.
- Fechas y horas en las que el usuario puede acceder al sistema.
- Protocolo que utiliza el usuario (por ejemplo PPP).
- MTU de las tramas de enlace intercambiadas con el usuario (si está bien ajustado, permite evitar la fragmentación por culpa del túnel).
- Direcciones a asignar al usuario dentro de la red privada (IP y máscara de red). Puede ser fija, u obtenida de un rango.
- Entradas de rutas a añadir en la tabla de encaminamiento del equipo cliente.
- Parámetros de gestión de ancho de banda y QoS.

Observando los anteriores atributos, se puede imaginar la potencia que supone emplear un sistema como RADIUS. Además, RADIUS es un sistema de gestión de usuarios muy extendido, que se aplica también a otros tipos de túneles, como IPSec, gestión de usuarios en redes corporativas, integración con las cuentas de sistemas Unix, gestión de usuarios de ISPs o de servidores de Internet, etc.

RADIUS también se utiliza en otras aplicaciones que requieren autenticación, como es el caso de las redes WLAN IEEE 802.11. Las últimas definiciones sobre seguridad para este estándar, 802.11i (WPA2), incorporan la configuración de autentificación basada en servidores como RADIUS. En este caso, son los puntos de acceso (AP) de la red inalámbrica los clientes del servidor RADIUS.

2.2. VPN con PPTP

PPTP (*Point-to-Point Tunneling Protocol*) es un estándar de Internet (RFC 2637) que define un conjunto de protocolos para establecer y utilizar un túnel de una VPN. Lo primero a tener en cuenta es que hay dos flujos de datos entre el equipo del usuario y el NAS que trabajan en paralelo: una conexión **TCP** sobre la que está el protocolo de aplicación **PPTP**, y un intercambio de paquetes encapsulados a través del túnel. La conexión TCP/PPTP es usada básicamente para el establecimiento y la liberación de la sesión de un túnel con el NAS correspondiente.

El túnel se pone en marcha cuando el equipo de usuario solicita el establecimiento de la conexión **TCP** con el servicio del puerto **1723** de la dirección pública del NAS, y el NAS acepta esa conexión. En esta conexión se envían paquetes TCP-IP sobre el nivel de enlace existente sin encapsulación. En las conexiones telefónicas, los ISP emplean habitualmente PPP como nivel de enlace para establecer la conexión punto a punto. Después de establecerse la conexión TCP, el usuario y el NAS usan el protocolo de aplicación PPTP para un establecimiento completo del túnel. Si el NAS rechaza la conexión TCP o los mensajes PPTP, el túnel no se establecerá.

Tras la conexión TCP/PPTP, comienza el intercambio de paquetes encapsulados por el túnel entre el usuario y el NAS. Se utiliza un túnel de nivel 2 donde se encapsula PPP (pasajero) dentro de paquetes IP (portador) con direcciones públicas, utilizando **GRE** (encapsulación). Aunque GRE soporta distintos protocolos pasajeros, se suele emplear **PPP** (*Point-to-Point Protocol*) por que, además de transportar paquetes IP, puede usar otros protocolos auxiliares (LCP, CHAP, IPCP…) para controlar el establecimiento de sesiones con autenticación, y enviar parámetros de configuración al usuario (dirección IP privada, puerta de enlace, MTU…). El paquete encapsulado tiene la forma de la **Figura 8**.

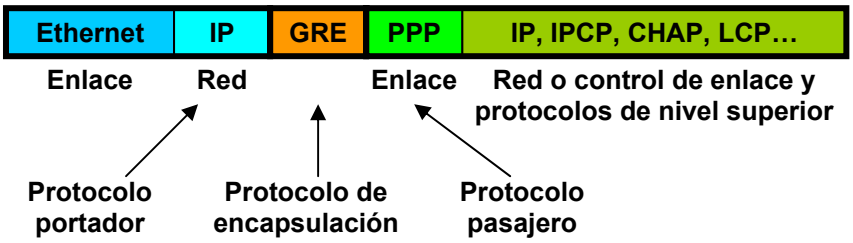

Figura 8. Formato de un paquete encapsulado con PPTP.

Los primeros paquetes que circulan por túnel son del protocolo **LCP** (*Link Control Protocol*) sobre PPP. El usuario y el NAS intercambian paquetes PPP-LCP para ponerse de acuerdo en cosas como el formato de encapsulación o el protocolo de autentificación que se va a usar. PPP admite diferentes protocolos de autentificación, como **PAP** (*Password Authentication Protocol*), **PPP-CHAP** (PPP *Challenge Handsake Autentification Protocol*), o **MS-CHAP**, (Microsoft CHAP).

Tras acordar el protocolo de autentificación (por ejemplo PPP-CHAP), el usuario y el NAS intercambian paquetes PPP-CHAP encapsulados para comprobar que el usuario tiene acceso a la VPN. Primero el NAS envía un paquete PPP-CHAP para solicitar al usuario que se autentifique (esto se denomina "desafío"), al que el usuario debe responde con otro paquete PPP-CHAP con su nombre de usuario y la contraseña cifrada al NAS. El NAS validará los datos del usuario accediendo a un sistema de gestión de usuarios, como puede ser RADIUS. Si el usuario es válido, el NAS aceptará al usuario y continuará con el túnel, enviándole un paquete PPP-CHAP de "éxito". Si el usuario no es válido, el NAS lo rechazará con un paquete PPP-CHAP de "rechazo", y finalizará el túnel y su conexión TCP/PPTP.

Tras autentificarse un usuario valido, el NAS puede configurarlo según el perfil dado por el sistema de gestión de usuarios. El NAS puede indicar al usuario los datos para el direccionamiento privado de nivel de red, como por ejemplo una dirección IP, una máscara de red, y una puerta de enlace. Esto se hace con otro protocolo como **NCP** (*Network Control Protocol*) o **IPCP** (*IP Control Protocol*), que van dentro de las tramas de PPP. Por ejemplo, con IPCP, es el usuario quién toma la iniciativa, y envía al NAS su configuración actual. Habitualmente el NAS contestará rechazando esa configuración y enviándole una nueva, conforme al perfil dado por el sistema de gestión de usuarios.

El establecimiento del túnel acabará con algunas actuaciones del NAS dentro de la red privada. Así, el NAS enviará primero una trama **ARP** con la dirección IP privada del usuario para indicar a sus vecinos que el da acceso a esa IP (a través del túnel). Es decir, cuando algún equipo de la red privada reciba una trama procedente del usuario, debe contestar al NAS, para que este la envíe al usuario por el túnel. El NAS también puede usar algún protocolo de encaminamiento dinámico, como **RIP** o **EIGRP**, para informar a otros routers de la red privada de que él da acceso al nuevo usuario.

Tras la configuración con éxito del túnel, el equipo del usuario ya puede intercambiar paquetes con la red privada que hay tras el NAS, usando el direccionamiento privado. Para indicar que el túnel sigue activo en momentos en los que no se intercambian datos, el usuario y el NAS pueden enviarse tramas **GRE** sin contenido (sin pasajero). La **Figura 9** muestra como es, por ejemplo, la encapsulación de un paquete de aplicación HTTP por el túnel entre el cliente y el NAS.

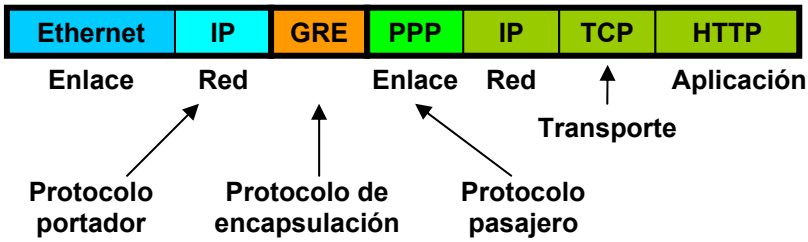

Figura 9. Formato de un paquete HTTP en un túnel PPTP sin cifrado.

Cabe mencionar que existen otros protocolos como **MPPE** (*Microsoft Point-to-Point Encryption*) para cifrar el contenido de las tramas PPP, o **MPPC** (*Microsoft Point-to-Point Compression*) que se utiliza para comprimir el contenido de PPP.

La conexión puede finalizar por iniciativa del equipo del usuario o del NAS, para lo cual ambos equipos intercambian paquetes del protocolo PPP-LCP sobre la finalización. Después también se intercambian mensajes de PPTP sobre la solicitud y aceptación de la desconexión, y se acaba finalizando la conexión TCP al puerto 1723.

2.3. VPN con L2TP

Debido a que las VPN permiten transmitir información del ámbito privado de una organización a través de una WAN pública, a los protocolos de VPN actuales se les exigen dos características muy importantes: el cifrado de la información transmitida, y un proceso robusto para autentificar al usuario que garantice completamente que esté es el usuario válido que dice ser. El problema principal de PPTP es que los procesos de establecimiento y autentificación de la conexión se realizan siempre antes de que se haya podido establecer un cifrado de la información del túnel, lo que implica que el cifrado no se aplique a los parámetros de configuración del cliente. Además, la autentificación de PPTP basada en una simple clave de usuario es un método muy simple.

L2TP (*Layer 2 Tunneling Protocol*) es un estándar de Internet (RFC 2661) que ofrece una seguridad mucho mejor que PPTP. Así, con L2TP se puede cifrar la información transmitida desde el primer momento, incluyendo todos los datos de configuración del cliente y las tramas del proceso de autentificación. Además, L2TP permite realizar autentificación del equipo origen mediante un certificado digital, además de la autentificación del usuario con PPP-CHAP, lo que ayuda a garantizar que el origen es válido y dificulta mucho la alteración de los paquetes. Para todo esto, L2TP se apoya en el estándar de Internet IPSec (RFC 2401: *Internet Portocol Security*), que define unos protocolos añadidos a IPv4 que permiten cifrar las transmisiones sobre el protocolo de red IP. Cabe mencionar que con la versión IPv6, las capacidades de autentificación y encriptación ya están incluidas en el propio protocolo IP, y no es necesario IPSec. El problema principal de L2TP con IPSec es que originalmente no estaba soportado por NAT, pero hoy en día muchos routers ya permiten hacer NAT a L2TP.

Por otra parte, en contraste con PPTP, L2TP utiliza el protocolo de transporte **UDP** como portador de todos los datos, habitualmente con el puerto **1701**. Esto facilita el procesamiento de los paquetes por NAT al disponer de un puerto de transporte, sin llegar a la complejidad de una conexión TCP. El protocolo pasajero es PPP, a igual que con PPTP. Y como protocolo de encapsulación, L2TP define uno propio. Así, el aspecto básico de un paquete encapsulado con L2TP es el mostrado en la **Figura 10**.

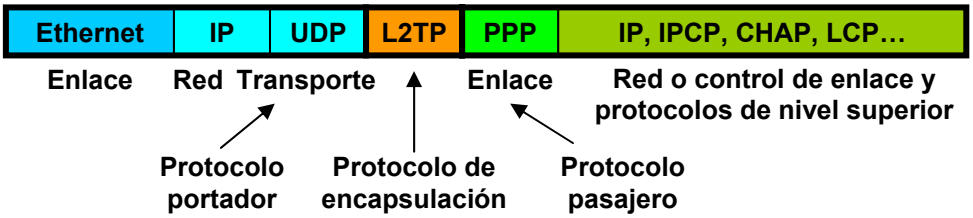

Figura 10. Formato básico de un paquete encapsulado con L2TP.

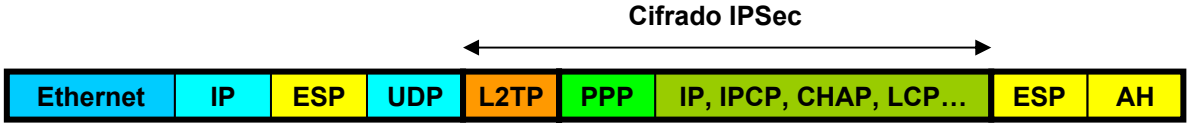

Figura 11. Formato de un paquete encapsulado con L2TP con cifrado IPSec.

Aunque en esta práctica no se abordará como trabaja IPSec, sí que conviene conocer el formato de L2TP cuando se utiliza IPSec con L2TP, que es lo recomendable y habitual. En este caso se añaden también al paquete las cabeceras de los protocolos de cifrado ESP (*Encapsulating Security Payload*) y autentificación AH (*Authentication Header*), como muestra la **Figura 11**. Mientras que ESP se encarga de la encriptación, AH se encarga de la integridad del mensaje, de la autentificación del origen, y de una asociación de seguridad entre los extremos de la conexión. ESP y AH se pueden usar en conjunto o de forma independiente. Todo el contenido del protocolo de encapsulación y del pasajero queda protegido por los procesos de encriptación e integridad del paquete.

En todas las tramas relativas al túnel, desde su establecimiento a su liberación, se utiliza como protocolo de encapsulación **L2TP**, que también actúa como protocolo de control de la conexión. El establecimiento del túnel L2TP comienza con el intercambio de mensajes de control del protocolo L2TP entre el cliente y el NAS. Si la conexión se acepta y se utiliza IPSec, se procede al intercambio de claves y a la autentificación IPSec, para comenzar a cifrar los paquetes. Después, se siguen tres pasos muy similares a los de PPTP (ver apartado 5.2): configurar aspectos de la conexión mediante **PPP-LCP**, autentificar el usuario con **PPP-CHAP**, y, si el usuario es aceptado por el NAS, configuración de los parámetros de direccionamiento del cliente con **PPP-IPCP**. Además, con L2TP, el cliente y el NAS pueden intercambiar tramas **PPP-CCP** (*Compresión Control Protocol*) para negociar opciones de compresión y cifrado sobre PPP. Por ejemplo, en sistemas MS. Windows, el cliente y el NAS usan PPP-CCP para negociar si se utilizan los protocolos **MPPE** (*Microsoft Point-to-Point Encryption*) y **MPPC** (*Microsoft Point-to-Point Compression*).

Tras un proceso de conexión válido, ya se puede intercambiar información entre el cliente y el NAS. Por ejemplo, si se envía un paquete de aplicación HTTP sobre usa una conexión L2TP sin IPSec se tendrá una trama como la mostrada en la **Figura 12**.

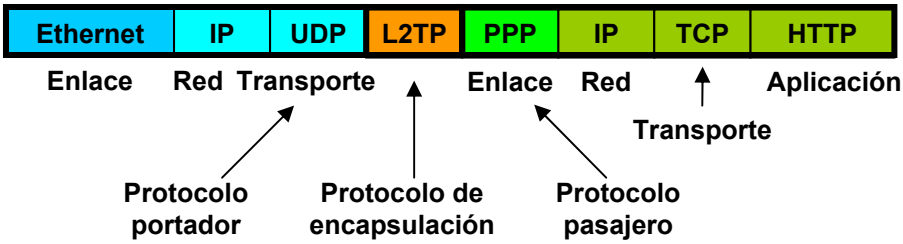

Figura 12. Formato de un paquete HTTP sobre un túnel L2TP sin IPSec.

La desconexión de L2TP se efectúa primero mediante el intercambio de tramas de control PPP-LCP, y después con mensajes de control de L2TP.

Finalmente, cabe comentar que en la definición de L2TP, al equipo cliente se le conoce también como LAC (*L2TP Access Concentrator*) mientras que al servidor o NAS se le denomina LNS (*L2TP Network Server*).

2.4. Ventajas e inconvenientes que presenta el uso de túneles

De las ventajas que puede ofrecer el uso de túneles en la interconexión de redes, destacan las siguientes:

- Sobre un enlace que emplea un protocolo simple (por ejemplo IP) se pueden enviar paquetes de diferentes protocolos de red (IPX, Apple-Talk, el mismo IP, etc.).
- Sobre una red que no admite un protocolo se pueden enviar paquetes de ese protocolo como pasajero.
- Posibilidad de una completa gestión de los usuarios, con un sistema como RADIUS.
- Mediante VPN es posible que usuarios remotos accedan a la infraestructura de una red privada de una empresa, como si estuviesen trabajando presencialmente en ella. Los usuarios pueden acceder incluso desde dispositivos móviles.
- Al contenido del protocolo portador se puede aplicar técnicas de seguridad: autorización, autentificación y cifrado. De ésta manera se puede enviar el paquete pasajero dentro de un túnel seguro por una red portadora insegura.

A pesar de las ventajas y aplicaciones que aporta esta técnica, también presenta uno inconvenientes a tener en cuenta:

- El proceso de encapsulación y su inverso puede suponer un coste de proceso importante en los *routers*, sobretodo si el contenido el túnel está autenticado y cifrado. Aunque en la actualidad muchos *routers* pueden realizar el proceso rápidamente, para el caso de VPN con muchos usuarios hay que utilizar modelos comerciales de *servidores de túneles* como los llamados VPN *Concentrators*.
- Para sacar todo el partido de una VPN se debe disponer de un enlace a redes públicas con suficiente ancho de banda (tanto descendente como ascendente), lo que implica un coste adicional.
- Se puede exponer en el ámbito de una WAN pública la información de un entorno local si no se usan protocolos de seguridad como IPSec. Pero usar protocolos de encriptación, puede disminuir el rendimiento de la conexión por la carga adicional en las tramas.
- El NAT de muchos routers sencillos no soportan la traducción de paquetes con encapsulación de nivel 2 (VPN). Si además se usa IPSec, se requiere un router con soporte especial.
- Si no evita específicamente, el contenido del protocolo pasajero puede viajar sin problemas a través de todo el túnel, sin obedecer a las medidas de seguridad o de control de calidad de servicio (QoS) establecidas para el protocolo portador.
- El retardo real que sufren los paquetes pasajeros entre los extremos del túnel puede causar problemas con protocolos pasajeros diseñados para entornos locales, que consideran *timeouts* pequeños.
- La cuenta de saltos para protocolos pasajeros como IP queda engañada, al mostrar un menor número de saltos del que realmente hay. Además, si no se tiene

precaución, esto puede hacer que surjan bucles en el enrutamiento, ya que los protocolos de enrutamiento también son engañados.

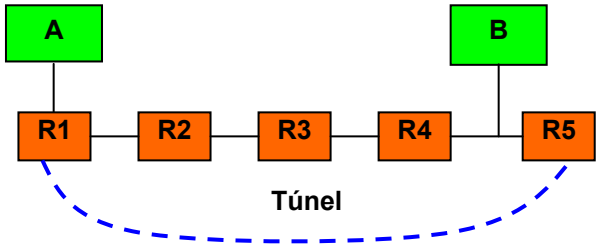

Figura 13. Ejemplo de un bucle producido por un túnel.

Para ilustrar el último inconveniente, considérese el siguiente ejemplo. Sobre una red como la **Figura 13**, donde se usa IP para los protocolos pasajero y portador, el equipo **B** quiere enviar un paquete al equipo **A**. El *gateway* por defecto del equipo **B** es **R5**, y por ello el equipo **B** pasa su paquete a **R5**. Este router tiene configurado en su tabla de rutas que para enviar paquetes a **R1** debe hacerlo a través del túnel **R1-R5** que atraviesa los routers **R4** a **R2**. Así, el paquete original es encapsulado y pasa de **R5** a **R4**. Pero en la tabla de rutas de **R4**, a causa del túnel, se ha incluido una entrada dinámica que dice que el camino más corto para ir a **R1** es a través de **R5** (pasando por el túnel). Esto puede ocurrir, ya que para los protocolos de enrutamiento como RIP, el túnel resulta transparente y aparenta un camino más corto. Así, el paquete encapsulado es enviado a **R5** para ser nuevamente encapsulado y enviado por el túnel. Aquí surge un proceso recursivo que puede agotar los recursos de la red.

3. Herramientas para la práctica

3.1. Configuración de los routers y equipos del laboratorio

La estructura y equipos de la red del laboratorio son los mismos que en la práctica 1, pero incluyendo cierta configuración para establecimiento de túneles.

En el laboratorio se ha configurado un túnel de nivel 3 que comunica el router Cisco 1720 con el Cisco 1601. En este caso, tanto el protocolo pasajero como el portador son IP. Como el camino del túnel pasa por la red Ethernet 172.20.43.192/26, se pueden capturar los paquetes encapsulados con el monitor de red, aunque debe utilizarse de forma remota "tcpdump" en el Linux 2 o en el Linux 3.

Para experimentar como funcionan los túneles de nivel 2 con PPTP, el router Cisco 1720 está configurado como NAS o servidor de túneles que atiende peticiones desde los equipos PC del laboratorio que actúan como clientes. El Linux 2 mantiene el servidor RADIUS al que accede el NAS.

Finalmente, se establecerán túneles L2TP entre los PC con Windows XP del laboratorio, ya que este sistema operativo incorpora tanto servidor como cliente para VPN.

3.2. Configuración de VPN en Windows XP

Para poder realizar los experimentos de VPN propuestos en los apartados 5.2 y 5.7, es necesario tener configurado correctamente el PC con Windows XP. Para los experimentos sobre VPN con PPTP (apartado 5.2), hay que configurar una conexión cliente de VPN en el equipo que se conectará con el router Cisco 1720. Para los experimentos sobre VPN con L2TP

(apartado 5.2), cada pareja de alumnos deberá configurar uno de sus PCs como servidor y el otro como cliente, para establecer un túnel entre ambos equipos.

3.2.1. Cliente PPTP

MS. Windows XP incluye por defecto los controladores necesarios para crear conexiones VPN, actuando como servidor o como cliente. La gestión de los accesos VPN se realiza a través de la ventana con las opciones de "Conexión de Red e Internet" en la vista estilo XP del "Panel de Control". También se puede acceder a las propiedades de "Conexión de Red e Internet" con el menú de contexto que aparece al pulsar con el botón derecho del ratón sobre el icono del "Mis sitios de red" que hay en el escritorio.

Para configurar el cliente PPTP de MS. Windows XP en PC del laboratorio para realizar las cuestiones de la práctica, se deben seguir los siguientes pasos:

1. **Comprobar si existe el acceso VPN**. Hay que verificar en la lista de "Conexiones de red" dentro de "Conexión de Red e Internet" que hay una conexión llamada "**VPN STDII**" en el apartado "Red Privada Virtual". Si no existe, habrá que crearla según se explica en los puntos 2 y 3 siguientes. Si la conexión existe, pero se quiere aprender a configurarla desde el principio, lo mejor es eliminarla y crearla según se explica en los puntos 2 y 3. Finalmente, se puede usar una conexión existente, verificando antes que su configuración es correcta, según el punto 3.

2. **Crear el acceso VPN**. Se debe ejecutar el asistente "Asistente Para Conexión Nueva", al que se puede acceder desde "Menú de inicio > Programas > Accesorios > Comunicaciones", o desde la lista de "Conexiones de red" dentro de "Conexión de Red e Internet". También se puede usar el asistente "Crear una conexión a la red del trabajo" que hay dentro de "Conexión de Red e Internet".

   Tras iniciar el asistente, seleccionar "Conectarse a la red de mi trabajo", y después "Conexión de red privada virtual". Se debe especificar un nombre para la conexión: "**VPN STDII**". Después seleccionar "No usar conexión inicial", ya que en este caso el equipo accede a Internet directamente por una tarjeta de red que siempre está activa. Esta opción es interesante si se requiere establecer una conexión previa, como puede ser con un módem telefónico o GPRS. A continuación hay que especificar el nombre o dirección del equipo al que hay que conectarse, esto es, la dirección IP del NAS: **172.20.43.230** (router Cisco 1720). Luego hay que escoger "No usar mi tarjeta inteligente", ya que no se va a utilizar un certificado para autentificar al usuario. Finalmente se puede agregar al escritorio un acceso directo para iniciar la conexión.

   Al acabar de crear el acceso puede aparecer una ventana en donde se pide la autentificación para comenzar una conexión VPN. Pero antes de realizar la autentificación es conveniente revisar las propiedades del acceso creado.

3. **Editar propiedades del acceso**. Se puede acceder a las propiedades con el botón "Propiedades" que aparece en la ventada de autentificación tras iniciar la conexión, o pulsando con el botón derecho del ratón sobre el icono de una conexión creada anteriormente y listada en la ventana "Conexiones de red" dentro de "Conexión de Red e Internet". Conviene comprobar la dirección del NAS, y las siguientes opciones:

   – Opciones: "Pedir nombre y contraseña" activado, "Incluir dominio de inicio de sesión de Windows" desactivado.

   – Seguridad: Avanzada. En la configuración de la seguridad avanzada hay que escoger "Cifrado opcional" y permitir sólo el protocolo "Chap".

- Funciones de red: el "Tipo de red privada virtual" debe ser "Red Privada Virtual (VPN) con **PPTP**", y en la configuración hay que desactivar "Habilitar compresión por software" y dejar activada sólo la opción "Habilitar extensiones LCP". En las propiedades de TCP/IP hay que verificar que se obtiene la dirección IP y el DNS automáticamente. En Opciones avanzadas de la configuración TCP/IP, debe estar activada la opción "Utilizar la puerta de enlace predeterminada en la red remota".
- Opciones avanzadas: desactivar "permitir a usuarios de otras redes conectarse a través de la conexión a Internet de este equipo".

Después de comprobar que el acceso VPN está instalado y configurado, se puede utilizar pulsando el icono "**VPN STDII**" que hay en la lista de "Conexiones de Red". Tras introducir los datos de autentificación se iniciará el proceso de establecimiento del túnel. Para la autentificación debe utilizarse el usuario "**std<*X*>**", y para la contraseña "**std<*X*>**", siendo **<*X*>** el número con dos dígitos del PC usado (01, 02, 03 a 30). Si la autentificación tiene éxito, aparecerá un icono en bandeja de la barra de tareas. Se puede comprobar cómo queda la configuración del equipo cuando accede a la VPN con el comando "netstat –rn".

Para finalizar el túnel, se debe pulsar con un botón del ratón en el icono de la bandeja.

3.2.2. Servidor VPN (NAS)

1. **Comprobar si existen conexiones entrantes de VPN**. En la lista de "Conexiones de red" dentro de "Conexión de Red e Internet" del "Panel de control" hay que comprobar si está presente algún ícono de "Conexiones entrantes". Si no existe, habrá que seguir el punto siguiente para preparar el servidor. Si el icono está presente, se pueden editar sus propiedades para ver que son las correctas, o se puede eliminar y crear de nuevo.
2. **Crear una conexión entrante de VPN**. Se debe ejecutar el asistente "Asistente Para Conexión Nueva", al que se puede acceder desde "Menú de inicio > Programas > Accesorios > Comunicaciones", o desde la lista de "Conexiones de red" dentro de "Conexión de Red e Internet".

   Tras iniciar el asistente, seleccionar "Configurar conexión avanzada", y después seleccionar "Aceptar conexiones entrantes". En el siguiente paso, no hay que seleccionar ningún dispositivo de conexión, ya que está se realizará directamente por LAN. Después hay que seleccionar "Permitir conexiones virtuales". A continuación se puede seleccionar los usuarios que podrán conectarse a la VPN como clientes. Se creará un usuario nuevo con nombre "**alumnos**" y contraseña "**alumnos**", si no existe ya. Si ese usuario existe, conviene asegurarse de que su contraseña es la correcta editando sus propiedades. Finalmente, en la configuración TCP/IP hay que marcar "Permitir a quienes llaman acceder a la LAN", y especificar unas "Direcciones TCP/IP" concretas. Como hay que especificar un rango de direcciones para los clientes de la VPN que incluya también al servidor, se indicarán las direcciones **10.1.2.<*X*>** y **10.1.2.<*X+1*>**, siendo <*X*> y <*X+1*> los números los dos PCs consecutivos usados como cliente y servidor en el experimento. Por ejemplo, si los PCs utilizados son el 23 como cliente y el 24 como servidor, se indicarán las direcciones IP 10.1.2.23 y 10.1.2.24.

   Tras acabar, debe aparecer el icono "Conexiones entrantes" en la lista de "Conexiones de red". El equipo ya está preparado para aceptar conexiones VPN.

3.2.3. Cliente L2TP

El proceso de configuración de un cliente L2TP es prácticamente igual al de uno PPTP:

1. **Comprobar si existe el acceso VPN**. Hay que verificar en la lista de "Conexiones de red" dentro de "Conexión de Red e Internet" que hay una conexión llamada "**VPN STDII-XP<*X*>"** en el apartado "Red Privada Virtual". Si no existe, habrá que crearla según se explica en los puntos 2 y 3 siguientes. Si la conexión existe, pero se quiere aprender a configurarla desde el principio, lo mejor es eliminarla y crearla según se explica en los puntos 2 y 3. Finalmente, se puede usar una conexión existente, verificando antes que su configuración es correcta, según el punto 3.
2. **Crear el acceso VPN**. Se debe ejecutar el asistente "Asistente Para Conexión Nueva", al que se puede acceder desde "Menú de inicio > Programas > Accesorios > Comunicaciones", o desde la lista de "Conexiones de red" dentro de "Conexión de Red e Internet". También se pude usar el asistente "Crear una conexión a la red del trabajo" que hay dentro de "Conexión de Red e Internet".

   Tras iniciar el asistente, seleccionar "Conectarse a la red de mi trabajo", y después "Conexión de red privada virtual". Se debe especificar un nombre para la conexión: "**VPN STDII-XP**<X>" siendo <**X**> el número del otro PC configurado como servidor de VPN**.** Después seleccionar "No usar conexión inicial". A continuación hay que especificar la dirección del equipo al que hay que conectarse, esto es, la dirección IP real del otro PC configurado como servidor VPN, que será una dirección de la red 172.20.43.192/26 como por ejemplo **172.20.43.228**. Luego hay que escoger "No usar mi tarjeta inteligente.

   Al acabar de crear el acceso puede aparecer una ventana en donde se pide la autentificación para comenzar una conexión VPN. Pero antes de realizar la autentificación es conveniente revisar las propiedades del acceso creado.
3. **Editar propiedades del acceso**. Se puede acceder a las propiedades con el botón "Propiedades" que aparece en la ventada de autentificación tras iniciar la conexión, o pulsando con el botón derecho del ratón sobre el icono de una conexión creada anteriormente y listada en la ventana "Conexiones de red" dentro de "Conexión de Red e Internet". Conviene comprobar las siguientes opciones:
   - Opciones: "Pedir nombre y contraseña" activado, "Incluir dominio de inicio de sesión de Windows" desactivado.
   - Funciones de red: el "Tipo de red privada virtual" debe ser "Red Privada Virtual (VPN) con **L2TP/IPsec**", y en la configuración hay que desactivar "Habilitar compresión por software" y dejar activada sólo la opción "Habilitar extensiones LCP". En las propiedades de TCP/IP hay que verificar que se obtiene la dirección IP y el DNS automáticamente. En Opciones avanzadas de la configuración TCP/IP, debe estar activada la opción "Utilizar la puerta de enlace predeterminada en la red remota".

Después de comprobar que el acceso VPN está instalado y configurado, se puede utilizar pulsando el icono "**VPN STDII-XP<*X*>**" que hay en la lista de "Conexiones de Red". Tras introducir los datos de autentificación se iniciará el proceso de establecimiento del túnel. Para la autentificación debe utilizarse el usuario "**alumnos**", y para la contraseña "**alumnos**". Si la autentificación tiene éxito, aparecerá un icono en bandeja de la barra de tareas. Se puede comprobar cómo queda la configuración del equipo cuando accede a la VPN con el comando "netstat –rn".

Para finalizar el túnel, se debe pulsar con un botón del ratón en el icono de la bandeja, y escoger "Desconectar".

3.3. Notas sobre la utilización de los monitores de red Wireshark y tcpdump

Para resolver las actividades propuestas se puede emplear las distintas herramientas utilizadas en la práctica 1, y especialmente los monitores de red "Wireshark" y "tcpdump". Al realizar las cuestiones sobre túneles, habrá que tener en cuenta lo siguiente: cuando en los monitores de red se establecen **filtros por direcciones IP**, estos se aplican al protocolo **IP portador** en el caso de paquetes encapsulados que incluyan varias cabeceras IP, aunque luego en la ventana de exploración de paquetes se muestren también las direcciones de red del protocolo portador.

También hay que tener en cuenta que, debido a que los PCs del laboratorio se interconectan con un *switch*, para poder obtener los resultados es algunas actividades de las propuestas será necesario utilizar el monitor de red de línea de comando "**tcpdump**" en los equipos **Linux 2** o **Linux 3** como se hacía en la práctica 1.

Por defecto el monitor de red "tcpdump" solo captura los primeros 68 o 96 bytes de las tramas. La mayoría de las veces es suficiente con ese tamaño, ya que incluye la cabecera de los protocolos típicos. Si es necesario capturar mayor tamaño de las tramas para ver mejor su contenido hay que usar la opción "**-s** <longitud>" de "tcpdump". Por ejemplo:

```
sudo /usr/sbin/tcpdump –i eth0 –w miarchivo.cap –s 200
```

Otro aspecto a tener en cuenta es la interfaz de red en la que capturar los paquetes en el PC de trabajo cuando este equipo está conectado a una VPN. Para ver todo el tráfico implicado en la VPN, lo mejor es usar capturar por la interfaz de red Ethernet. Pero también se puede capturar las tramas de la interfaz PPP asociada a la conexión VPN, lo que debería mostrar sólo los datos intercambiados dentro de esta conexión.

Para poder distinguir el tráfico de una conexión de VPN frente al resto, es muy conveniente utilizar algún filtro. Por ejemplo, se puede emplear un filtro de visualización como el siguiente para Wireshark, que muestra, además de los paquetes del equipo de usuario indicado, los otros paquetes relativos la conexión. La dirección 10.1.1.27 es la asignada por el NAS, mientras que 172.20.43.224 es la dirección real del equipo de usuario.

```
(ip.addr==172.20.43.224 || ip.addr==10.1.1.27 || eigrp || radius || rip) &&
not (nbns || browser || syslog || loop || igmp || http || ssh))
```

Finalmente, conviene además verificar que el monitor Wireshark no reensambla fragmentos de paquetes IP al visualizarlos. Para ello hay que comprobar que la opción "Reassemble IP" está desactivada. Esta opción se encuentra dentro del menú "Edit", en "Preferentes", dentro de la lista "Protocols", en "IP".

3.4. Cliente de RADIUS

Los equipos de los alumnos con MS. Windows no tienen por defecto ningún cliente activado para acceder a un servidor RADIUS, por lo que no se puede ver tráfico de ese tipo. Pero se puede utilizar una aplicación cliente de prueba de RADIUS para MS. Windows de las muchas que existen. Una aplicación simple y fácil de instalar (basta con descomprimir y copiar el archivo ejecutable) es NtRadiusPing, de Novell. Esta se puede descargar desde el Campus Virtual de la asignatura (apartado de Materiales, carpeta de "Prácticas") o desde su dirección original:

http://www.novell.com/coolsolutions/tools/14377.html.

Para usar esta herramienta en el laboratorio se utilizará como servidor RADIUS el Linux 3, para no interferir con la configuración de VPN en el Linux 2. El cliente necesita saber la dirección IP del servidor RADIUS la del Linux 3 (**172.20.43.233**), y la clave privada de acceso a RADIUS ("**alumnos**"). Para las pruebas se puede considerar la autentificación del usuario "**std <x>**" y la contraseña "**std <x>**" (<x> es el número del PC utilizado), marcando además "**CHAP**". Después se pueden realizar peticiones como "*Authentification request*" mientras se analiza el tráfico generado con WireShark.

4. Referencias

- Documentación sobre tecnologías disponible en el Web de Cisco Systems:
  http://www.cisco.com
- The FreeRADIUS Server Project:
  http://www.freeradius.org/
- Manual de GNU RADIUS:
  http://www.gnu.org/software/radius/manual/html_mono/radius.html
- NTRadPing 1.5 RADIUS Test Utility:
  http://www.novell.com/coolsolutions/tools/14377.html
- RFC 1661. The Point-to-Point Protocol (PPP).
- RFC 1701. Generic Routing Encapsulation (GRE).
- RFC 1702. Generic Routing Encapsulation over IPv4 Networks.
- RFC 2058. Remote Authentication Dial In User Service (RADIUS).
- RFC 2059. RADIUS Accounting.
- RFC 2401. Internet Protocol Security (IPSec).
- RFC 2406. IPsec ESP: IP Encapsulating Security Payload.
- RFC 2637. Point-to-Point Tunneling Protocol (PPTP).
- RFC 2661. Layer Two Tunneling Protocol, version 2 (L2TP).
- RFC 2809. Implementation of L2TP Compulsory Tunneling via RADIUS.

En el Campus Virtual de "Sistemas de Transporte de Datos" están disponibles varios de los documentos anteriores.

5. Experimentos a realizar

No olvides ejecutar el script "**C:\pracredes.bat**" del PC del laboratorio antes de realizar los experimentos.

5.1. Experimentos sobre túneles de nivel 3

Para esta primera parte **NO** hay que utilizar las VPN.

1. Examina la tabla de encaminamiento del router Cisco 1720 (con "stdprac 1720 rutas" en el equipo Linux 2), y localiza la entrada que está asociada al túnel (interfaz "Tunnel0"), y la dirección IP destino a la que se aplica.
2. Averigua cual es la dirección IP destino del túnel representado por el interfaz "Tunnel0" ("stdprac 1720 intf" en Linux 2).
3. Determina el camino seguido por los paquetes portadores, analizando para ello las tablas de encaminamiento de los equipos de la red. Parte de la tabla del router Cisco 1720. Determina también que router está conectado a la red 10.5.2.0/24.
4. Inicia el monitor de red "tcpdump" en el Linux 2 o el Linux3 con para capturar paquetes de la red 172.20.43.192/26, y envía con tu PC paquetes IP-ICMP con el comando "ping" a la dirección IP 10.5.2.2. Analiza la captura e identifica los paquetes originales y los encapsulados, y en estos últimos, localiza el protocolo portador y el pasajero. Comprueba que el paquete pasajero se corresponde con el original enviado. Por ejemplo, para la captura en Linux 3 se puede usar el siguiente comando:

   ```
   sudo /usr/sbin/tcpdump -i eth0 –w <archivo>
   ```

5. ¿Cuántas cabeceras IP aparecen en los paquetes del túnel? ¿Qué protocolo es el portador y cual el pasajero? ¿Qué direcciones tiene el paquete IP portador? ¿Y el pasajero? ¿Existe protocolo de encapsulación?
6. ¿Qué valor tiene el campo TTL en el paquete original enviado? ¿Qué valor tiene en el paquete encapsulado? ¿Ha cambiado dicho campo? ¿Cuenta un salto el reenvío que hace el router Cisco 1720 del paquete?
7. ¿Qué camino siguen los paquetes IP-ICMP de "respuesta al eco" del comando "ping"? ¿Van también por el túnel? ¿El túnel es unidireccional o bidireccional?
8. ¿Cuántos saltos reales implica el túnel en el camino de ida entre los dos routers?
9. Usa el comando "tracert –d" en una ventana de línea de comandos de tu equipo de prácticas para determinar el camino seguido hasta la IP 10.5.2.2, así como el número de saltos. ¿Cuántos saltos da el paquete enviado por tu PC hasta llegar al destino? ¿Por qué la información obtenida no detalla todos los routers atravesados por los paquetes?
10. Inicia el monitor de red "tcpdump" en el Linux 2 o el Linux3 para capturar paquetes de la red 172.20.43.192/26, y envía paquetes IP-ICMP de tamaño 2000 con el comando "ping –l 2000" a la dirección IP 10.5.2.2. ¿Hay fragmentación en el paquete del túnel? ¿Cuántos fragmentos se generan? Analiza cómo ha dividido los fragmentos el router Cisco 1720. Para asegurar que se capturan los paquetes enteros conviene utilizar la opción "-s" del monitor (ver apartado 3.3):

    ```
    sudo /usr/sbin/tcpdump –s 1600 -i <intf> –w <archivo>
    ```

11. Utiliza el monitor de red "tcpdump" en el equipo Linux 2 ó en el Linux 3 para capturar los paquetes del túnel que circulan por la red 172.20.41.240/28 cuando ejecutas "ping 10.5.2.2". ¿Qué direcciones tienen los protocolos portador y pasajero? ¿Qué direcciones cambian con respecto a los paquetes del túnel en la red 172.20.43.192/26?

5.2. Experimentos sobre VPN con PPTP: establecimiento de la VPN

Antes de realizar las siguientes cuestiones, comprueba que la configuración del acceso VPN es correcta, según se explica en los apartado 3.2.

1. Usa el comando "netstat –rn" en una ventana de línea de comandos de tu equipo para ver cómo está configurada la tabla de encaminamiento de tu equipo.
2. Inicia una captura del monitor de red en tu equipo (ver apartado 3.2.2). Después inicia la conexión "**VPN STDII**" desde el PC que estás utilizando, tal y como se indica en el apartado 3.2. Cuando aparezca el icono en la barra de estado indicando una conexión activa, para la captura. Conviene que guardes la captura en un archivo, pues las siguientes preguntas tratan también sobre ella.
3. Localiza la conexión TCP/PPTP de control del túnel, y los paquetes PPP-LCP que se intercambian para establecer del túnel. ¿Se ven encapsulados estos paquetes?
4. ¿Qué protocolo de autentificación se utiliza (PAP, PPP-CHAP ó MS-CHAP)? ¿Se puede ver la clave de usuario en esos paquetes? ¿Qué protocolo de control se utiliza para configurar tu equipo (PPP-LCP, PPP-NCP, PPP-IPCP…)?
5. Localiza los paquetes PPP-IPCP con los que el NAS configura los parámetros del equipo del usuario, incluida su dirección IP privada. ¿Qué dirección IP asigna el NAS a tu equipo para que acceda a la VPN?
6. Busca en la captura una trama ARP enviada por el NAS (origen 00:07:0E:8C:8C:FF) entre los mensajes PPP-IPCP y analiza su significado. ¿Qué función tiene esa trama?
7. Busca en la tabla de encaminamiento del router Cisco 1720 la entrada cuyo destino es la dirección IP privada que ha asignado el NAS a tu equipo. ¿Qué interfaz tiene asociada? ¿Tiene una puerta de enlace o está conectada directamente? ¿Qué significa esa entrada?

5.3. Experimentos sobre VPN con PPTP: encaminamiento dinámico

1. En la misma captura de los experimentos anteriores, analiza los mensajes EIGRP *Update* y *Ack* relativos a la red 172.20.43.192/26 que aparecen poco después de los mensajes PPP-IPCP. ¿Entre qué equipos se intercambian? ¿Qué ruta difunden los mensajes *Update*? ¿Para que sirven? Aproximadamente, ¿Cuánto tiempo pasa entre que se autentifica positivamente el equipo de usuario y se envía el primer mensaje EIGP *Update* con la ruta correspondiente?
2. Busca en las tablas de encaminamiento del routers Cisco 1601 y Cisco 2513 la entrada cuyo destino es la dirección IP privada que ha asignado el NAS a tu equipo. ¿Qué puerta de enlace tiene? ¿Es estática o dinámica? Si es dinámica, ¿Qué protocolo ha añadido esa entrada, RIP ó EIGRP? ¿Saben estos routers alcanzar tu PC del laboratorio para su dirección de la VPN?
3. Busca mensajes RIP posteriores a los mensajes RADIUS en la captura. ¿Puedes localizar algún mensaje RIP con una entrada de ruta que informe sobre la dirección IP privada que ha asignado el NAS a tu equipo? Si puedes localizar el mensaje RIP, determina aproximadamente cuánto tiempo pasa desde que se autentifica el equipo de usuario hasta el mensaje RIP. ¿Qué protocolo actúa antes, EIGRP o RIP?

5.4. Experimentos sobre VPN con PPTP: RADIUS

1. Inicia el monitor de red "tcpdump" en el Linux 2 o el Linux3 para capturar paquetes de la red 172.20.43.192/26, y realiza una nueva conexión VPN desde el PC que estás utilizando. Localiza las tramas con los mensajes RADIUS relativas a tu conexión. Identifica el mensaje *Access-request* que el NAS (172.20.43.230) hace al servidor RADIUS (Linux 2), y el mensaje *Access-accept* en sentido contrario. ¿Con qué información de configuración responde el servidor RADIUS al NAS? ¿En qué paso de la secuencia de paquetes relativos al establecimiento del túnel se encuentran los mensajes de RADIUS?
2. ¿Hay otros tipos de mensajes de RADIUS relacionados con tu conexión VPN? Si los hay, indica como se denominan.
3. Utiliza la aplicación "NtRadiusPing" para generar peticiones "*Authentification request*" al Linux3 (ver 3.4), y captura los mensajes enviados y recibidos por tu equipo con Wireshark. Analiza la estructura de los mensajes de RADIUS.

5.5. Experimentos sobre VPN con PPTP: intercambio de datos

1. Continuando con la conexión VPN anterior, o después de establecer una nueva, comprueba con el comando "netstat –rn" en una ventana de línea de comandos de tu equipo la tabla de encaminamiento de tu equipo. ¿Hay entradas nuevas con respecto al resultado de la primera cuestión del apartado 5.2? ¿Qué función tienen esas entradas nuevas?
2. Inicia una nueva captura con el monitor de red, y después ejecuta el comando "ping 10.3.2.0" (u otro destino fuera de la red 172.20.43.192/26) en una ventana MS-DOS de tu PC. Para la captura y localiza los paquetes enviados con "ping". ¿Qué estructura de protocolos tienen las tramas que genera tu equipo? ¿Se puede observar encapsulación? ¿Qué tipo de túnel de nivel 2 se está empleando? ¿Qué protocolo de encapsulación se utiliza?

5.6. Experimentos sobre VPN con PPTP: desconexión de la VPN

1. Continuando con la conexión VPN anterior (o después de establecer una nueva), inicia una nueva captura y cierra la conexión VPN de tu PC. ¿Qué protocolos están implicados en el mecanismo de desconexión?
2. Localiza los mensajes EIGRP *Query* y *Ack* relativos a la red 172.20.43.192/26 que aparecen en el momento de la desconexión. ¿Entre qué equipos se intercambian? ¿Qué información de ruta difunden los mensajes EIGRP *Query*? ¿Para qué sirven?
3. Busca en las tablas de encaminamiento del routers Cisco 1720, 1601 y 1720 la entrada cuyo destino es la dirección IP privada que ha asignado el NAS a tu equipo. ¿Qué ha pasado con esa entrada?
4. ¿Envían los routers algún paquete RIP en el momento de la desconexión para informar de que el PC de usuario ya no está presente en la red privada 10.1.0.0?

5.7. Experimentos sobre VPN con L2TP

Para realizar las siguientes cuestiones, prepara solo o con ayuda de tu compañero dos PCs del laboratorio con números consecutivos para funcionar como cliente y servidor de VPN, según se explica en los apartados 3.2.2 y 3.2.3.

1. En el PC cliente, inicia una captura con Wireshark, y conecta con PC servidor mediante la configuración "**VPN STDII-XP<X>**". Con una ventana de línea de comandos en el cliente, ejecutar "ping 10.1.2.<X>", donde <X> es el número del PC servidor. Finalmente, finalizar la conexión VPN, y parar la captura.
2. Con la captura realizada en el punto anterior, analizar el proceso de conexión de L2TP, y compararlo con el de PPTP. ¿Son diferentes o parecidos?
3. Analizar estructura de protocolos de los mensajes ICMP intercambiados. Buscar el protocolo portador, el de encapsulación, y el pasajero de los mensajes. ¿Cuántas cabeceras de protocolos son necesarias para enviar los datos de ICMP (contando la de ICMP)? ¿Qué relación hay entre el tamaño total de la trama y los datos de ICMP? ¿Qué porcentaje del tamaño de la trama son las cabeceras? ¿Qué pasaría si en vez de ICMP fuese un paquete de aplicación de HTTP con 32 bytes de datos?
4. Determina si la conexión utiliza IPSec o no.