_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DISEÑO DE REDES PRIVADAS VIRTUALES CON ROUTERS CISCO

Andrés Roig, Alejandro.

Tutor: Romero Martínez, José Oscar

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2016-17

Valencia, 08 de Marzo de 2017

Resumen

En este Trabajo de Fin de Grado se tratará el diseño de redes privadas virtuales con routers Cisco en el que estimaremos varios de los parámetros más importantes en cualquier VPN, ya sea para una red corporativa o para un particular como puede ser el tiempo, la seguridad, la configuración…. En primer lugar, haremos un análisis de los tipos de VPN más comunes como por ejemplo la autenticación, el control de acceso, la encriptación, el formato de las cabeceras… Posteriormente, nos centraremos en la aplicación práctica de los conceptos teóricos nombrados anteriormente mediante unas pruebas en el laboratorio con routers Cisco. Programaremos los routers con diferentes VPN y mediremos los tiempos que tardan en transmitir la información de un sitio a otro con unas velocidades y unos volúmenes de información previamente establecidos.

Nos centraremos en ofrecer una explicación técnica del método de medidas utilizadas, para obtener una visión general de una herramienta tan utilizada y demandada en los últimos años como son las VPN. Son utilizadas tanto a nivel particular como de empresa con sedes en diferentes partes del mundo debido a que en los últimos años ha aumentado considerablemente la necesidad de poder enviar información de forma segura a través de internet.

Resum

En aquest Treball de Fi de Grau es tractarà el disseny de xarxes privades virtuals amb routers Rebombori en què estimarem alguns dels paràmetres més importants en qualsevol VPN, ja siga per a una xarxa corporativa o per a un particular com pot ser el temps, la seguretat, la configuració.... En primer lloc, farem una anàlisi dels tipus de VPN més comuns com per exemple l'autenticació, el control d'accés, l'encriptació, el format de les capçaleres.. posteriorment, ens centrarem en l'aplicació pràctica dels conceptes teòrics anomenats anteriorment per mitjà d'unes proves al laboratori amb routers Rebombori. Programarem els routers amb diferents VPN i mesurarem els temps que tarden a transmetre la informació d'un lloc a un altre amb unes velocitats i uns volums d'informació prèviament establits.

Ens centrarem a oferir una explicació tècnica del mètode de mesures utilitzades, per a obtindre una visió general d'una ferramenta tan utilitzada i demandada en els últims anys com són les VPN. Són utilitzades tant a nivell particular com d'empresa amb seus en diferents parts del món pel fet que els últims anys ha augmentat considerablement la necessitat de poder enviar informació de forma segura a través d'internet.

Abstract

In this work Final Esay I will discuss the design of virtual private networks with Cisco routers in which we will estimate several of the most important parameters in any VPN, either to a corporate network or for a particular, as can be the time, security, settings…. First of all, we will make an analysis of the types of VPNs more common for example the authentication, access control, encryption, the headers of the format… Later, we will focus on the practical application of the theoretical concepts previously appointed by some tests in the laboratory with Cisco routers. We will validate the routers with different VPN and we will measure the time it takes to transmit information from one site to another with speeds and some volumes of information previously established.

We will focus in offering a technical explanation of the method of measures used to obtain an overview of a tool as used and demanded in recent years as is the VPN. They are both used individually and incompanies with offices in different parts of the world due to the fact that in the past few years has considerably increased the need to be able to send information securely over the internet.

Índice

Capítulo 1. Introducción

En este Trabajo Fin de Grado voy a explicar los fundamentos teóricos y prácticos de las redes privadas virtuales en routers CISCO.

En primer lugar, se evaluará las VPN que se pueden crear con los equipos de Cisco. Además se explicarán los fundamentos teóricos de un VPN, como pueden ser los diferentes métodos que existen o como se encapsula y desencapsulan los paquetes. En segundo lugar, se llevarán a la práctica estos fundamentos. Se programarán los métodos más comunes de VPN y se transmitirán diferentes volúmenes de información a diferentes velocidades.

Para finalizar, una vez alcanzados nuestros objetivos, es decir, poder ofrecer los conocimientos teóricos y prácticos haremos una evaluación y comparación de los diversos datos obtenidos para una misma topología, consiguiendo así una referencia para poder explicar las conclusiones del conjunto del proyecto.

Capítulo 2. Objetivos

El objetivo de este trabajo es aportar los conocimientos y herramientas necesarias a cualquier persona o empresa que se proponga utilizar una VPN (Virtual Private Network).

En primer lugar, evaluaremos las VPN que se pueden crear con router Cisco. En segundo lugar, se realizará un estudio teórico de los principios fundamentales de los distintos tipos de VPN y los métodos más actuales como pueden ser PPTP (Point to Point Tunneling rotocol), IPSEC (Internet Protocol security) o L2TP (Layer 2 Tunneling Protocol).

Por otro lado, aprenderemos a montar una red seleccionando los cables adecuados, el software necesario, el funcionamiento entre los distintos dispositivos de las redes, analizaremos las cabeceras más interesantes con el Wireshark….

Razonaremos un método para realizar las medidas de forma objetiva, es decir comprobaremos las prestaciones de los routers Cisco cuando encriptan los datos y la pérdida de prestaciones.

Por último, compararemos los resultados obtenidos a diferentes velocidades y propondremos un razonamiento lógico de los resultados obtenidos.

Capítulo 3. Fundamentos teóricos

3.1 Introducción.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Debido a que los routers pueden enrutar paquetes entre redes, los dispositivos que están en redes distintas se pueden comunicar

Las capas que nos van a importar a nivel de generación de trama enviado por la red serán la capa de transporte, nosotros utilizaremos TCP, la capa IP encargada de facilitar a los routers el encaminamiento a través de la red y para finalizar la capa de enlace de datos cuyo tecnología engloba la capa física.

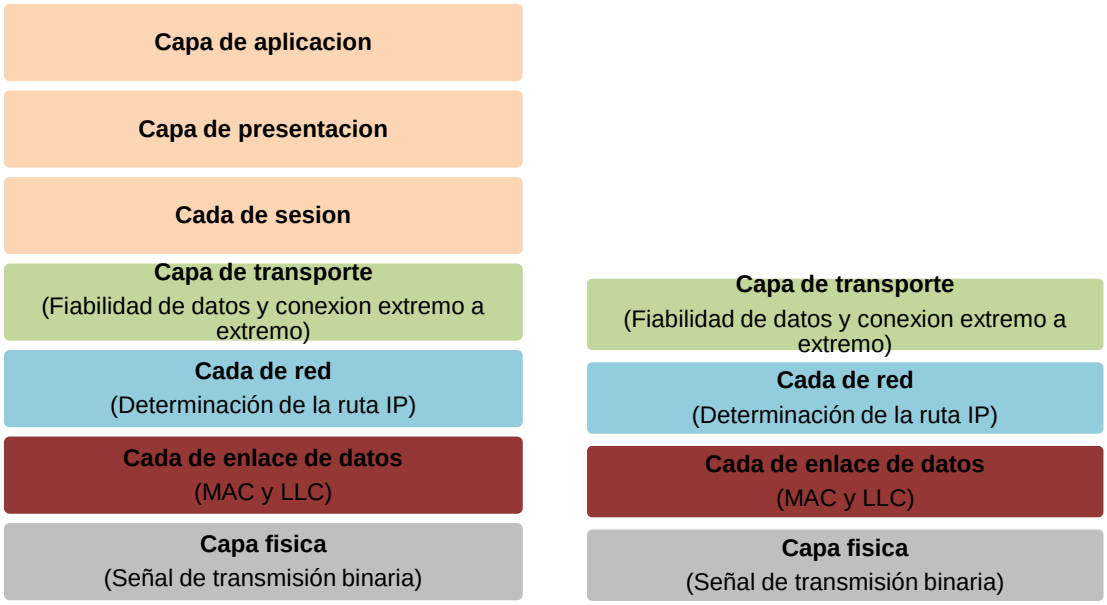


Figura 1. Pila de protocolo y Capas utilizadas.

Explicaremos brevemente como hace un router para reenviar paquetes hacia su destino. Se utiliza la función switching, que es un proceso para aceptar un paquete de una interfaz y reenviarlo por la interfaz correspondiente. Un router utiliza la función de rutas para seleccionar la interfaz de salida, una vez realizado este paso el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

Si el paquete tiene como destino otra red diferente deberá seguir los siguientes pasos:

- Desencapsular el paquete de capa 3 y eliminar el tráiler de la capa dos y el encabezado.
- Determinar la mejor ruta con la tabla de enrutamiento.
- Cuando el router encuentre una ruta hacia el destino, encapsular el paquete de capa 3 en una nueva trama de capa 2 y reenvía la trama por la interfaz de salida.

Como se muestra en la siguiente figura, los dispositivos tienen direcciones IPv4. Por ejemplo, el PC1 se configuró con la dirección IPv4 192.168.1.10 y una dirección MAC de ejemplo 0A-10. A medida que un paquete se desplaza desde el dispositivo de origen hacia el dispositivo de destino final, las direcciones IP de capa 3 no se modifican.

Por otra lado, las direcciones de enlace de datos de capa 2 cambian en cada salto cuando cada router desencapsula y vuelve a encapsular el paquete en una nueva trama hasta llegar su destino.

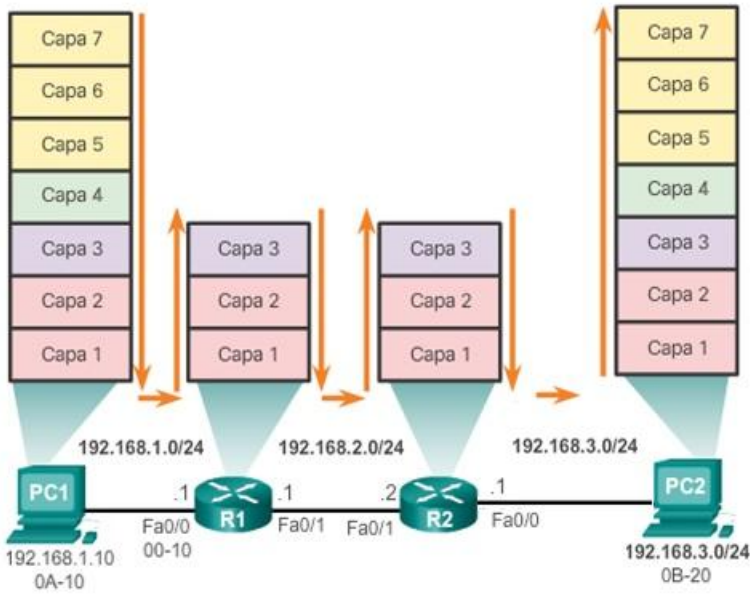


Figura 2.Encapsulamiento y desencapsulamiento de un paquete.

3.2 Redes Privadas Virtuales (VPN).

Una Red Privada Virtual (VPN) es una red de información privada que hace uso de una infraestructura de telecomunicaciones, que conecta diferentes segmentos de red o usuarios a una red principal. Utilizando una protocolo de tunneling para mantener la privacidad.

Los aspectos fundamentales de una VPN son: coste, desarrollo, confianza y seguridad. Siendo esta última la más importante de todas, debido a que la principal característica de una VPN es la confidencialidad de los datos.

Una red privada virtual se basa en un protocolo denominado protocolo de tunneling, es decir, un protocolo que cifra los datos que se transmiten y emula las propiedades de un enlace privado punto a punto.

El Tunneling simboliza el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella. Por lo tanto, ninguna persona que no tenga acceso a ese túnel le serian incompresibles los datos que viajan en él. El paquete original no se puede encaminar por si solo por el túnel al tener un espacio de direcciones diferentes, por este motivo se le añade una cabecera adicional. La cabecera adicional sirve para proporcionar información de encaminamiento dentro de la red de transito.
Para conseguir un enlace privado entre las dos segmentos del túnel se encriptan los datos para proporcionar confidencialidad al inicio del túnel. Cuando el paquete llega al otro extremo del

túnel los desencapsula y finalmente los envía al usuario. A continuación podemos observar un pequeño diagrama de cómo funciona el proceso:

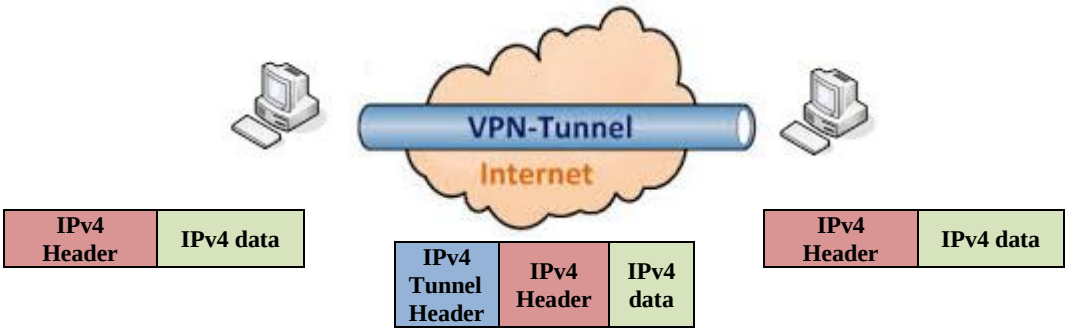


Figura 3.Funcionionamiento Tunneling.

Las tres propiedades que tiene todo túnel son encriptación, encapsulación y autentificación. La encapsulación añade cabeceras a los datos originales para crear el túnel y poder así transmitir la información. Por otra parte, la encriptación añade la confidencialidad de los datos transmitidos, solo el emisor y receptor conocen la clave para cifrar y descifrar datos. De esta manera nadie que intercepte los datos podrá leer el contenido de la información. Por último, la autentificación se divide en autentificación de usuario y de datos. Según la configuración solo hace falta la autentificación del usuario o la autentificación mutua. En cambio la autentificación de los datos se puede utilizar un hash encriptación mediante una contraseña conocida solo por el emisor y receptor

3.3 Tipos de conexiones VPN.

Para una conexión VPN son necesarios tres elementos: el cliente, el servidor y el túnel. Explicaremos las principales características de cada uno de los tres elementos:

En el servidor:

- El servidor acepta conexiones VPN desde un cliente VPN.
- Se debe realizar una configuración para que un cliente pueda realizar conexiones con el servidor.
- El escenario site-to-site acepta conexiones entre routers.

En el cliente:

- Un extremo inicia una conexión VPN hacia un servidor.
- En un escenario site-to-site es un router que quiere iniciar una conexión con otro router

- En un escenario VPDN será un computador individual que quiere conectar a una red privada a través de un servidor de acceso VPN. Necesitará configurar una nueva dirección perteneciente al rango de la red a la que conecta.

Figura 4. Cliente, túnel y servidor.

Existen principalmente dos tipos de conexiones VPN: Conexiones VPN de acceso remoto (VPDN) y conexiones router a router (site-to-site).
Las conexiones VPDN se realizan con la conexión de un usuario individual a una red privada para acceder a los recursos de un servidor VPN. Al usuario se le asigna una dirección de red privada a la que se conecta. Por último, el usuario se debe autentificar y según la configuración el servidor también lo tendrá que hacer (autentificación mutua).
Por otra parte, las conexiones site-to-ste, se realizan de router a router para conectar dos segmentos de la misma red privada. Igual que en las conexiones VPDN, se puede realizar un proceso de autentificación mutua.

3.4 Protocolos.

Para finalizar, los protocolos más enfocados para conexiones de acceso remoto son PPTP y L2TP (capa 2). Mientras que IPSEC se enfoca mayoritariamente para conexiones site-to-site (capa 3), aunque también se podrían hacer conexiones de acceso remoto.

Capítulo 4. GRE

4.1 Introducción.

GRE (GenericRoutingEncapsulation) desarrollado por CISCO, es un protocolo genérico de encapsulación que permite ser utilizado con cualquier protocolo de nivel de red que funcione como protocolo de tránsito, creando un enlace punto a punto virtual a routers Cisco.
El paquete resultante se encapsula con el protocolo de transito tras ser encapsulado y enrutado (Payload) como muestra la siguiente figura:

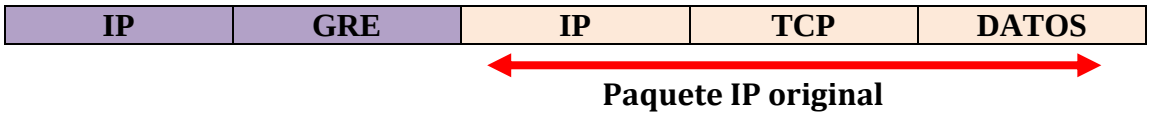


Figura 5. Protocolo GRE.

GRE se diseñó para administrar el tráfico multidifusión y multiprotocolo IP entre dos o más sitios. Permitiendo encapsular dentro de un túnel varios tipos de paquetes de un protocolo como se muestra a continuación:

- Un protocolo de encapsulación como GRE
- Un protocolo encapsulado como IPv6, AppleTalk o IPv4.
- Un protocolo de transporte como IP

4.2 Características de GRE en IPv4.

Las principales características de GRE en IPv4 son las siguientes:

- GRE se define como un estándar IETF (Internet EngineeringTaskForce) (RFC 2784).
- El número 47 es el identificador que sirve para indicar que lo que sigue es un encabezado GRE.
- No incluye ningún mecanismo de autentificación ni de confidencialidad.
- No incluye ningún mecanismo de control de flujo de manera predeterminada.
- Los paquetes que se envían por el túnel tienen una sobrecarga de al menos 24 bytes debido al encabezado GRE junto con el encabezado de tunneling IP.
- Si GRE se encapsula por primera en IP se utiliza el ID Protocol 2048.
- Una de las opciones más comunes y sencillas es utilizar GRE con PPTP.

A continuación, se muestra el formato de la cabecera GRE:

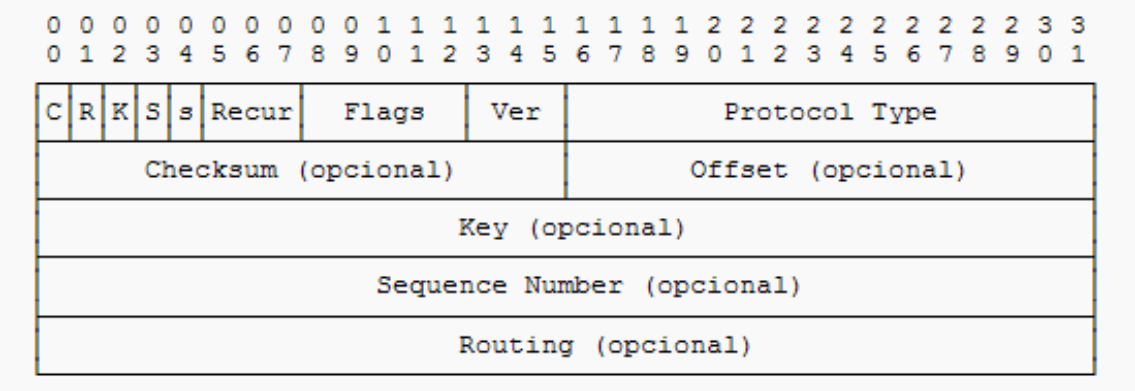


Figura 6. Campos en un paquete GRE.

4.3 Configuración.

La configuración de un túnel GRE es muy sencilla. Para definir el túnel sólo es necesario indicar las direcciones IP de ambos extremos, y realizar la encapsulación como podemos observar en el siguiente ejemplo.
Podríamos seleccionar el interfaz de salida en vez de la dirección IP destino.

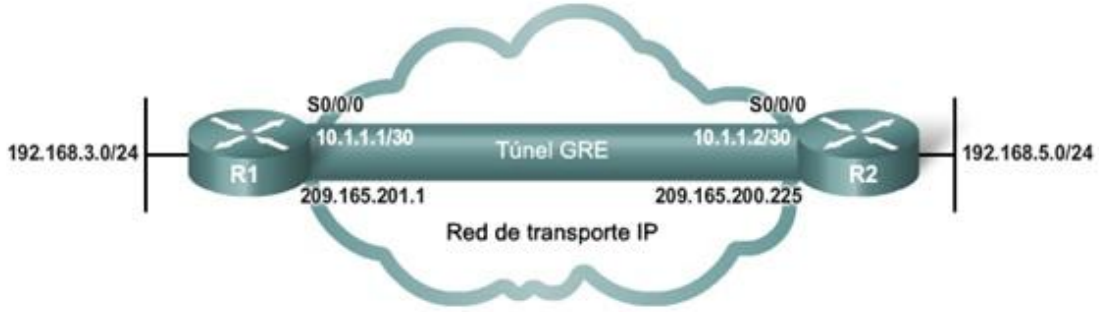


Figura 7. Topología Túnel GRE.

A continuación, podemos observar el código utilizado:

Router 1	**Router 2**
interface tunnel 0	interface tunnel 0
ip address 10.1.1.1 255.255.255.252	ip address 10.1.1.2 255.255.255.252
tunnel source 209.165.201.1	tunnel source 209.165.200.225
tunnel destination 209.165.200.225	tunnel destination 209.165.201.1
keepalive 5 4	keepalive 5 4
interface S0/0/0	interface S0/0/0
ip address 209.165.201.1 255.255.255.0	ip address 209.165.200.225 255.255.255.0
interface fe0/0	interface fe0/0
ip address 192.168.3.1 255.255.255.0	ip address 192.168.5.1 255.255.255.0

Figura 8.Configuracióntunel GRE.

En la siguiente ilustración podemos comprobar los diferentes campos en un túnel GRE.

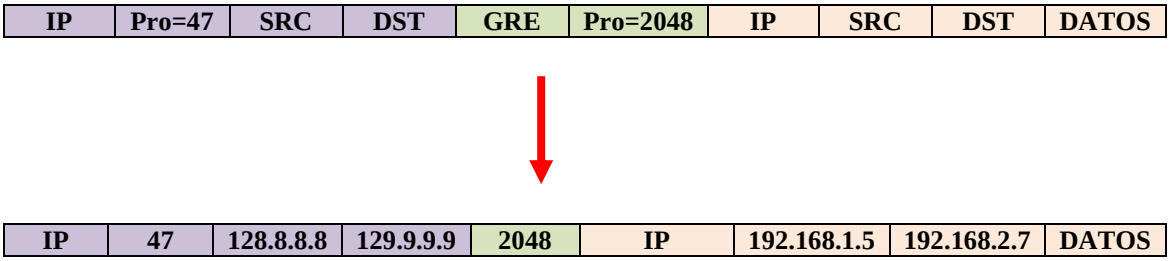


Figura 9. Antes y después de una túnel GRE.

4.4 Funcionamiento de Keepalive.

Los interfaces del túnel GRE (protocolo sin estado) no tienen un mecanismo que permita saber si el otro extremo del túnel está activado o desactivado. El mecanismo Keepalive permite saber si los extremos del túnel están activos o no y así poder tomar rutas alternativas (rutas de backup) sin necesidad de emplear protocolos de enrutado (routing) como RIP (Routing Information Control) u OSPF (Open Shortest Path First).

Capítulo 5. PPTP

5.1 Introducción.

PPTP (Protocolo de arquitectura de túneles punto a punto) desarrollado por Microsoft. Es un protocolo de capa 2 que forma un túnel iniciado por un cliente encapsulando paquetes en datagramas IP que se envían mediante redes basadas en TCP/IP. Normalmente se utiliza en VPDN (VPN de acceso remoto) aunque también cabe la posibilidad de conexiones VPN site-to-site. Se utiliza como alternativa de túneles L2F y L2TP. Se describe en la RFC 2637.

Emplea conexión TCP, llamada control de conexión PPTP para mantener el túnel

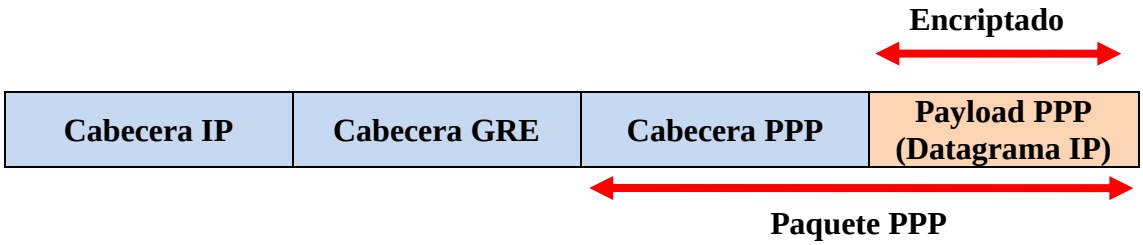


Figura 10.Conexión PPTP.

5.2 Encapsulación.

En el siguiente apartado analizaremos los diferentes campos de un paquete PPP. Posteriormente haremos un análisis de las medidas realizadas con Wireshark.

A continuación, podemos observar los campos junto con su explicación de un paquete PPP:

Indicador	Dirección	Control	Protocolo	Datos	FCS	Indicador

Figura 11.Campos de la trama PPP.

- **Indicador.** Compuesto por la secuencia binaria 01111110. En tramas PPP sucesivas sólo se usa un carácter de señalador único.
- **Dirección.** Un único byte que contiene la secuencia binaria 11111111, la dirección de difusión estándar.
- **Control**. Un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial.
- **Protocolo**. Campo de información de la trama. El campo Protocolo es de 1 byte para la identificación del protocolo en el rango de 0x00-00 a 0x00-FF.
- **Datos.** La longitud máxima predeterminada del campo de información es de 1500 bytes.

En las siguientes figuras mostraremos capturas de Wireshark realizadas con las medidas **del** laboratorio.

En la figura 12 podemos ver todas las cabeceras que se transmiten en una conexión PPTP. Nosotros nos centraremos en el análisis de las 3 últimas: Generic Routing Encapsulation, Point-to-Point y PPP Compresed Datagram.

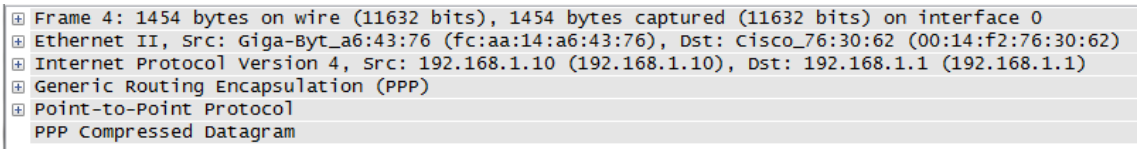


Figura 12. Captura de Wireshark PPTP.

Por otra parte, los campos que se muestran en la siguiente figura son los mismos que en la figura 6, los cuales corresponden al formato de la cabecera GRE.

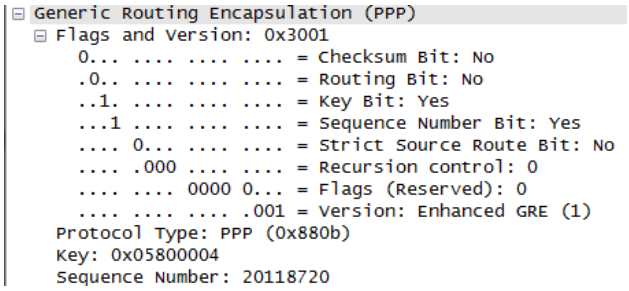


Figura 13. Campos de GRE en PPP.

En la figura 13 y 14 comprobamos que con las capturas de Wireshark obtenemos los mismos campos y valores que hemos explicado en este mismo apartado.
Para finalizar, PPP Compressed Datagram hace referencia a los datos cifrados que no podemos ver.

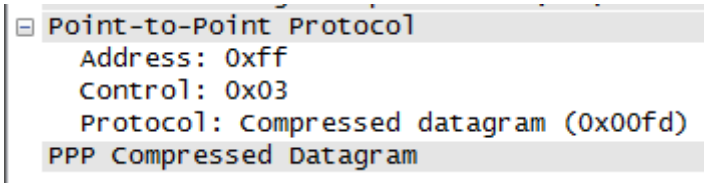


Figura 14.Campos paquete PPP.

5.3 Arquitectura

En una conexión PPTP principalmente se involucran 3 procesos:

- **Conexión PPP entre el ISP y el cliente**. Si el usuario tiene conectividad a través de una LAN este elemento no aparece.
- **Control de la conexión PPTP**. Este tipo de conexión solo transporta comandos de control. Si el cliente tiene una conexión con Internet, crea una conexión de control con un server VPN.
- **Encapsulación de datos.** Los datos transportados a través del túnel utilizando encapsulación de paquetes PPP en paquetes GRE.

La encapsulación de datos-Control de la conexión tiene las siguientes características:

- Se utiliza la versión 1 de GRE en PPTP.
- Para indicar que se transporta encapsulado GRE se utiliza el valor 47 en ID protocol.
- El tipo de protocolo en la cabecera GRE es 0x880B para indicar que encapsula PPP.

5.4 Seguridad en PPTP

La seguridad en PPTP compone principalmente de 2 partes:

• Autentificación y control de acceso.

• Encriptación de datos.

5.4.1 Autentificación y control de acceso.

Existen diversos protocolos de autenticación como pueden ser: PAP, CHAP, EAP o MS-CHAP. Nosotros nos centramos en las características de este último (MS-CHAP):

Es un protocolo de autenticación es de Desafío / Respuesta.

El protocolo de cifrado es Punto a Punto Encryption (MPPE).

Desarrollaron una nueva versión denominada MS-CHAP versión 2 (MS-CHAPv2), debido a que la primera versión era muy vulnerable. Aunque la mayoría de redes de PPTP usan MS-CHAPv1.

A continuación, observamos una tabla comparativa entre las dos versiones de MS-CHAP.

MS-CHAP versión 1	MS-CHAP versión 2
CHAP con un valor algoritmo de 0x80.	CHAP con un valor algoritmo de 0x81.
El servidor genera un valor de autenticación de 8 bytes.	El servidor genera un valor de autenticación de 16 bytes.
La respuesta del servidor es Éxito o Fracaso.	La respuesta del servidor es Éxito o Fracaso, además lleva una cuenta.
El cliente decide terminar o continuar según la respuesta.	El cliente decide terminar o continuar según la respuesta. Además, de comprobar la validez de la respuesta del autenticador.

Tabla 1. Comparación entre MS-CHAP v1 y v2.

5.4.2 Encriptación de datos.

En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC-4 a partir del password del usuario. La longitud de dicha clave puede ser 128 bits o 40 bits.

La encriptación de cada paquete es independiente de los demás. Los paquetes pueden llegar fuera de orden. Si el servidor requiere una clave de longitud mayor que la proporcionada por el cliente, se rechaza la conexión.

5.5 Vulnerabilidades de PPTP

La seguridad de PPTP ha sido rota completamente, Microsoft recomienda que todas las redes que utilicen PPTP deberían ser reemplazadas por protocolos más seguros. Se ha descubierto que MS-CHAP para la autenticación, PPTPv1 y PPTPv2 son vulnerables para ataques offline. Además, que diferentes programas te permiten descifrar el tráfico de la VPN.

Capítulo 6. L2TP

6.1 Introducción.

L2TP (RFC 2661) es un protocolo de redes privadas virtuales que se utiliza generalmente en VPDN (VPN de acceso remoto). Es una combinación de L2F (Layer 2 Forwarding) y PPTP para corregir la deficiencia de los estos dos protocolos y establecerse como un estándar. Las principales características son:

- Protocolo de nivel 2 que encapsula tramas PPP.
- Se encapsula sobre UDP.
- Se utiliza generalmente en VPDN pero es posible configurar conexión Site-to-Site.
- Los mensajes de control y de datos tienen la misma estructura.
- Al tener una estructura como la de PPP los métodos de autenticación son los mismos(PAP, CHAP, MS-CHAP o EAP)
- Los datos en un paquete PPP encapsulados en L2TP se pueden comprimir o encriptar.
- Se suele utilizar en combinación con IPSEC.

Aunque algún campo opcional no aparece el espacio no existirá. Por otro lado los campos de control están obligados a que aparezcan. A continuación podemos observar cual sería la cabecera de un paquete L2TP.

T	L	X	X	S	X	O	P	X	X	X	X	Ver	Lenght(Opt)
Tunel ID													Session ID
Ns (Opt)													Nr(Opt)
Offset Size(opt)													Offset pad…(Opt)

Figura 15.Cabeceras L2TP.

Las fases conexión L2TP están compuestas por 3 partes:

1. **Negociación IPSec SA (Security Associations)**. Se intercambian mediante IKE (Internet key Exchange). Se utilizan claves públicas, contraseña compartida o X.509 (certificados) para determinar la autenticación de los usuarios y seguridad de los datos.
2. **Conexión L2TP**. Se intercambian mensajes L2TP mediante mensajes de control para establecer una conexión.
3. **Conexión PPP**. La negociación de los parámetros se realiza a través de un canal seguro. Cuando se establece el túnel L2TP se realiza el encapsulado de las tramas PPP y se envían por el túnel.

6.2 Mensajes de control.

En el momento de la configuración de la conexión L2TP, se intercambian paquetes de control entre el servidor y cliente para establecer el túnel y la sesión para cada dirección. A continuación podemos ver una lista de mensajes de control L2TP que se intercambia entre el cliente y servidor es la siguiente junto con un diagrama de intercambio de mensajes:

- Control de la gestión de conexiones
  - (reserved)
  - 1 (SCCRQ) Start-Control-Connection-Request
  - 2 (SCCRP) Start-Control-Connection-Reply
  - 3 (SCCCN) Start-Control-Connection-Connected
  - 4 (StopCCN) Stop-Control-Connection-Notification
  - 5 (reserved)
  - 6 (HELLO) Hello

- Call Management
  - 7 (OCRQ) Outgoing-Call-Request
  - 8 (OCRP) Outgoing-Call-Reply
  - 9 (OCCN) Outgoing-Call-Connected
  - 10 (ICRQ) Incoming-Call-Request
  - 11 (ICRP) Incoming-Call-Reply
  - 12 (ICCN) Incoming-Call-Connected
  - 13 (reserved)
  - 14 (CDN) Call-Disconnect-Notify

- Errores:
  - 15 (WEN) WAN-Error-Notify

- Control de sesión PPP
  - 16 (SLI) Set-Link-Info

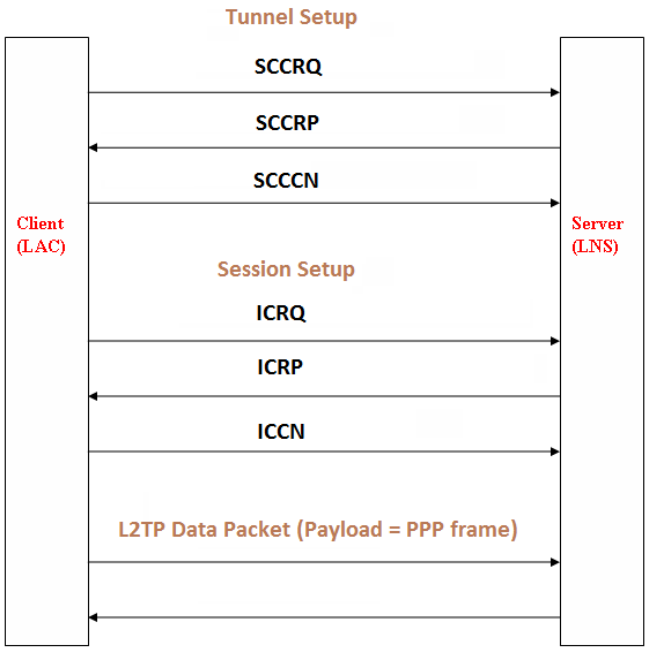


Figura 16. Intercambio de mensajes de control en L2TP.

Las principales características del intercambio de mensajes de control en L2TP son las siguientes:

- El cliente y el servidor L2TP utilizan el mismo puerto, UCDP 1701.
- No se utiliza una conexión separada en el mantenimiento o en el control como sucede en PPTP.
- No se utiliza ningún mecanismo para retransmitir si se pierde algún mensaje de datos.

- Para reordenar o detectar perdidas se utilizan números de secuencia. También son utilizados para el control de congestión.
- L2TP soporta múltiples sesiones sobre el mismo túnel.

6.3 Seguridad en L2TP.

La seguridad en L2TP compone principalmente de 2 partes:

- Autenticación
- Encriptación de datos.

Autenticación

Se utiliza una autenticación a dos niveles: Autenticación del computador y del usuario. Para la autenticación del computador es necesario tener instalado en ambos computadores uno certificado. Por otra parte, para la autenticación del usuario debido que L2TP no proporciona autenticación por sí mismo es necesario utilizar uno de los métodos que utiliza PPP (CHAP, PAP, MS-CHAP o EAP).

Para la integridad de los datos podemos utilizar HMAC (Hash Algorithm Authentication Code), MD5 (Message Digest 5) o HMAC SHA (Secure Hash Algorithm).

Encriptación de datos.

L2TP soporta algoritmo de encriptación DES, con clave de 56 bits pero no está recomendada, ya que es muy vulnerable. Un mecanismo muy utilizado es utilizar 3 veces seguidas la encriptación DES, denominada 3DES, que utilizaría tres claves de 56 bits.

Capítulo 7. IPSEC

7.1 Introducción.

IPSEC es un protocolo de capa 3 creado por el IETF, es capaz de enviar datos cifrado. Es una mejora la seguridad del protocolo IP para garantizar la privacidad, control de acceso, integridad, confidencialidad y autentificación del origen de los datos. Descrita en las RFC 2401 a 2412 y revisadas en la 4301 a 4309.

Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación
- Permite construir una red corporativa segura sobre redes públicas, eliminando el coste de las líneas dedicadas y el mantenimiento de las mismas.

- Aumento de las prestaciones de seguridad del nivel 4,5,6 y 7 (SSL, TLS, SSH)
- Es transparente para las aplicaciones y protege la información a partir del nivel 3.

Los componentes de IPSEC son:

- Protocolos de seguridad: AH (Authentication Header) RFC 2402 y ESP(Encapsulation Security Payload) RFC 2406
- Asociaciones de seguridades (SA)
- Protocolo de gestión de claves: IKE (Internet Key Enchange) RFC 2409
- Algoritmos de autentificación y cifrado. Es un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3

Figura 17.Complementariedad de varias técnicas.

7.2 Modos de operación.

Modo Túnel. En el modo túnel, el paquete IP entero (cabecera + datos) es cifrado y autenticado. Este paquete será encapsulado en un nuevo paquete IP

Modo Transporte. El modo transporte, asegura la comunicación extremo a extremo pero los extremos deben saber de la existencia del protocolo IPsec para poder entenderse. No protege la cabecera IP.

7.3 Protocolos de seguridad.

AH (Authentication Header)

El protocolo AH (Authentication Header) se sitúa dentro de IPSec para garantizar la integridad y autenticación de los datos. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y verificar que dichos datos no han sido alterados en el trayecto. Sin embargo, no incluye ninguna confidencialidad de los mismos, es decir, los datos transmitidos pueden ser vistos por terceros.
Tal como indica su nombre, AH es una cabecera de autenticación que se sitúa entre la cabecera IP (tanto IPv4 como IPv6) y los datos transportados. Funciona tanto con TCP, UDP o ICMP.

El campo protocolo de la cabecera IP contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente. AH solo proporciona integridad y autenticidad de la cabecera IP y de los datos transportados pero no de la los campos variables: TOS, TTL, flags, offset y checksum.

El funcionamiento de AH se basa en un algoritmo HMAC. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave. Se utilizan como mínimo los protocolos HMAC-MD5-96 y HMAC-SHA-1-96

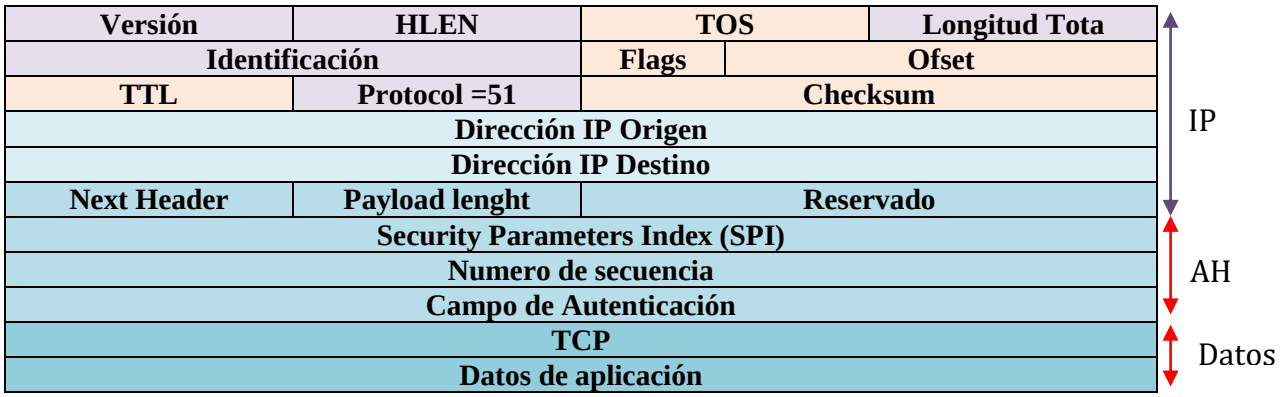


Figura 18. AH

ESP (Encapsulation Security Payload)

El protocolo ESP garantiza confidencialidad. Cifra los datos que se desean enviar y se incluyen en un paquete IP. Por otra parte, ofrece servicios de integridad y autenticación del origen de los datos incorporando un sistema parecido a AH. Al ofrecer más funciones que ESP las cabeceras con más complejas. Al igual que AH se puede utilizar tanto con TCP, UDP, ICMP o incluso un paquete IP completo.
El IANA ha asignado en el campo Protocolo el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

Se utiliza un cifrado de clave simétrica para el cifrado del protocolo ESP. Normalmente, algoritmos de cifrado bloque, de modo que los datos a cifrar tienen que ser un múltiplo del tamaño del bloque (8 o 16 byte). Se pueden utilizar diferentes algoritmos de cifrado: DES, 3DES, RC5…

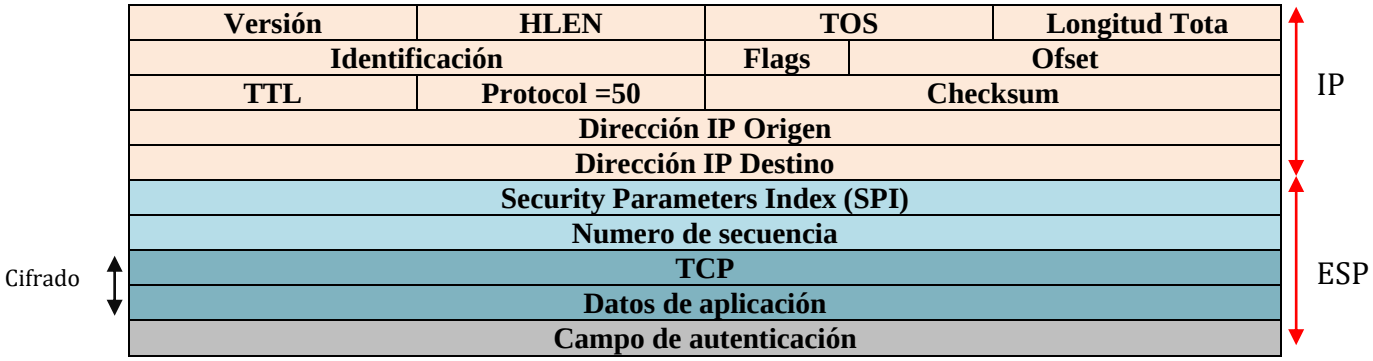


Figura 19. ESP.

A continuación podemos observar un pequeño resumen entre el modo Transporte y modo Túnel, tanto para ESP o AH:

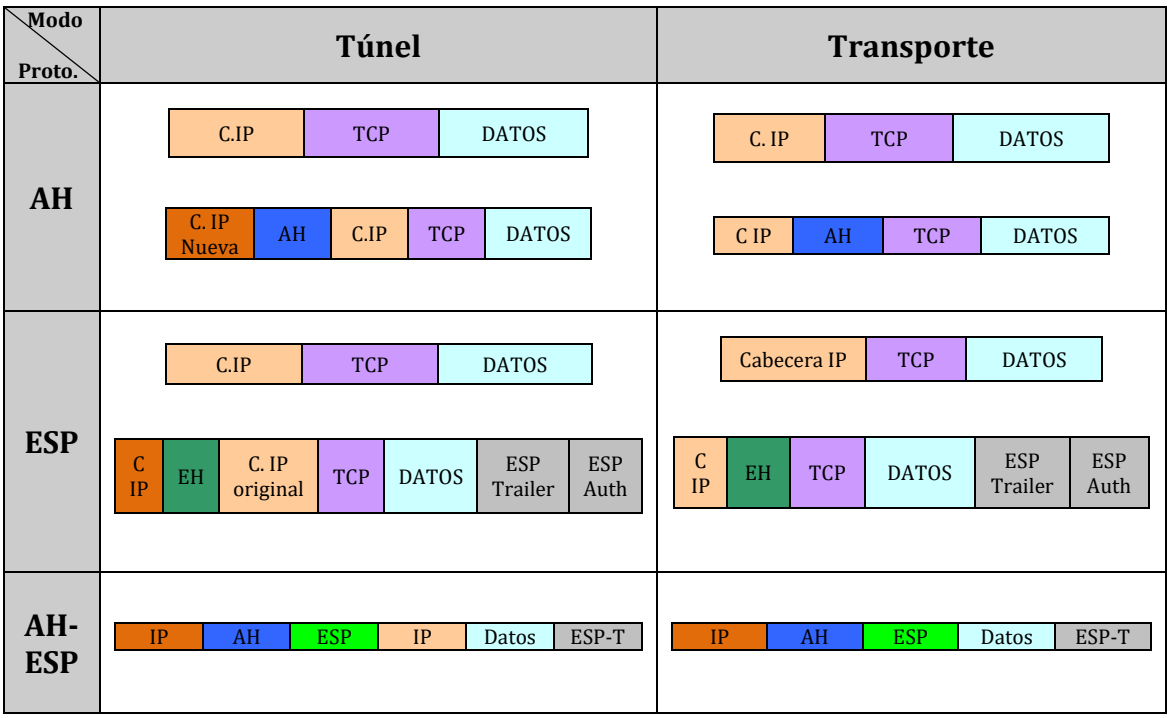


Figura 20.Diferencia entre ESP y AH en modo túnel y transporte.

7.4 Asociación de seguridad (SA).

Una asociación de seguridad (SA) es un tipo de conexión que permite establecer los servicios de seguridad del tráfico. Una única SA protege los datos en una dirección, es decir si queremos proteger los datos en ambas direcciones requieren dos SA.

Los tres elementos siguientes identifican una SA IPsec de modo exclusivo:

- El protocolo de seguridad AH o ESP. Solo pudiendo utilizar uno de ellos y no los dos.
- La dirección IP de destino
- El SPI (Security Parameter Index), es un valor arbitrario de 32 bits.

Las SA se almacenan en una base de datos de asociaciones de seguridad (SADB). Posteriormente, una interfaz administrativa, permite que las aplicaciones privilegiadas gestionen la base de datos. Por ejemplo, la aplicación IKE.

7.5 IKE.

El IETF definió el protocolo IKE (puerto UDP 500) no solo como parte especifica de IPSEC si no que se utiliza en funciones de gestión automática de claves como el establecimiento de las SAs correspondientes u otros protocolos como OSPF o RIPv2. IKE es un protocolo hibrido basado en el marco ISAKMP y Oakley. El primero define la forma genérica del protocolo de comunicación y la sintaxis del mensaje, mientras que Oakley se encarga de la lógica del cómo se realizaran de forma segura el intercambio de claves.
El objetivo principal del IKE es establecer una conexión cifrada y autenticada entre dos entidades a través del cual se intercambiaran información. Se divide en dos fases:

- En la primera frase, la negociación para establecer un canal seguro y autenticado, para proteger la fase 2. El canal seguro se establece mediante el uso de un algoritmo de cifrado y un HMAC. Las claves necesarias proceden de una clave maestra que se obtiene mediante el intercambio de claves Diffie-Hellman. Aunque este procedimiento no garantizaría la identidad de los nodos.

- En la segunda fase el canal IKE es usado para negociar parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSEC. Durante la segunda fase, se negocia si la conexión será ESP o AH y los parámetros que llevan asociado. El emisor propondrá posibles opciones que tenga configuradas de seguridad y con su prioridad. Dependiendo de las características del receptor podrá aceptar la proposición o no. Además, ambos nodos se informarán del tráfico que se van intercambiando.

Para realizar la autenticación se puede realizar con dos técnicas diferentes. La primera opción es una Clave Pre-compartida PSK (Pre-shared key), a partir de la cual se crea un hash de autenticación que intercambian ambos pares. El segundo método es mediante Firmas RSA (requiere certificados). El hash se cifra con la clave privada.

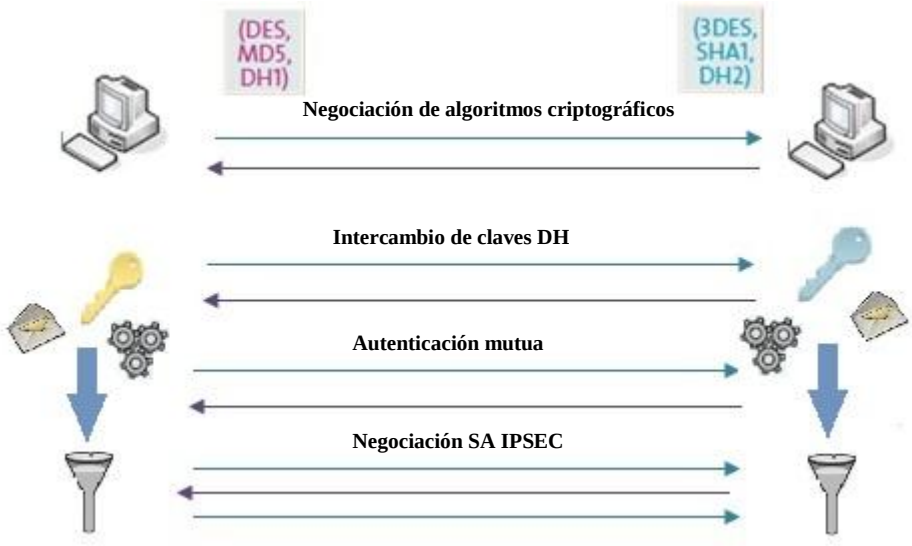


Figura 21. Negociación IKE.

En la figura 22, se muestran los componentes de la configuración de IPSec. Se deben seleccionar cuatro componentes básicos del marco de IPSec. La combinación de estos componentes es la que proporciona las opciones de confidencialidad, integridad y autenticación para las VPN con IPSec.

- Protocolo del marco de IPSec
- Confidencialidad (si se implementa IPSec con ESP)
- Integridad
- Autenticación
- Grupo de algoritmos DH

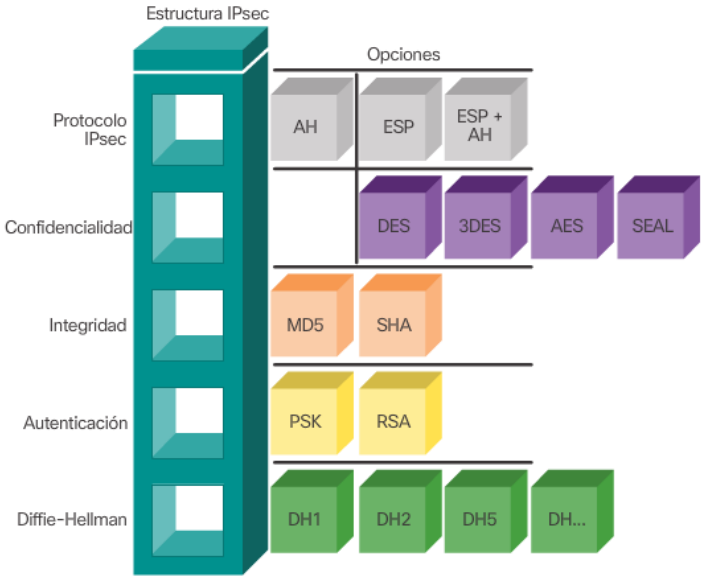


Figura 22.Componentes de la configuración IPSEC.

7.6 Wireshark.

En las figuras 24 y 25 podemos observar capturas realizadas en el laboratorio. Se tratan de las cabeceras que se transmiten en una conexión IPSEC. Nosotros nos centraremos en el análisis de las 2 últimas: Internet Protocol versión 4 y Encapsulating Security Payload.

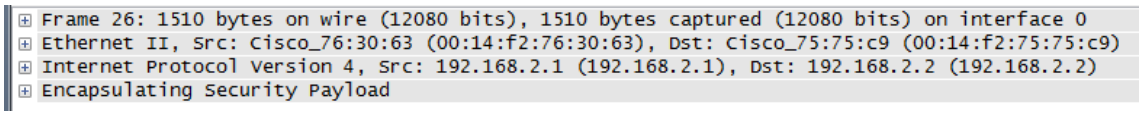


Figura 23. Captura de Wireshark PPTP.

En la siguiente figura podemos comprobar con más detalle cada una de las cabeceras nombradas anteriormente. Si observamos la figura 19, que es la estructura teórica de un paquete ESP y la figura 24 podemos comprobar que los resultados teóricos coinciden con lo que se transmite.

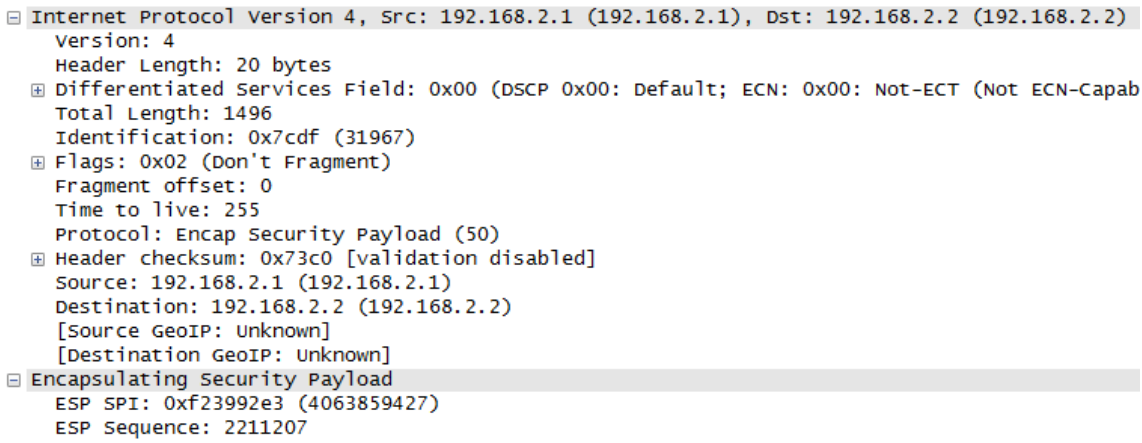


Figura 24. Campos ESP.

Capítulo 8. Base Práctica

8.1 Equipos utilizados.

En el siguiente apartado nombraremos los equipos utilizados para la toma de medidas y sus características técnicas.

8.1.1.1 PCs (Host).

Los PCs empleados son todos iguales para intentar mitigar el error en las medidas lo máximo posible, son los del laboratorio de redes. Las especificaciones son las siguientes:

Sistema operativo	Windows 7 Professional Service Pack 1
Tipo de Sistema	Sistema operativo de 64 bits
Procesador	Intel(R) Core(TM) i3-4160 CPU @ 3.30GHz
Número de procesadores principales	2
Memoria RAM total	6.00 GBytes
Gráficos	Intel® HD Graphics 4400
Memoria de gráficos disponible	2 GBytes
Disco Duro principal	>100 Gbytes disponibles HDD
Adaptador de red	Realtek RTL8168/8111 PCI-E Gigabit Ethernet Adapter

Tabla 25.Especificaciones Pc.

8.1.1.2 Routers.

El modelo de Cisco 1841, es el router más común del laboratorio de redes. Todas las mediciones están hechas con los mismos routers para que tengan la misma versión y reducir al mínimo el error en las mediciones. A continuación podemos observar una fotografía y sus características.

Figura 26.Router CISCO 1841

Características técnicas del modelo 1841:

Forma	Desktop, 1-rack-unit
Dimensiones	(altura x anchura x profundidad) = (4.75 x 34.3 x 27.4 cm)
Peso	2.8 kg
Memoria DRAM	Synchronous dual in-line memory module (DIMM) DRAM 256 MBytes por defecto (384 MBytes máximo)
Memoria *Flash*	64 MBytes por defecto (128 MBytes máximo)
Ranuras modulares	dos (Slot 0: Serial x2 / Slot 1: Fast Ethernet x4)
Puertos *Ethernet*	dos 10/100 Mbps
Puerto USB	uno (1.1)
Puerto de Consola	uno (hasta 115.2kbps)
Puerto Auxiliar	uno (hasta 115.2kbps)
Fuente de Alimentación Interna	Sí
Alimentación	100 - 240V AC @ 50 - 60 Hz
Procesador	RM5261A-256H @ 250 MHz, Controlador Marvell GT96103A
Sistema Operativo	Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), v12.4(25d)

Tabla 2. Especificaciones Router.

8.1.1.3 Switch CISCO Catalyst 2950 series.

El Switch Cisco Catalyst es el más común en el laboratorio. Tiene 24 puertos capaces de funcionar a 10BaseT y 100BaseTX, que corresponden a Ethernet, 10 Mbps, y a Fast Ethernet, 100 Mbps, respectivamente. A continuación podemos ver una fotografía del Switch CISCO Catalyst 2950 series tanto por delante como por detrás

Figura 27.Switch CISCO Catalyst 2950 series por delante.

Figura 28.Switch CISCO Catalyst 2950 series por detrás.

8.1.1.4 Cables utilizados.

Para poder realizar las medidas se ha tenido que utilizar 3 tipos diferentes de cables: directos, cruzados y de consola

Cable directo

El cable directo es un RJ-45 utilizado normalmente para conectar dispositivos desiguales, en nuestro caso lo utilizaremos para conectar el PC con el Switch y PC con router, pero también lo podríamos utilizar para conectarlo con un hub. Los ambos extremos del cable tienen la misma distribución. A continuación podemos ver una fotografía.


Figura 29. Cable directo.

Cable cruzado

El cable cruzado es un RJ-45 utilizado normalmente para conectar dispositivos iguales, en nuestro caso lo utilizaremos para conectar el PC con el router pero también lo podríamos utilizar para conectar PC con PC. Ambos extremos del cable tienen diferente distribución. A continuación podemos ver una fotografía.

Figura 30. Cable cruzado.

En la siguiente ilustración podemos ver la diferencia entre un cable T568A y un T568B, como se reparten los pares de cables en cada uno de los casos.

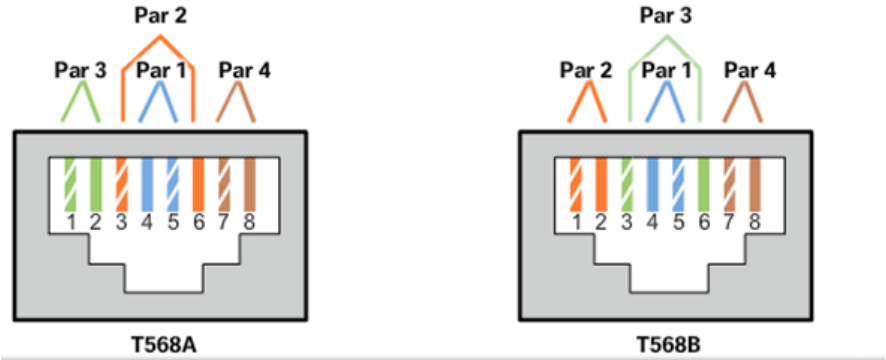


Figura 31. Distribución de pares.

Cable consola.

El cable consola está compuesto por dos tipos de conectores diferentes. Por una parte, se conecta macho RJ45 y por otra parte un conector hembra DB-9.
Un cable de consola cisco proporciona la conexión entre un PC y un equipo de red Cisco, para poder realizar las configuraciones necesarias de este y así poder hacer que este sea utilizable. En nuestro caso lo utilizaremos para conectar el PC con el router y el PC con el switch para poder realizar las configuraciones necesarias.

Figura 32. Cable consola.

En la siguiente ilustración podemos ver la diferencia entre cable directo, cable cruzado y consola con más detalle.

Tipo de cable	Estándar	Aplicación
Cable directo	Ambos extremos son T568A o T568B	Conexión de un host de red a un dispositivo de red como un switch o hub.
Cable cruzado.	Un extremo es T568A y otro extremo T568B.	Conecta dos hosts o dos dispositivos de red intermedios.
Consola	Cisco	Puerto serial de una estación de trabajo al puerto consola de un router utilizado en el adaptador.

Tabla 3. Comparativa entre cables.

8.1.2 Software empleado para las medidas.

- HyperTerminal
- IP Traffic – Test and Measure
- Wireshark

8.1.2.1 HyperTerminal.

Existen varias formas de acceder al entorno de la CLI y configurar el dispositivo. Los métodos más comunes son los siguientes:

- **Shell seguro (SSH):** Método utilizado para establecer de forma remota una conexión segura a través de una interfaz virtual, en una red. A diferencia de la conexión de consola, las sesiones de SSH requieren servicios de red activos en el dispositivo, que incluye una interfaz activa configurada con una dirección.
- **Telnet:** Es un método no seguro para establecer de forma remota una sesión de CLI a través de una interfaz virtual en una red. Telnet no proporciona una conexión cifrada segura. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.
- **Consola:** Este es un puerto de administración que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda se refiere al acceso mediante un canal de administración dedicado que se utiliza únicamente para el mantenimiento del dispositivo.
  Se ha elegido la última opción de consola con el programa HyperTerminal.

8.1.2.2 Wireshark.

Wireshark es un analizador de protocolos de software o una aplicación "husmeador de paquetes" que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolos.

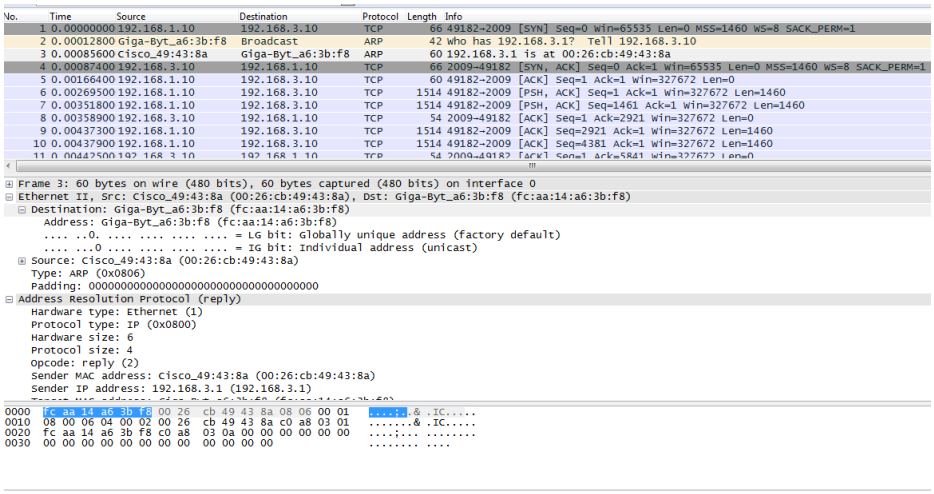


Figura 33.PantallaWireshark.

8.1.2.3 IP Traffic – Test and Measure.

Para finalizar, utilizaremos el programa IP Traffic – Test and Measure que fue desarrollado por la empresa ZTI Communications. En las medidas obtenidas hemos utilizado la versión 2.8 December 2015 - (64 bits).

Para realizar las medidas hemos obtenido diferentes ficheros con tamaños de: 0.1MB, 1MB, 5MB, 10MB, 50 MB, 200 MB, 512 MB, 1024 MB, 5GM y 10GB.Enviaremos estos ficheros para las velocidades 10Mb/s, 30Mb/s, 50Mb/s y 80Mb/s y mediremos el tiempo que tardan en transmitirse. Como se muestra en la tabla 4.

		Velocidad (Mb/s)			
		10	30	50	80
Espacio (MB)	0,1				
	1				
	5				
	10				
	50				
	200				
	512				
	1024				
	5120				
	10240				

Tabla 4. Tabla de referencia.

Realizaremos dos veces cada medida para obtener una medida más aproximada y así disminuir los errores en las medidas.

Vamos a explicar cómo utilizar el programa que se ejecutará entre los dos ordenadores (emisor - receptor) que van a estar conectados mediante el dispositivo a analizar.

En primer lugar, configuramos el PC emisor de tráfico.
Para configurar el PC emisor necesitaremos configurar los siguientes parámetros.

1. Ip Address or Host Name.
2. Protocolo. En nuestro caso TCP.
3. Numero de puerto a utilizar. En nuestro caso utilizaremos el predeterminado, 2009.
4. Parameters. Podemos seleccionar diferentes configuraciones.

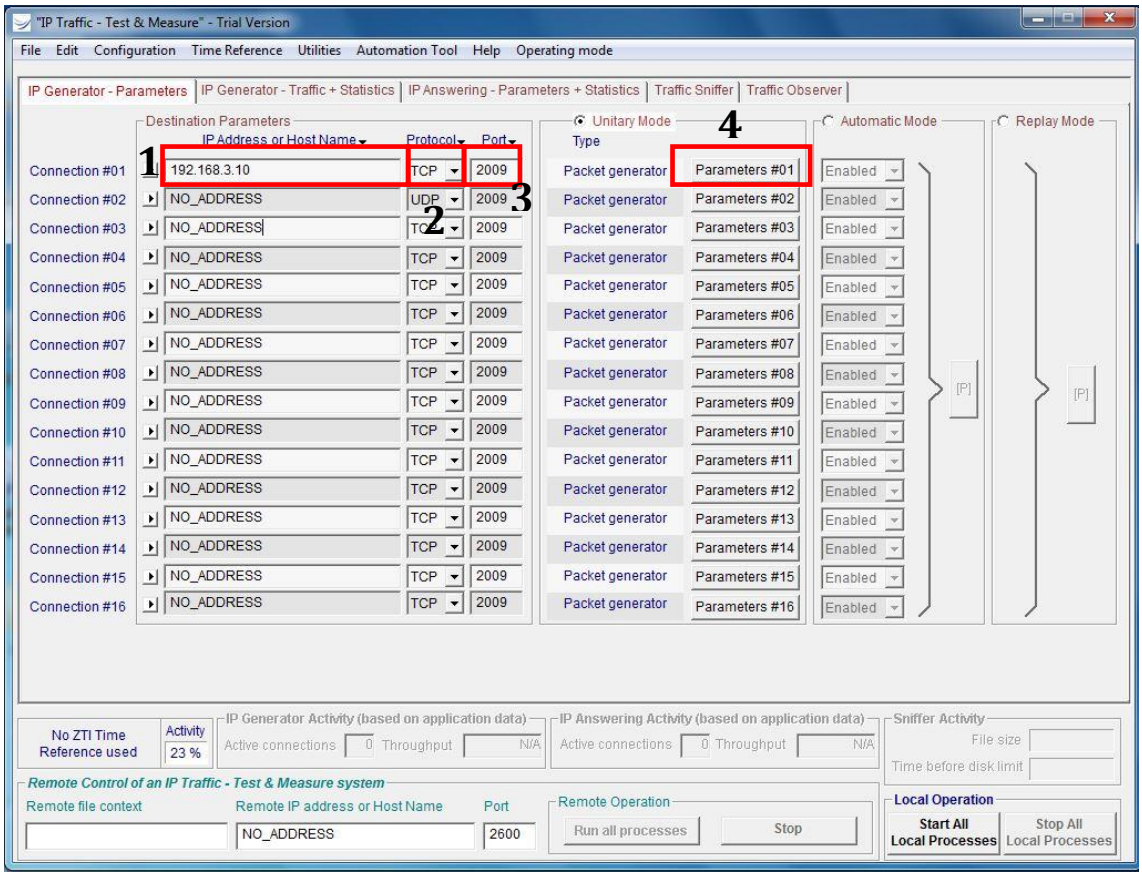


Figura 34.Pantalla principal IP Traffic

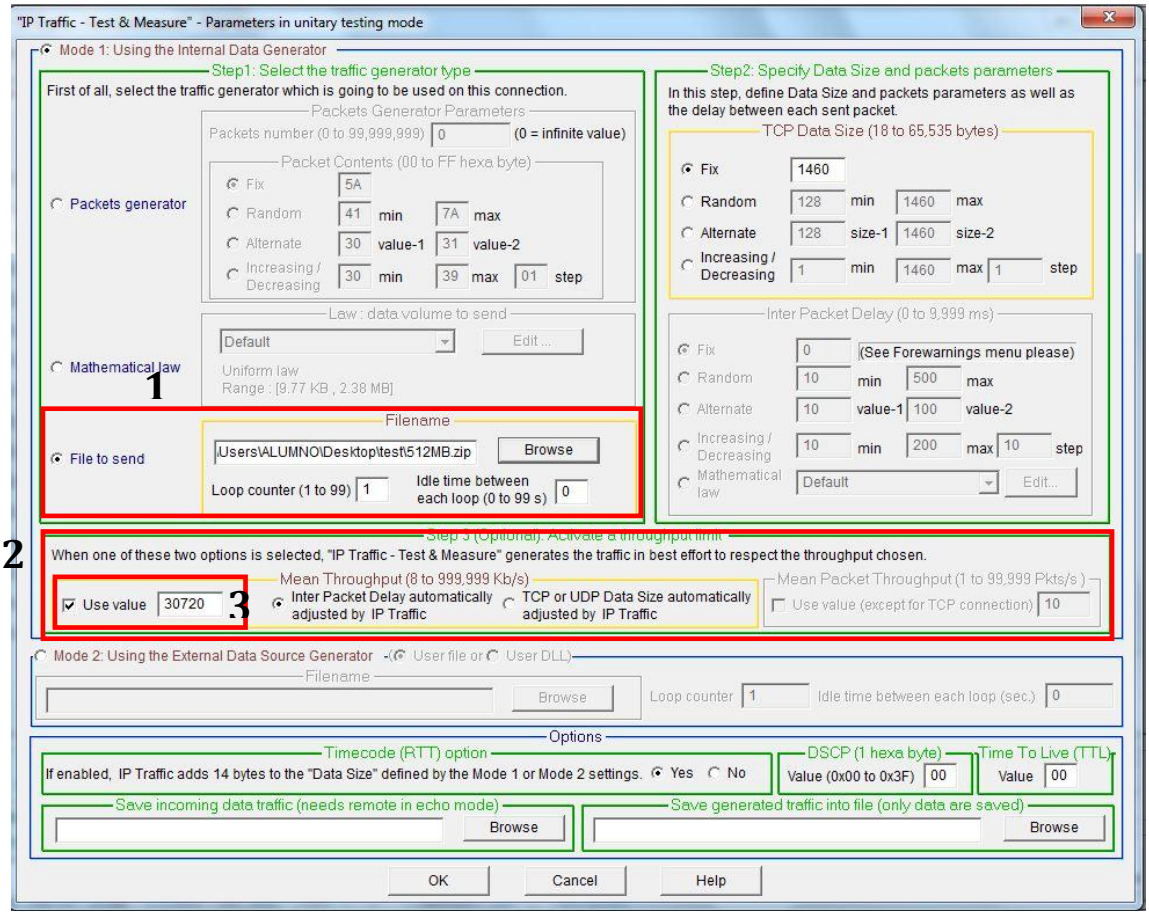


Figura 35.Opciones*IP Traffic*

Dentro de Parameters hemos seleccionado las siguientes opciones:

1. File to send. Seleccionamos el fichero con el tamaño deseado para ser enviado.
2. Activamos el limitador de throughput.
3. Seleccionamos el valor deseado.

Para finalizar, tenemos que pulsar el botón StarAll Local Proceses (1) y podremos observar diferentes opciones como el número de Conexiones activadas (2), Throughput (3) o el porcentaje de actividad (4).

Figura 36.Medidas*IP Traffiic.*

En el receptor lo único que tenemos que configurar es el puerto por el que escuchará.

8.2 Método y Configuración.

Para realizar las medidas oportunas antes tenemos que configurar el PC, Router y Switch.

8.2.1 PC.

Para la configuración del PC realizamos los siguientes pasos:

1. Hacemos click en “Conexión de área local”.

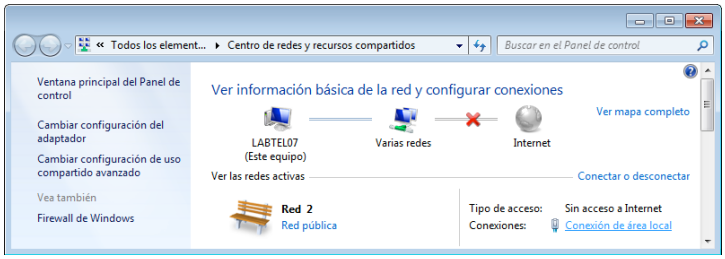


Figura 37. Centro de redes.

2. Pulsamos "Propiedades".

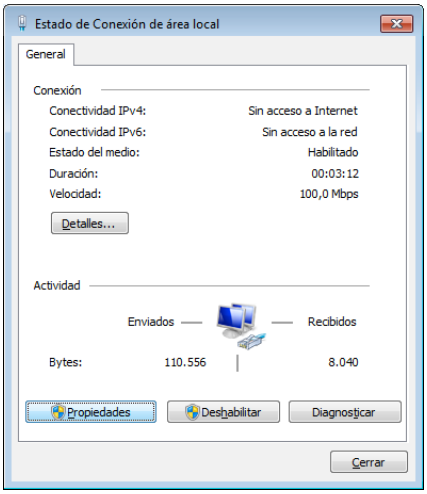
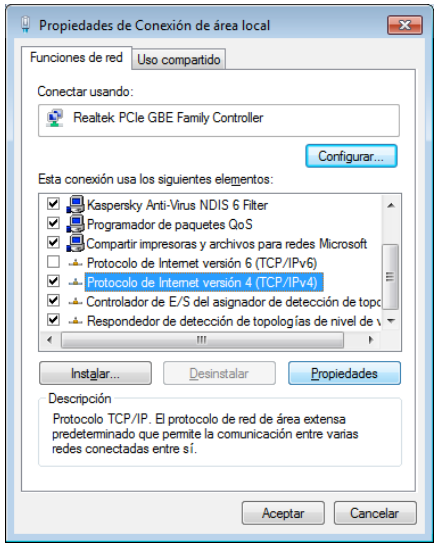


Figura 38. Estado de Conexión de área local.

3. Pulsamos "Protocolo Internet TCP/IP" y hacemos click en "Propiedades" para poder seleccionar la IP.



.

Figura 39. Propiedades de conexión de área local.

4. Introducimos la dirección en (IPv4), máscara de red y puerta de enlace predeterminada y pulsamos *"Aceptar"*.

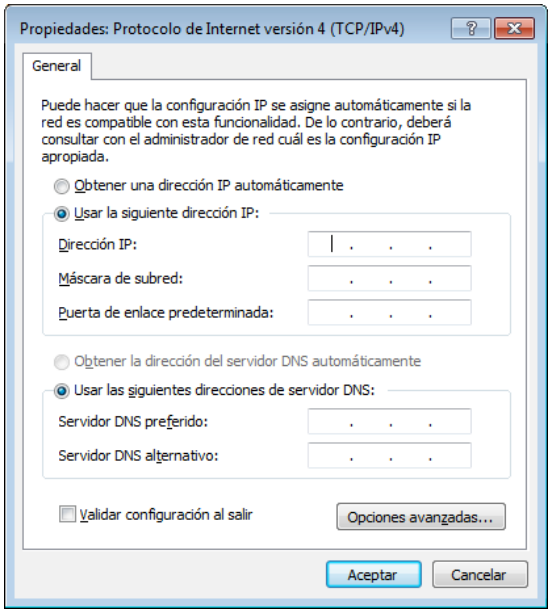


Figura 40. Propiedades de Internet

8.2.2 ROUTER.

En segundo lugar, para poder configurar el router necesitaremos enchufar el conector macho RJ-45 en el router y el conector hembra DB-9 con el PC. A continuación podemos ver una ilustración que te indica cómo se haría.

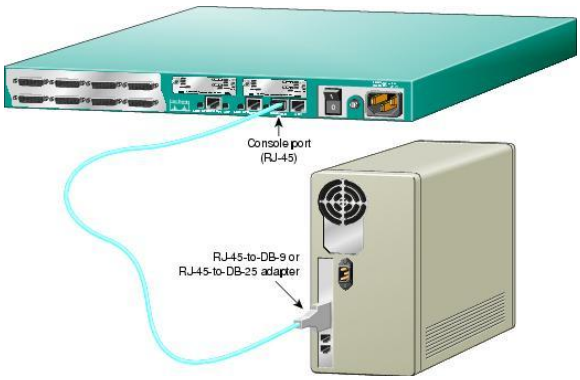


Figura 41. Conexión cable consola con PC

Para cargar la configuración correspondiente en cada uno de los routers es necesario iniciar una sesión de administración. Para ello utilizaremos el Hyperterminal de Windows, como se ha explicado en el apartado 8.1.2.1. A continuación se indican los pasos a seguir:

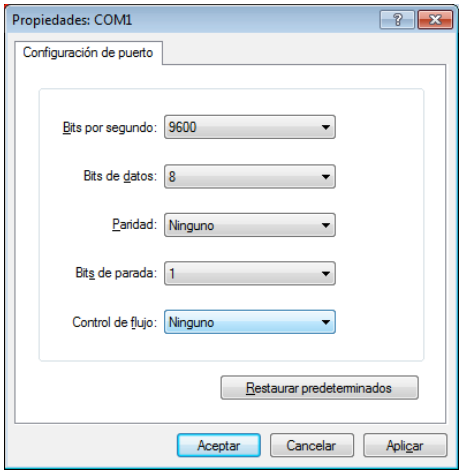


Figura 42.Propiedades COM1.

1. Pulsamos "*Enter*" en la ventana del Hyperterminal en la que nos aparecerá lo siguiente:

"Would you like to enter the initial configuration dialog? [yes/no]:"

2. Responderemos "*no*". Antes de comenzar a programar los routers es necesario asegurarnos de que no hay ninguna configuración previa, por eso mismo reiniciaremos la configuración del router:

Router>enable
Router#erase startup-config(confirmad con la tecla "Enter")
Router#reload

System configuration has been modified. Save? [yes/no]:

3. Responderemos" *no*" y posteriormente pulsamos "*Enter*".

Proceedwithreload? [confirm]

4. Mientras se reinicia el router aparecerán diversos mensajes los cuales dejaremos que aparezcan. Cuando finalicen los mensajes nos aparecerá la siguiente pregunta.

Would you like to enter the initial configuration dialog? [yes/no]:

5. Nuevamente respondemos "*no*" y tras contestar nos saldrá la siguiente pregunta a la que confirmaremos con "*Enter*"

Would you like to terminate autoinstall? [yes]:

6. En este mismo momento el router no tiene cargada ninguna configuración. Un vez realizado todos los pasos podremos empezar a configurar los routers sin temor que hubiera algo configurado previamente.

8.2.3 Realización de medidas.

En el siguiente apartado explicaremos paso a paso como hemos realizado las medidas.

1- Configuramos los equipos (routers, PC, switch) como se indica en el apartado 8.2.1 y 8.2.2
2- Configuramos los programas como se indica en los apartados 8.1.2.1, 8.1.2.2 y 8.1.2.3.
3- Mientras la información se transmite de PC a PC deberemos activar el Wireshark para capturar el tráfico en la red.
4- Cuando haya terminado de transmitirse toda la información filtramos por TCP como se puede observar en la figura 43.

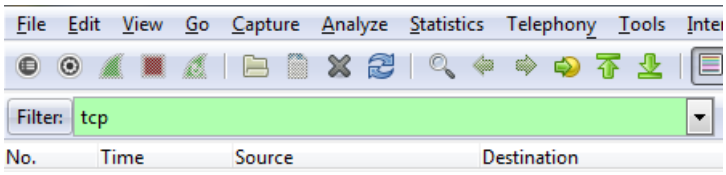


Figura 43.FiltroWireshark.

5- Para comprobar el tiempo que tarda en transmitirse toda la información tenemos dos métodos:

1ºOpción. Seleccionamos la opción Set Time Reference para seleccionar un paquete de referencia. De esta manera eliminaremos posibles paquetes TCP que se hayan podido enviar previamente y puedan modificar el tiempo.

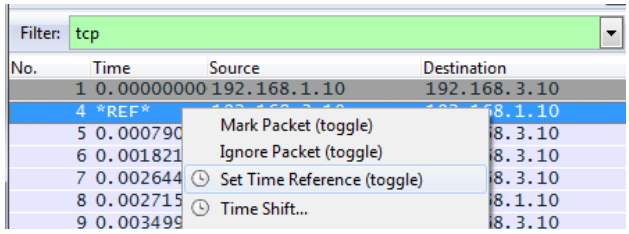


Figura 44.Paquete de referencia Wireshark.

5.1.2 Para finalizar, nos vamos al último paquete y en la columna Time podemos comprobar cuanto tiempo ha tardado en enviarse el fichero.

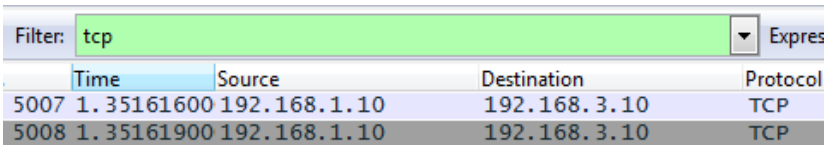


Figura 45.PaqueteWireshark.

2ºOpción. Otra manera de comprobar el tiempo que tarda en transmitirse el fichero es restar el tiempo del último paquete menos el tiempo del primer paquete, como muestra la siguiente figura:

$$Tiempo_{total} = Tiempo_{último\ paquete} - Tiempo_{primer\ paquete}$$

$$Tiempo_{total} = 1.3551619 - 0.0008740 = 1.3542879$$

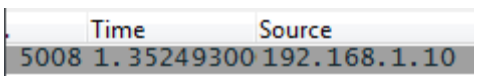


Figura 46.Ultimo paquete Wireshark.

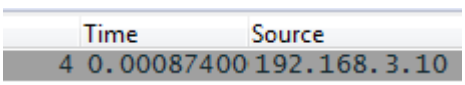


Figura 47.Primer paquete Wireshark.

Capítulo 9. Medidas

En el siguiente apartado hemos realizado diferentes medidas con las siguientes configuraciones.

- Teórico
- SIN CIFRAR
- CIFRADAS
    - IPSEC-AES
    - IPSEC-DES
    - PPTP

Hemos realizado dos veces cada una de las medidas para poder minimizar el error. Tras observar que cada una de las medidas no se desviaban de su homólogo hemos realizado la media entre las dos.

9.1 Teórico.

Es una medida teórica, será la que utilizaremos como referencia y comparativa con las demás medidas. A continuación, podemos observar cual sería la topología que hemos utilizado.

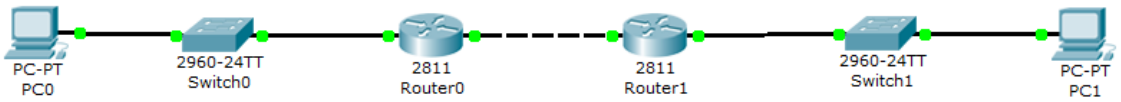


Figura 48. Topología medida enlace Ethernet en entre dos PCs.

Los resultados teóricos, es decir el tiempo que tarda un paquete desde que sale del PC0 (Transmisor) pasado por los routers 0,1 y llegando al PC1 (Receptor). A continuación podemos observar el tiempo teórico en segundos.

		Velocidad (Mb/s)			
		10	**30**	**50**	**80**
Espacio (MB)	**0,1**	0,08	0,03	0,02	0,01
	1	0,80	0,27	0,16	0,10
	5	4,00	1,33	0,80	0,50
	10	8,00	2,67	1,60	1,00
	50	40,00	13,33	8,00	5,00
	200	160,00	53,33	32,00	20,00
	512	409,60	136,53	81,92	51,20
	1024	819,20	273,07	163,84	102,40
	5120	4096,00	1365,33	819,20	512,00
	10240	8192,00	2730,67	1638,40	1024,00

Tabla 5. Tabla datos.

Para el cálculo de los tiempos teóricos hemos realizado el siguiente cálculo:

$$Tiempo_{total} = \frac{Espacio(MB) * 8}{velocidad\ (\frac{Mb}{s})} \quad \textbf{(9.1)}$$

A continuación podemos observar una tabla comparativa en escala logarítmica de base 10, con las diferentes velocidades y tamaño transmitido. Podemos observar que los tiempos se mantienen de forma lineal para dentro de la misma velocidad y disminuye de forma paralela según aumentamos la velocidad.

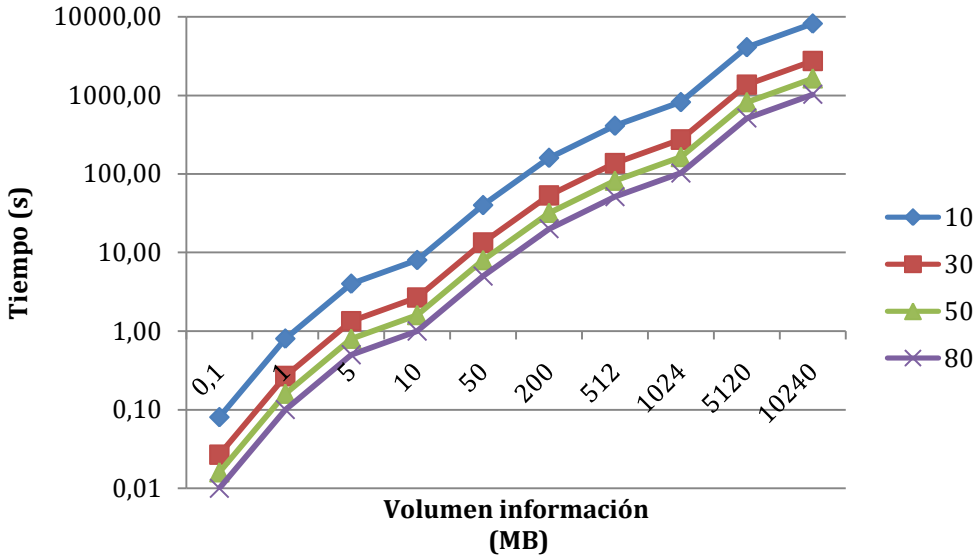


Figura 49. Tiempos para situación Teórica.

9.2 SIN CIFRAR.

En esta medida analizaremos la transmisión de paquetes sin cifrar los datos. La topología utilizada en el packet tracer y con los routers del laboratorio es la siguiente respectivamente:

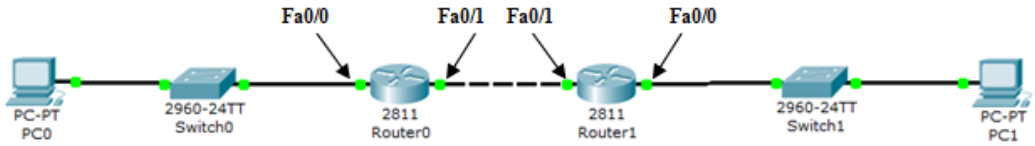


Figura 50. Topología medida enlace Ethernet entre dos PCs.

Figura 51. Topología medida enlace Ethernet entre dos PCs.

A continuación podemos observar la configuración de los router 0 y 1 junto con la de los pcs 0 y 1.

Device	Interface	IP Address	SubnetMask	Default Gateway
R0	Fa 0/0	192.168.1.1	255.255.255.0	N/A
	Fa 0/1	192.168.2.1	255.255.255.0	N/A
R1	Fa 0/0	192.168.3.1	255.255.255.0	N/A
	Fa 0/1	192.168.2.2	255.255.255.0	N/A
PC-0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC-1	NIC	192.168.3.10	255.255.255.0	192.168.2.1

Tabla 6. Configuración routers y pcs.

El código utilizado pequeña parte del código utilizado para la configuración de los routers:

```
Router>enable
Router# configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
```

A continuación podemos observar el tiempo de transmisión en segundos de los datos sin cifrar:

		velocidad (Mb/s)			
	Sin cifrar	**10**	**30**	**50**	**80**
espacio (MB)	**0,1**	0,08	0,03	0,02	0,01
	1	0,81	0,27	0,16	0,10
	5	4,06	1,35	0,81	0,52
	10	8,10	2,70	1,62	1,01
	50	40,47	13,49	8,10	5,60
	200	161,87	53,97	32,79	20,24
	512	414,37	138,19	86,50	51,81
	1024	828,73	277,16	166,05	103,62
	5120	4145,54	1381,47	837,86	525,21
	10240	8233,25	2763,97	1675,72	1058,87

Tabla 7. Tabla datos.

En la siguiente gráfica podemos observar una tabla comparativa en escala logarítmica de base 10 con las diferentes velocidades y volumen de información enviado. Podemos observar como los resultados obtenidos se aproximan al resultado teórico, algo que era esperado.

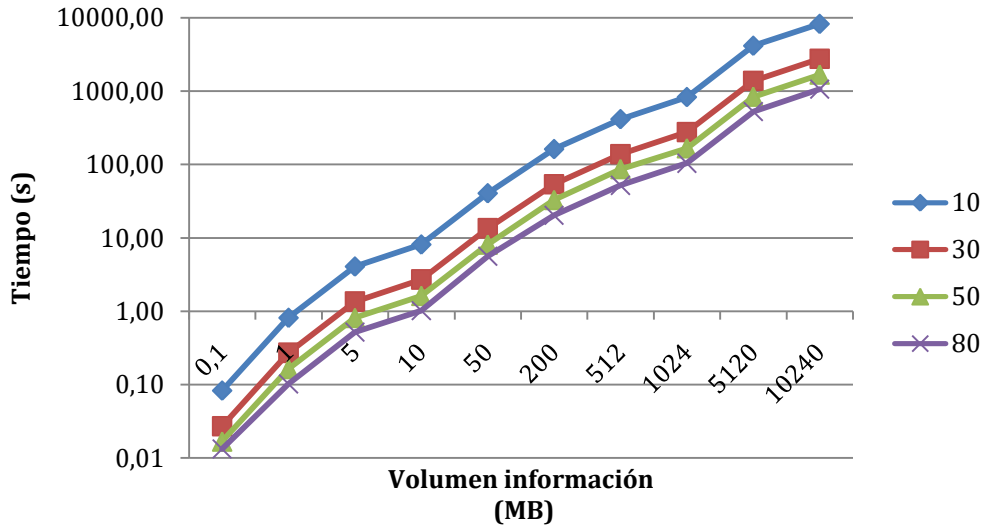


Figura 52. Tiempos para situación Sin Cifrar.

9.3 IPSEC.

En el siguiente apartado hemos configurado los router de dos maneras diferentes, para poder comparar con otros tipos de VPN y dentro de un mismo tipo de VPN, como se comporta el tiempo según la configuración. A continuación podemos observar la topología utilizada tanto con el packet tracert como con los routers del laboratorio.

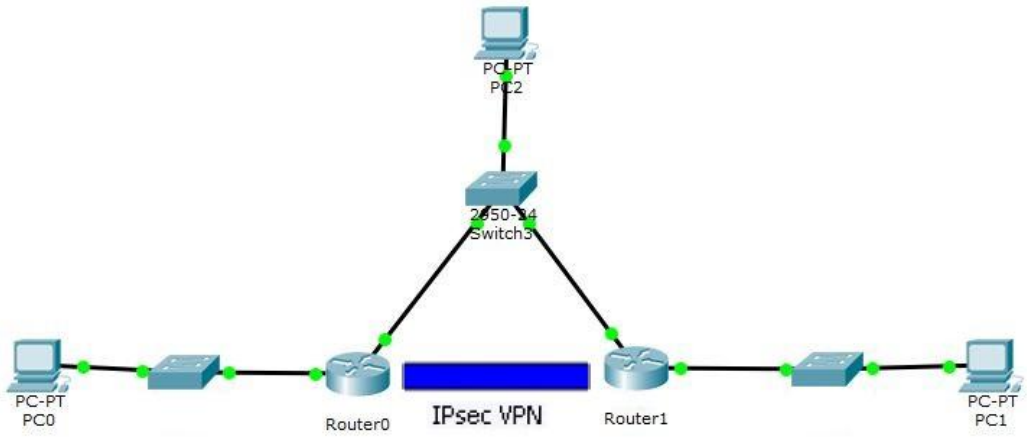


Figura 53. Topología medida enlace Ethernet en entre dos PCs.

En la siguiente figura podemos observar cómo hemos realizado el montaje de los aparatos para que sea como la figura 53. Hemos realizado un túnel IPSEC entre los routers 0 y 1. Como la encriptación y desencriptación se realiza entre los routers, hemos configurado un switch entre medias para poder ver el tráfico. Tanto para su posterior análisis como para comprobar que se está realizando correctamente el túnel.

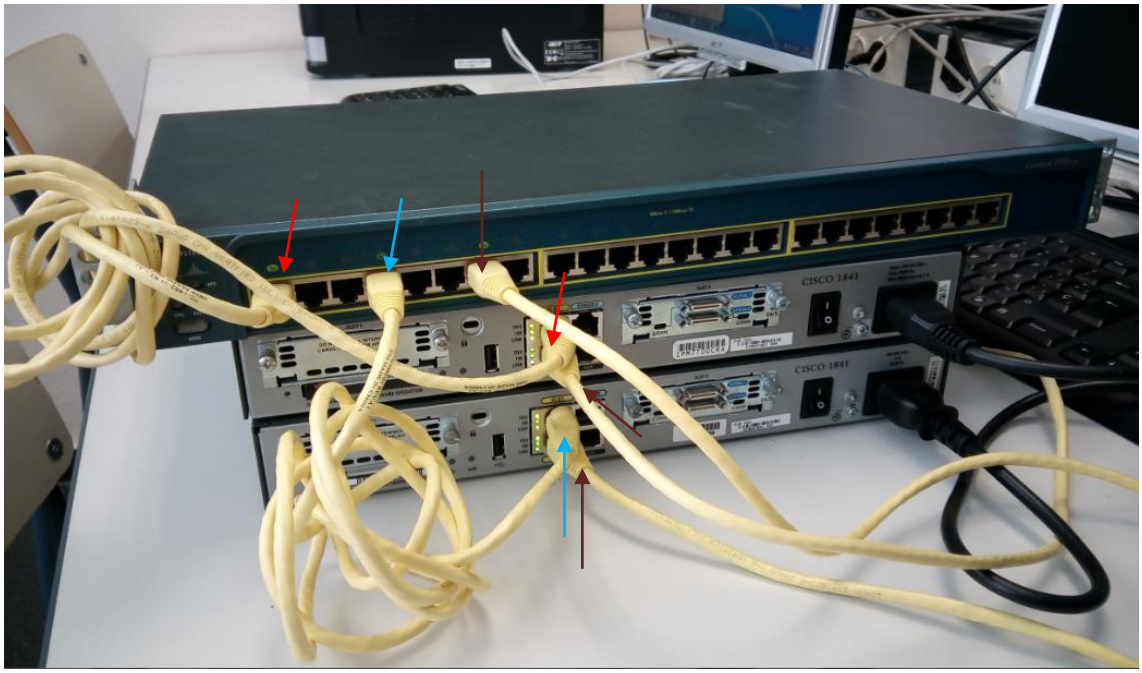


Figura 54. Topología medida enlace Ethernet en entre dos PCs.

Las flechas rojas y azules son las que van del router 0 y 1 al switch respectivamente, mientras que las marrones son las que van del PC al router en el caso del PC 0 y 1 y al PC 2.

A continuación podemos observar la configuración de los router 0 y 1 junto con la de los PCs 0 y 1. Hemos utilizado la misma topología y la misma configuración para las dos medidas de IPSEC.

Device	Interface	IP Address	SubnetMask	Default Gateway
R0	Fa 0/0	192.168.1.1	255.255.255.0	N/A
	Fa 0/1	192.168.2.1	255.255.255.0	N/A
R1	Fa 0/0	192.168.3.1	255.255.255.0	N/A
	Fa 0/1	192.168.2.2	255.255.255.0	N/A
PC-0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC-1	NIC	192.168.3.10	255.255.255.0	192.168.2.1
PC-2	NIC	192.168.2.3	255.255.255.0	192.168.2.10

Tabla 8. Configuración routers y pcs.

En ninguna de las dos medidas ni configuraciones la velocidad no sobrepasa de 31,1 Mb/s debido a que los routers tardan un tiempo en cifrar y descifrar los datos.

Figura 55. Velocidad máxima IPSEC.

9.3.1 IPSEC-AES.

Los tiempos obtenidos para la primera configuración de IPSEC son los siguientes:

		velocidad (Mb/s)			
	IPSEC	10	30	50	80
espacio (MB)	0,1	0,55	0,51	0,49	0,25
	1	0,84	0,80	0,82	0,81
	5	4,05	1,97	1,87	1,87
	10	8,10	3,34	3,17	3,16
	50	40,47	14,02	13,66	13,50
	200	161,86	54,47	52,79	53,23
	512	414,38	138,69	134,36	131,58
	1024	828,73	276,83	268,38	260,89
	5120	4143,65	1557,69	1325,68	1306,85
	10240	8328,15	2766,85	2650,80	2631,56

Tabla 9. Tabla datos.

A continuación podemos observar una tabla comparativa en escala logarítmica de base 10 con las diferentes velocidades y volumen de información enviado.

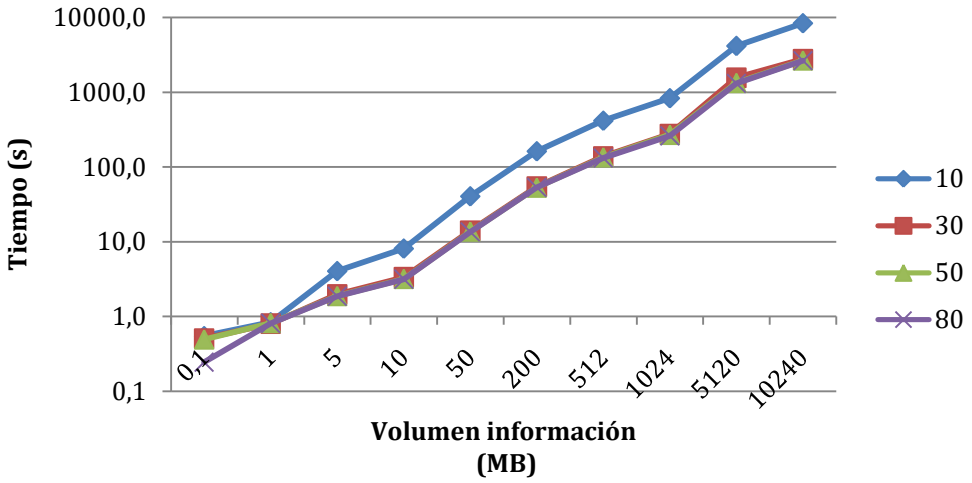


Figura 56. Tiempos para situación IPSEC.

Seguidamente explicaremos los apartados que hay que configurar en una VPN de IPSEC:

- Especifica los detalles iníciales de seguridad.
- Como los paquetes IPSEC serán encapsulados.
- El tráfico que activará la VPN.
- Crea un mapa criptográfico que combina: la política ISAKMP, la ACL, la dirección entre pares y las transformaciones de IPSEC.
- Los interfaces que son activados para crear la VPN.

Parametros	Comentario	R1	R3
Método de distribución de claves	Manual o ISAKMP	ISAKMP	ISAKMP
Algoritmo de cifrado	DES, 3DES o AES	AES	AES
Algoritmo hash	MD5 o SHA-1	SHA-1	SHA-1
Método de autenticación	Claves previamente compartidas o RSA	Previamente compartidas	Previamente compartidas
Intercambio de claves	Grupo DH 1, 2 o 5	DH 2	DH 2
Vida útil de SA IKE	86 400 segundos o menos	86 400	86 400
ISAKMP Key (Llave USB)	-	cisco	cisco

Tabla 9. Características IPSEC.

9.3.2 IPSEC-DES.

Los tiempos obtenidos para la segunda configuración de IPSEC son los siguientes:

		Velocidad (Mb/s)			
	IPSEC2	10	30	50	80
Espacio (MB)	0,1	0,55	0,54	0,51	0,50
	1	0,81	0,84	0,83	0,81
	5	4,05	1,94	1,90	1,89
	10	8,09	2,97	2,90	3,20
	50	40,47	15,66	14,35	13,82
	200	161,87	54,49	52,78	51,33
	512	414,38	143,55	135,94	134,88
	1024	828,75	277,43	271,87	268,52
	5120	4143,77	1560,32	1328,02	1320,62
	10240	8331,17	2773,83	2661,27	2645,57

Tabla 10. Tabla datos.

A continuación podemos observar una tabla comparativa en escala logarítmica de base 10 con las diferentes velocidades y volumen de información enviado.

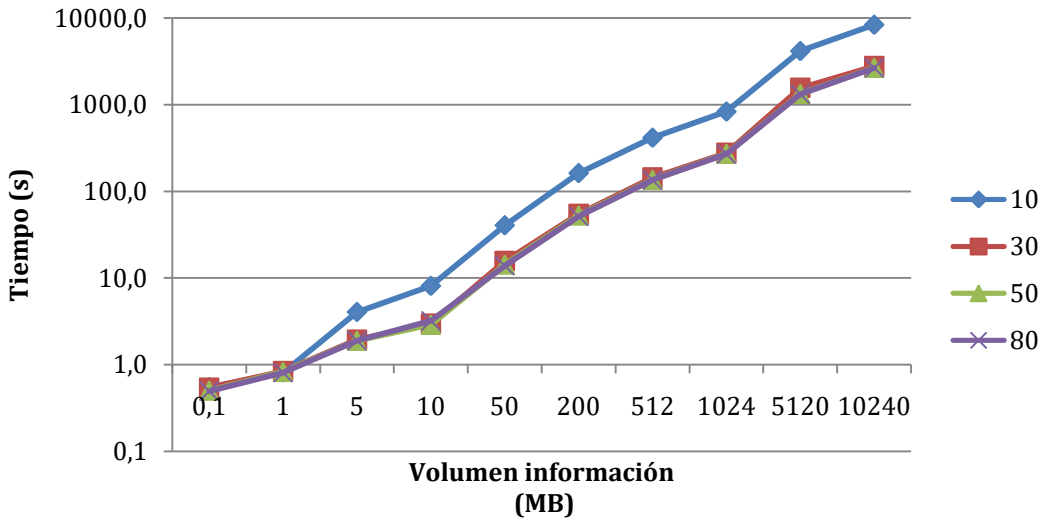


Figura 57. Tiempos para situación IPSEC.

Parametros	Cometario	R1	R3
Método de distribución de claves	Manual o ISAKMP	ISAKMP	ISAKMP
Algoritmo de cifrado	DES, 3DES o AES	DES	DES
Algoritmo hash	MD5 o SHA-1	MD5	MD5
Intercambio de claves	Grupo DH 1, 2 o 5	DH 2	DH 2
Vida útil de SA IKE	86 400 segundos o menos	86 400	86 400
ISAKMP Key (Llave USB)	-	cisco	cisco

Tabla 11. Características IPSEC.

Comparando las tablas 9 y 10 y cogiendo los dos tiempos que más se distancian no llega ni al 0,6% de diferencia. Con lo que podemos concluir que para dos configuraciones diferentes de IPSEC el tiempo que tarda en enviar la información es prácticamente idéntico.

9.4 PPTP.

A continuación analizaremos las medidas para PPTP. En la siguiente figura muestra la topología utilizada.

Figura 58. Topología medida enlace.

A continuación podemos observar los resultados cifrados con PPTP, es decir el tiempo que tarda un paquete desde que sale del PC0 (Transmisor) hasta el router.

		Velocidad (Mb/s)			
	PPTP	10	30	50	80
Espacio (MB)	0,1	0,09	0,07	0,06	0,06
	1	0,91	0,72	0,71	0,57
	5	4,06	3,26	2,88	2,87
	10	8,11	6,09	5,77	5,74
	50	40,47	28,69	28,50	28,50
	200	161,88	115,12	115,35	115,30
	512	414,38	293,83	293,60	293,53
	1024	828,74	586,90	585,40	586,96
	5120	4143,69	2933,32	2930,48	2925,47
	10240	8287,37	5881,42	5862,30	5850,28

Tabla 12. Tabla datos.

A continuación podemos observar una tabla comparativa en escala logarítmica de base 10 con las diferentes velocidades y volumen de información enviado.

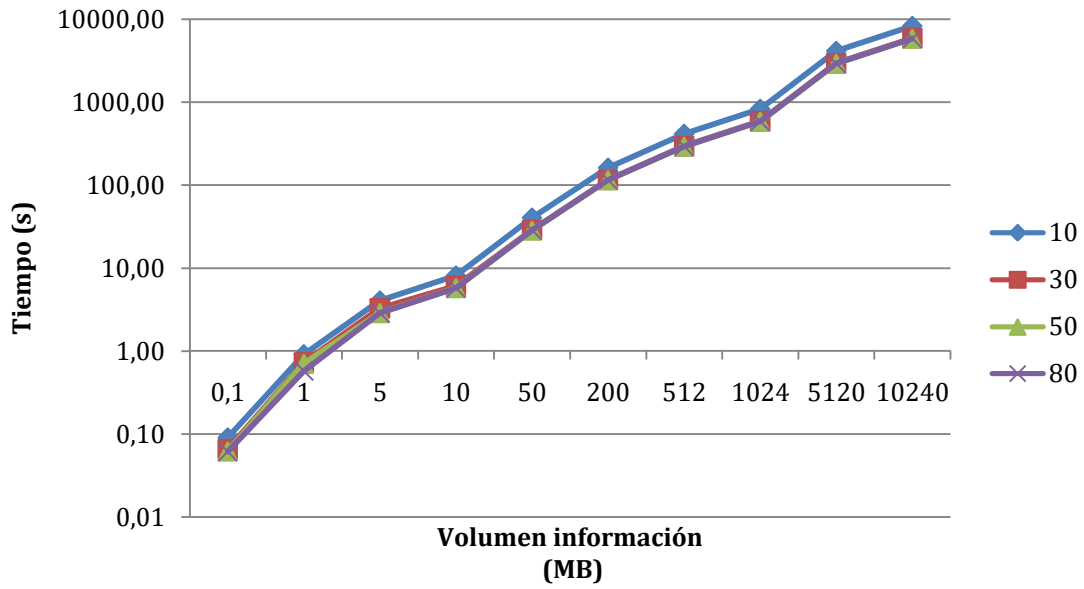


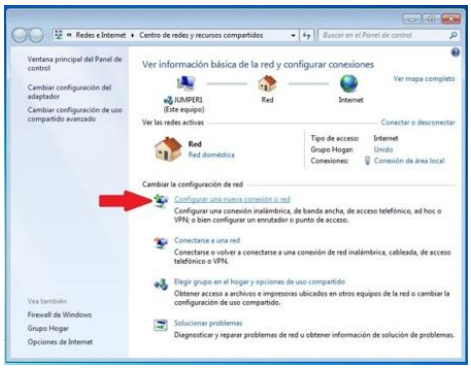
Figura 59. Tiempo PPTP.

Como podemos observar en la anterior figura 59 y en la tabla 12 de la tabla de datos podemos ver que a partir de 14.1Mb/s los tiempos son prácticamente idénticos para diferente volumen de información y aunque aumente la velocidad de transmisión.

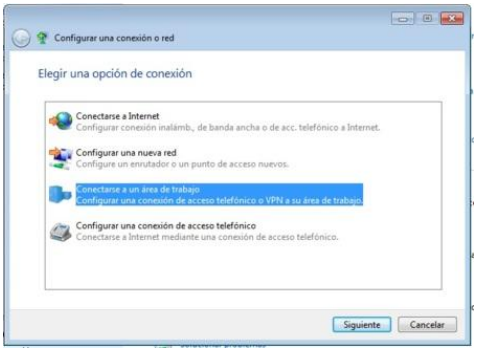
Configuración del PC.

Para configurar una VPN en PPTP en Windows en el PC hay que hacer los siguientes pasos:

1- Configurar una nueva conexión o red

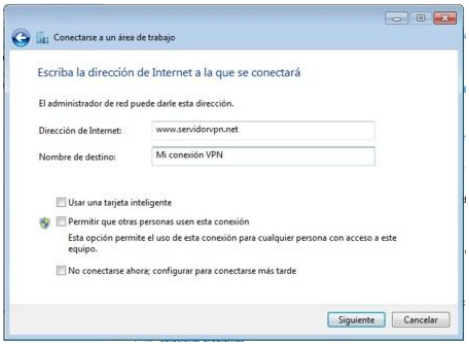


2-Conectarse a un área de trabajo



3- Usar mi conexión a Internet (**VPN).**

4- Dirección del servidor y nombre del destino.



5-usuario y contraseña de la VPN, y opcionalmente el nombre del dominio.

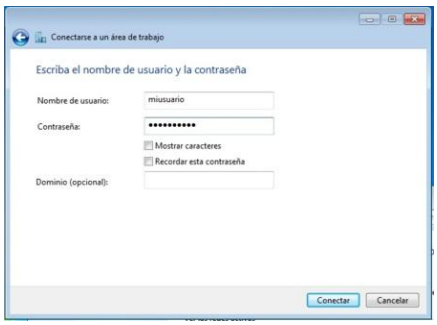


Figura 60. Pasos para un VPN.

9.5 Comparativa y conclusiones.

9.5.1Comparativa.

En este apartado nos centraremos en comparar los resultados obtenidos con las medidas realizadas en el apartado anterior. Seguidamente daremos una explicación para cada una de las siguientes gráficas. Hemos comparado las gráficas con cada una de las velocidades (10Mb/s, 30Mb/s, 50Mb/s y 80Mb/s).

En la gráfica siguiente podemos observar los diferentes resultados obtenidos con los diferentes métodos y el que sería el teórico para una velocidad de 10Mb/s.
Como podemos comprobar los resultados son prácticamente idénticos, a excepción del primer valor de IPSEC. Al ser un volumen de información tan pequeño podríamos afirmar que se tardaría prácticamente el mismo tiempo este encriptado o no la información.

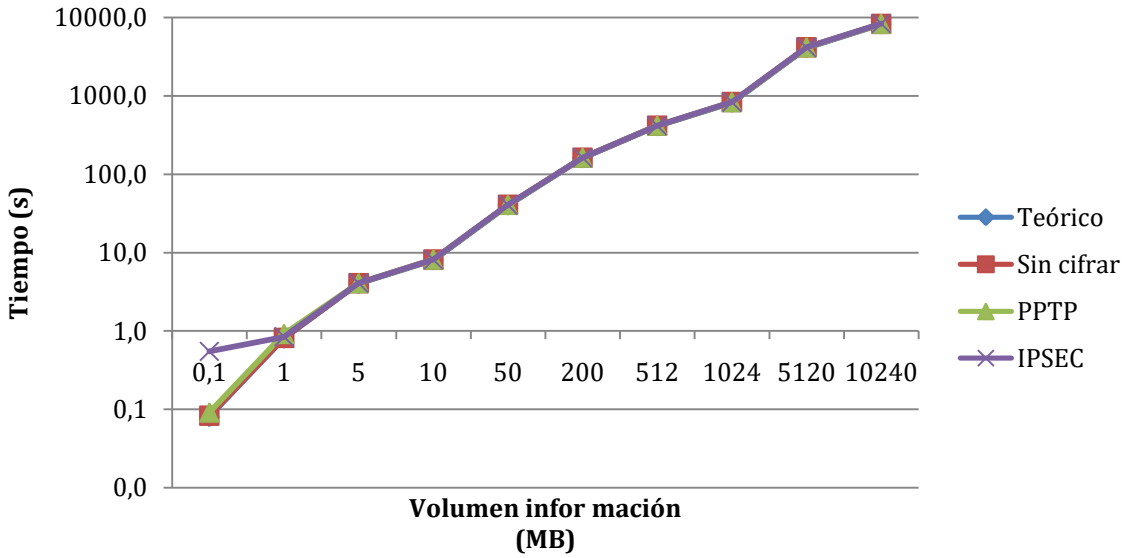


Figura 61. Velocidad para 10 Mb/s

En la gráfica seria para una velocidad de 30Mb/s.

En la gráfica podemos comprobar cómo el tiempo teórico, sin cifrar e IPSEC son prácticamente iguales, con la excepción que hemos hablado en la gráfica anterior. Por otro lado, podemos observar que para PPTP el tiempo es ligeramente mayor debido a que la velocidad de cifrado como hemos mencionado en la figura 61, no sobrepasa de 14,1 Mb/s.

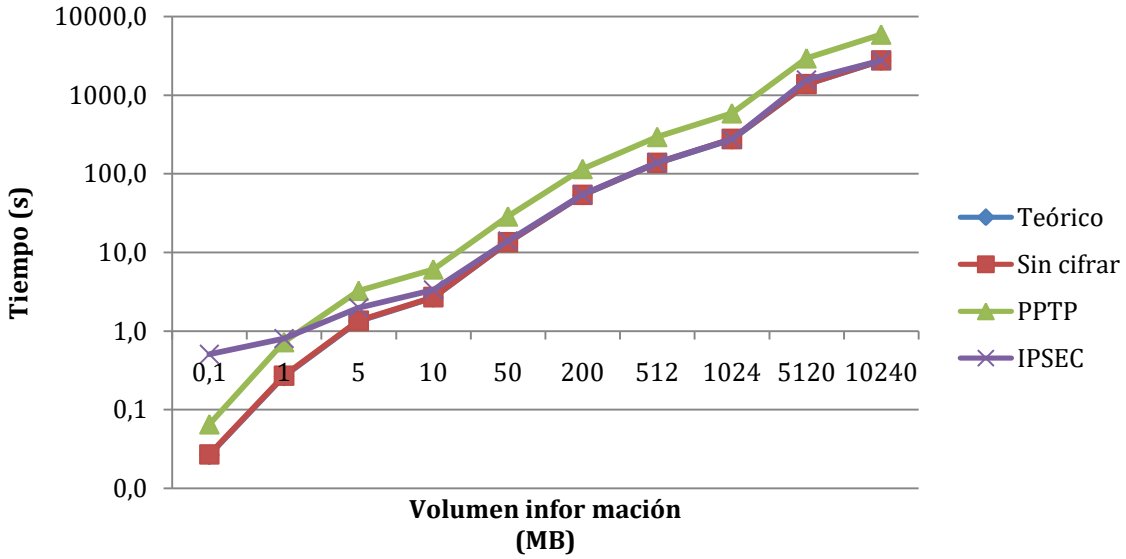


Figura 62. Velocidad para 30 Mb/s

En la gráfica seria para una velocidad de 50Mb/s.

Podemos observar que el tiempo teórico y sin cifrar siguen siendo bastante similares, pero en algunos momentos hay una ligera fluctuación. Por otra parte, podemos comprobar como para PPTP aumenta aún más el tiempo de transmisión. De la misma manera que IPSEC, pero sin ser tan significativo. Los motivos son los mismos que para PPTP y es que IPSEC no puede pasar de 31,1Mb/s.

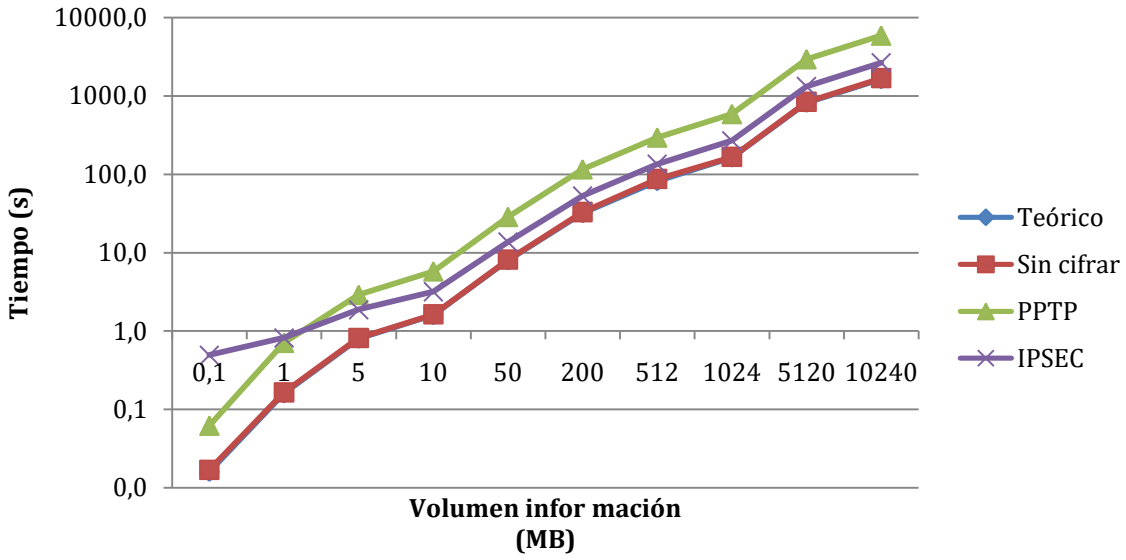


Figura 63.Velocidad para 50 Mb/s

En la gráfica seria para una velocidad de 80Mb/s.

Para finalizar, tenemos la gráfica para 80Mb/s en la que podemos decir que sigue la misma tendencia que las anteriores gráficas, es decir para PPTP e IPSEC el tiempo de transmisión aumenta.

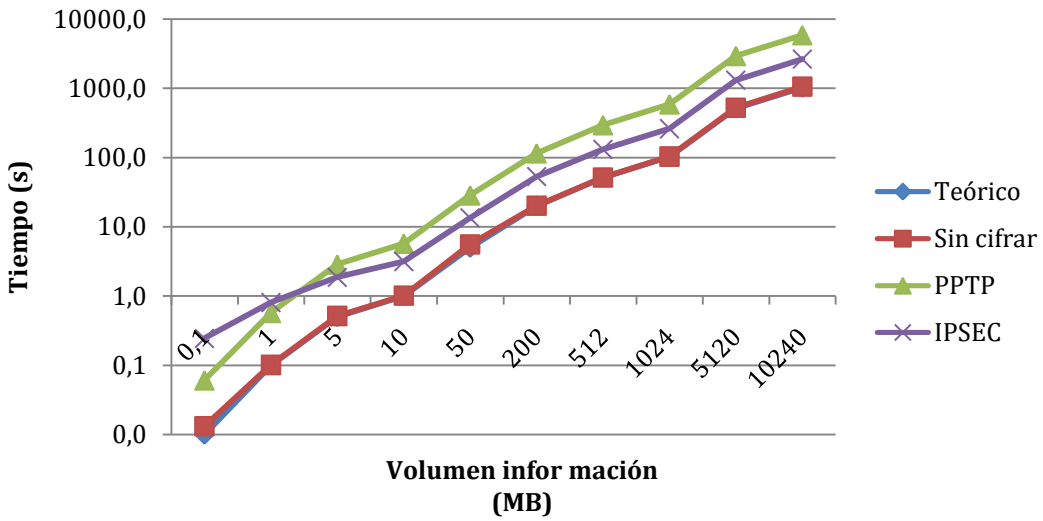


Figura 64.Velocidad para 80 Mb/s

En conclusión, haciendo un balance general de las figura 61, 62, 63 y 64 podemos decir que los tiempos teóricos y sin cifrarse se mantienen similares por mucho que aumente la velocidad o el volumen de información.
Por otra parte, IPSEC y PPTP tienen una "barrera" de 31,1 Mb/s y 14,1Mb/s respectivamente, que no les deja aumentar la velocidad de transmisión. Por ese motivo, la diferencia de tiempos es mayor según aumentamos la velocidad
Esto se debe principalmente a dos motivos**;** El primero de ellos, es debido al cifrado y descifrado, ya que tarda un tiempo en procesarse. El segundo motivo, es debido al software y hardware de los equipos, tanto de los routers como de las tarjetas de red de los ordenadores.

9.5.2Conclusiones.

Si analizamos el estudio realizado durante este trabajo fin de grado, podemos comprobar que hemos cumplido los objetivos que teníamos marcados previamente. Trataban de aportar unos conocimientos y herramientas necesarios para todos aquellos que quieran utilizar una VPN, realizar un estudio teórico de los métodos más utilizados, diferencias los distintitos tipos de cables, software, routers… y realizar medidas en el laboratorio para comprobar cuanto tiempo tarda cada tipo de VPN para diferentes velocidades y volúmenes de información.
Por otra parte, hemos conseguido medir con exactitud los tiempos. Por todo esto, podemos concluir que conseguimos superar considerablemente los objetivos previamente marcados.

Capítulo 10. Futuras líneas de trabajo.

En primer lugar, marcaremos unas futuras líneas de trabajo para poder mejorar este trabajo y tener una visión más global.

El siguiente trabajo que haríamos seria:

1. Configurar los routers en IPV4 con más variedades de VPN tanto para Site-to-Site como para VPDN como por ejemplo L2TP. Posteriormente, comparar los resultados obtenidos como hemos realizado anteriormente.
2. Realizar las mismas configuraciones efectuadas anteriormente (PPTP, IPSEC, GRE y L2TP) en IPv6 para comprobar si el tiempo de transmisión es el mismo en los ambos casos.
3. Realizar una topología en cadena como se muestra en la siguiente figura. Con diferentes VPN en cada uno de los enlaces, para comprobar si la suma de los tiempos en cada enlace es la suma total de los enlaces o tendríamos que añadirle un factor de desviación.

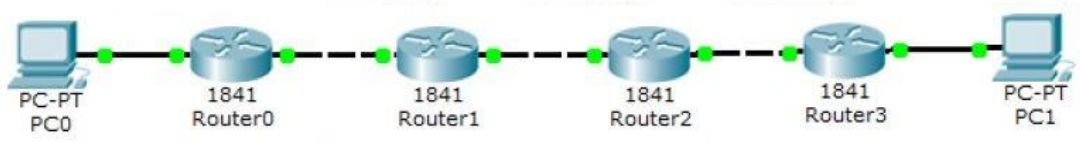


Figura 65.Topología en cadena

$$Tiempo_{total} = N * (Tiempo_{tipo\ 1\ VPN} + Tiempo_{tipo\ 2\ VPN} + \cdots + Tiempo_{tipo\ N\ VPN}) \quad (\mathbf{10.1})$$

$\boldsymbol{N}$, Número$deenlaces$ según el tipo de VPN.
$\boldsymbol{Tiempo_{tipo\ N\ VPN}}$, Tiempo que tarda en transmitir la información en cada etapa.
Para realizar esta medida se podría utilizar el mismo método utilizado anteriormente. Abriendo el Wireshark y seleccionando un paquete de referencia o restando la llegada del último paquete menos la recepción del primer paquete.
Por otra parte, si deseáramos saber si se están transmitiendo exactamente el tipo de cifrado o los paquetes que se están transmitiendo necesitaríamos situar un switch o un hub entre dos routers. De esta manera con el Wireshark o con otro analizador de protocolos lo podríamos comprobar fácilmente.

Capítulo 11. Bibliografía.

[1] IP Traffic – Test and Measure, web: < http://www.zti-communications.com/iptraffic/ >

[2] Descarga Wireshark, web: < https://www.wireshark.org/#download >

[3] CISCO, web: < https://www.cisco.com/c/en/us/index.html >

[4] RFC 1701, web: <https://tools.ietf.org/html/rfc1701>

[5] RFC 1702, web: <https://tools.ietf.org/html/rfc1702>

[6] RFC 2401, web: <https://www.ietf.org/rfc/rfc2401.txt>

[7] RFC 2412, web: <https://tools.ietf.org/html/rfc2412>

[8] RFC 2637, web: <https://tools.ietf.org/html/rfc2637>

[9] RFC 2661, web: < https://tools.ietf.org/html/rfc2661>

[10] RFC 2784, web: <https://tools.ietf.org/html/rfc2784>

[11] RFC 4301, web: <https://tools.ietf.org/html/rfc4301>

[12] RFC 4309, web: <https://tools.ietf.org/html/rfc4309>

Anexo. Glosario de comandos:

- **Enable.** Ingresa al modo EXEC Privilegiado
- **configure terminal**. Entrar en el modo de configuración global
- **show version**. Mostrar información sobre el software cargado en ese momento junto con el hardware y la información del dispositivo
- **ping**. Enviar un ping a la dirección deseada
- **copy running-config startup-config**. Guarda la configuración activa en la NVRAM
- **erase startup-config**. Borra el contenido de la NVRAM
- **reload.** Reinicia el router
- **show startup-config.** Muestra la configuración que se ha guardado, que es el contenido de la NVRAM
- **access-list***Nro_ACL***[permit|deny]***Proto Origen Destino* **[***Operador Nro_puerto***][established][echo |echo-reply].** Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes.
- **Enablepassword***contraseña.* Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio.
- **Enablesecret***contraseña.* Especifica una capa de seguridad adicional mediante el comando enable password.
- **Hostname** ***nombre.*** Modifica el nombre del router.
- **line** ***tipo número.*** Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración.
- **ipaddress***dirección_ipmascara_red.* Asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz.
- **no shutdown.** Reinicia una interfaz desactivada
- **Iproute***dirección_red máscara dir_ip_salto***[***distancia_administrativa***].** Establece rutas estáticas.
- **crypto isakmp key.** configura como la identidad, la clave previamente compartida debe estar configurada con la dirección IP del otro extremo para que el proceso funcione cuando se utiliza IKE en modo principal.
- **Ipunnumbered.** Para deshabilitar el procesamiento de IP en la interfaz