PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS Y COMPUTACIÓN

TEMA: GUÍA PRÁCTICA PARA CREAR UNA INFRAESTRUCTURA DE RED SEGURA UTILIZANDO IPSEC CON TÚNELES GRE Y CET.

NOMBRE: LUIS FERNANDO AGUAS BUCHELI

DIRECTOR: ING. FRANCISCO RODRÍGUEZ CLAVIJO MSC.

QUITO, 2010

INTRODUCCION

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. "Hackers[1]", "crackers[2]", entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de redes.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

A la hora de plantearse en qué elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

- Protección de los sistemas de transferencia o transporte, en este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs (Mail Transport Agents)

[1] Experto en seguridad informática, programación, sistemas de información, Internet, sistemas de seguridad, con intenciones buenas.
[2] Experto en seguridad informática, programación, sistemas de información, Internet, sistemas de seguridad, con intenciones de hacer daño.

seguras, o la instalación de un firewall, que defiende el acceso a una parte protegida de una red.

- Aplicaciones seguras extremo a extremo, si pensamos, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de asegurar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Esta misma operatoria, puede usarse para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc. En ambos casos, un problema de capital importancia es la gestión de contraseñas.

Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro.

En este contexto, he elaborado este material. Con él nos propongo facilitar las tareas de todos aquellos que se encuentran actualmente involucrados en las decisiones respecto de las redes de información y de sus modos de administración, al tiempo de alertar sobre la importancia crítica de la seguridad. Creo que un adecuado tratamiento de esta problemática resulta absolutamente vital, debido a las amenazas cada vez mayores a las que la información se encuentra expuesta.

En el transcurso de las diversas secciones se desarrollarán básicamente, los siguientes temas:

- El valor de los datos
- Las políticas de seguridad informática
- Los procedimientos para el resguardo de la información
- Los principales ataques a las redes de información
- Las contraseñas
- Las herramientas de control y seguimiento de accesos

El material cuenta, además, con un glosario final en el que se definen los principales términos que se utilizan durante este trabajo.

Esperamos que constituya un buen punto de partida para la reflexión y el debate sobre estas problemáticas en su organización.

RESUMEN

Los Protocolos de Seguridad de Internet (IPsec), actúan en la capa de red, la capa 3 del modelo OSI[3]. Otros protocolos de seguridad para Internet de uso extendido, como el SSL[4], el protocolo de seguridad TLS[5] y SSH[6] operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP[7] y UDP[8], los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código**.**

IPsec está implementado por un conjunto de protocolos criptográficos para (1) asegurar el flujo de paquetes, (2) garantizar la autenticación mutua y (3) establecer parámetros criptográficos.

La arquitectura de seguridad IP[9] utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para

[3] Modelo de referencia de Interconexión de Sistemas Abiertos
[4] Capa de Seguridad de los zócalos
[5] Protocolo de Seguridad para la capa de transporte
[6] Intérprete de órdenes seguras
[7] Protocolo de Control de Transmisión
[8] Protocolo del nivel de transporte basado en el intercambio de datagramas
[9] Protocolo de Internet

un paquete entrante se realiza un procedimiento similar; en este caso IPsec coge las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast[10], se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

En el caso de GRE[11], este toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, lo que implica que el paquete que se envía a través del túnel es de mayor longitud por lo que puede ocurrir que esté excediendo la longitud permitida en la interfaz física. Esto provoca el descarte de ese paquete. El enlace sobre el túnel GRE no requiere ninguna información de estado, por lo que puede ocurrir que un extremo del túnel se encuentre en estado de desactivado y el otro continúe presentándose como activo.

Y CET[12], por medio del Cisco IOS[13], utiliza algoritmos de cifrado que permite proteger la información de una infraestructura de red hacia los visitantes no deseados, sean estos hackers o crackers.

[10] Servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente
[11] Protocolo para el establecimiento de túneles a través de Internet
[12] Tecnología de Cifrado de Cisco
[13] Sistema de Cisco usado en dispositivos de enrutamiento

DEDICATORIA

"Dedico este proyecto y toda mi carrera universitaria a mis padres, ya que gracias a ellos soy quien soy hoy en día, fueron los que me dieron ese cariño y calor humano necesario, son los que han velado por mi salud, mis estudios, mi educación alimentación entre otros, son a ellos a quien les debo todo, horas de consejos , de regaños, de reprimendas de tristezas y de alegrías de las cuales estoy muy seguro que las han hecho con todo el amor del mundo para formarme como un ser integral y de las cuales me siento extremadamente orgulloso"

AGRADECIMIENTO

Quiero expresar mi agradecimiento

- A mis padres y hermanas por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos.

- A mi madre por su cariño, comprensión y constante estímulo, por su paciencia y por enseñarme a enfrentar los obstáculos con alegría.

- A mi Director de Tesis, Ing. Francisco Rodríguez por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia científica en un marco de confianza, afecto y amistad, fundamentales para la concreción de este trabajo.

- A los Ingenieros. Javier Cóndor y Alfredo Calderón, por sus valiosas sugerencias y acertados aportes durante el desarrollo de este trabajo.

- A mis ex - compañeros del COTAC por su continuo y afectuoso aliento.

- A mis ex – profesores del COTAC, por sus enseñanzas no he tenido problemas en la Universidad.

- A mis amigos y amigas actuales, quienes me ayudan con su apoyo, su comprensión y sobre todo me escuchan.

INDICE:

CAPÍTULO I. INTRODUCCIÓN Y CONCEPTOS GENERALES

1. INTRODUCCIÓN Y CONCEPTOS BÁSICOS

Una red de computadoras (también llamada red de Computadores o Red informática) es un conjunto de equipos.

La mayoría de los componentes de una red media son los Computadores individuales, generalmente son sitios de trabajo (incluyendo Computadores personales) o servidores.

Las redes de computadores se clasifican de la siguiente manera: Clasificación por la distancia (MAN[1], WAN[2], etc...), Redes privadas virtuales (de acceso, de intranet, de extranet), las intranets y extranet, redes cliente – servidor, entre otras.

1.1. ¿QUÉ ES UNA RED?

Una red de computadoras (también llamada red de Computadores o Red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

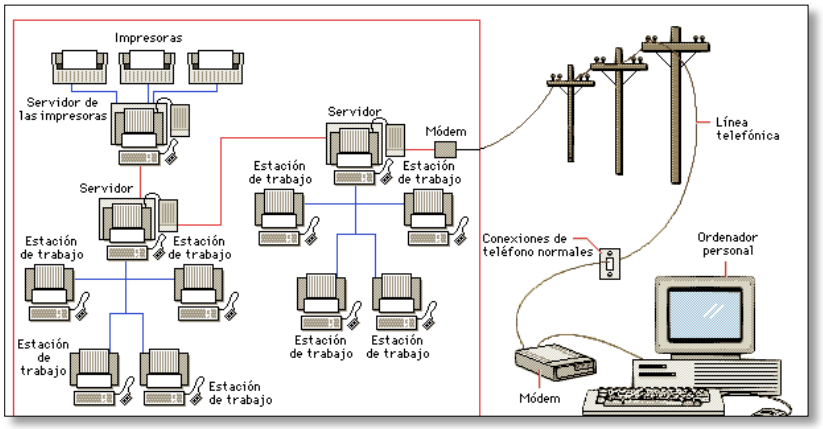

Figura I-1: Red de Computadores. **[B]**

[1] **MAN:** Red de Área Metropolitana
[2] **WAN:** Redes de Área Extendida.

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI[3] por la ISO[4], el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

Una intranet o una red interna se limitan en alcance a una sola organización o entidad. Generalmente ofrecen servicios como HTTP[5], FTP[6], SMTP[7], POP3[8] y otros de uso general.

En una intranet se pueden tener los mismos servicios que en Internet, pero éstos sólo quedan disponibles para los usuarios de esa red privada, no a los usuarios en general

1.2. COMPONENTES DE UNA RED

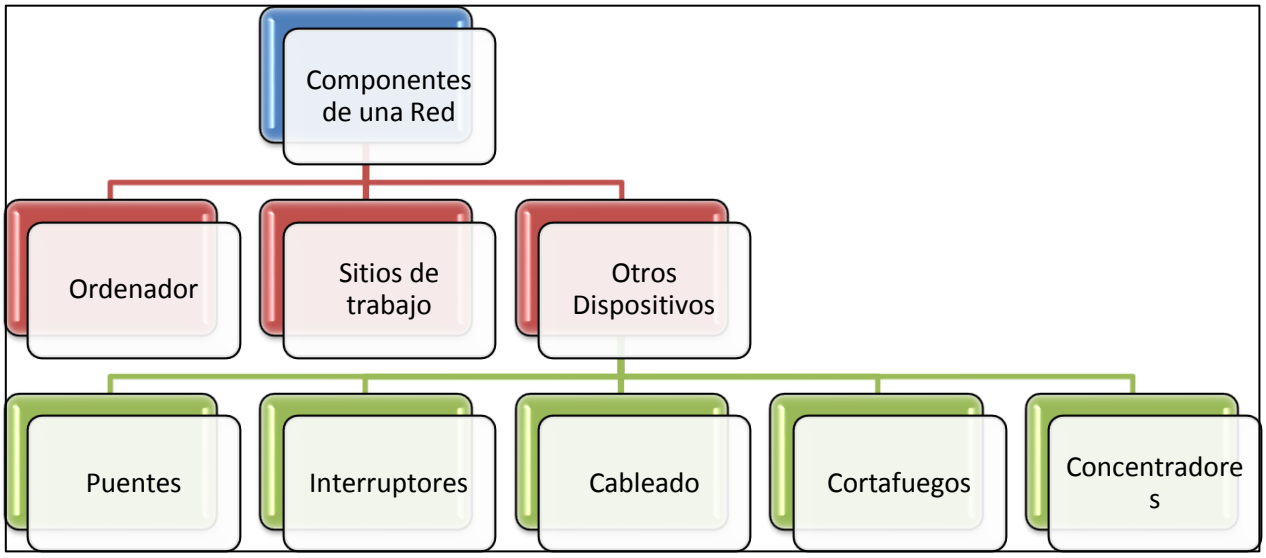

Figura I-2: Componentes de una red. **[A]**

1.3. EL COMPUTADOR

La mayoría de los componentes de una red media son los computadores individuales, generalmente son sitios de trabajo (incluyendo computadores personales) o servidores.

[3] **OSI:** Modelo de referencia de Interconexión de Sistemas Abiertos
[4] **ISO:** Organización de Estándares
[5] **HTTP:** Protocolo de transferencia de hipertexto
[6] **FTP:** Protocolo de Transferencia de Archivos
[7] **STMP:** Protocolo Simple de Transferencia de Correo
[8] **POP3:** (Post Office Protocol 3 - Protocolo 3 de Correo). Es un protocolo estándar para recibir mensajes de e-mail.

1.4. TIPOS DE SITIOS

Hay muchos tipos de sitios de trabajo que se pueden incorporar en una red particular, algo de la cual tiene sistemas con varios CPU, las cantidades grandes de RAM, las grandes cantidades de espacio de almacenamiento en disco duro, u otros componentes requeridos para las tareas de proceso de datos especiales, los gráficos, u otros usos intensivos del recurso.

1.5. TIPOS DE SERVIDORES

En las siguientes listas, hay algunos tipos comunes de servidores y de su propósito.

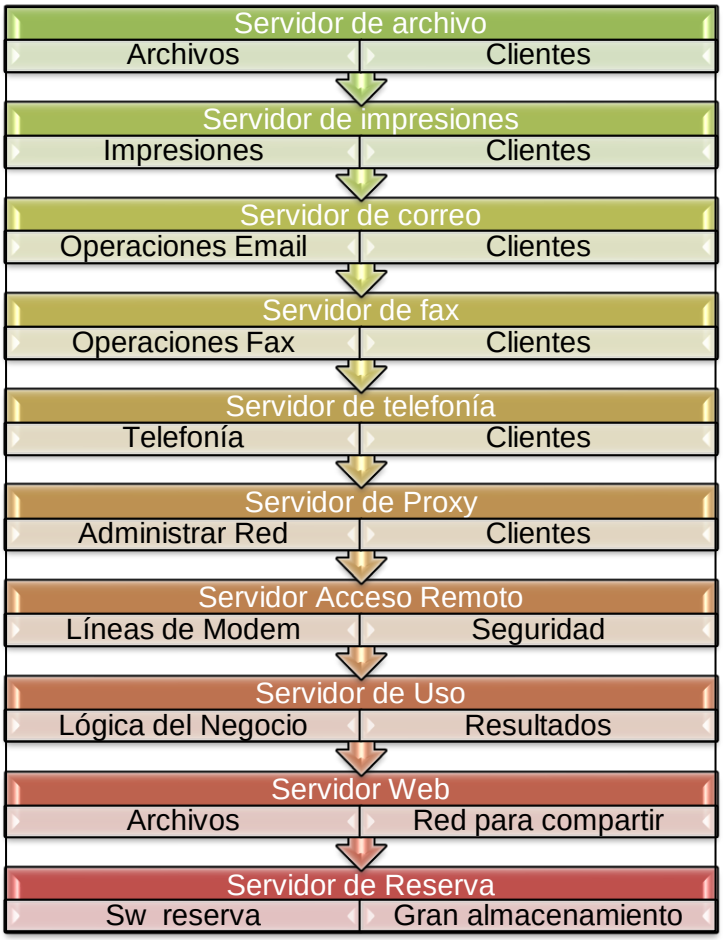

Figura I-3: Tipos de Servidores. **[A]**

1.6. IMPRESORAS

Muchas impresoras son capaces de actuar como parte de una red de Computadores sin ningún otro dispositivo, tal como un *"print server"*, a actuar como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión de ser terminado.

Figura I-4: Impresora. **[B]**

1.6.1. TERMINAL[9] TONTO

Muchas redes utilizan este tipo de equipos en lugar de puestos de trabajo para la entrada de datos. En estos sólo se exhiben datos o se introducen. Este tipo de terminales, trabajan contra un servidor, que es quien realmente procesa los datos y envía pantallas de datos a los terminales.

1.6.2. OTROS DISPOSITIVOS

Hay muchos otros tipos de dispositivos que se puedan utilizar para construir una red, muchos de los cuales requieren una comprensión de conceptos más avanzados del establecimiento de una red de la computadora antes de que puedan ser entendidos fácilmente (los puentes, los interruptores, los corta fuegos del hardware, etc.).

En las redes caseras y móviles, que conecta la electrónica de consumidor los dispositivos tales como consolas vídeo del juego está llegando a ser cada vez más comunes.

[9] **TERMINAL:** se refiere al dispositivo hardware usado para introducir o mostrar datos de una computadora.

1.7. TIPOS DE RED

Las redes de computadores se clasifican de la siguiente manera:

1.8. Clasificación por la distancia

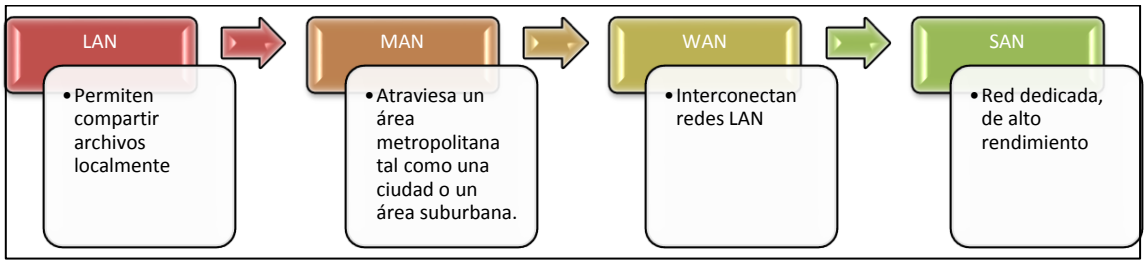

Figura I-5: Clasificación de las redes por la distancia. **[A]**

1.8.1. LAS REDES DE AREA LOCAL (LAN[10])

Las LAN consisten de los siguientes componentes:

Figura I-6: Dispositivos de LAN. **[A]**

1.8.2. LAS REDES DE AREA EXTENDIDA (WAN)

Las WAN interconectan LAN, lo que proporcionan acceso a las computadoras o a servidores de archivo en otras partes.

Debido a que las WAN conectan redes del usuario sobre un área geográfica grande, permiten que los negocios se comuniquen a través de grandes distancias. Usar WAN permite compartir las computadoras, las impresoras, y otros dispositivos en una LAN con localidades distantes.

[10] **LAN:** Redes de Área Local

El software de colaboración proporciona el acceso a la información y a los recursos en tiempo real lo que permite tener reuniones remotamente, en vez de forma presencial.

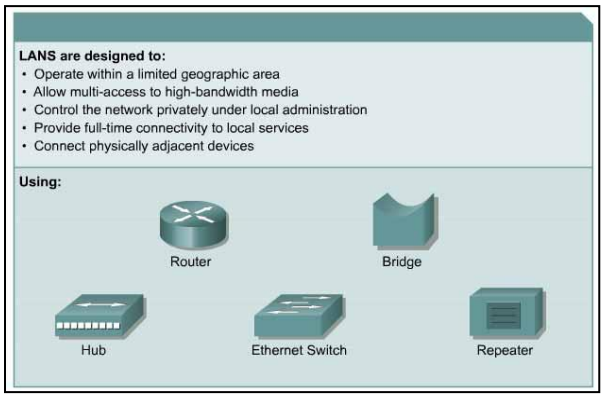

Figura I-7: Dispositivos para interconectar redes LAN. **[1]**

El establecimiento de las WAN también ha creado a una nueva clase de trabajadores llamados tele trabajadores[11], la gente que nunca tiene que salir de sus hogares para ir a trabajar.

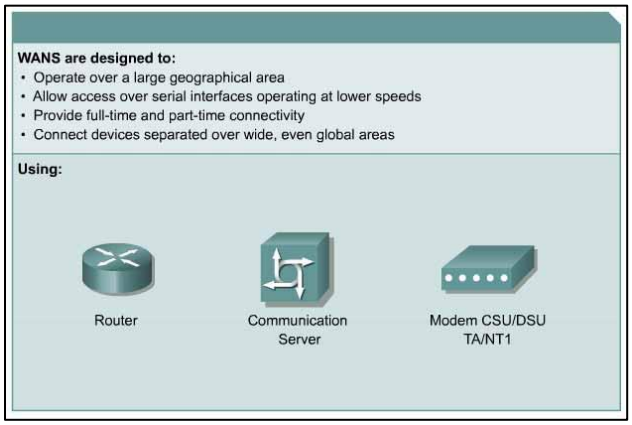

Figura I-8: Dispositivos para interconectar redes WAN. **[1]**

1.8.3. LAS REDES DE AREA METROPOLITANA (MAN)

Una MAN es una red que atraviesa un área metropolitana tal como una ciudad o un área suburbana. Una MAN consiste generalmente de dos o más LAN en un área geográfica común. Por ejemplo, un banco con varias agencias puede utilizar una MAN. Típicamente,

[11] **Tele trabajadores:** Personas que trabajan a través de la red

un proveedor de servicio se utiliza para conectar dos o más LAN usando líneas de comunicación privadas o servicios ópticos.

Una MAN puede también ser creada usando tecnología wireless[12] emitiendo señales a través de áreas públicas.

1.8.4. LAS REDES DE ALMACENAMIENTO (SAN[13])

Una SAN es una red dedicada[14], de alto rendimiento usada para mover datos entre los servidores y los recursos del almacenaje.

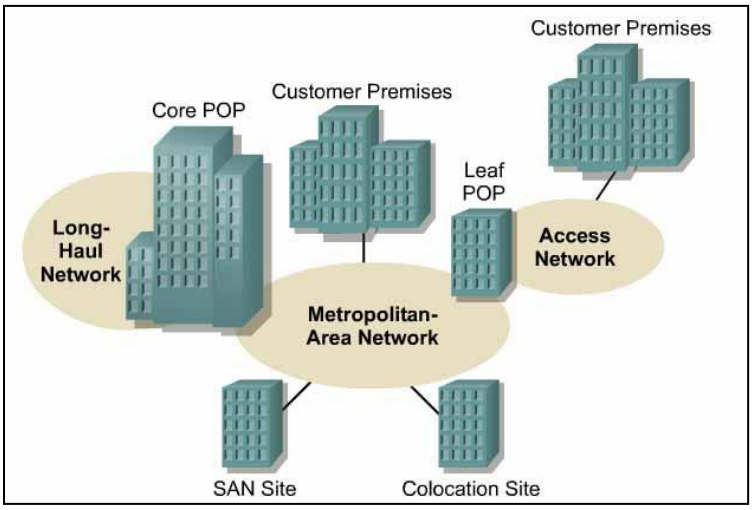

Figura I-9: Ejemplo de una red de área metropolitana. **[1]**

La tecnología de las SAN permite conectividad de alta velocidad.

[12] **WIRELESS:** Tipo de comunicación en la que no se utiliza un medio de propagación físico
[13] **SAN:** Red de almacenamiento
[14] **RED DEDICADA:** Es una denominación que usualmente se reserva para redes de comunicaciones en las cuáles existe un único tipo de tráfico con objetivos de calidad establecidos explícitamente en el contrato entre el operador y el usuarios.

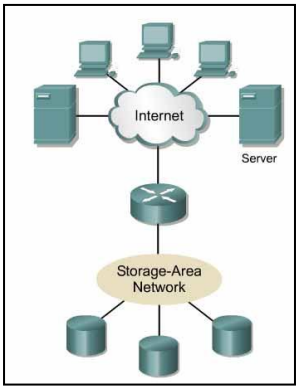

Figura I-10: Ejemplo de una red de almacenamiento SAN. **[1]**

Este método utiliza una infraestructura de la red separada que alivia cualquier problema asociado con conectividad existente de la red.

Las redes SAN ofrecen las siguientes características:

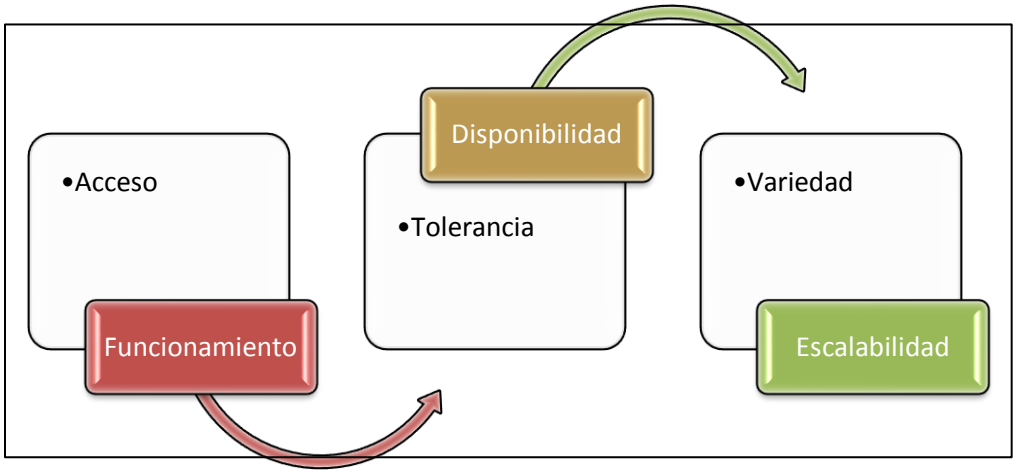

Figura I-11: Características SAN. **[1]**

1.8.5. REDES PRIVADAS VIRTUALES (VPN[15])

Las redes privadas virtuales se crean en infraestructuras públicas y además pueden ser de intranet, de acceso y de extranet.

[15] **VPN:** Redes Privadas Virtuales

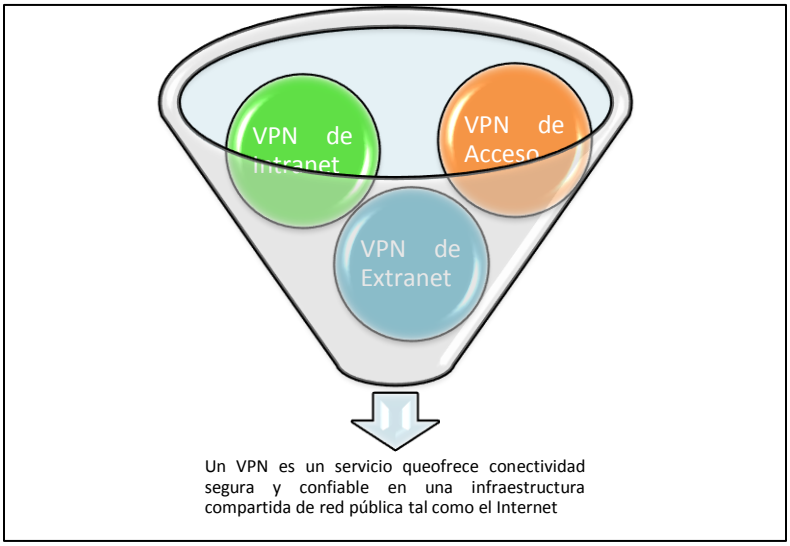

Figura I-12: Tipos de VPN. **[A]**

1.9. INTRANETS Y EXTRANETS

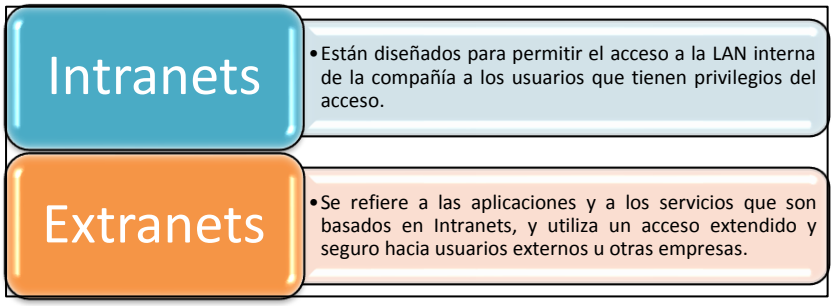

Figura I-13: Intranets y Extranets. **[A]**

Los Intranets están diseñados para permitir el acceso a la LAN interna de la compañía a los usuarios que tienen privilegios del acceso. Dentro de un Intranet, los servidores web están instalados dentro de la red.

Los browsers utilizan el FRONT END [16]para el acceso a la información.

Las extranets se refieren a las aplicaciones y a los servicios que son basados en Intranets, y utiliza un acceso extendido y seguro hacia usuarios externos u otras empresas.

[16] **FRONT END:** Parte que sirve para interactuar con los usuarios

Este acceso se logra generalmente con contraseñas, identificaciones de usuario, y la otra seguridad a nivel de aplicación. Por lo tanto, una Extranet es la extensión de dos o más estrategias del Intranet con una interacción segura entre las empresas participantes y sus intranets respectivas.

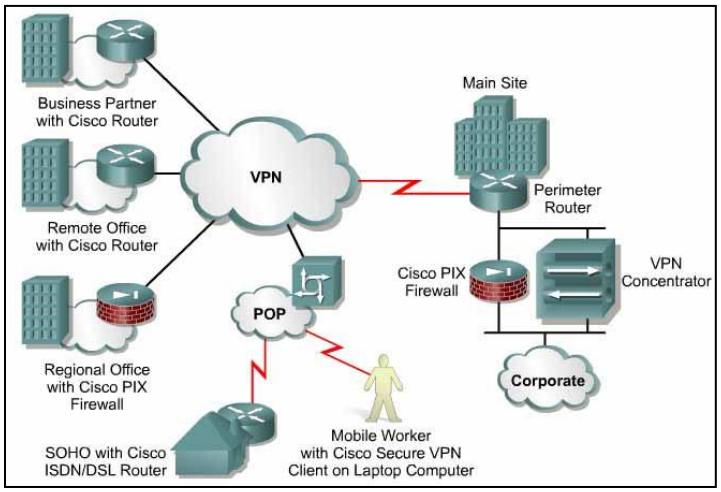

Figura I-14: Funcionamiento de una Intranet. **[1]**

1.10. REDES ALÁMBRICAS E INALÁMBRICAS

Alámbricas	Inalámbricas
•Son frecuentes las tecnologías que usan la línea telefónica como xDSL o ISDN.	•Se utiliza el modo basado en satélites y el modo de BWLL (Broadband Wireless Local Loop), (se ha comercializado también la suscripción a la red que usa comunicación láser).

Figura I-15: Redes alámbricas e inalámbricas. **[A]**

1.11. CLASIFICACIÓN SEGÚN SU DISTRIBUCIÓN LÓGICA

Todos los Computadores tienen un lado cliente y otro servidor: una máquina puede ser servidor de un determinado servicio pero cliente de otro servicio.

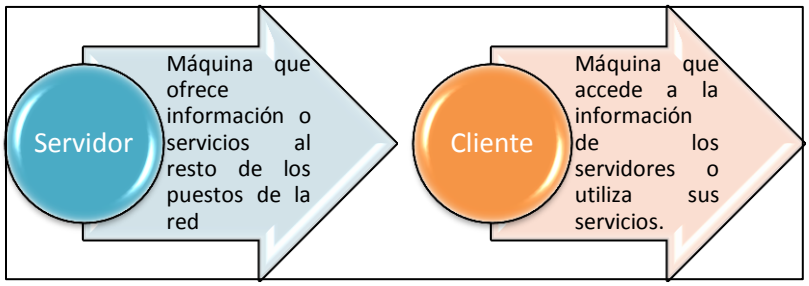

Figura I-16: Distribución lógica de las redes cliente-servidor. **[A]**

1.11.1. SERVIDOR

Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de IRC (charlas en Internet), de base de datos.

1.11.2. CLIENTE

Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un Computador remoto en la red (el servidor que tiene la impresora conectada).

1.12. REDES HFC[17] Y EL ESTANDAR DOCSIS[18]

Figura I-17: Redes HFC y DOCSIS. **[A]**

Las redes HFC nacieron como una evolución de las antiguas redes CATV [19]o Televisión de Antena Comunitaria (Community Antenna Television) o simplemente televisión por

[17] **HFC:** Redes híbridas de fibra y coaxial.
[18] **DOCSIS:** Especificación de Interfaz de Servicios de Datos Por Cable.
[19] **CATV**: Redes de televisión de Antena Comunitaria.

cable. Las redes CATV se desarrollaron desde 1949 hasta 1988. Estas redes nacieron para resolver problemas de recepción en zonas de mala cobertura por medio de una antena que se ubicaba en un sitio elevado con buena recepción y la señal se la enviaba hacia los usuarios hacia abajo (downstream). Estas redes utilizaban un cable coaxial de 75Ω, lo cual es lo normal de una antena de TV, y amplificadores cada 0.5 a 1 Km puestos en cascada hasta un máximo de 50. Estas redes son redes unidireccionales, es decir que la señal sólo es descendente ya que los amplificadores impedían la transmisión ascendente.

Debido a los avances de tecnología, el incremento de usuarios y mayor oferta de servicios se comenzaron a desarrollar las redes HFC a partir de 1988. Estas redes dividían la ciudad en zonas de entre 500 y 2000 viviendas y se envía la señal a cada zona por fibra para luego distribuirla en coaxial sólo dentro de la zona; aquí se limitaba a un máximo de 5, el número de amplificadores en cascada. Entre las ventajas de estas redes se encontraba que la reducción drástica en el número de amplificadores, simplificaba y abarataba el mantenimiento mejorando la calidad de la señal; cada zona podía tener canales independientes y también permitirá a la red ser bidireccional, ya que se instalaban amplificadores para tráfico ascendente. La mayoría de las redes CATV actuales son HFC. En los últimos años, la estandarización de las redes HFC se ha hecho a través del estándar DOCSIS.

1.13. TOPOLOGÍAS DE RED

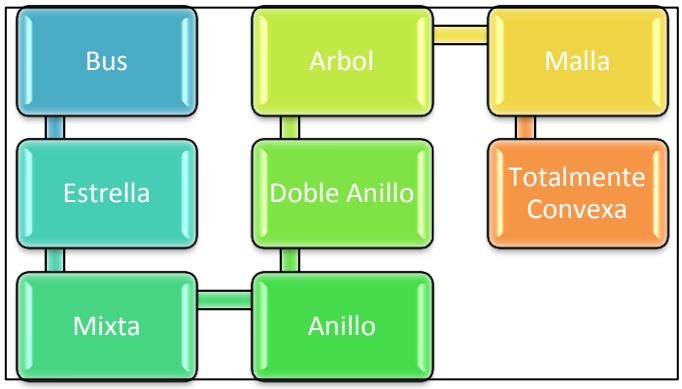

Figura I-18: Topologías de red más comunes. **[A]**

La topología de red es la disposición física en la que se conecta una red de Computadores.

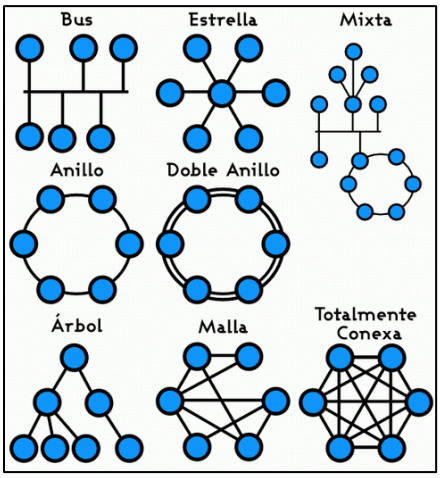

Figura I-19: Gráficos de las topologías de red. **[4]**

Las topologías físicas que se utilizan comúnmente son:

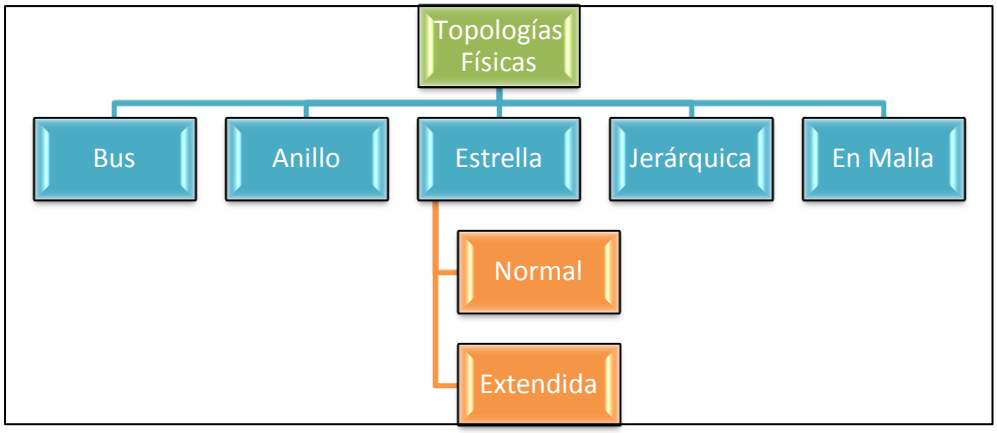

Figura I-20: Topologías Físicas. **[A]**

- **Topología de bus:** Utiliza un solo cable como backbone que termina en ambos extremos. Todos los hosts se conectan directamente con este backbone.

- **Topología de anillo**: conecta un host con el host siguiente. Esto crea un anillo físico de cable.

- **Topología de estrella**: conecta todos los cables con un punto central de la concentración.

- **Topología de estrella extendida**: une las estrellas individuales conectando los hubs y/o switches. Esta topología puede ampliar el alcance y cobertura de la red.

- **Topología jerárquica** es similar a una estrella extendida. Sin embargo, en vez de ligar los hubs y/o switches, el sistema se liga a una computadora que controle el tráfico en la topología.

- **Topología en malla:** Cada anfitrión tiene sus propias conexiones al resto de los anfitriones. Se pone en ejecución para proporcionar tanta protección como sea posible contra la interrupción del servicio.

La topología lógica de una red es cómo los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast o difusión y paso de tokens o testigo.

- La topología de “broadcast”, significa simplemente que cada host envía sus datos al resto de los hosts en el medio de la red. No hay un orden que las estaciones deban seguir para utilizar la red. El primero que viene, el primero que se sirve. Ejemplo de esta topología lógica es Ethernet

- El paso de “token”, controla el acceso a la red pasando un token electrónico secuencialmente a cada host. Cuando un host recibe el token, ese host puede enviar datos a través de la red.

1.14. REDES FUTURAS

Desde el punto de vista tecnológico, las redes de banda ancha vienen soportadas por tecnologías de naturaleza muy diversa, cuyas prestaciones técnicas, costes y aplicaciones varían sensiblemente de unas a otras.

En cuanto a las tecnologías cableadas, las tecnologías más introducidas actualmente son la ADSL y el cable. Otro escenario en el que se percibe un proceso gradual de convergencia tecnológica es el correspondiente al entorno doméstico, para el cual se pronostica una evolución progresiva hacia el denominado "hogar digital". Estos dispositivos por otra parte no viven aislados sino que tienden a interconectarse formando redes de telecomunicaciones en el hogar.

A modo de ejemplo puedo citar diferentes tecnologías que permiten esta interconexión de dispositivos en el hogar como Bluetooth[20] , CEBus[21] , HAVi[22] , HomePNA[23] , HomeRF[24] , LONWORKS[25] o UPnP[26]

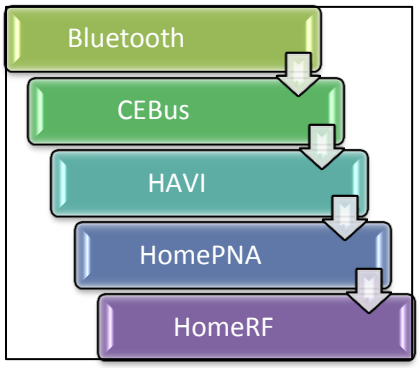

Figura I-21: Tecnologías Futuras de redes. **[A]**

Para más adelante se vislumbra la introducción de las tecnologías UWB[27], en el entorno doméstico, y WiMAX[28] para las comunicaciones inalámbricas a alta velocidad en el ámbito metropolitano. Sea cual sea la tecnología elegida, los expertos consideran que todas ellas

[20] **BLUETOOTH:** Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN).
[21] **CEBUS:** Protocolo de comunicación (Consumer Electronics Bus) es un estándar vigente en los Estados Unidos
[22] **HAVI:** Home Audio/Video Interoperativity", permitirá a los dispositivos Havi conectarse a redes
[23] **HOMEPNA:** Alianza de varias empresas que trabajan en el desarrollo de una tecnología que permita implementar redes
[24] **HOMERF:** Es una solución de redes inalámbricas para hogares "inteligentes": un sistema que permite a las familias y a las pequeñas oficinas u oficinas domésticas experimentar la libertad del acceso rápido a Internet, simultáneo e inalámbrico desde cualquier lugar de la casa.
[25] **LONWORKS:** Tecnología basada en el protocolo LonTalk que proporciona todas las herramientas para la implementación de redes de control distribuidas.
[26] **UPNP:** Conectar y Usar Universal, es una arquitectura software abierta y distribuida que de forma independiente al fabricante, sistema operativo, lenguaje de programación, etc. permite el intercambio de información y datos a los dispositivos conectados a una red
[27] **UWB:** Se define como un dispositivo de intercambio personal con el que podrás intercambiar con tus conocidos y de forma inalámbrica documentos
[28] **WIMAX:** Son las siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas). Es una norma de transmisión

coexistirán en mayor o menor grado en el futuro, dependiendo de las circunstancias y el entorno en que se encuentren los usuarios.

La implantación en la Unión Europea y en otras muchas áreas del mundo de la telefonía móvil de segunda generación (2G) ha constituido sin duda una historia de éxito, como es bien conocido. La implantación de la cuarta generación (4G), por su parte, tendrá lugar más allá de la próxima década.

Su introducción será que los usuarios puedan disfrutar y sacar partido de unas aplicaciones multimedia todavía más ricas en prestaciones, gracias a su gran capacidad y ancho de banda. En la 4G es la tecnología de acceso inalámbrico mediante ondas de radio. Ésta ha sido probada con transferencias de 1 Gbps a 20km/h.

El 4G proporcionará un ambiente donde las conexiones podrán operar entre sí, para proporcionar la sensación de interacción en tiempo real con los distintos servicios multimedia como vídeo de alta calidad y videoconferencia.

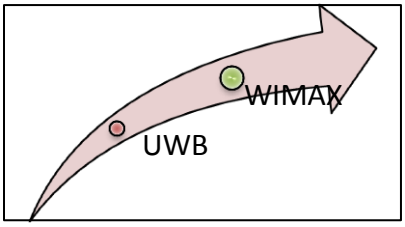

Figura I-22: Tendencia en las Comunicaciones Inalámbricas. **[A]**

CAPÍTULO II. PROTOCOLOS

2. PROTOCOLOS DE RED

Un conjunto de protocolos de red permiten la comunicación de la red a partir de un host pasando a través de la red hacia otro host. Un protocolo es una descripción formal de un sistema de reglas y las convenciones que gobiernan el aspecto particular de cómo los dispositivos en una red se comunican.

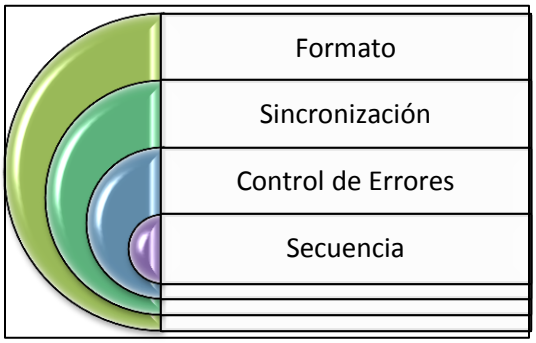

Figura II-1: Propiedades de los Protocolos. **[A]**

Sin protocolos, la computadora no puede reconstruir la corriente de bits entrantes desde otra computadora en el formato original que fueron transmitidos.

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluyen el siguiente:

- cómo se construye la red física
- cómo las computadoras se conectan a la red
- cómo los datos se ajustan a un formato para la transmisión
- cómo se envían esos datos
- cómo ocuparse de errores

Estas reglas de red son creadas y mantenidas por muchas y diversas organizaciones y comités.

2.1. PROTOCOLOS BÁSICOS DE RED

Los protocolos son reglas y procedimientos para la comunicación. El término «protocolo» se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

2.2. CÓMO FUNCIONAN LOS PROTOCOLOS

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos discretos, sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo.

2.3. EL EQUIPO ORIGEN

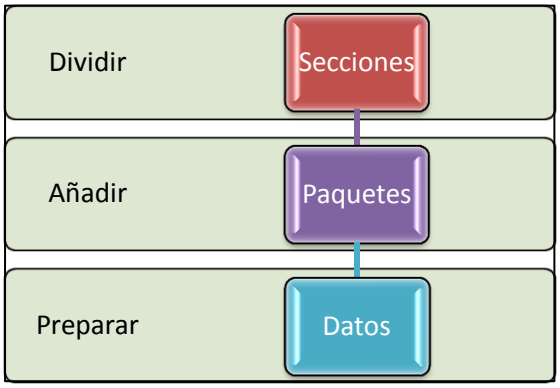

Figura II-2: Pasos del equipo origen. **[A]**.

Los protocolos en el equipo origen:

1. Se dividen en secciones más pequeñas, denominadas paquetes.
2. Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.

3. Prepara los datos para transmitirlos a través de la NIC[29]

2.4. EL EQUIPO DE DESTINO

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

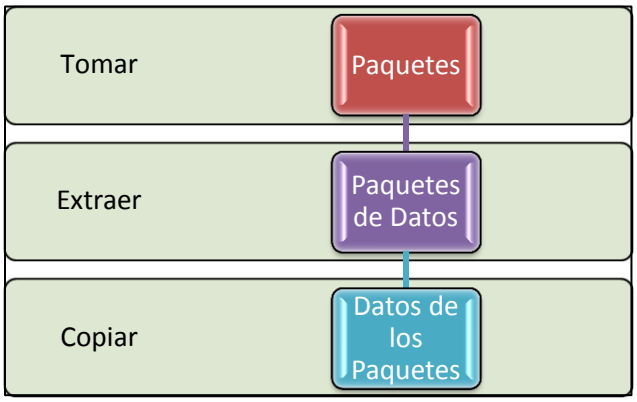

Figura II-3: Pasos del equipo destino. **[A]**

1. Toma los paquetes de datos del cable y los introduce en el equipo a través de la NIC.
2. Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
3. Copia los datos de los paquetes en un búfer para reorganizarlos enviarlos a la aplicación.

2.5. JERARQUÍAS DE PROTOCOLOS

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación.

Cada nivel tiene su propio conjunto de reglas. Los protocolos definen las reglas para cada nivel en el modelo OSI:

[29] **NIC:** Se denomina también NIC al chip de la tarjeta de red que se encarga de servir como interfaz de Ethernet entre el medio físico (por ejemplo un cable coaxial)

Nivel de aplicación	Inicia o acepta una petición
Nivel de presentación	Añade información de formato, presentación y cifrado al paquete de datos
Nivel de session	Añade información del flujo de tráfico para determinar cuándo se envía el paquete
Nivel de transporte	Añade información para el control de errores
Nivel de red	Se añade información de dirección y secuencia al paquete
Nivel de enlace de datos	Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física
Nivel físico	El paquete se envía como una secuencia de bits

Tabla II-1: Jerarquía de Protocolos. **[A]**

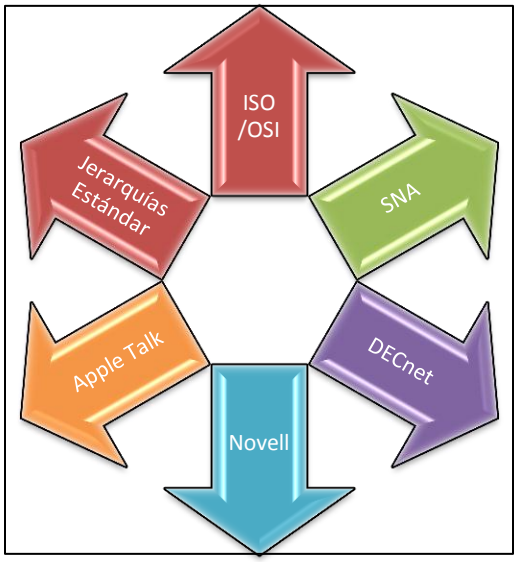

Figura II-4: Jerarquías Estándar de Protocolos. **[A]**

2.6. PROTOCOLOS DE APLICACIÓN

Entre los protocolos de aplicación más conocidos, tenemos los siguientes, según lo muestra la figura:

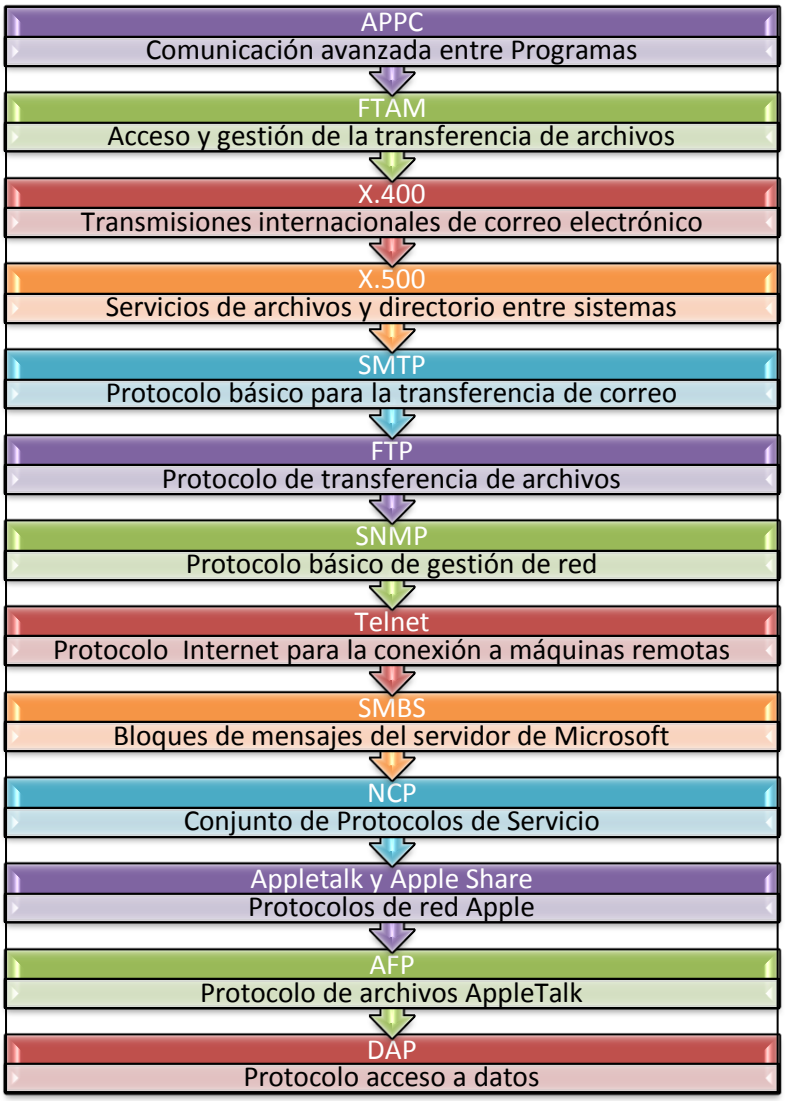

Figura II-5: Protocolos de Aplicación. **[A]**

Los protocolos de aplicación trabajan en el nivel superior del modelo de referencia OSI[30] y proporcionan interacción entre aplicaciones e intercambio de datos.

2.7. PROTOCOLOS DE TRANSPORTE

Los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

[30] **OSI:** El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) fue el modelo de red descriptivo

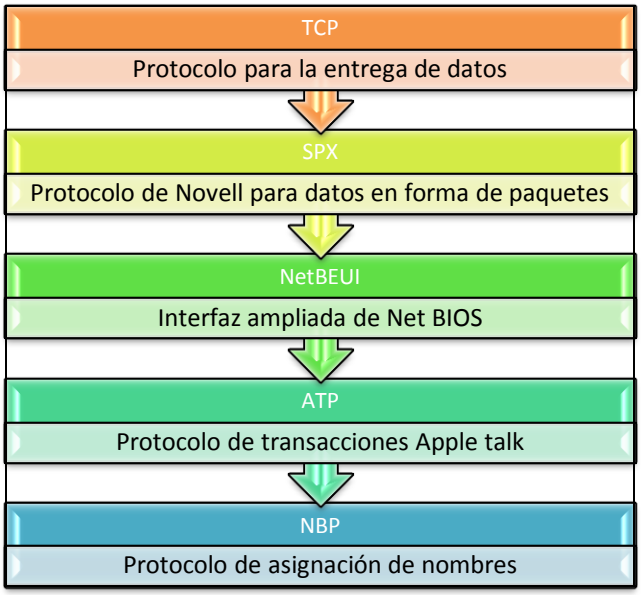

Figura II-6: Protocolos de Transporte. **[A]**

2.8. PROTOCOLOS DE RED

Los protocolos de red proporcionan lo que se denominan «servicios de enlace». Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

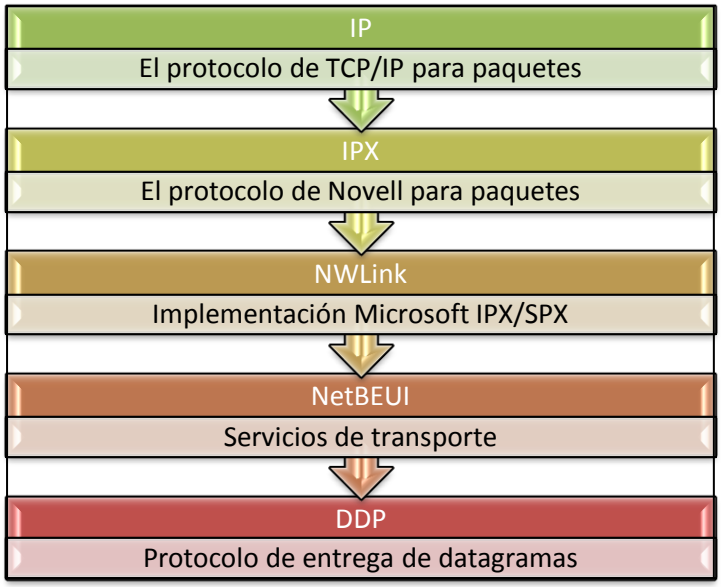

Figura II-7: Protocolos de Red. **[A]**

2.9. ESTÁNDARES DE PROTOCOLO

El modelo OSI se utiliza para definir los protocolos que se tienen que utilizar en cada nivel. Los productos de distintos fabricantes que se ajustan a este modelo se pueden comunicar entre sí.

La ISO, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ANSI (Instituto de Estandarización Nacional Americano), CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía), ahora llamado ITU (Unión Internacional de Telecomunicaciones) y otros organismos de estandarización han desarrollado protocolos que se correspondan con algunos de los niveles del modelo OSI.

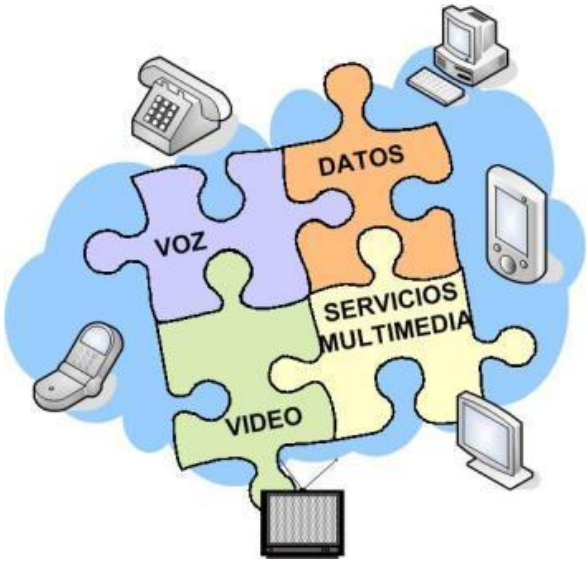

Figura II-8: Servicios varios en una Red. **[C]**

Un controlador MAC[31] está situado en el subnivel de Control de acceso al medio; este controlador de dispositivo es conocido como controlador de la NIC. Proporciona acceso a bajo nivel a los adaptadores de red para proporcionar soporte en la transmisión de datos y algunas funciones básicas de control del adaptador.

El IEEE[32] definió estos protocolos para facilitar la comunicación en el subnivel de Control de acceso al medio (MAC).

[31] **MAC:** En redes de computadoras la dirección MAC (siglas en inglés de Media Access Control o control de acceso al medio) es un identificador de 48 bits

[32] **IEEE:** Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos

Los protocolos de IEEE a nivel físico son:

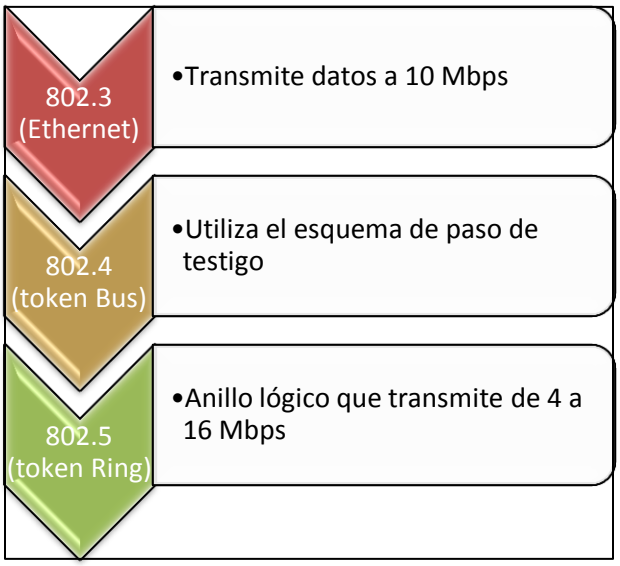

Figura II-9: Protocolos IEEE. **[A]**

2.10. TCP/IP

El Protocolo de control de transmisión/Protocolo Internet (TCP/IP[33]) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas.

TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes.

[33] **TCP/IP**: Son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés Transmission Control Protocol/Internet Protocol),

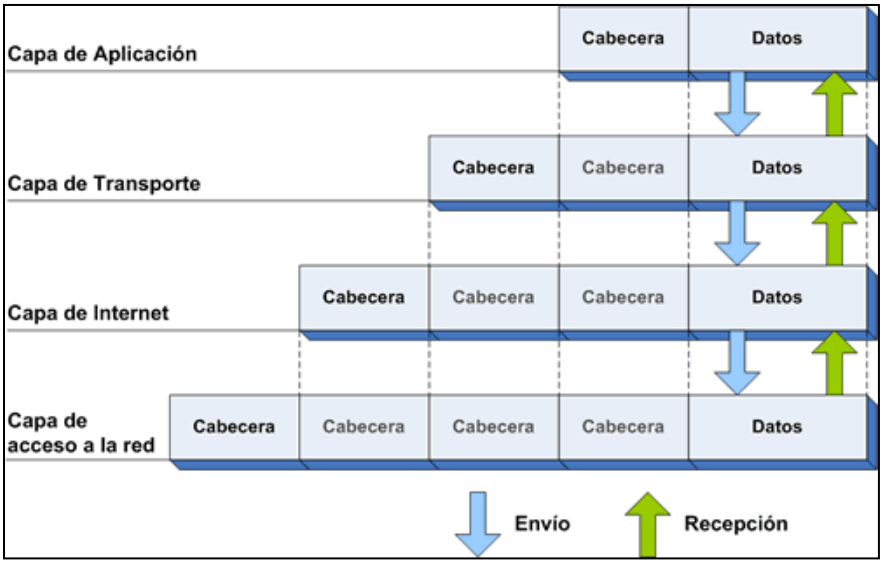

Figura II-10: Encapsulación TCP/IP. **[4]**

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

.

Figura II-11: Protocolos Generales TCP/IP. **[A]**

Diseñado para ser encaminable, robusto y funcionalmente eficiente, TCP/IP fue desarrollado por el Departamento de Defensa de Estados Unidos como un conjunto de protocolos para redes de área extensa (WAN).

Su propósito era el de mantener enlaces de comunicación entre sitios en el caso de una guerra nuclear.

Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet.

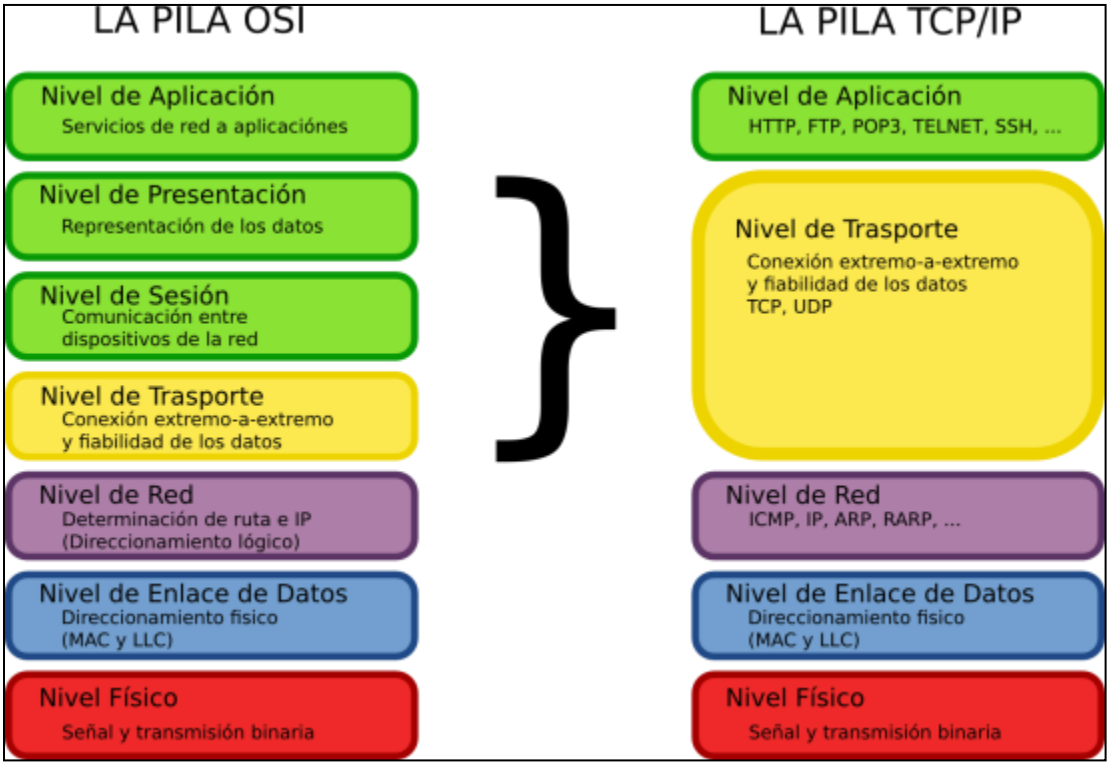

Figura II-12: Modelo OSI vs TCP/IP. **[4]**

La utilización de TCP/IP ofrece varias ventajas:

- **Es un estándar en la industria.** Como un estándar de la industria, es un protocolo abierto. Esto quiere decir que no está controlado por una única compañía, y está menos sujeto a cuestiones de compatibilidad. Es el protocolo, de hecho, de Internet.

- **Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes.** La conectividad entre un equipo y otro no depende del sistema operativo de red que esté utilizando cada equipo.

- **Utiliza una arquitectura escalable, cliente/servidor.** TCP/IP puede ampliarse (o reducirse) para ajustarse a las necesidades y circunstancias futuras. Utiliza sockets para hacer que el sistema operativo sea algo transparente.

2.11. SISTEMA BÁSICO DE ENTRADA/SALIDA EN RED

La mayoría de los servicios y aplicaciones que se ejecutan en el sistema operativo Windows utilizan la interfaz NetBIOS[34] o la Comunicación entre procesos (IPC[35]). NetBIOS se desarrolló sobre LAN y se ha convertido en una interfaz estándar para que las aplicaciones puedan acceder a los protocolos de red en el nivel de transporte con comunicaciones orientadas y no orientadas a la conexión. Existen interfaces NetBIOS para NetBEUI[36], NWLink[37] y TCP/IP. Las interfaces NetBIOS necesitan una dirección IP y un nombre NetBIOS para identificar de forma única a un equipo.

NetBIOS realiza cuatro funciones importantes:

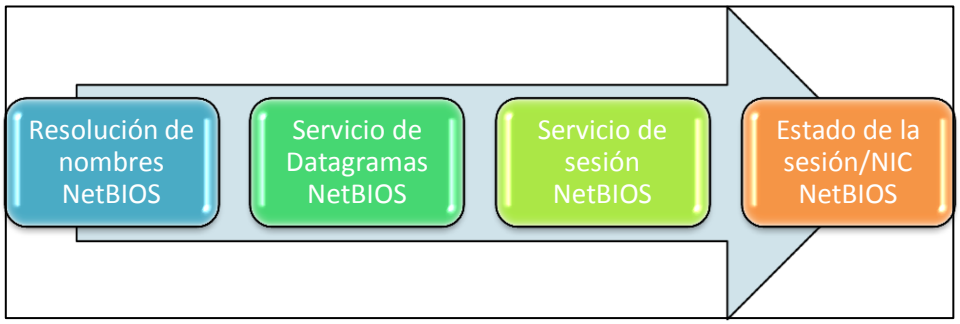

Figura II-13: Funciones NetBIOS. **[A]**.

Originalmente, IBM[38] ofrecía NetBIOS como un producto separado, implementado como un programa residente (TSR). Actualmente, este programa TSR es obsoleto; si se encuentra uno de estos sistemas, debería sustituirlo con la interfaz NetBIOS de Windows.

2.12. PROTOCOLO INTERNET (IP)

El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento. Cuando se transmite un paquete, este protocolo

[34] **NETBIOS:** "Network Basic Input/Output System", es, en sentido estricto, una especificación de interfaz para acceso a servicios de red.
[35] **IPC:** Comunicación entre procesos
[36] **NetBEUI:** (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sin encaminamiento
[37] **NWLINK:** es la implementación de Microsoft del protocolo IPX/SPX de Novell Netware. NWLink se usa normalmente en entornos donde los clientes
[38] **IBM:** International Business Machines o IBM (NYSE: IBM) (conocida coloquialmente como el Gigante Azul) es una empresa multinacional

añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico. IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor.

Figura II-14: Representación simbólica del Protocolo IP. **[C]**

Además, IP es el responsable del empaquetado y división de los paquetes requerido por los niveles físicos y de enlace de datos del modelo OSI. Cada paquete IP está compuesto por una dirección de origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un TTL (tiempo de vida, del inglés *time to live).* El TTL indica a cada uno de los routers de la red entre el origen y el destino cuánto tiempo le queda al paquete por estar en la red. Funciona como un contador o reloj de cuenta atrás.

Cuando el paquete pasa por el router, éste reduce el valor en una unidad (un segundo) o el tiempo que llevaba esperando para ser entregado. Por ejemplo, si un paquete tiene un TTL de 128, puede estar en la red durante 128 segundos o 128 saltos (cada parada, o router, en la red), o una combinación de los dos. El propósito del TTL es prevenir que los paquetes perdidos o dañados (como correos electrónicos con una dirección equivocada) estén vagando en la red. Cuando la cuenta TTL llega a cero, se retira al paquete de la red.

2.13. PROTOCOLOS DE RESOLUCION DE DIRECCIONES (ARP[39])

Antes de enviar un paquete IP a otro host se tiene que conocer la dirección hardware de la máquina receptora.

[39] **ARP:** Address Resolution Protocol (protocolo de resolución de direcciones) para la resolución de direcciones en informática

El ARP determina la dirección hardware (dirección MAC) que corresponde a una dirección IP. Si ARP no contiene la dirección en su propia caché, envía una petición por toda la red solicitando la dirección.

2.14. PROTOCOLO INVERSO DE RESOLUCIÓN DE DIRECCIONES (RARP[40])

Un servidor RARP mantiene una base de datos de números de máquina en la forma de una tabla (o caché) ARP que está creada por el administrador del sistema. A diferencia de ARP, el protocolo RARP proporciona una dirección IP a una petición con dirección de hardware.

2.15. PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET (ICMP[41])

El ICMP es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo. Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Si el flujo de datos es demasiado rápido para un router, pide a los otros routers que reduzcan la velocidad de transmisión.

[40] **RARP:** Concepto del término rarp: (Reverse Address Resolution Protocol - Protocolo de Resolución de Dirección de Retorno). Protocolo de bajo nivel.

[41] **ICMP:** El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación

CAPÍTULO III. PROTOCOLOS DE SEGURIDAD

3. DEFINICIONES DE IPSEC, GRE Y CET

IPSEC fue proyectado para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes, en el que los Computadores de los extremos finales realizan el procesado de seguridad, o en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo. Dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de IPSEC: modo transporte y modo túnel.

3.1. IPSEC

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPSEC también incluye protocolos para el establecimiento de claves de cifrado

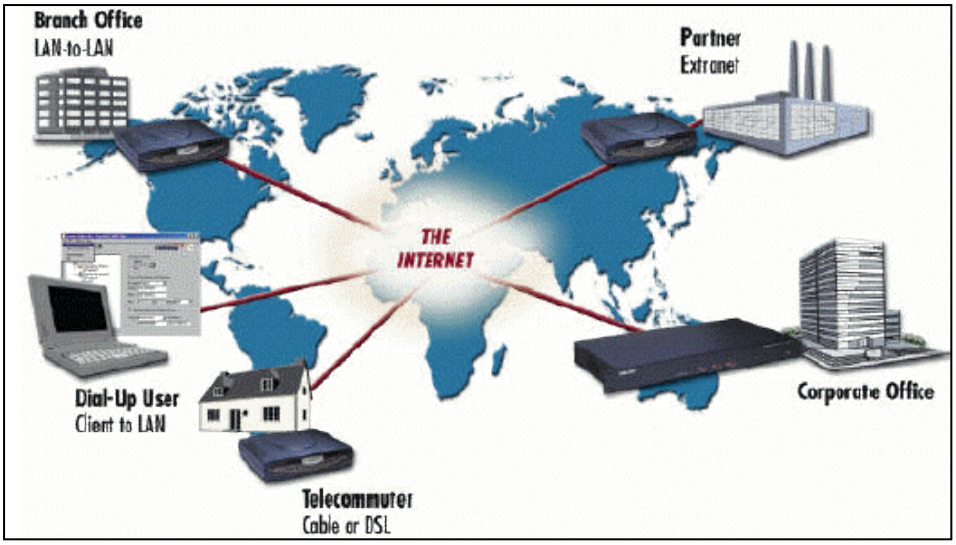

Figura III-1: Redes usando IPSEC. **[5]**

Es un conjunto de estándares abiertos desarrollados por el Internet Engineering Task Force (IETF[42]). Ofrece protección en la transmisión de información sensible sobre redes

[42] **IETF:** Grupo de Trabajo en Ingeniería de Internet, es una organización internacional abierta de normalización

inseguras tal como es la propia Internet. IPSEC actúa en la capa de red, protegiendo y autentificando paquetes IP entre los dispositivos participantes.

3.1.1. ESTRUCTURA DE IPSEC

IPSEC tiene tres componentes principales:

Figura III-2: Componentes IPSEC. **[A]**

El IPSEC entre sus características tiene:

- Interoperabilidad.
- Independiente de algoritmos criptográficos actuales.
- Soporta tanto IPv4[43] como IPv6 [44]
- Es una componente obligada en IPv6.

3.1.2. ARQUITECTURA IPSEC

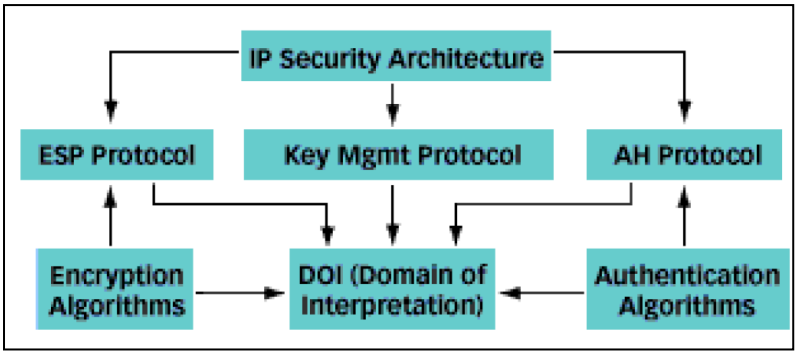

Figura III-3: Arquitectura IPSEC. **[5]**

Los protocolos de IPSEC actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL[45], TLS[46] y SSH[47]

[43] **IPV4:** Es la versión 4 del Protocolo IP (Internet Protocol).
[44] **IPV6:** El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4).

operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPSEC sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP[48] y UDP, los protocolos de capa de transporte más usados. IPSEC tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPSEC no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código**.**

IPSEC está implementado por un conjunto de protocolos criptográficos para (1) asegurar el flujo de paquetes, (2) garantizar la autenticación mutua y (3) establecer parámetros criptográficos.

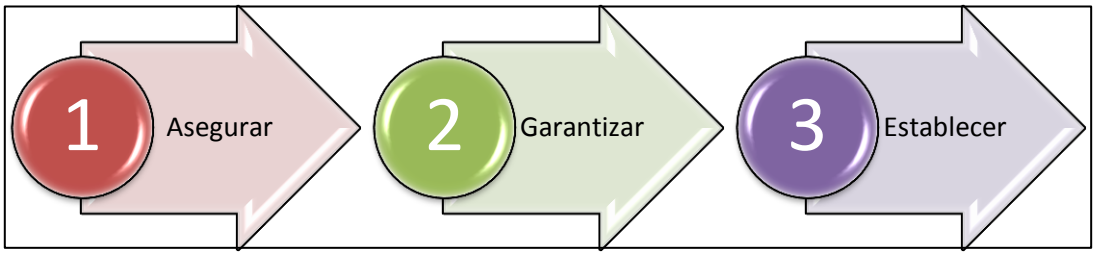

Figura III-4: Funciones de los protocolos criptográficos de IPSEC. **[A]**

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPSEC.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPSEC utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que

[45] **SSL:** Protocolo de Capa de Conexión Segura.
[46] **TLS:** Seguridad de la Capa de Transporte- (TLS), su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
[47] **SSH:** Secure Shell, en español: intérprete de órdenes seguro, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas
[48] **TCP:** (Transmission-Control-Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet

juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPSEC coge las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs[49], y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

IPSEC es una parte obligatoria de IPv6, y su uso es opcional con IPv4. Aunque el estándar está diseñado para ser indiferente a las versiones de IP, el despliegue y experiencia hasta 2007 atañe a las implementaciones de IPv4.

Los protocolos de IPSEC se definieron originalmente en las RFC[50]s 1825 y 1829, publicadas en 1995. En 1998 estos documentos fueron sustituidos por las RFCs 2401 y 2412, que no son compatibles con la 1825 y 1829, aunque son conceptualmente idénticas. En diciembre de 2005 se produjo la tercera generación de documentos, RFCs 4301 y 4309. Son en gran parte un superconjunto de la 2401 y 2412, pero proporcionan un segundo estándar de Internet Key Exchange. Esta tercera generación de documentos estandarizó la abreviatura de IPSEC como "IP" en mayúsculas y "sec" en minúsculas.

3.1.3. PROPÓSITO DE DISEÑO

IPSEC fue proyectado para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes, en el que los Computadores de los extremos finales realizan el procesado de seguridad, o en modo túnel (puerta a puerta) en el que la

[49] **SPI:** (del inglés *Serial Peripheral Interface*) es un estándar de comunicaciones, usado principalmente para la transferencia de información entre circuitos integrados en equipos electrónicos

[50] **RFC: R**equest **F**or **C**omments (*"Petición De Comentarios"* en español) son una serie de notas sobre Internet que comenzaron a publicarse en 1969

seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

IPSEC puede utilizarse para crear VPNs en los dos modos, y este es su uso principal.

Hay que tener en cuenta, sin embargo, que las implicaciones de seguridad son bastante diferentes entre los dos modos de operación.

La seguridad de comunicaciones extremo a extremo a escala Internet se ha desarrollado más despacio de lo esperado. Parte de la razón a esto es que no ha surgido infraestructura de clave pública universal o universalmente de confianza (DNSSEC[51] fue originalmente previsto para esto); otra parte es que muchos usuarios no comprenden lo suficientemente bien ni sus necesidades ni las opciones disponibles como para promover su inclusión en los productos de los vendedores.

Como el Protocolo de Internet no provee intrínsecamente de ninguna capacidad de seguridad, IPSEC se introdujo para proporcionar servicios de seguridad tales como:

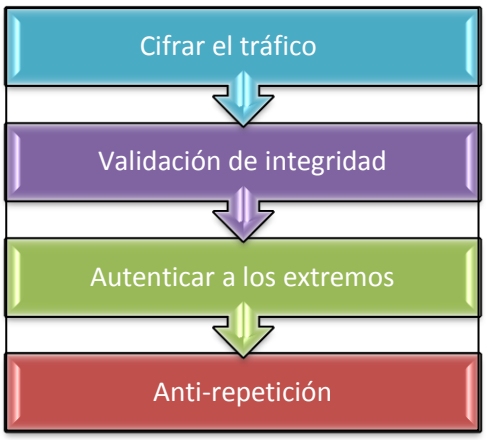

Figura III-5: Servicios de seguridad. **[C]**

1. Cifrar el tráfico (de forma que no pueda ser leído por nadie más que las partes a las que está dirigido)
2. Validación de integridad (asegurar que el tráfico no ha sido modificado a lo largo de su trayecto)

[51] **DNSSEC:** Domain Name System Security Extensions (DNSSEC) es un conjunto de especificaciones

3. Autenticar a los extremos (asegurar que el tráfico proviene de un extremo de confianza)
4. Anti-repetición (proteger contra la repetición de la sesión segura).

3.1.4. MODOS

Así pues y dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de IPSEC: modo transporte y modo túnel.

- **MODO TRANSPORTE**

En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones Computador a Computador.

Una forma de encapsular mensajes IPSEC para atravesar NAT[52] ha sido definida por RFCs que describen el mecanismo de NAT-T[53].

- **MODO TÚNEL**

En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones Computador a red u Computador a Computador sobre Internet.

3.1.5. DETALLES TÉCNICOS

[52] **NAT:** Network Address Translation - Traducción de Dirección de Red)es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes

[53] **NAT-T:** Es un mecanismo en IPsec para la encapsulación UDP de los paquetes ESP para que pasen mejor a través de los cortafuegos

IPSEC consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- **Cabecera de Autentificación ó Authentication Header** (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

- **Carga de seguridad encapsuladora ó Encapsulating Security Payload** (ESP) proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.

Los algoritmos criptográficos definidos para usar con IPSEC incluyen HMAC- SHA1[54] para protección de integridad, y DES-CBC[55] y AES-CBC para confidencialidad.

- **AUTHENTICATION HEADER (AH)**

AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos.

AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits, he aquí un diagrama de cómo se organizan:

[54] **HMAC- SHA1:** Calcula un código de autenticación de mensajes basado en hash (HMAC) mediante la función hash SHA1.
[55] **DES-CBC:** Es un algoritmo de bloque de clave secreta simétrica

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Tabla III-1: Encabezado o cabecera de autentificación. **[A]**

Significado de los campos:

- Next header: Identifica el protocolo de los datos transferidos.
- Payload length: Tamaño del paquete AH.
- RESERVED: Reservado para uso futuro (hasta entonces todo ceros).
- Security parameters index (SPI): Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
- Sequence number: Un número siempre creciente, utilizado para evitar ataques de repetición.
- HMAC: Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

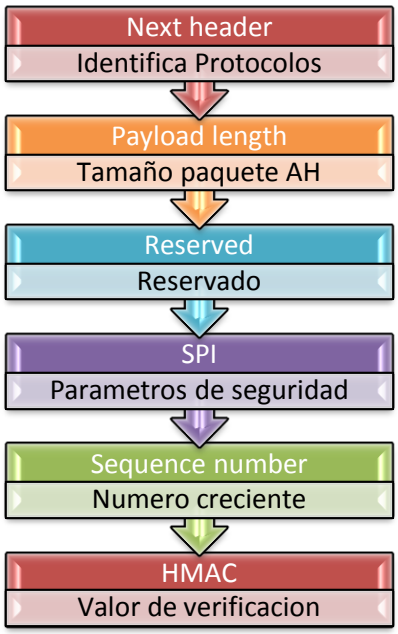

Figura III-6: Campos de la cabecera de autentificación. **[A]**

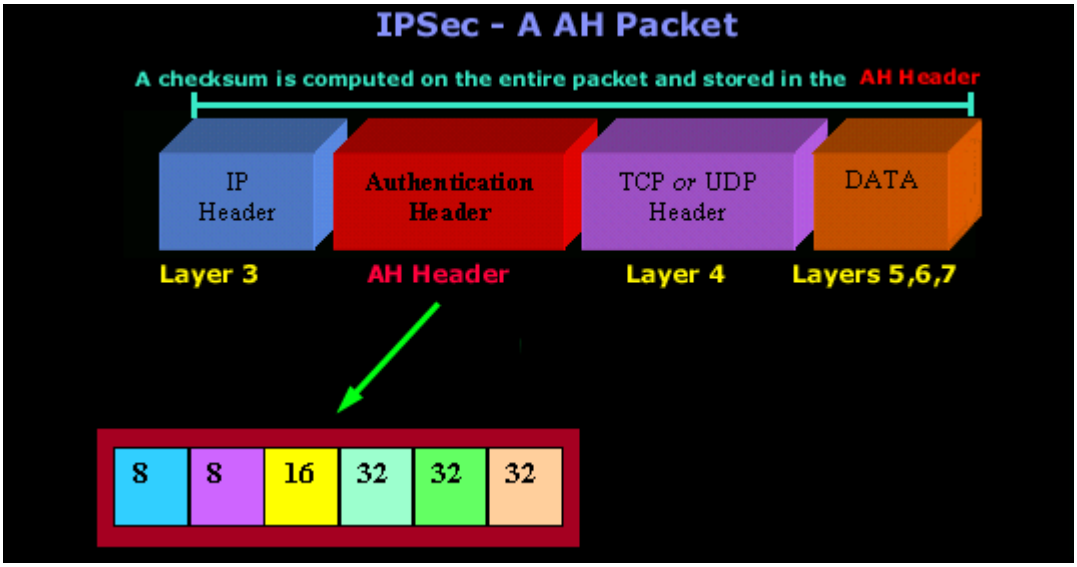

Figura III-7: Paquete AH. **[1]**

- **ENCAPSULATING SECURITY PAYLOAD (ESP)**

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

Significado de los campos

- Security parameters index (SPI): Identifica los parámetros de seguridad en combinación con la dirección IP.
- Sequence number: Un número siempre creciente, utilizado para evitar ataques de repetición.
- Payload data: Los datos a transferir.

- Padding: Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.
- Pad length: Tamaño del relleno en bytes.
- Next header: Identifica el protocolo de los datos transferidos.
- Authentication data: Contiene los datos utilizados para autenticar el paquete.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
	Padding (0-255 bytes)		
		Pad Length	Next Header
Authentication Data (variable)			

Tabla III-2: Diagrama de paquete ESP. **[A]**

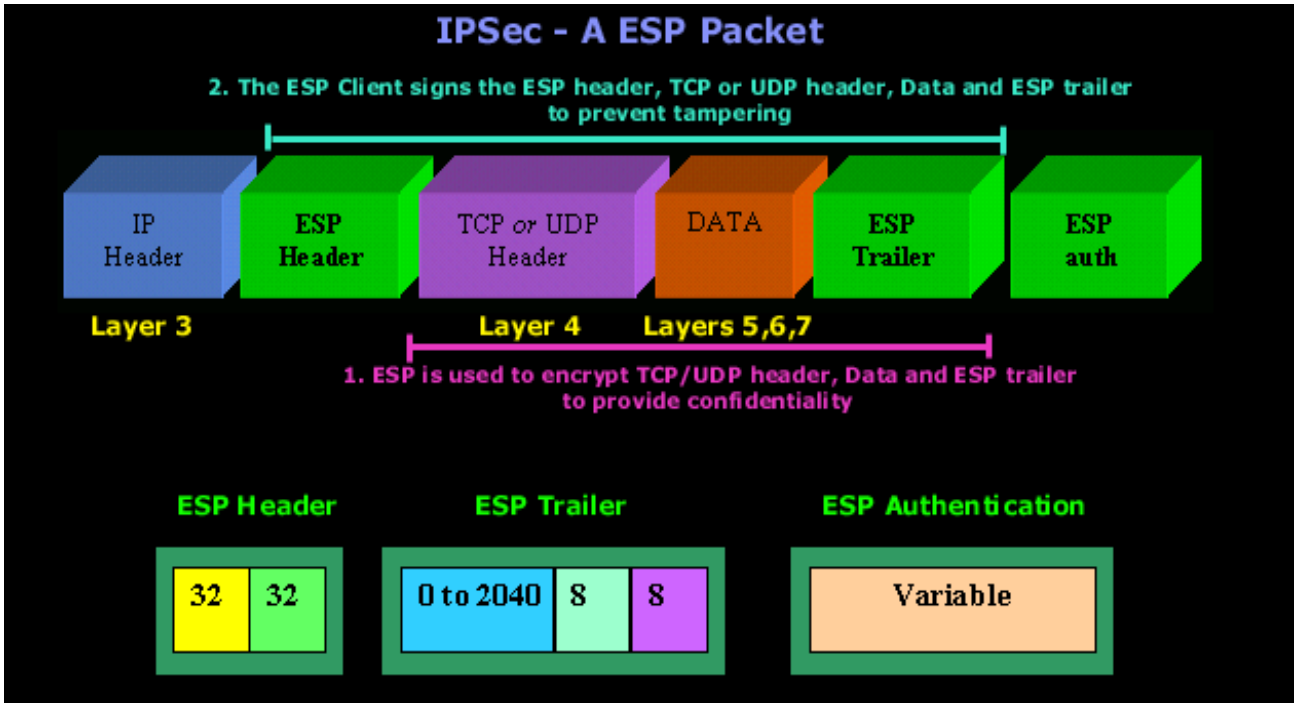

Figura III-8: Paquete ESP. **[1]**

3.1.6. IMPLEMENTACIONES

El soporte de IPSEC está normalmente implementado en el núcleo con la gestión de claves y negociación de ISAKMP/IKE[56] realizada en espacio de usuario. Las implementaciones de IPSEC existentes suelen incluir ambas funcionalidades. Sin embargo, como hay un interfaz estándar para la gestión de claves, es posible controlar una pila IPSEC de núcleo utilizando las herramientas de gestión de claves de una implementación distinta.

Por esta razón, hay confusión en los orígenes de la implementación de IPSEC que se encuentra en el núcleo de Linux. El proyecto FreeS/WAN[57] realizó la primera implementación completa y de código abierto de IPSEC para Linux. Consiste en una pila IPSEC de núcleo KLIPS[58], junto con un demonio (pluto) y muchos scripts de Shell. El proyecto FreeS/WAN fue desmantelado en marzo de 2004. Openswan[59] y strongSwan [60]son continuaciones de FreeS/WAN. El proyecto KAME[61] también implementó soporte IPSEC completo para NetBSD[62] y FreeBSD[63]. Su demonio de gestión de claves se llama racoon. OpenBSD[64] hizo su propio demonio ISAKMP/IKE, llamado simplemente isakmpd (y ha sido portado a otros sistemas, incluyendo Linux).

Sin embargo, ninguna de estas pilas IPSEC de núcleo estaba integrada en el núcleo de Linux. Alexey Kuznetsov y David S. Miller escribieron desde cero una implementación de IPSEC de núcleo para el núcleo de Linux alrededor de finales de 2002. Esta pila fue posteriormente lanzada como parte de Linux 2.6, y es llamada por varios "nativa"o "NETKEY".

[56] **ISAKMP/IKE:** Describe un protocolo híbrido cuyo propósito es negociar y proveer
[57] **FreeS/WAN:** Es una implementación de IPSec y posteriores al (Ip security) para sistemas Linux. IPSec provee servicios de cifrado y autenticación.
[58] **KLIP:** Interface de IPSEC
[59] **Openswan:** Implementación de IPSEC para Linux 2.2.
[60] **strongSwan:** Implementación de IPSEC para Linux 2.4.
[61] **Proyecto KAME:** Deshabilita la Cabecera de Encaminamiento IPv6 de Tipo 0
[62] **NetBSD:** Es un sistema operativo de la familia Unix (en sí no se le puede llamar "un Unix", ya que ésta es una marca comercial de AT&T
[63] **FreeBSD:** Es un sistema operativo libre para computadoras basado en las CPU de arquitectura Intel
[64] **OpenBSD:** Es un sistema operativo libre tipo Unix, multiplataforma

Por lo tanto, contrariamente a la creencia popular, la pila IPSEC de Linux no se originó en el proyecto KAME. Como soporta el protocolo estándar PF KEY (RFC 2368) y el interfaz nativo XFRM para gestión de claves, la pila IPSEC de Linux puede utilizarse junto con *pluto* de Openswan/strongSwan, *isakmpd* del proyecto OpenBSD, *racoon* del proyecto KAME o sin ningún demonio ISAKMP/IKE (utilizando claves manuales).

Las nuevas arquitecturas de procesadores de red, incluyendo procesadores multinúcleo con motores de cifrado integrados, han cambiado la forma en que las pilas IPSEC son diseñadas. Un Fast Path dedicado es utilizado para descargar el procesado de las tareas de IPSEC (SA, búsquedas SP, cifrado, etc.).

Hay bastantes implementaciones de los protocolos IPSEC e ISAKMP/IKE. Entre otras:

- 6WINDGate, pila IPSEC Fast Path para procesador de red multinúcleo
- NRL IPSEC, una de las fuentes originales de código IPSEC
- OpenBSD, con su propio código derivado de NRL IPSEC
- La pila de KAME, que está incluida en Mac OS X, NetBSD y FreeBSD
- "IPSEC" en el software IOS de Cisco
- "IPSEC" en Microsoft Windows, incluyendo Windows XP, Windows 2000, y Windows 2003
- Las herramientas QuickSec de SafeNet
- IPSEC en Solaris
- El sistema operativo AIX de IBM
- z/OS de IBM
- IPSEC e IKE en HP-UX (HP-UX IPSEC)
- IPSEC e IKE en VxWorks

Figura III-9: Implementaciones IPSEC. **[A]**

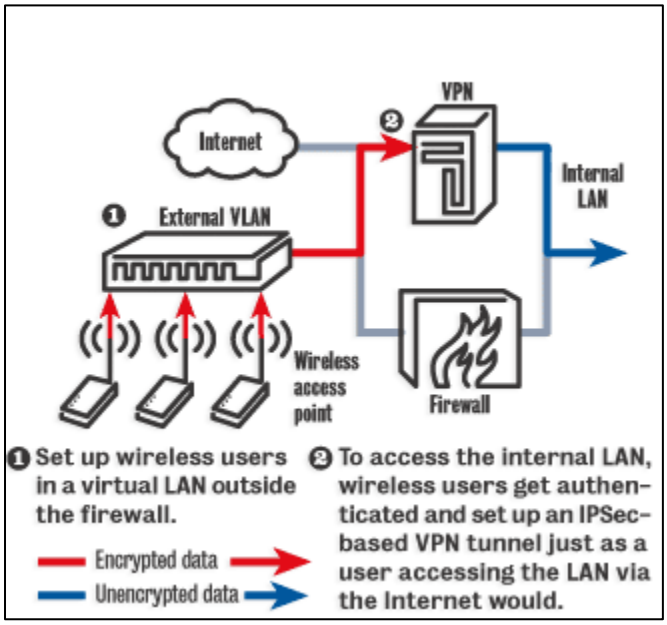

Figura III-10: IPsec en Wireless **[C]**

3.1.7. CINCO PASOS PARA EL IPSEC

Pasos	Nombre	Descripción
Paso 1	**Tráfico Interesante**	Determinar el tráfico que debe ser protegido como parte de una política de seguridad.
Paso 2	**Fase 1 - IKE** **1) Main Mode** **2) Agressive Mode**	a) Negociar la Política. b) Autenticación de los peers. c) Establecer un canal seguro.
Paso 3	**Fase 2 – IKE**[65] **1) Quick Mode**	a) Negociar Transformada y parámetros de seguridad del IPSEC. b) Establecer SA[66] c) Renegociar periódicamente las SA para garantizar la seguridad d) Opcionalmente desempeña un intercambio adicional usando DH.
Paso 4	**Sesión IPSEC**	a) Las SA son intercambiadas entre peers. b) Los servicios de seguridad son aplicados al tráfico.
Paso 5	**Terminación del Túnel**	a) Terminación del túnel: + Si hay un timeout en el tiempo de vida de la SA. + Si el contador del paquete es excedido. b) Remueve la SA del IPSEC.

Tabla III-3: Cinco pasos para el IPSec. **[A]**.

3.1.8. CONFIGURACIÓN DE IPSEC

Tarea	Nombre	Descripción	Comandos
Tarea 1	Paso 1	Determinar la política IKE	

[65] **IKE:** Se ocupa incluso de renovar periódicamente las claves
[66] **SA:** Asociación de Seguridad

<table>
<tr>
<td>Preparar IKE e IPSEC</td>
<td>Determinar la Política IKE.

(Política)

(IKE Fase 1)</td>
<td>(IKE Fase 1)

<table>
<tr><th>Parámetro</th><th>Fuerte</th><th>Mas Fuerte</th></tr>
<tr><td>Algoritmo de Cifrado</td><td>DES (56 bits)</td><td>3DES (168 bits)</td></tr>
<tr><td>Algoritmo Hash</td><td>MD5 (HMAC)</td><td>SHA-1 (HMAC)</td></tr>
<tr><td>Método de Autenticación</td><td>Pre-Shared</td><td>+Cifrado RSA
+Firmas RSA</td></tr>
<tr><td>Intercambio de llave</td><td>DH Grupo 1 (768 its)</td><td>DH Grupo 2 (1024 bits)</td></tr>
<tr><td>Tiempo de vida de IKE SA</td><td>86400 seg</td><td><86400 seg</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paso 2
Determinar la Política IPSEC.

(Transformada)

(IKE Fase 2)</td>
<td>Determinar la política IPSEC
(IKE Fase 2)

<table>
<tr><th>Transformada</th></tr>
<tr><td>ah-md5-hmac</td></tr>
<tr><td>ah-sha-hmac</td></tr>
<tr><td>esp-des</td></tr>
<tr><td>esp-3des</td></tr>
<tr><td>esp-md5-hmac</td></tr>
<tr><td>esp-sha-hmac</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>esp-null

Configuración completa
<table>
<tr><th>Política</th><th>Parámetros</th></tr>
<tr><td>Transformada</td><td>ESP-DES, túnel</td></tr>
<tr><td>Nombre del peer</td><td>Router x</td></tr>
<tr><td>IP del peer</td><td>172.30.2.2</td></tr>
<tr><td>Host o red cifrado</td><td>10.0.1.3</td></tr>
<tr><td>Tipo de tráfico a cifrarse</td><td>TCP</td></tr>
<tr><td>Establecimiento SA</td><td>ipsec-isakmp</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paso 3
Checar la Configuración Actual.</td>
<td>3.1 La configuración debe ser revisada para verificar si existen politicas IPSEC configuradas y que puedan interferir con las políticas que se planean configurar.</td>
<td>show running-configuration

show crypto isakmp policy

show crypto map

show crypto IPsec transform-set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2 Asegurarse que la red funcione sin cifrado.</td>
<td>ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.3 Asegurarse que las listas de acceso sean compatibles con IPSEC.

Permitiendo los protocolos 50 (ESP) y</td>
<td>show access-lists</td>
</tr>
</table>

		51 (AH) así como el puerto UDP 500 (ISAKMP). En el pix firewall se usa el comando sysopt connection permit ipsec.	
Tarea 2 Configurar IKE	Paso 1 Habilitar o deshabilitar IKE.	Habilita o Deshabilita IKE de manera global. IKE está habilitado por default. IKE se habilita globalmente en todas las interfaces del router. Una ACL puede bloquear IKE en una interfaz particular.	**[no] crypto isakmp enable**
	Paso 2 Crear la Política IKE.	Define la política IKE la cual es un conjunto de parámetros usados durante la negociación IKE Fase 1. Las políticas se ejecutan en orden ascendente.	**crypto isakmp policy priority** **authentication pre-shared** **encryption des** **group 1** **hash md5** **lifetime 86400**
	Paso 3 Configuración de la identidad ISAKMP.	Los peers IPSEC se autentican mutuamente durante la negociación ISAKMP usando la llave pre-compartida y la identidad ISAKMP. Esta identidad puede ser la IP o el nombre del host. El software Cisco IOS usa como método de identidad la dirección IP	**crypto isakmp identity {address | hostname}**

		por default. Se configura el nombre o IP del host remoto.	
	Paso 4 Configuración de la llave pre-compartida	Configuración de la llave para la autenticación pre-compartida	**crypto isakmp key cisco123 address 172.30.2.2**
	Paso 5 Verificar la configuración IKE.	Hasta este momento es recomendable verificar que la política haya sido configurada correctamente.	**show crypto isakmp policy** **show crypto isakmp sa**
Tarea 3 Configurar IPSEC	Paso 1 Configuración de la transformada.	Transformada AH: Mecanismo para la autenticación del payload. Transformada ESP: Mecanismo para el cifrado del payload. Modo IPSEC: Modo transporte, Modo túnel. La transformada es negociada durante un quick mode en la fase 2 de IKE. Se pueden configurar múltiples transformadas y después asignarla por medio de un crypto map. Durante la negociación los peers buscan un conjunto de transformadas que sean idénticas en ambos peers.	**crypto IPsec transform-set name transform1 [transform2] [trasnform3]**
	Paso 2 Configuración	El tiempo de vida de la SA determina cuanto tiempo una SA de IPSEC	**crypto IPsec security-**

	global del tiempo de vida de las SA de IPSEC.	permanecerá válida antes de ser renegociada. El tiempo de vida de la SA es negociado durante la fase 2 de IKE Los tiempos de vida en las SA de IPSEC en los crypto mapas sobre escriben los tiempos de vida globales de las SA de IPSEC. Cuando una SA expira una nueva es negociada sin interrumpir el flujo de datos.	**association lifetime {seconds | kilobytes} 86400**
	Paso 3 Crear una Crypto ACL.	Las crypto ACLs identifican el flujo del tráfico que va a ser protegido. El tráfico que coincide con la ACL es protegido y cifrado. El tráfico que no coincide con la ACL viaja en texto claro. Permit = Cifrado Deny = Texto Claro Las crypto ACLs deben ser simétricas cuando se usan con IPSEC.	**access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255**
	Paso 4 Crear crypto mapas.	Los crypto mapas agrupan todas las partes de la configuración de IPSEC: 1) La ACL empleada. 2) El peer VPN remoto. 3) La transformada a utilizarse.	**crypto map mymap 110 IPsec-isakmp** **match address 110**

		4) El método de administración de llaves. 5) El tiempo de vida de las SA Los crypto mapas pueden aplicarse a una sola interfaz. Múltiples interfaces pueden compartir el mismo crypto mapa si se desea aplicar la misma política a múltiples interfaces. CET: Cisco Encryption Technology 1) IPSEC con IKE 2) IPSEC con configuración manual de SA. PFS: Perfect Forward Secrecy Provee una seguridad adicional en la Solicitud de SA.	**set peer 172.30.2.2** **set peer 172.30.3.2** **set pfs group1** **set transform-set mine** **set security-association lifetime 86400**
	Paso 5 Aplicar los crypto mapas a las interfaces.	Aplicación del crypto mapa a la interfaz designada.	**interface e0/1** **crypto map mymap**
Tarea 4 Prueba y verificación de IPSEC.	Paso 1 Despliega las políticas IKE configuradas		**show crypto isakmp policy**
	Paso 2 Despliega la transformada configurada		**show crypto IPsec transform set**
	Paso 3		**show crypto**

	Despliega el estado actual de las SAs de IPSEC		**IPsec sa**
	Paso 4 Despliega los crypto mapas		**show crypto map**
	Paso 5 Habilita la salida del debug para los eventos IPSEC.		**debug crypto IPsec**
	Paso 6 Habilita la salida del debug para los eventos ISAKMP.		**debut crypto isakmp**

Tabla III-4: Configuración estándar de IPSEC. **[A]**.

3.1.9. CONFIGURACIÓN DE IPSEC USANDO RSA

Tarea	Nombre	Descripción	Comandos
Tarea 1 Preparación para IPSEC	Políticas RSA	Determinar detalladamente las políticas de seguridad para el cifrado asimétrico o publico como lo es RSA incluyendo la distribución de las llaves.	
Tarea 2 Configuración de las llaves RSA.	Paso 1 Plan para las llaves RSA		

	Paso 2 Configuración del nombre del router y del nombre del dominio.	Solo si no han sido configurados	**hostname nombre** **ip domain-name nombre**
	Paso 3 Generar llaves RSA		**crypto key generate rsa usage keys**
	Paso 4 Establecer las llaves publicas RSA del peer		**crypto key pubkey-chain** **crypto key pubkey-chain rsa** **addressed-key key address** **named-key key name** **key-string**
	Paso 5 Verificar la configuración de las llaves		**show crypto key mypubkey rsa** **show crypto key pubkey-chain rsa**
	Paso 6 Administración de las llaves RSA.		**crypto key zeroize rsa**
Tarea 3 **Configurar IKE**	Paso 1 Habilitar o deshabilitar IKE.	Habilita o Deshabilita IKE de manera global. IKE está habilitado por	**[no] crypto isakmp enable**

		default. IKE se habilita globalmente en todas las interfaces del router. Una ACL puede bloquear IKE en una interfaz particular.	
	Paso 2 Crear la Política IKE.	Define la política IKE la cual es un conjunto de parámetros usados durante la negociación IKE Fase 1. Las políticas se ejecutan en orden ascendente.	**crypto isakmp policy priority** **authentication pre-shared** **encryption des** **group 1** **hash md5** **lifetime 86400**
	Paso 3 Configuración de la identidad ISAKMP.	Los peers IPSEC se autentican mutuamente durante la negociación ISAKMP usando la llave pre-compartida y la identidad ISAKMP. Esta identidad puede ser la IP o el nombre del host. El software Cisco IOS usa como método de identidad la dirección IP por default. Se configura el nombre o IP del host remoto.	**crypto isakmp identity {address | hostname}**

Tarea 4 Configurar IPSEC	Paso 1 Configuración de la transformada.	Transformada AH: Mecanismo para la autenticación del payload. Transformada ESP : Mecanismo para el cifrado del payload. Modo IPSEC : Modo transporte, Modo túnel. La transformada es negociada durante un quick mode en la fase 2 de IKE. Se pueden configurar múltiples transformadas y después asignarla por medio de un crypto map. Durante la negociación los peers buscan un conjunto de transformadas que sean idénticas en ambos peers.	**crypto IPsec transform-set name transform1 [transform2] [trasnform3]**
	Paso 2 Configuración global del tiempo de vida de las SA de IPSEC.	El tiempo de vida de la SA determina cuanto tiempo una SA de IPSEC permanecerá válida antes de ser renegociada. El tiempo de vida de la SA es negociado durante la fase 3 de IKE Los tiempos de vida en las	**crypto IPsec security-association lifetime {seconds | kilobytes} 86400**

		SA de IPSEC en los crypto mapas sobre escriben los tiempos de vida globales de las SA de IPSEC. Cuando una SA expira una nueva es negociada sin interrumpir el flujo de datos.	
	Paso 3 Crear una Crypto ACL.	Las crypto ACLs identifican el flujo del tráfico que va a ser protegido. El tráfico que coincide con la ACL es protegido y cifrado. El tráfico que no coincide con la ACL viaja en texto claro. Permit = Cifrado Deny = Texto Claro Las crypto ACLs deben ser simétricas cuando se usan con IPSEC.	**access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255**
	Paso 4 Crear crypto mapas.	Los crypto mapas agrupan todas las partes de la configuración de IPSEC: 1) La ACL empleada. 2) El peer VPN remoto. 3) La transformada a utilizarse.	**crypto map mymap 110 IPsec-isakmp** **match address 110** **set peer 172.30.2.2**

		4) El método de administración de llaves. 5) El tiempo de vida de las SA Los crypto mapas pueden aplicarse a una sola interfaz. Múltiples interfaces pueden compartir el mismo crypto mapa si se desea aplicar la misma política a múltiples interfaces. CET: Cisco Encryption Technology 1) IPSEC con IKE 2) IPSEC con configuración manual de SA. PFS: Perfect Forward Secrecy Provee una seguridad adicional en la Solicitud de SA.	**set peer 172.30.3.2** **set pfs group1** **set transform-set mine** **set security-association lifetime 86400**
	Paso 5 Aplicar los crypto mapas a las interfaces.	Aplicación del crypto mapa a la interfaz designada.	**interface e0/1** **crypto map mymap**
Tarea 5 Prueba y verificación de	Paso 1 Despliega las políticas IKE		**show crypto isakmp policy**

IPSEC.	configuradas		
	Paso 2 Despliega la transformada configurada		**show crypto IPsec transform set**
	Paso 3 Despliega el estado actual de las Sas de IPSEC		**show crypto IPsec sa**
	Paso 4 Despliega los crypto mapas		**show crypto map**
	Paso 5 Habilita la salida del debug para los eventos IPSEC.		**debug crypto IPsec**
	Paso 6 Habilita la salida del debug para los eventos ISAKMP.		**debut crypto isakmp**

Tabla III-5: Configuración del IPSec usando RSA. **[A]**

3.1.10. CONFIGURACIÓN DE VPNS CON IPSEC USANDO AUTORIDADES CERTIFICADORAS

Tarea	Nombre	Descripción	Comandos
Tarea 1 Preparación para IKE e IPSEC	Paso 1 Plan para el soporte de CA	<table><tr><th>Parámetro</th><th>Servidor CA</th></tr><tr><td>Tipo de</td><td>Windows</td></tr></table>	

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td>servidor CA</td><td>2000</td></tr>
<tr><td>Hostname</td><td>Vpnca</td></tr>
<tr><td>IP Address</td><td>172.30.1.51</td></tr>
<tr><td>URL</td><td>Vpnca.cisco.com</td></tr>
<tr><td>Administrator contacto</td><td>55990424</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paso 2
Determinar la Política IKE.

(Política)

(IKE Fase 1)</td>
<td>Determinar la política IKE
(IKE Fase 1)
<table>
<tr><th>Parámetro</th><th>Fuerte</th><th>Mas Fuerte</th></tr>
<tr><td>Algoritmo de Cifrado</td><td>DES (56 bits)</td><td>3DES (168 bits)</td></tr>
<tr><td>Algoritmo Hash</td><td>MD5 (HMAC)</td><td>SHA-1 (HMAC)</td></tr>
<tr><td>Método de Autenticación</td><td>Pre-Shared</td><td>+Cifrado RSA +Firmas RSA</td></tr>
<tr><td>Intercambio de llave</td><td>DH Grupo 1 (768 bits)</td><td>DH Grupo 2 (1024 bits)</td></tr>
<tr><td>Tiempo de vida de IKE SA</td><td>86400 seg</td><td><86400 seg</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paso 3</td>
<td>Determinar la política IPSEC</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Determinar la Política IPSEC.

(Transformada)

(IKE Fase 2)</td>
<td>(IKE Fase 2)

<table>
<tr><th>Transformada</th></tr>
<tr><td>ah-md5-hmac</td></tr>
<tr><td>ah-sha-hmac</td></tr>
<tr><td>esp-des</td></tr>
<tr><td>esp-3des</td></tr>
<tr><td>esp-md5-hmac</td></tr>
<tr><td>esp-sha-hmac</td></tr>
<tr><td>esp-null</td></tr>
</table>

Configuración completa
<table>
<tr><th>Política</th><th>Parámetros</th></tr>
<tr><td>Transformada</td><td>ESP-DES, túnel</td></tr>
<tr><td>Nombre del peer</td><td>Router x</td></tr>
<tr><td>IP del peer</td><td>172.30.2.2</td></tr>
<tr><td>Host o red cifrado</td><td>10.0.1.3</td></tr>
<tr><td>Tipo de tráfico a cifrarse</td><td>TCP</td></tr>
<tr><td>Establecimiento SA</td><td>ipsec-isakmp</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paso 4
Checar la configuración actual</td>
<td>Verificación de la configuración</td>
<td>show running-configuration

show crypto isakmp policy

show crypto map</td>
</tr>
<tr>
<td></td>
<td>Paso 5</td>
<td></td>
<td>ping</td>
</tr>
</table>

	Garantizar que la red funcione sin cifrado		
	Paso 6 Garantizar que las ACLs sean compatibles con IPSEC		**show access-lists**
Tarea 2 Procedimiento de Configuración del CA del Cisco IOS	Paso 1 (Opcional) Manejo del uso de la memoria NVRAM	Tipos de certificados almacenados en el router. 1) El router posee su propio certificado de identidad 2) El certificado raíz de la CA 3) Certificados RA (Vendedor específico de CA) El número de CRLs almacenadas en el router. 1) Uno si la CA no soporta RA 2) Múltiples CRLs si la CA soporta RA	**crypto ca certificate query** (evita que los certificados y CRLs se almacenen localmente en el router.)
	Paso 2 Establecer la hora y fecha en el router	La hora y fecha deben de estar de acuerdo con el servidor CA.	**clock timezone *cst -6*** **clock set *23:59:59 31 december 2003***
	Paso 3 Configuración el nombre del host y dominio del		**hostname *name*** **ip domain-name *name***

	router		**ip host *name address*** (IP del servidor CA)
	Paso 4 Generar un par de llaves RSA	Genera la llave pública y privada de RSA.	**crypto key generate rsa usage-keys**
	Paso 5 Declarar la CA	Especifica el nombre del servidor CA.	**crypto ca trustpoint *name*** **enrollment url http://vpnca/certsrv/mscep/mscep.dll** **enrollment mode ra** (solo si el sistema CA prove una RA) **crl optional** (opcional)
	Paso 6 Autenticar la CA	El router necesita autenticar al CA para verificar que este es válido. El router hace esto obteniendo el certificado del CA que contiene la llave publica del CA.	**crypto ca authenticate *name***
	Paso 7 Solicitar el certificado propio	Solicita certificados del CA para los pares de llaves de todos routers	**crypto ca enroll *name***
	Paso 8 Salvar la configuración		**copy running-config startup-config**

	Paso 9 (Optional) Monitorear y mantener la interoperabilidad de la CA	Los siguientes pasos son opcionales dependiendo de los requerimientos particulares: 1) Solicitud de la CRL 2) Borrar las llaves RSA del router 3) Borrar los certificados de la configuración 4) Borrar las llaves publicas de los peers	**crypto ca trustpoint *name*** 1) Solicitud de la CRL **crypto ca crl request *name*** 2) Borrar las llaves RSA del router **crypto key zeroise rsa** 3) Borrar los certificados de la configuración. 3.1) Preguntar al administrador CA para revocar el certificado del router en el CA. Se deberá proporcionar la contraseña creada originalmente durante la obtención del certificado del router con el comando crypto ca enroll 3.2) Remover manualmente el certificado del router de la configuración del mismo.

			3.2.1) Despliega el certificado almacenado en el router **show crypto ca certificates** 3.2.2) Acceder al modo de configuración de la cadena del certificado **crypto ca certificates chain *name*** 3.2.3) Borra el certificado **no certificate *certificate-serial-number*** 4) Borra las llaves publicas de los peers 4.1) Accede al modo de configuración de la cadena de la llave publica. **crypto key pubkey-chain rsa** 4.2) Borra una llave pública RSA del peer remoto. **no named-key**

			key_name [encryption|signature] o **no addressed-key key-address [encryption|signature]**
	Paso 10 Verificar la configuración soportada por la CA.		**show crypto ca certificates** **show crypto key mypubkey | pubkey-chain**
Tarea 3 Configurar IKE	Paso 1 Habilitar o deshabilitar IKE.	Habilita o Deshabilita IKE de manera global. IKE está habilitado por default. IKE se habilita globalmente en todas las interfaces del router. Una ACL puede bloquear IKE en una interfaz particular.	**[no] crypto isakmp enable**
	Paso 2 Crear la Política IKE.	Define la política IKE la cual es un conjunto de parámetros usados durante la negociación IKE Fase 1. Las políticas se ejecutan en orden ascendente.	**crypto isakmp policy priority** **authentication pre-shared** **encryption des** **group 1** **hash md5** **lifetime 86400**

	Paso 3 Configuración de la identidad ISAKMP.	Los peers IPSEC se autentican mutuamente durante la negociación ISAKMP usando la llave pre-compartida y la identidad ISAKMP. Esta identidad puede ser la IP o el nombre del host. El software Cisco IOS usa como método de identidad la dirección IP por default. Se configura el nombre o IP del host remoto.	**crypto isakmp identity {address | hostname}**
	Paso 4 Verificar la configuración IKE.	Hasta este momento es recomendable verificar que la política haya sido configurada correctamente.	**show crypto isakmp policy** **show crypto isakmp sa**
Tarea 4 Configuración de IPSEC	Paso 1 Configuración de la transformada.	Transformada AH: Mecanismo para la autenticación del payload. Transformada ESP: Mecanismo para el cifrado del payload. Modo IPSEC : Modo transporte, Modo túnel. La transformada es negociada durante un quick mode en la fase 2 de IKE. Se pueden configurar múltiples transformadas y después asignarla por medio de un crypto map. Durante la negociación los peers buscan un conjunto de	**crypto IPsec transform-set name transform1 [transform2] [trasnform3]**

		transformadas que sean idénticas en ambos peers.	
	Paso 2 Configuración global del tiempo de vida de las SA de IPSEC.	El tiempo de vida de la SA determina cuanto tiempo una SA de IPSEC permanecerá válida antes de ser renegociada. El tiempo de vida de la SA es negociado durante la fase 3 de IKE Los tiempos de vida en las SA de IPSEC en los crypto mapas sobre escriben los tiempos de vida globales de las SA de IPSEC. Cuando una SA expira una nueva es negociada sin interrumpir el flujo de datos.	**crypto IPsec security-association lifetime {seconds | kilobytes} 86400**
	Paso 3 Crear una Crypto ACL.	Las crypto ACLs identifican el flujo del tráfico que va a ser protegido. El tráfico que coincide con la ACL es protegido y cifrado. El tráfico que no coincide con la ACL viaja en texto claro. Permit = Cifrado Deny = Texto Claro Las crypto ACLs deben ser simétricas cuando se usan con IPSEC.	**access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255**

	Paso 4 Crear crypto mapas.	Los crypto mapas agrupan todas las partes de la configuración de IPSEC: 1) La ACL empleada. 2) El peer VPN remoto. 3) La transformada a utilizarse. 4) El método de administración de llaves. 5) El tiempo de vida de las SA Los crypto mapas pueden aplicarse a una sola interfaz. Múltiples interfaces pueden compartir el mismo crypto mapa si se desea aplicar la misma política a múltiples interfaces. CET: Cisco Encryption Technology 1)IPSEC con IKE 2)IPSEC con configuración manual de SA. PFS: Perfect Forward Secrecy Provee una seguridad adicional en la Solicitud de SA.	**crypto map mymap 110 IPsec-isakmp** **match address 110** **set peer 172.30.2.2** **set peer 172.30.3.2** **set pfs group1** **set transform-set mine** **set security-association lifetime 86400**
	Paso 5 Aplicar los crypto mapas a las interfaces.	Aplicación del crypto mapa a la interfaz designada.	**interface e0/1** **crypto map mymap**
Tarea 5 Prueba y verificació	Paso 1 Despliega las políticas IKE		**show crypto isakmp policy**

n de IPSEC.	configuradas		
	Paso 2 Despliega la transformada configurada		**show crypto IPsec transform set**
	Paso 3 Despliega el estado actual de las Sas de IPSEC		**show crypto IPsec sa**
	Paso 4 Despliega los crypto mapas		**show crypto map**
	Paso 5 Habilita la salida del debug para los eventos IPSEC.		**debug crypto IPsec**
	Paso 6 Habilita la salida del debug para los eventos ISAKMP.		**debug crypto isakmp**
	Paso 7 Habilita la salida del debug para los eventos CA.		**debug crypto key-exchange** **debug crypto pki {messages | transactions}**

Tabla III-6: Cisco Easy VPN. **[A]**.

Nuevas Funciones de Easy VPN

1) Mode configuration version 6 support
2) Xauth version 6 support
3) IKE DPD
4) Split tunneling control
5) Initial Contact
6) Group-based policy control

3.1.11. ATRIBUTOS SOPORTADOS POR IPSEC EN EASY VPN

Opciones	Atributos
Algoritmos de autenticación	HMAC-MD5 HMAC-SHA1
Tipos de autenticación	Pre-shared keys RSA digital signaturas
Grupos Diffie-Hellman	2, 5
Algoritmos de cifrado (IKE)	DES, 3DES
Algoritmos de cifrado (IPSEC)	DES, 3DES, NULL
Identificadores del protocolo IPSEC	ESP, IPCOMP, LZS
Modo del protocolo IPSEC	Modo Túnel

Tabla III-7: Atributos soportados de IPSEC en Easy VPN. **[A]**

3.1.12. ATRIBUTOS NO SOPORTADOS POR IPSEC EN EASY VPN

Opciones	Atributos
Tipos de autenticación	DSS
Grupos Diffie-Hellman	1
Identificador del protocolo IPSEC	IPSEC AH
Modo del protocolo IPSEC	Modo Transporte
Miscelánea	Llaves Manuales, PFS

Tabla III-8: Atributos no soportados por IPSEC en Easy VPN. **[A]**

3.1.13. MODO DE OPERACIÓN

Modo de operación	Descripción
Modo Cliente	1) Especifica el NAT/PAT a ser utilizado 2) El cliente automáticamente configura la translación NAT/PAT y la ACL necesaria para implementar el túnel VPN. 3) Soporta Split-tunneling
Modo Extensión de Red	1)Especifica que el host en el lado del cliente de la conexión VPN utiliza direcciones IP ruteables 2)Pat no es utilizado 3)Soporta Split Tunneling

Tabla III-9: Modo de Operación. **[A]**

3.2. GRE

GRE es un protocolo de tunelizado que desarrollo Cisco originalmente, y que puede hacer unas cuantas cosas más que los túneles IP-sobre-IP. Por ejemplo, puede transportar tráfico multicast e IPv6 sobre un túnel GRE. En Linux, necesitara el modulo ip_gre.o.

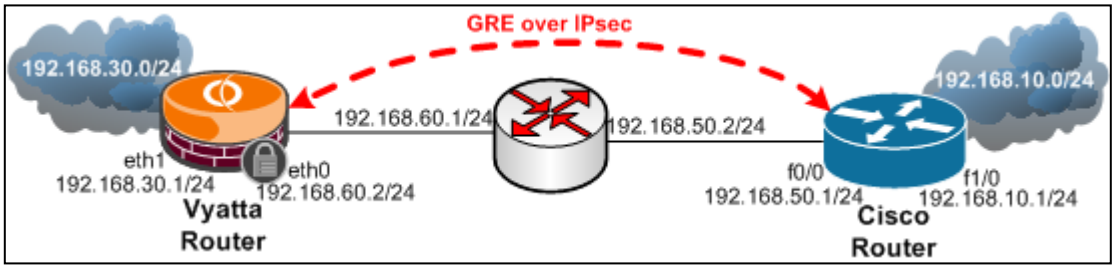

Figura III-11: GRE sobre IPsec. **[1]**

Generic Routing Encapsulation (GRE) es un protocolo originalmente desarrollado por Cisco Systems que se ha convertido en un estándar de la industria definió en las RFC 1701, 1702 y 2784. Es un protocolo de túnel, es decir, que permite transportar paquetes de una red a través de otra red diferente. Por ejemplo, permite establecer un enlace de la red 10.0.0.0 a través de la red 172.16.0.0.

3.2.1. ¿CUÁNDO UTILIZAR GRE?

- Cuando, por ejemplo, es necesario trabajar con un protocolo que no es enrutable como NetBIOS o con protocolos enrutables diferentes de IP a través de una red IP. Se puede constituir un túnel GRE para trabajar con IPX o AppleTalk sobre una red IP.
- Cuando debemos conectar dos puntos remotos de una misma red (antes mencioné el ejemplo de la red 10.0.0.0) y para ello necesitamos utilizar enlaces que pertenecen a una red diferente (en el ejemplo, la 172.16.0.0).

3.2.2. ¿CÓMO SE CONFIGURA UN TÚNEL GRE?

Configurar el túnel GRE es en principio una tarea relativamente sencilla. Para revisar los comandos debemos considerar ambos extremos del enlace a través del cual debe operar el túnel, usando la configuración sugerida según CISCO IOS:

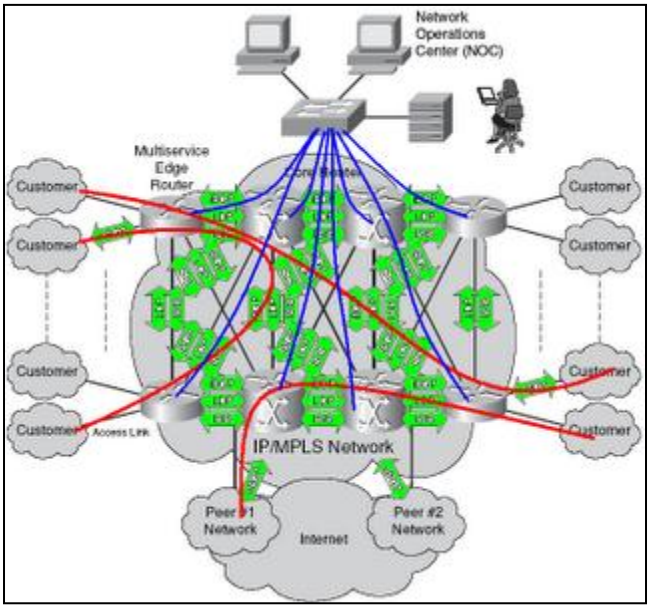

Figura III-12: Implementación de túneles GRE. **[3]**

En este sencillo ejemplo se ha creado una interfaz virtual en cada router: las interfaces túnel. Estas interfaces utilizan su propia red, comportándose como un enlace punto a punto. El tráfico de este túnel será físicamente enviado a través de las interfaces seriales.

De este modo, entre ambos routers aparecerán ahora 2 rutas posibles: la ruta a través de las interfaces seriales y la ruta a través de la interfaz túnel. Este túnel puede transportar tanto tráfico no rateadle como que utilice otros protocolos enrutados.

En el caso del ejemplo el túnel se realiza sobre un enlace privado que podría pertenecer, por ejemplo, a una red frame-relay[67]. También puede realizarse sobre Internet; en este caso se puede utilizar algún protocolo de encripción como IPSec para brindar privacidad y seguridad.

Tenga en cuenta que la configuración es bastante sencilla. Lo realmente importante aquí es el diseño: definir con claridad los puntos de inicio y fin del túnel, y el tráfico que se va a enviar a través del mismo.

Router A

```
interface                  Ethernet0/1
ip   address   10.2.2.1   255.255.255.0
!
interface                    Serial0/0
ip address 172.16.4.1 255.255.255.252
!
interface                      Tunnel0
ip address 10.10.10.2 255.255.255.252
tunnel        source         Serial0/0
tunnel     destination      172.16.4.2
!
```

Tabla III-10: Configuración router A usando GRE. **[4]**

Router B

```
interface             FastEthernet0/1
ip  address  10.1.1.1  255.255.255.0
!
interface                   Serial0/0
ip        address         172.16.4.2
```

[67] **RED FRAME RELAY:** es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.

```
255.255.255.252
!
interface                    Tunnel0
ip         address         10.10.10.1
255.255.255.252
tunnel        source        Serial0/0
tunnel     destination     172.16.4.1
!
```

Tabla III-11: Configuración router B usando GRE. **[4]**

Las interfaces túnel son interfaces virtuales que son tratadas por Cisco IOS como una interfaz más:

```
RouterB#          sh          ip          int          brief
Interface . . . . IP-Address .OK? .Method .Status . . . Protocol
FastEthernet0/0  .  10.1.1.1  .  .YES  .manual  .up  .  .  .  .  up
Serial0/0  .  .  .  .  172.16.4.2  .YES  .manual  .up  .  .  .  .  up
Serial0/1  .  .  .  .  unassigned  .YES  .unset  .  admin down  .  down
Tunnel0  .  .  .  .  .  10.10.10.1 .YES .manual .up . . . . . up
```

Tabla III-12: Interfaces virtuales. **[4]**

3.2.3. CONSIDERACIONES ADICIONALES

- GRE toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, lo que implica que el paquete que se envía a través del túnel es de mayor longitud por lo que puede ocurrir que esté excediendo la longitud permitida en la interfaz física. Esto provoca el descarte de ese paquete.

- Para solucionar este inconveniente se puede aplicar el comando ip tcp adjust-mss 1436 sobre la interfaz túnel para asegurarse de que no se supere el MTU permitido sobre el enlace.

- El enlace sobre el túnel GRE no requiere ninguna información de estado, por lo que puede ocurrir que un extremo del túnel se encuentre en estado de down y el otro continúe presentándose como up.

- Para evitar esta situación habilite keepalive en cada extremo del túnel. De este modo cada extremo enviará mensajes de keepalive sobre el túnel y si un extremo no recibe los mensajes enviados por el otro entonces pasará al estado de down

3.2.4. TUNELES IPV4

Primero hago un túnel IPv4:

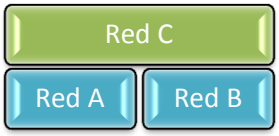

Figura III-13: Redes Intermedias A, B, C. **[A]**

Tengo 3 redes: las redes internas A y B, y una red intermedia C (por ejemplo, Internet).

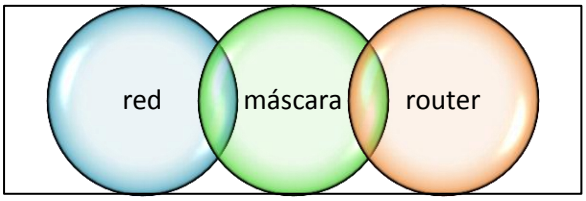

Figura III-14: Diagrama de configuración. **[A]**

De manera que tenemos la red A:

```
red 10.0.1.0
máscara de red 255.255.255.0
router  10.0.1.1
```

Tabla III-13: Red A. **[A]**

El router tiene la dirección 172.16.17.18 en la red C. Llamo a esta red neta (ok, no es muy original)

Y la red B:

```
red 10.0.2.0
máscara de red 255.255.255.0
router  10.0.2.1
```

Tabla III-14: Red B. **[A]**

El router tiene la dirección 172.19.20.21 en la red C. Llamo a esta red netb

Hasta donde concierne a la red C, asumiré que dejara pasar los paquetes enviados de A a B y viceversa...

En el router de la red A, haré lo siguiente:

```
ip tunnel add netb mode gre remote 172.19.20.21 local 172.16.17.18
ttl 255
ip link set netb up
ip addr add 10.0.1.1 dev netb
ip route add 10.0.2.0/24 dev netb
```

Tabla III-15: Router -Red A. **[A]**

Miro esto con más atención. En la línea 1, he añadido un dispositivo de túnel, y le he llamado netb (bastante obvio porque es a donde quiero llegar). Más aun, le he dicho que use el protocolo GRE (mode gre), que la dirección remota es 172.19.20.21 (el router en el otro extremo), que mis paquetes de túnel deberían ser originados por 172.16.17.18 (lo que permite a mi router tener varias direcciones IP en la red C y decidir cual usar para el tunelizado) y que el campo TTL del paquete debería establecerse en 255 (ttl 255).

La segunda línea habilita el dispositivo.

En la tercera línea le he dado a la recién nacida interfaz netb la dirección 10.0.1.1. Esto está bien para redes pequeñas, pero cuando empiece una expedición de (MUCHOS

túneles), quizá debiera considerar usar otro rango de IP para las interfaces de túneles (en este ejemplo, podría usar 10.0.3.0).

En la cuarta línea he establecido la ruta hacia la red B. Fíjese la notación diferente para la máscara de red. Si no está familiarizado con esta notación, así es como funciona: escriba la máscara de red en forma binaria, y cuente todos los unos. Si no sabe cómo hacerlo, limítese a recordar que 255.0.0.0 es /8, 255.255.0.0 es /16 y 255.255.255.0 es /24. Ah, y 255.255.254.0 es /23, en caso de que tuviera curiosidad.

Router de la red B.

```
ip tunnel add neta mode gre remote 172.16.17.18 local 172.19.20.21
ttl 255
ip link set neta up
ip addr add 10.0.2.1 dev neta
ip route add 10.0.1.0/24 dev neta
```

Tabla III-16: Router -Red B. **[A]**

Y cuando vaya a eliminar el túnel del router A:

```
ip link set netb down
ip tunnel del netb
```

Tabla III-17: Eliminación Router A. **[A]**

Por supuesto, puede cambiar netb por neta para el router B.

3.2.5. TUNELES IPV6

Vamos con los túneles.

Asumo que tiene la siguiente red IPv6, y que quiero conectarme a la 6bone, o con una amiga.

```
Red 3ffe:406:5:1:5:a:2:1/96
```

Tabla III-18: IPv6 . **[A]**

Su dirección IPv4 es 172.16.17.18, y el router 6bone tiene la dirección IPv4 172.22.23.24.

```
ip tunnel add sixbone mode sit remote 172.22.23.24 local
172.16.17.18 ttl 255
ip link set sixbone up
ip addr add 3ffe:406:5:1:5:a:2:1/96 dev sixbone
ip route add 3ffe::/15 dev sixbone
```

Tabla III-19: IPv6 con sixbone. **[A]**

En la primera línea, he creado un dispositivo de túnel llamado sixbone. Le he dado modo sit (que es un túnel IPv6 sobre IPv4) y le digo donde debe ir (remote) y de donde viene (local). TTL se pone al máximo, 255.

Después activo el dispositivo (up). Tras esto, añado mi propia dirección de red, y establezco una ruta para 3ffe::/15 (que actualmente es la totalidad de la 6bone) a través del túnel.

Los túneles GRE son actualmente el tipo preferido de túneles. Es un estándar que está ampliamente adoptado fuera de la comunidad de Linux.

3.3. CET

Cifrado Tecnología de Cisco (CET) es un conjunto entre 40 y 56-bits de cifrado de datos estándar (DES), en la capa de red de cifrado está disponible desde la versión del software Cisco IOS 11.2.

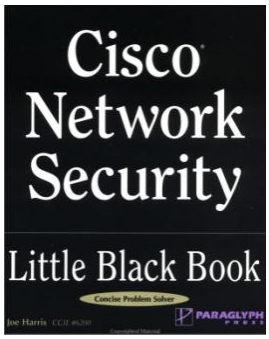

Figura III-15: Portada del libro Cisco Red Security. **[4]**

3.3.2. ¿POR QUÉ CIFRAR LOS DATOS?

Los datos se pueden leer, alterados o falsificados por cualquiera que tenga acceso a la ruta que toma sus datos. Por ejemplo, un analizador de protocolos puede leer y obtener los paquetes de información clasificada. O bien, una parte enemiga puede alterar los paquetes y causar daños al obstaculizar, reducir o impedir las comunicaciones de red dentro de su organización.

El Cifrado proporciona un medio para salvaguardar los datos de la red que viaja de un router de Cisco a otro a través de redes no aseguradas. El cifrado es especialmente importante si se han clasificado, los datos críticos que se está enviando.

La siguiente figura indica la codificación de un paquete IP a medida que viaja a través de una red no segura.

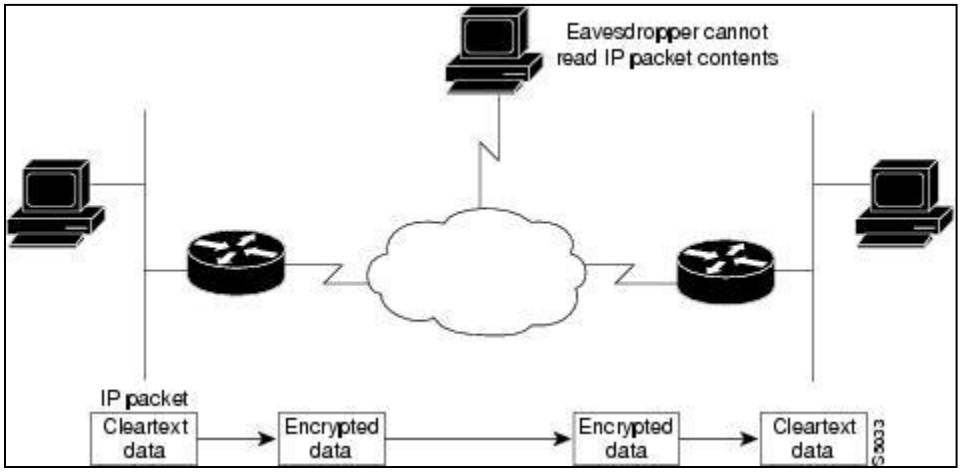

Figura III-16: Codificación de un paquete IP. **[1]**

3.3.3. ¿QUÉ LE DA CIFRADOS?

La red de cifrado de datos es proporcionada en el paquete IP, si se desea cifrar un protocolo de red que no sea de propiedad intelectual, se debe encapsular el protocolo dentro de un paquete IP.

Un paquete IP se cifra o se descifra si el paquete cumple los criterios que establezca al configurar un router para el cifrado. Cuando los datos están cifrados, los paquetes IP pueden ser detectados durante la transmisión, pero el contenido de paquetes IP no se puede leer.

En concreto, el encabezado IP y el protocolo de la capa superior, las cabeceras (por ejemplo, TCP o UDP) no están cifrados, pero todos los datos de la carga útil en el paquete TCP o UDP serán encriptados y, por tanto, no se pueden leer durante la transmisión.

3.3.4. ¿CÓMO FUNCIONA EL TRABAJO DE CIFRADO DE CISCO?

Cuando una sesión de cifrado se está creando, cada router verifica y autentifica las claves asignadas, lo cual se puede observar en el siguiente gráfico:

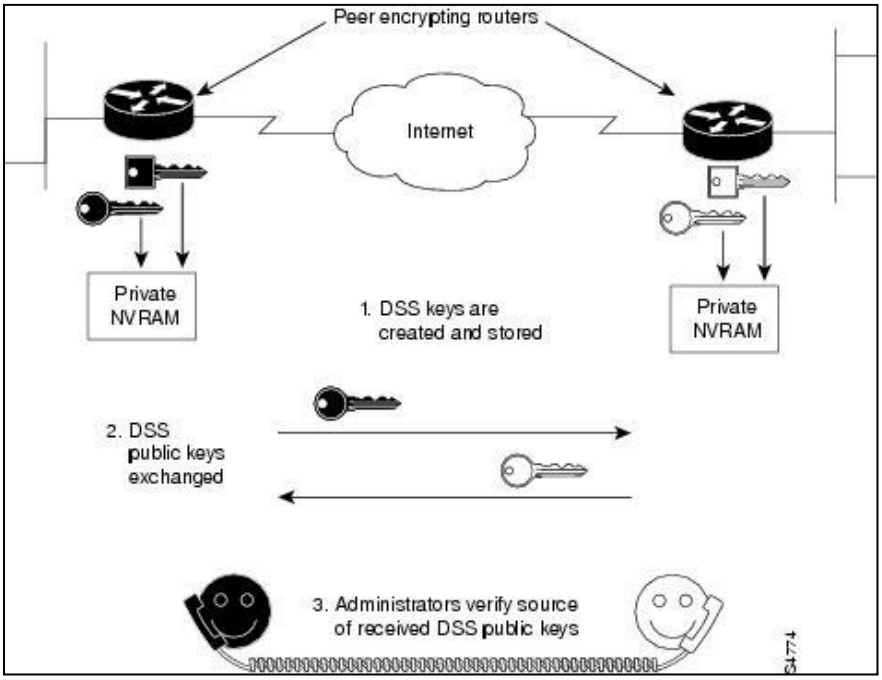

Figura III-17: Autentificación de claves publicas.**[1]**

Un período de sesiones encriptadas deben establecerse antes de que un router Cisco pueda enviar datos cifrados a un compañero router. Un período de sesiones encriptadas se establece cuando un router detecta un paquete IP que debe ser cifrado

Para establecer una sesión, debe haber dos routers de conexión para el intercambio de mensajes. Estos mensajes tienen dos objetivos:

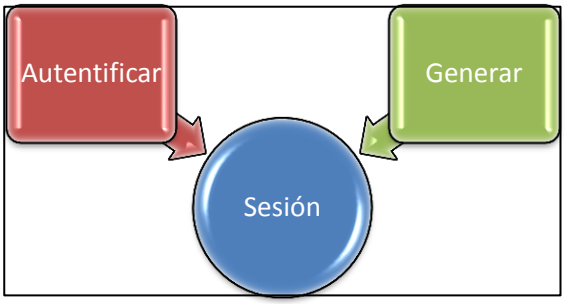

Figura III-18: Inicio de sesión entre dos routers. **[A]**

- El primer objetivo es autenticar cada router a la otra, la autenticación se logra atando "firmas" para la conexión de los mensajes: Una firma es una cadena de caracteres que se crea por cada enrutador local utilizando sus propios DSS. Una firma es siempre única para el envío del router y no puede ser forjada por cualquier otro dispositivo.
- El segundo objetivo de la conexión mensajes es generar una clave DES temporal ("clave de sesión"), que es la clave que se utiliza para cifrar los datos en realidad durante el período de sesiones encriptadas.

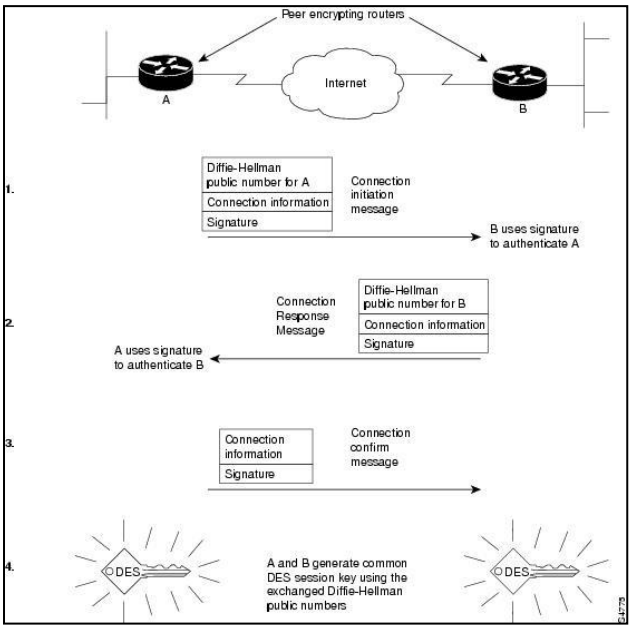

Figura III-19: Establecimiento de sesión. **[1]**

Cuando termina el período de sesiones, tanto el número de DH y la clave DES se descartan.

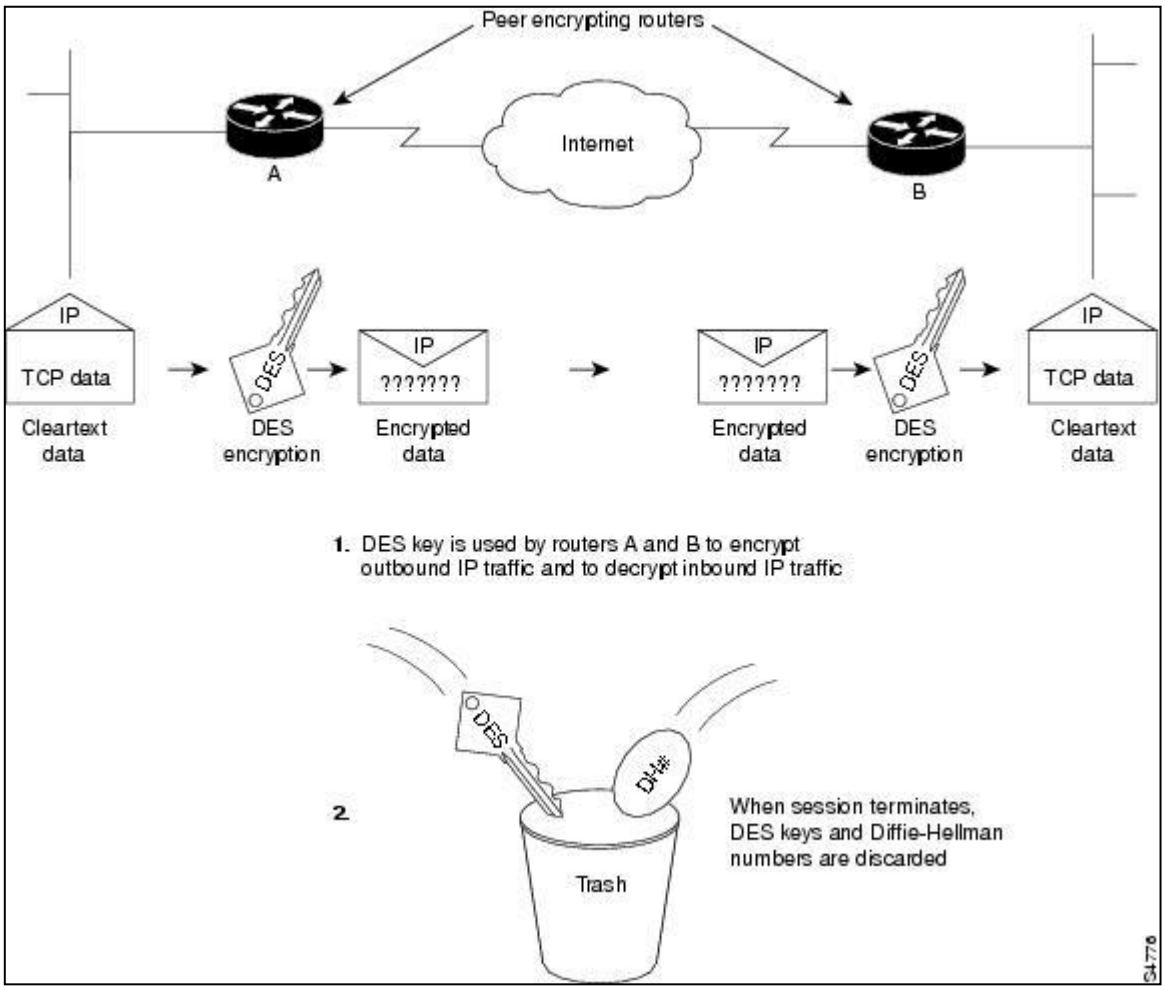

Figura III-20: Generación de claves DES. **[1]**

3.3.5. ANTES DE LA CONFIGURACIÓN DE CIFRADO

Hay verificar los siguientes puntos:

- Identificar los routers
- Considerar la topología de la red
- Identificar los motores de cifrado (crypto) de cada router

Figura III-21: Antes del Cifrado. **[A]**

3.3.6. IDENTIFICAR LOS ROUTERS

Usted debe identificar todos los routers que estarán participando en el cifrado.

3.3.7. CONSIDERAR LA TOPOLOGÍA DE LA RED

Tenga cuidado en la elección de una topología de red, se debe establecer la red de modo que un flujo de paquetes IP, ya que podría existir errores en la encriptación, por lo cual se recomienda usar una topología de red común.

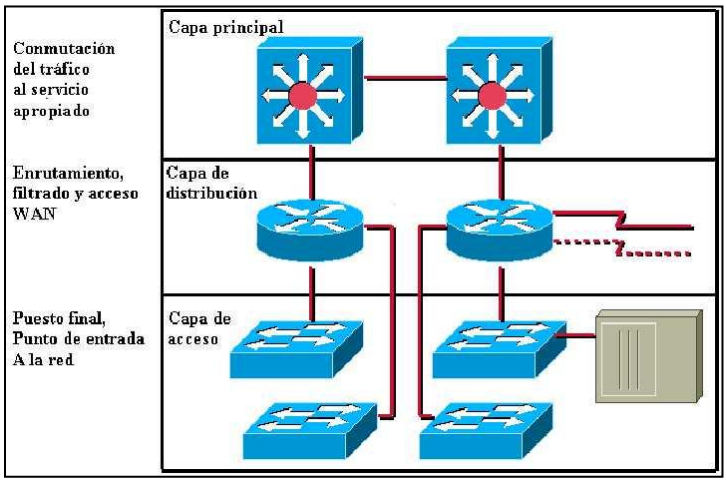

Figura III-22: Ejemplo de una conexión común entre routers. **[C]**

3.3.8. IDENTIFICAR LOS MOTORES DE CIFRADO (CRYPTO) DE CADA ROUTER

El cifrado es un software proporcionado por un servicio llamado motor de cifrado. Para realizar el cifrado en un router, primero debe configurar el motor de cifrado. Dependiendo de su configuración de hardware, los distintos motores de criptografía se reguirá diferentes interfaces del router. En algunos casos, puede que incluso necesita configurar múltiples motores de criptografía. Hay tres tipos de motores de criptografía: Cisco-IOS, la VIP2, y la ESA.

3.4. EL MOTOR DE CIFRADO DE CISCO IOS

Cada router con Cisco IOS software de encriptación tiene un motor de cifrado de Cisco IOS. Para muchos routers de Cisco, el Cisco IOS motor de cifrado, es el único motor de cifrado disponible. Las únicas excepciones son los routers 7200, RSP7000, 7500, que también puede tener otros motores de cifrado

3.5. EL VIP2 CRYPTO ENGINE (RSP7000 Y CISCO 7500 SERIES ROUTERS)

El motor de cifrado, VIP2 regula la adyacentes VIP2 puerto. El motor de cifrado de Cisco IOS regula el resto de las interfaces del router. VIP2 el motor de cifrado, se identifican por el número de ranura del chasis de la VIP2.

3.5.1. ENCAPSULACIÓN

Se puede usar cualquier tipo de encapsulado con IP cifrado, a excepción de: Si se tiene una segunda generación del procesador de Interfaz Versátil (VIP2) con una interfaz en serie, el cifrado no funcionará para el tráfico en la interfaz en serie a menos de que use el punto a -Point Protocol (PPP), el cual dará un alto nivel de enlace de datos de Control (HDLC).

Adaptador de puerto de apoyo					
Interfaz	Encapsulación	7200 de software	7200 ESA	7500/VIP Distribución de Software	7500/VIP ESA
4E, 8E, 5EFL	— --	Sí	Sí	Sí	Sí
FE	— --	Sí	Sí	Sí	Sí
4R	— --	Sí	Sí	Sí	Sí
FDDI	— --	Sí	Sí	Sí	Sí
100VG	— --	Sí	Sí	Sí	Sí
4T	PPP, HDLC,	No	No	Sí	No

	Frame Relay				
4T +, 8T	PPP	Sí	Sí	Sí	Sí
	HDLC	Sí	Sí	Sí	Sí
	Frame Relay	Sí	Sí	Sí	Sí
	X.25	Sí	Sí	No	No
	SMDS	Sí	Sí	No	No
HSSI	PPP	Sí	Sí	Sí	Sí
	HDLC	Sí	Sí	Sí	Sí
	Frame Relay	Sí	Sí	Sí	Sí
	X.25	Sí	Sí	No	No
	SMDS	Sí	Sí	No	No
CT1, CE1	PPP	Sí	Sí	Sí	Sí
	HDLC	Sí	Sí	Sí	Sí
	Frame Relay	Sí	Sí	Sí	Sí
	X.25	Sí	Sí	No	No
	SMDS	Sí	Sí	No	No
PRI	HDLC PPP	Sí	Sí	No	No
		Sí	Sí	No	No
BRI	HDLC	Sí	Sí	No	No
	PPP	Sí	Sí	No	No
ATM	— --	Sí	Sí	Sí	No
CT3	— --	No	No	Sí	No

Tabla III-20: Adaptadores de puertos de apoyo. **[A]**

3.5.2. CONFIGURACIÓN DE CIFRADO

Para pasar el tráfico cifrado entre dos routers, se debe configurar el cifrado en ambos routers. Para generar DSS para un motor de cifrado, se lo hace utilizando al menos el primero de los siguientes comandos en el modo de configuración global:

Comando	Propósito
Router (config)# crypto key	DSS genera claves públicas y

generate dss key-name [slot]	privadas.
Router# show crypto key mypubkey dss [slot]	Muestra DSS clave pública (clave privada no visible).
Router (config)# copy system:running-config nvram:startup-config	Guarda DSS claves privadas NVRAM. (Complete esta tarea sólo para los motores de criptografía de Cisco IOS).

Tabla III-21: Comandos para la configuración de cifrado. **[A]**.

Usted debe intercambiar las claves públicas DSS con todos los routers. Esto permite autenticar mutuamente en el inicio de las sesiones de comunicación. Para permitir el intercambio de conexión se lo hace utilizando el siguiente comando en el modo de configuración global:

Comando	Propósito
Router (config)# crypto key exchange dss passive [tcp-port]	Permite un intercambio de conexión.

Tabla III-22: Comandos para el intercambio en la conexión. **[A]**.

Para iniciar una relación de intercambio y envía una clave pública DSS utilizando el siguiente comando en el modo de configuración global:

Comando	Propósito
Router (config)# crypto key exchange dss ip-address key-name [tcp-port]	Inicia una conexión y envía la clave pública DSS.

Tabla III-23: Comandos para el intercambio en la conexión usando claves publicas DSS. **[A]**.

En la siguiente figura observamos el proceso de intercambio de claves:

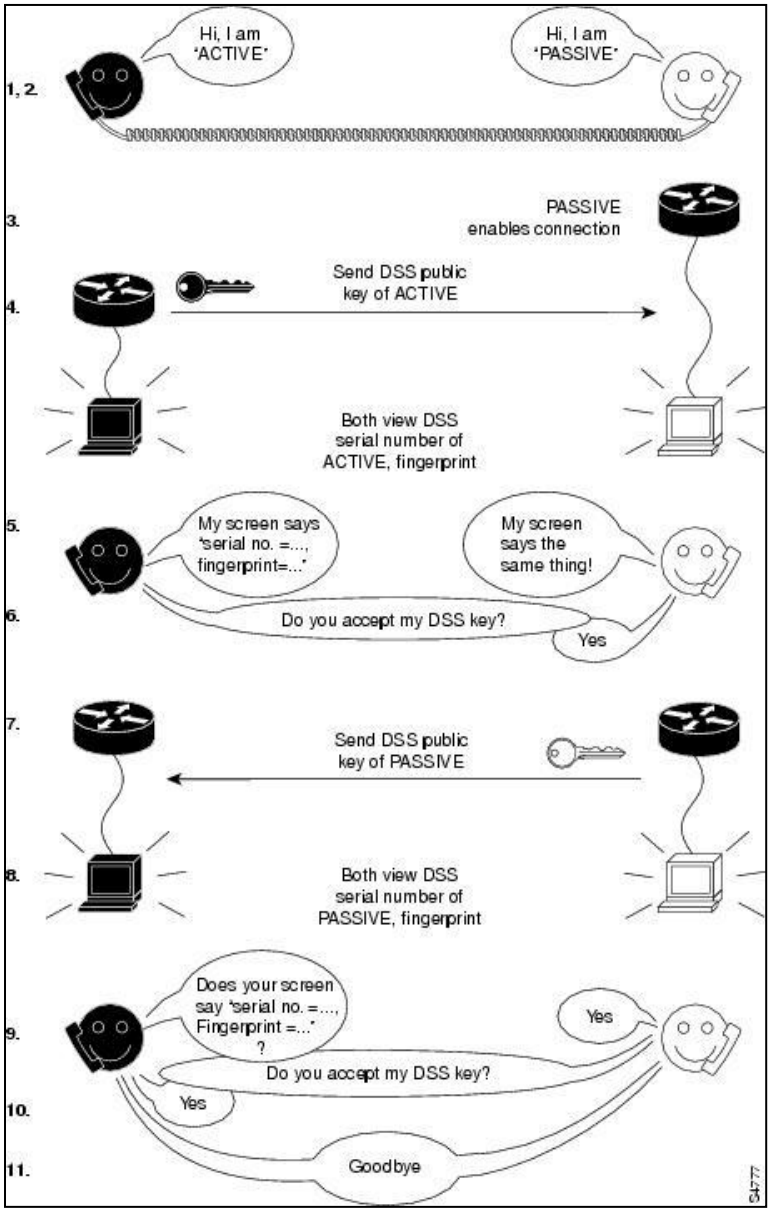

Figura III-23: Proceso de Intercambio de claves publicas DSS. **[1]**.

3.6. Algoritmos de cifrado DES[68] de habilitación

Si un algoritmo DES no está habilitado a nivel mundial, no podrá ser utilizado. Para llevar a cabo un período de sesiones encriptadas, se debe habilitar al menos un algoritmo DES. Debe configurar el mismo algoritmo DES en ambos routers para el cifrado.

[68] **DES:** Encripción de datos estándar

CET soporta cuatro algoritmos de cifrado:

• DES con 8-bits de cifrado (CFB[69])
• DES with 64-bit CFB
• 40-bit de variación de DES con 8-bit (CFB)
• 40-bit de variación de DES con 64-bit (CFB)

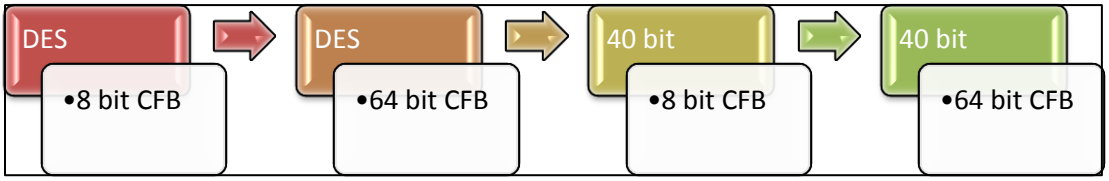

Figura III-24: Algoritmos básicos para el cifrado soportados por el CET. **[A]**.

Un algoritmo DES está habilitado para un router por defecto. Si no va a utilizar el algoritmo DES por defecto, se puede optar por desactivarlo. Si no sabe si su imagen es exportable o no exportable, puede utilizar el programa cisco de algoritmos de criptografía para determinar DES algoritmos que se encuentran actualmente habilitadas. Para verificar a qué nivel uno o varios algoritmos DES se están utilizando usamos los siguientes comandos en el modo de configuración global:

Comando	Propósito
Router (config)# crypto cisco algorithm des [cfb-8 | cfb-64]	Permite con 8-bit o 64-bits CFB.
Router (config)# crypto cisco algorithm 40-bit-des [cfb-8 | cfb-64]	Permite DES de 40 bits con 8-bit o 64-bits CFB.
Router# show crypto cisco algorithms	Muestra todas permitido DES algoritmos.

Tabla III-24: Comandos para verificar que algoritmos DES están habilitados. **[A]**.

[69] **CFB:** Cifrado de retroalimentación (Cipher Feedback)

3.7. DEFINICIÓN DE CRYPTO MAPAS

El objetivo de esta tarea es decir a las interfaces del router que debe cifrar o descifrar en el tráfico, y también que tipo de algoritmo de cifrado DES es usado para la encriptación de los paquetes. En realidad, hay tres pasos requeridos para completar esta tarea:

- Configuración de la lista de acceso de cifrado
- Definición de Crypto Mapas
- Mapas de la aplicación Crypto Interfaces

3.7.1. CONFIGURACIÓN DE LA LISTA DE ACCESO DE ENCRIPTACIÓN

Para crear listas de acceso para el cifrado de paquetes IP se lo hace utilizando cualquiera de los siguientes comandos en el modo de configuración global:

Comando	Propósito
Router (config)# access-list access-list-number [dynamic dynamic-name [timeout minutes]] { deny | permit } protocol source source-wildcard destination destination-wildcard [precedence precedence] **Router (config)# ip access-list extended name**	Especifica las condiciones en el intercambio de paquetes IP

Tabla III-25: Comandos para la lista de acceso a la encripción. **[A]**.

3.7.2. DEFINICIÓN DE CRYPTO MAPAS

Para definir crypto mapas usamos los siguientes comandos:

	Comando	Propósito
Paso 1	Router (config)# crypto map map-name seq-num [cisco]	Ingresamos al modo de configuración de los crypto mapas
Paso 2	Router (config-crypto-map)# set peer key-name	Especifica el router
Paso 3	Router (config-crypto-map)# match address [access-list-id | name]	Especifica la última encripción de acceso
Paso 4	Router (config-crypto-map)# set algorithm des [cfb-8 | cfb-64] or o Router (config-crypto-map)# set algorithm 40-bit-des [cfb-8 | cfb-64]	Especifica el algoritmo de encripción

Tabla III-26: Configuración de lo crypto mapas. **[A]**.

3.7.3. MAPAS DE LA APLICACIÓN CRYPTO INTERFACES

Utilizamos los siguientes comandos:

Comando	Propósito
Router (config-if)# crypto map map-name	Aplica un crypto mapa en una interface

Tabla III-27: Configuración de lo crypto interfaces. **[A]**.

Para resetear el ESA[70] necesitamos los siguientes comandos:

[70] **ESA:** Encripción estándar de Autenticación

	Comando	Propósito
Paso 1	Router (config)# crypto card clear-latch slot	Resetea el ESA
Paso 2	Router (config)# password	Crea una contraseña

Tabla III-28: Comandos para resetear el ESA. **[A]**.

Resetea el ESA, previamente usado sin conocer la contraseña del ESA, usando los siguientes comandos:

Comando	Propósito
Router (config)# crypto key zeroize dss slot	Limpia el ESA

Tabla III-29: Comandos para resetear el ESA sin conocer la contraseña. **[A]**.

Para habilitar el ESA en routers Cisco 7200 series se usan los siguientes comandos:

Comando	Propósito
Router (config)# crypto card enable slot	Habilita el ESA.

Tabla III-30: Comandos para habilitar ESA en routers 7200. **[A]**.

Seleccionamos el Cisco IOS y a la vez el motor de cifrado en el modo de configuración global usando lo siguiente:

Comando	Propósito
Router (config)# crypto card shutdown slot	Deshabilita el ESA.

Tabla III-31: Comandos para deshabilitar ESA. **[A]**.

Para borrar las claves DSS, usamos los comandos en el modo EXEC:

	Comando	Propósito
Paso 1	Router# show crypto key mypubkey dss	Visualiza todas las existentes claves DSS (ESA y Cisco IOS keys).
Paso 2	Router# show crypto engine configuration	Determina el crypto engine activo.
Paso 3	Router (config)# crypto card enable slot Router (config)# crypto card shutdown slot	Usamos el crypto card enable para Cisco IOS crypto engine Usamos el crypto card shutdown para ESA crypto engine.
Paso 4	Router# show crypto engine configuration	Verificamos el motor de cifrado
Paso 5	Router (config)# crypto key zeroize dss Router (config)# crypto key zeroize dss slot	Borramos las claves DSS del motor de cifrado

Tabla III-32: Comandos para borrar claves DSS. **[A]**.

Para cambiar el tiempo de sesión de la encriptación usamos los siguientes comandos:

	Comando	Propósito
Paso 1	Router (config)# crypto cisco key-timeout minutes	Definimos el máximo tiempo de duración de las sesiones cifradas

Paso 2	Router# show crypto cisco key-timeout	Define la duración de las sesiones encriptadas

Tabla III-33: Comandos para cambiar el tiempo de sesión. **[A]**.

Para pre-generar los números DH, usamos los siguientes comandos:

Comando	Propósito
Router (config)# crypto cisco pregen-dh-pairs count [slot]	Pregenera los números DH

Tabla III-34: Comandos para habilitar ESA en routers 7200. **[A]**.

Para cambiar los límites por defecto de las entidades encriptadas usamos los siguientes comandos:

Comando	Propósito
Router (config)# crypto cisco entities number	Cambia el número máximo de hosts o subnets que se pueden definir en la lista de cifrado de acceso.
Router (config)# crypto cisco connections number	Cambia el número máximo de destinarios (hosts o subnets)

Tabla III-35: Comandos para cambiar límites por defecto de las entidades encriptadas. **[A]**.

Para plataformas Cisco 7200 usamos los siguientes comandos:

Comando	Propósito
Router (config)# crypto key zeroize dss [slot] 1	Elimina las DSS

Tabla III-36: Comandos para eliminar las claves DSS en routers Cisco 7200. **[A]**.

Para probar la configuración del cifrado lo hacemos en el modo EXEC privilegiado

	Comando	Propósito
Paso 1	Router# test crypto initiate-session src-ip-addr dst-ip-addr map-name seq-num	Prueba el cifrado
Paso 2	Router# show crypto cisco connections	Visualiza el estado de la conexión

Tabla III-37: Comandos para la configuración del cifrado. **[A]**.

Si se necesita verificar el estado de la conexión, se usa los siguientes comandos en modo EXEC privilegiado:

Comando	Propósito
Router# show crypto cisco connections	Verifica el estado de cifrado de las conexiones.
Router# show crypto map	Chequea el estado de un crypto map
Router# show crypto engine connections active	Chequea la conexión establecida de los paquetes que están siendo cifrados

Tabla III-38: Comandos para verificar el estado de la conexión. **[A]**.

En el siguiente grafico visualizamos el intercambio de claves entre routers

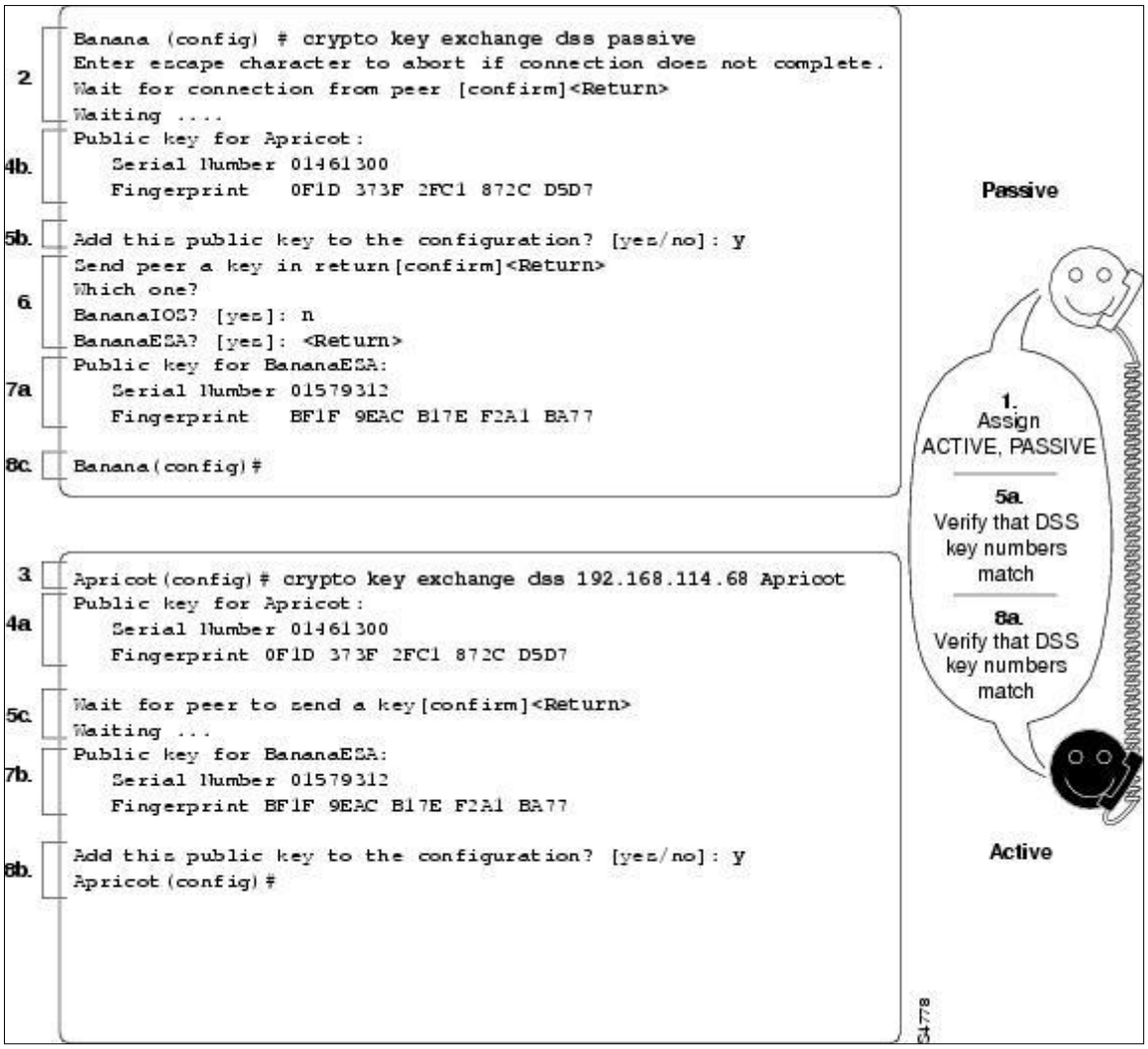

Figura III-25: Intercambio de claves, entre dos routers. **[1]**.

En la siguiente red, se ejemplificara la configuración usando algoritmos de cifrado

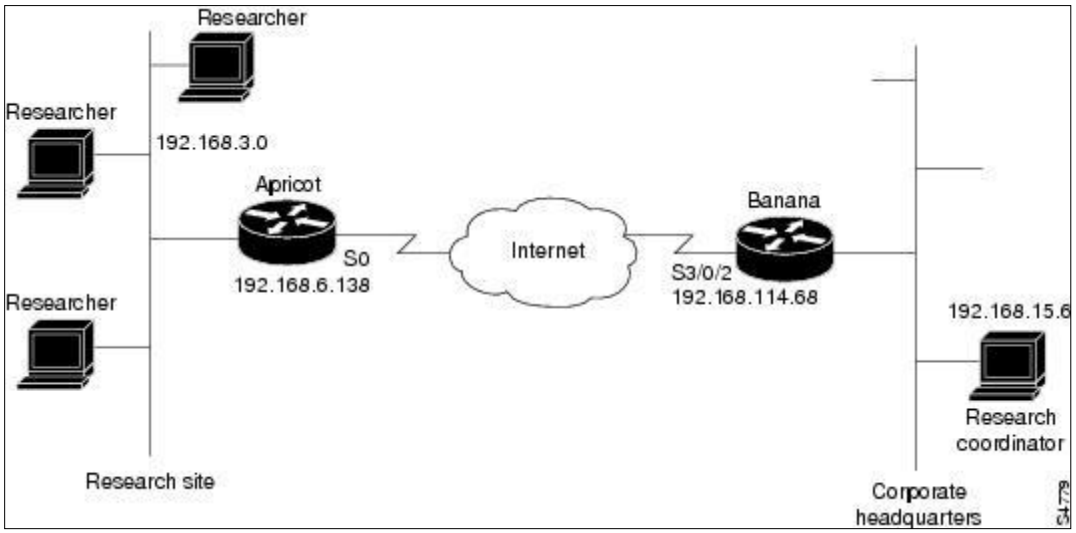

Figura III-26: Ejemplo de red de computadores, que usa algoritmos de cifrado a través de dos routers. **[1]**.

Apricot es un router Cisco 2500 y Banana es un router Cisco 7500

Configuración:

Router Apricot

```
Apricot(config)# access-list 101 permit tcp 192.168.3.0 0.0.0.15
host 192.168.15.6
Apricot(config)# crypto map Research 10
Apricot(config-crypto-map)# set peer BananaESA
Apricot(config-crypto-map)# set algorithm des cfb-8
Apricot(config-crypto-map)# match address 101
Apricot(config-crypto-map)# exit
Apricot(config)# interface s0
Apricot(config-if)# crypto map Research
Apricot(config-if)# exit
Apricot(config)#
```

Figura III-27: Router Apricot **[1]**.

Router Banana

```
Banana(config)# access-list 110 permit tcp host 192.168.15.6
192.168.3.0 0.0.0.15
Banana(config)# crypto map Rsrch 10
Banana(config-crypto-map)# set peer Apricot  Banana(config-crypto-
map)# set algorithm des cfb-8
```

```
Banana(config-crypto-map)# set algorithm des cfb-64
Banana(config-crypto-map)# match address 110
Banana(config-crypto-map)# exit
Banana(config)# interface s3/0/2
Banana(config-if)# crypto map Rsrch
Banana(config-if)# exit
Banana(config)#
```

Figura III-28: Router Banana **[1]**.

CAPÍTULO IV. SEGURIDAD INFORMÁTICA

4. ¿QUÉ ES SEGURIDAD?

El concepto de red global incluye todos los recursos informáticos de una organización, aún cuando estos no estén interconectados:

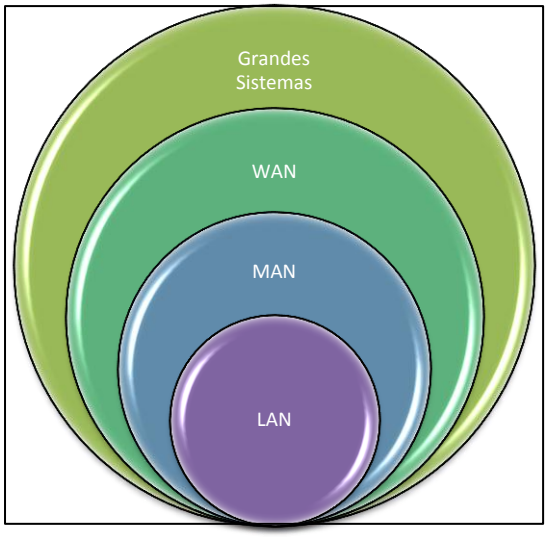

Figura IV-1: Sistemas interconectados. **[A]**.

De manera que, seguridad global es mantener bajo protección todos los componentes de una red global.

Al fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad. (Por ejemplo: permite que se determine exactamente lo que debe hacer cada uno y cómo debe hacerlo, y, también las

desviaciones que se pueden producir). De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene.

Para realizar esto, lo más usado, y que da muy buenos resultados es hacer “grupos de trabajo” en los cuales se informen los fines, objetivos y ganancias de establecer medidas de seguridad, de tal manera que los destinatarios finales se sientan informados y tomen para sí los conceptos. Este tipo de acciones favorece, la adhesión a estas medidas.

4.1. IMPACTO EN LA ORGANIZACIÓN

La implementación de políticas de seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. ¿Cómo pueden impactar si se implementan para hacer más seguro el sistema? En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativa.

Por otro lado, al poner en funcionamiento una nueva norma de seguridad, ésta traerá una nueva tarea para la parte técnica (por ejemplo, cambiar los derechos a algo de algunos usuarios) y administrativamente, se les deberá avisar por medio de una nota de los cambios realizados y en qué les afectará.

4.2. VISIBILIDAD DEL PROCESO

En un reciente estudio de Datapro Research Corp. se resumía que los problemas de seguridad en sistemas basados en redes responden a la siguiente distribución:

- Errores de los empleados 50%
- Empleados deshonestos 15%
- Empleados descuidados 15%
- Intrusos ajenos a la Empresa 10%
- Integridad física de instalaciones 10%

Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos:

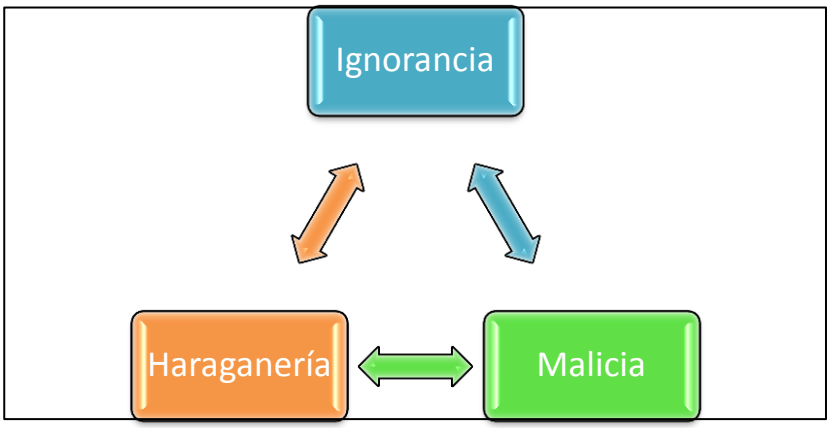

Figura IV-2: Problemas en los sistemas informáticos. **[A]**.

4.3. ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)?

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

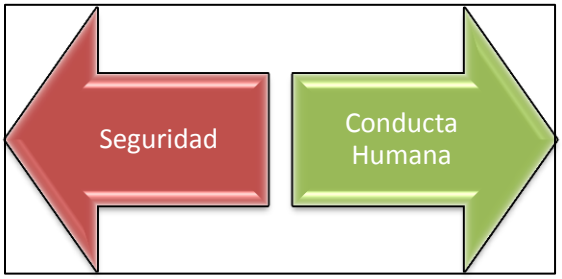

Figura IV-3: Relación conducta humana vs seguridad. **[A]**.

4.4. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como mencionábamos en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

Figura IV-4: Elementos PSI. **[A]**.

4.5. CORTA FUEGOS

Un corta fuegos es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, bien permitiéndolas bien prohibiéndolas según las políticas de red que haya definido la organización responsable de la misma. La ubicación habitual de un corta fuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la

red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Figura IV-5: Corta Fuegos. **[C]**.

4.5.1. CORTA FUEGOS DE CAPA DE RED O DE FILTRADO DE PAQUETES

Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino, etc. A menudo en este tipo de corta fuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC. Este es un de los principales tipos de corta fuegos.

4.5.2. CORTA FUEGOS DE CAPA DE APLICACIÓN

Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

4.5.3. CORTA FUEGOS PERSONAL

Es un caso particular de corta fuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Es recomendable para uno mismo.

4.5.4. VENTAJAS DE UN CORTA FUEGOS

- **Protege de intrusiones.-** El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- **Protección de información privada.-** Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.

- **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

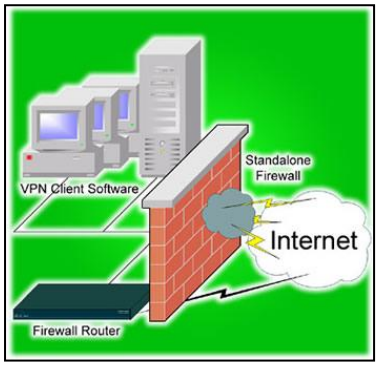

Figura IV-6: Ejemplo de un Corta fuegos en una red. **[3]**.

4.5.5. LIMITACIONES DE UN CORTA FUEGOS

Las limitaciones se desprenden de la misma definición de corta fuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el corta fuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un corta fuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

- El corta fuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El corta fuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.

- El corta fuegos no puede proteger contra los ataques de ingeniería social.

- El corta fuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

- El corta fuegos no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

4.5.6. POLÍTICAS DEL CORTA FUEGOS

Hay dos políticas básicas en la configuración de unos corta fuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El corta fuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

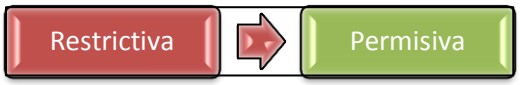

Figura IV-7: Políticas de un Corta fuegos en una red. **[A]**.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

4.6. ATAQUES REMOTOS.

En el presente apartado, se describirán los modos de ataques que podrían ocurrir más frecuentemente en las redes de información. Debido a la pérdida de dinero y de tiempo que estos ataques pueden ocasionar, se presentarán también algunas formas de prevención y de respuesta a los mismos.

4.6.1. DENIAL OF SERVICE

Denial of service es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

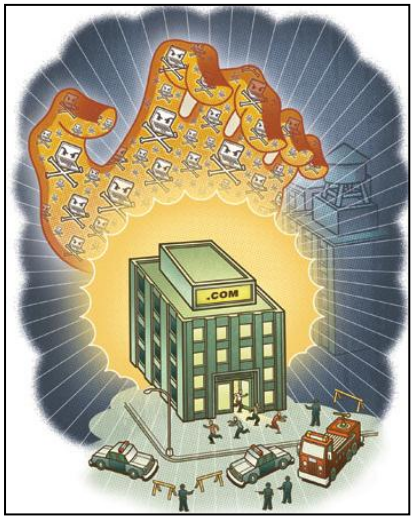

Figura IV-8: Ataques a la infraestructura de la red. **[C]**.

Algunos ejemplos de este tipo de ataque son:

- Tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma.
- Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio.

- Tentativas de evitar que una determinada persona tenga acceso a un servicio.
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario.

4.6.2. MODOS DE ATAQUE

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina “ataque asimétrico”. Por ejemplo, un atacante con una vieja PC y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados “nukes” en los cuales caen instalaciones grandes.

Hay tres tipos de ataques básicos de negación de servicios:

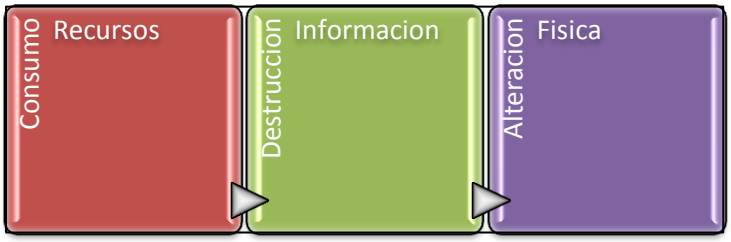

Figura IV-9: Ataques básicos. **[A]**.

4.6.3. SISTEMA DE DETECCIÓN DE INTRUSOS

- Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

- Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.

- Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

- Los IDS: aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

4.6.4. CRIPTOGRAFÍA

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en puridad, esta técnica no se considera criptografía, sino esteganografía[71]. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usados para justificar un texto. La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

4.7. HERRAMIENTAS COMUNES DE SEGURIDAD

[71] **ESTEGANOGRAFÍA:** es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

Según una encuesta hecha por *Insecure.com* a 1200 usuarios del *NMAP* en su lista de correo, las herramientas de seguridad preferidas e independientemente de la plataforma, son las siguientes:

Ordenadas empezando por la más popular, se agrupan utilidades como scanners, sniffers y demás programas de seguridad. Se incluye el enlace para descargarlas y una breve explicación sobre su uso y/o utilidad.

- **Nessus** (http://www.nessus.org**):** este programa es un scanner de seguridad empleado para hacer más de una auditoría en busca de vulnerabilidades. Consta de dos partes, cliente y servidor (nessusd) con versiones para Windows, Java y Unix (la parte cliente) y sólo para Unix el servidor. El servidor /daemon realiza los ataques mientras que el cliente interactúa con el usuario a través de un interface gráfico.
  Pros: desarrolla una completa exploración de todos los puertos y servicios y presenta los puntos vulnerables que encuentra y sus posibles soluciones. **Contras:** es un poco lento. Como comentario decir que es comparable al Retina.

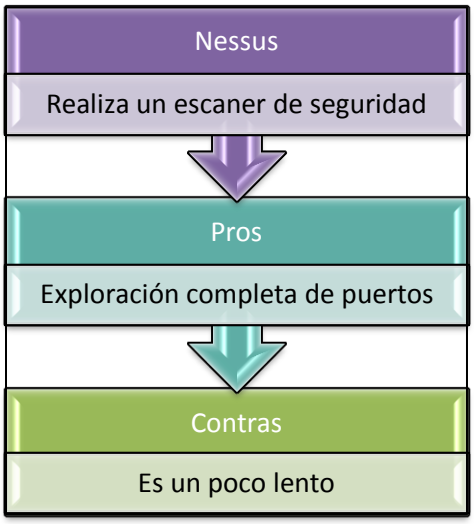

Figura IV-10: Pros y Contras Nessus. **[A]**.

- **Netcat (**http://www.atstake.com/research/tools/nc11nt.zip**):** esta sencilla utilidad para Windows y Unix sirve para escuchar y analizar las conexiones de red usando los protocolos TCP o UDP. Se ha usado bastante para explotar el bug del ISAPI en los servidores IIS.

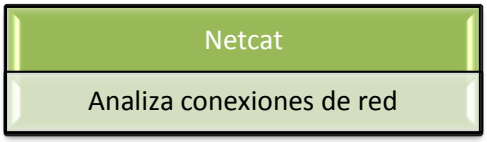

Figura IV-11: Netcat. **[A]**.

- **TCPDump (**http://www.tcpdump.org**):** este sniffer para Unix sirve para monitorizar todo el tráfico de una red, recolectar toda la información posible y detectar así posibles problemas como *ataques ping*. Combinado con SNORT se convierte en una poderosa herramienta solventando las carencias que ambos programas tienen por separado. Es curioso porque podemos servirnos del propio TCPDump para evadir IDSs de los que forma parte porque presenta una vulnerabilidad en las capacidades de decodificación de DNS y puede entrar en un loop infinito que nos permita saltarnos ese IDS (Sistema de Detección de Intrusos).

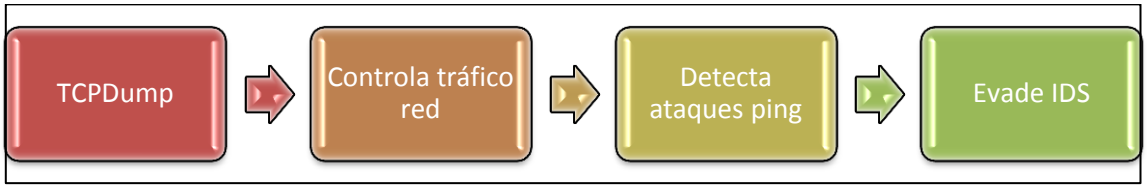

Figura IV-12: Ciclo TCPDump. **[A]**.

- **Snort (**http://www.snort.org**):** sniffer/logger, Snort sirve para detectar intrusiones y ataques tipo búfer overflows, CGI, SMB, escaneo de puertos, etc. Snort puede enviar alertas en tiempo real, enviándolas directamente al archivo de Unix *syslog* o incluso a un sistema Windows mediante SAMBA. Las versiones anteriores a la 1.8.1 presentan una vulnerabilidad en la codificación Unicode que posibilita que un atacante evada dicha detección.

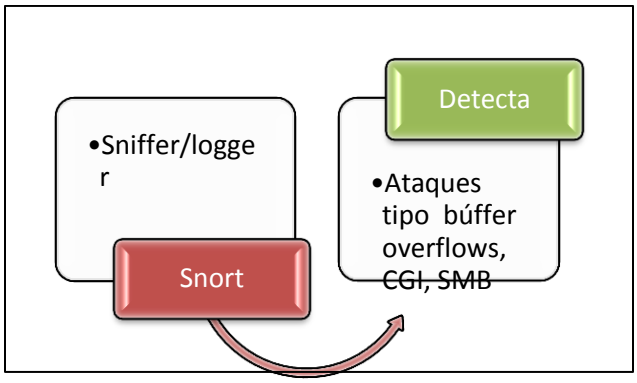

Figura IV-13: Ciclo Snort. **[A]**.

- **Saint (**http://www.wwdsi.com/saint**):** Security Administrator's Integrated Red Tool (SAINT) es una evolución del conocido SATAN para plataformas Unix que sirve para evaluar toda la seguridad de un sistema recibiendo incluso múltiples updates desde el CERT y CIAC.

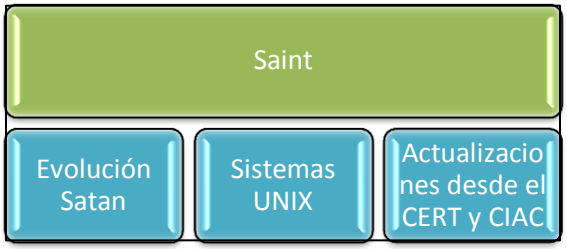

Figura IV-14: Evolución Saint. **[A]**.

- **Ethereal (**http://ethereal.zing.org**):** este sniffer de red para Unix tiene un entorno gráfico y soporta decodificación de diversos protocolos pero presenta una vulnerabilidad de búfer overflow (versiones anteriores a la 0.8.14).

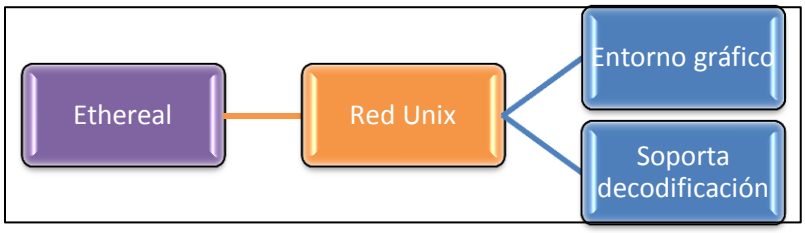

Figura IV-15: Proceso de Ethereal en Unix. **[A]**.

- **ISS (**http://www.iss.net**):** Internet Security Scanner es una herramienta comercial de análisis de vulnerabilidades para Windows

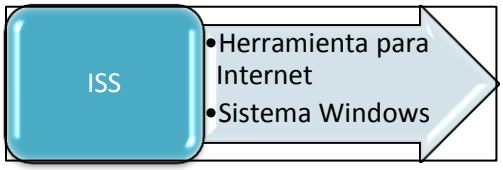

Figura IV-16: ISS. **[A]**.

- **Abacus Portsentry (**http://www.psionic.com/abacus/portsentry**):** Demonio de Unix para detectar escaneos de puertos contra nuestros sistemas capaz de bloquear al atacante mediante host.deny, filtrar las rutas o reglar el firewall

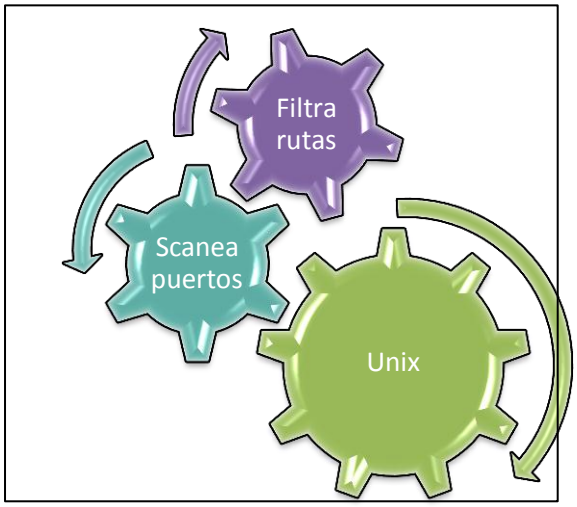

Figura IV-17: Proceso Abacus Portsentry. **[A]**.

- **DSniff (**http://naughty.monkey.org/~dugsong/dsniff**):** El nombre ya lo dice todo... este es un sniffer para buscar contraseñas y el resto de información de una red incluyendo técnicas sofisticadas para defender la "protección" de los switchers de red

Figura IV-18: Proceso para buscar contraseñas. **[A]**.

CAPÍTULO V. TÚNELES DE CONEXIÓN SEGURA

5. ¿QUÉ ES UN TÚNEL?

Un túnel es creado al usar el protocolo PPTP[72], extensión de PPP[73], el cual aporta niveles de seguridad adicional a la información transmitida.

5.1. Funcionamiento

El cliente remoto se conecta al ISP[74] (mediante PPP), y la segunda llamada se establece entre el cliente y el servidor de la red privada creándose un túnel PPTP seguro.

La trama PPTP está compuesta de encabezados IP, GRE y PPP, los cuales cumplen la función de encapsular en GRE los datos originales.

5.2. IAS[75] y los túneles

La creación de túneles, también conocida como encapsulación, es un modo de utilizar una infraestructura de redes de un protocolo para transferir una carga. En algunas ocasiones, la carga está formada por tramas (o paquetes) de otro protocolo. En lugar de enviarse tal y como la produce el host de origen, la trama se encapsula con un encabezado adicional.

Este encabezado adicional proporciona información de enrutamiento para que la carga encapsulada pueda atravesar un conjunto de redes públicas y privadas intermedias (también conocido como conjunto de redes públicas y privadas de tránsito). Luego, los paquetes encapsulados se enrutan entre los extremos del túnel a través del conjunto de redes públicas y privadas de tránsito. Una vez los paquetes de carga encapsulados llegan a su destino en el conjunto de redes públicas y privadas de tránsito, la trama se desencapsula y se reenvía a su destino final.

Todo el proceso de encapsulación, transmisión y desencapsulación de paquetes se denomina túnel. El túnel es la ruta de acceso lógica en el conjunto de redes públicas y privadas de tránsito a través de la cual viajan los paquetes encapsulados.

[72] **PPTP:** Permite el seguro intercambio de datos de un cliente a un server formando un Virtual Private Network
[73] **PPP:** Protocolo punto a punto, es un protocolo de nivel de enlace estandarizado
[74] **ISP:** Proveedor de servicios de Internet
[75] **IAS:** Infraestructura de autentificación estándar

En las conexiones de red privada virtual de acceso remoto (VPN), existen dos tipos de túneles:

1. Túneles voluntarios
2. Túneles obligatorios

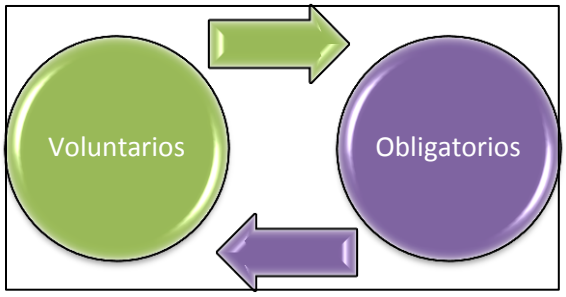

Figura V-1: Reciprocidad entre túneles voluntarios y obligatorios. **[A]**.

5.2.1. Túneles voluntarios

Un equipo usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un enrutador utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente.

En una situación de acceso telefónico, que es la más común, el cliente debe establecer primero una conexión de acceso telefónico con el conjunto de redes para poder crear un túnel. Un buen ejemplo de esto es el usuario de acceso telefónico a Internet que, para crear un túnel a través de Internet, debe llamar primero a un ISP.

El túnel voluntario no es diferente de otros tipos de acceso a la red e IAS se puede utilizar para la autenticación, autorización y administración de cuentas.

5.2.2. Túneles obligatorios

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de

los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El equipo o dispositivo de red que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) en PPTP, concentrador de acceso (LAC) de L2TP[76] en L2TP o puerta de enlace de Seguridad IP en IPSec. El término FEP se utiliza para describir la función de creación de túneles, independientemente del protocolo utilizado. Para realizar su función, el FEP debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión. El servicio Enrutamiento y acceso remoto de Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; Windows Server 2003, Datacenter Edition y Windows 2000 no se puede usar como FEP.

Una organización puede contratar a un ISP para que implemente un conjunto de FEP por toda la nación. Estos FEP pueden establecer túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización.

Existen dos tipos de túneles obligatorios. En el primer tipo, el túnel se crea antes de autenticar al cliente de acceso. El FEP envía una petición de acceso a un servidor IAS en función del nombre de territorio o el Id. de autor se llama del cliente de acceso. El servidor IAS devuelve una aceptación de acceso (Access-Accept) inmediata con atributos RADIUS [77]para la creación del túnel sin realizar autenticación ni autorización. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel.

En el segundo tipo de túnel obligatorio, el túnel se crea después de que el FEP autentica al cliente de acceso. En este caso, el FEP envía el mensaje de petición de acceso (Access-Request) con las credenciales de cliente a un servidor IAS. El servidor IAS autentica y autoriza el intento de conexión y devuelve atributos RADIUS en el mensaje de aceptación de acceso (Access-Accept), que indican al NAS cómo iniciar un túnel a un servidor VPN.

[76] **L2TP:** Protocolo de túnel en la capa 2

[77] **RADIUS:** (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP

El extremo del túnel (el servidor VPN donde termina el túnel), se puede cambiar en función de determinadas condiciones de la directiva de acceso remoto, Por ejemplo, según el nombre de usuario o la pertenencia a grupos de cuentas de usuario. El control de túneles obligatorios con directivas de acceso remoto proporciona mayor flexibilidad que los túneles estáticos (que requieren un servidor de acceso a la red dedicado) o que los túneles basados en territorios (que requieren que todos los usuarios de un mismo territorio tengan la misma configuración de túnel).

5.2.3. Atributos RADIUS que se usan con los túneles obligatorios

En la siguiente lista se enumeran los atributos RADIUS que se utilizan para transportar la información de túnel obligatorio desde el servidor IAS al FEP. Se utiliza el mismo conjunto de atributos sea cual sea el tipo de túnel obligatorio.

- Atributos utilizados sólo en la autorización:
  - Tunnel-Preference
  - Tunnel-Password

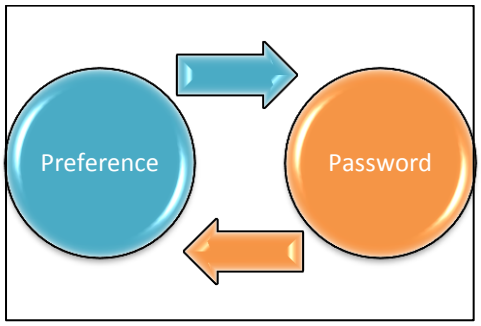

Figura V-2: Reciprocidad entre los atributos usados en la autorización. **[A]**.

Este atributo no se debe utilizar con proxy[78] RADIUS.

- Atributos utilizados en la autorización y la administración de cuentas:
  - Tunnel-Type (por ejemplo, PPTP y L2TP)
  - Tunnel-Medium-Type (por ejemplo, X.25, ATM, Frame Relay e IP)
  - Tunnel-Client-Endpoint

[78] **PROXY:** Sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

- Tunnel-Server-Endpoint
- Tunnel-Private-Group-ID
- Tunnel-Assignment-ID
- Tunnel-Client-Auth-ID
- Tunnel-Server-Auth-ID

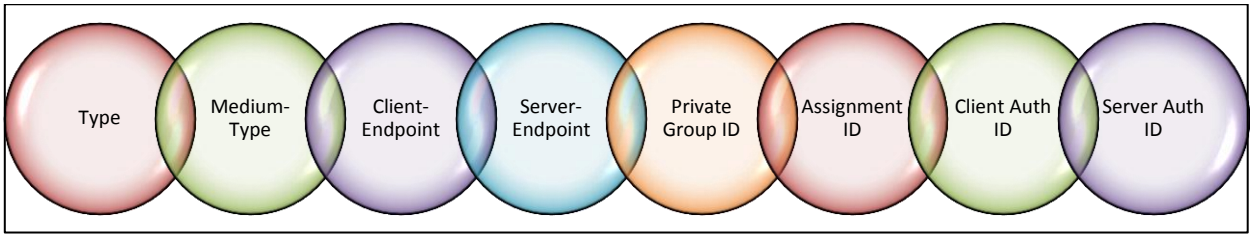

Figura V-3: Túneles no usados en RADIUS. **[A]**.

- Atributos utilizados sólo en la administración de cuentas:
  - Acct-Tunnel-Connection-ID

Atributo	Valor
Framed-Protocol	PPP
Service-Type	Outbound-User
Tunnel-Medium-Type	IP (IP versión 4)
Tunnel-Password	og*37y#cW@95?4xT
Tunnel-Server-Endpt	131.107.9.41
Tunnel-Type	Protocolo de túnel de capa dos (L2TP)

Tabla V-1: Atributos usados en la administración de cuentas. **[A]**

5.3. FUNCIONES DEL TÚNEL GRE

Los túneles GRE están diseñados para ser completamente interdependientes. Esto significa que cada punto final del túnel no guarda ninguna información sobre el estado de disponibilidad o el mando a distancia túnel punto final. Una consecuencia de ello es que los entes locales no tienen la capacidad para poner la línea de protocolo de la interfaz, si el extremo remoto del túnel no es accesible.

La posibilidad de marcar una interfaz como cuando el extremo remoto de la conexión no está disponible se utiliza para eliminar cualquier ruta en la tabla de enrutamiento que utilizan de salida. En concreto, si la línea de protocolo para una interfaz se cambia a abajo, cualquier ruta se elimina de la tabla de enrutamiento. Esto permite la instalación de un suplente (flotante) o la ruta para las Políticas Based Routing (PBR) para seleccionar un sustituto próximo-hop o interfaz.

Normalmente, una interfaz de túnel GRE aparece tan pronto como está configurado y que se mantiene activo. El túnel de la dirección IP destino también debe ser enrutable, esto es a veces cierto, incluso si la otra parte del túnel no se ha configurado, esto significa que una ruta o el reenvío de paquetes sigue en vigor a pesar que el túnel GRE no llega al otro extremo.

Entre las tres razones para un túnel GRE deba ser cerrado, tenemos las siguientes:

- No hay camino hacia el túnel (dirección de destino).
- La interfaz fuente es el túnel.
- La ruta a la dirección de destino del túnel es por el túnel en sí.

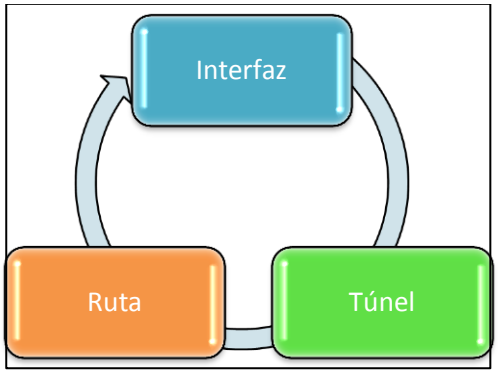

Figura V-4: Problemas en Túnel GRE. **[A]**

Estas tres normas (la ruta que faltan, la interfaz y mal encaminado túnel destino) son problemas locales al router en el túnel de parámetros y no cubren los problemas en el

intervalo de red. Por ejemplo, estas normas no cubren el caso en que el túnel GRE de paquetes se transmita con éxito, pero se pierden antes de llegar al otro extremo del túnel.

Esto hace que los paquetes de datos que pasan por el túnel GRE, a pesar de que use una ruta alternativa, utilice los derechos de obtentor. Los keepalives [79]sobre la interfaz de túnel GRE se utilizan con el fin de resolver este problema de la misma manera que se utilizan en las interfaces físicas.

Con Cisco IOS ® Software Release la 12.2 (8) T, es posible configurar keepalives en un punto del túnel GRE. Con este cambio, el túnel de la interfaz dinámica se apaga si el keepalive falla por un período determinado

5.4. Mecanismos comunes Keepalive

Los mensajes son enviados por un dispositivo de red a través de un circuito físico o virtual para informar a otro dispositivo de red. El intervalo es el período de tiempo entre cada KeepAlive (mensaje) que es enviado por un dispositivo de red

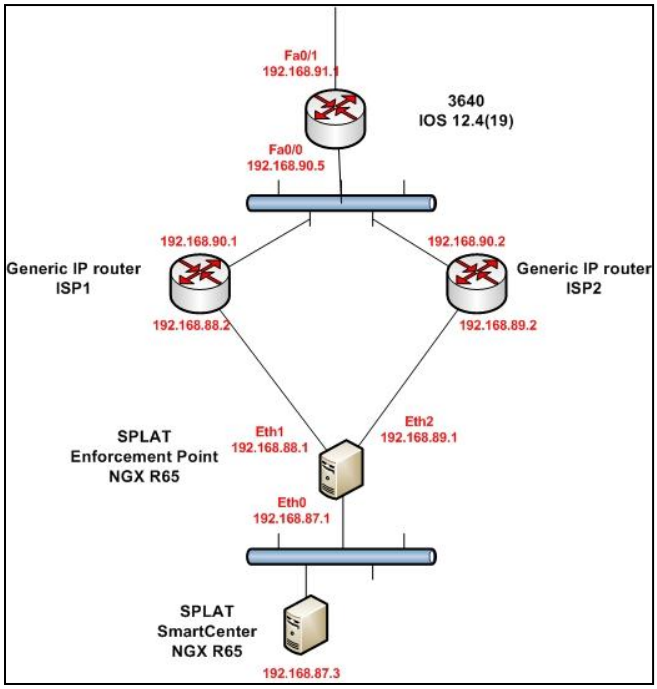

Figura V-5: Red de computadoras, que posee keepalives. **[3]**

[79] **Keepalive:** Mensajes que dicen el dispositivo está con vida, ósea activo.

5.5. Ethernet[80] Keepalives

Sobre los medios de comunicación como Ethernet, los keepalives son ligeramente diferentes. Dado que hay muchos vecinos sobre la posible Ethernet, la KeepAlive no está diseñada para determinar si la ruta de acceso a cualquier particular. Sólo está diseñado para comprobar que el sistema local tenga e; acceso de lectura y escritura para el propio cable de Ethernet. El router Ethernet produce un paquete con sí mismo como el origen y el destino de la dirección MAC de Ethernet y un especial tipo de código 0x9000.

El hardware Ethernet envía este paquete en el cable Ethernet y, a continuación, inmediatamente recibe este paquete de nuevo. Esto comprueba el envío y la recepción de hardware en el adaptador Ethernet y la integridad básica del cable.

Source MAC	Destination MAC	Protocol Type	Data	Layer-2 Padding
00-00-0C-04-EF-04	00-00-0C-04-EF-04	9000	0000 0100	0000 ... 0000

Figura V-6: Ejemplo de Ethernet Keepalive**. [4]**

5.6. HDLC KEEPALIVES

Los keepalives se envían en serie de ida y vuelta entre dos routers y los keepalives son reconocidos. Con el uso de números de secuencia, cada router realiza un seguimiento de los paquetes enviados.

Router 1
17:21:09.685: Serial0/0: HDLC myseq 0, mineseen 0*, yourseen 1, line up
17:21:19.725: Serial0/0: HDLC myseq 1, mineseen 1*, yourseen 2, line up
17:21:29.753: Serial0/0: HDLC myseq 2, mineseen 2*, yourseen 3, line up
17:21:39.773: Serial0/0: HDLC myseq 3, mineseen 3*, yourseen 4, line up
17:21:49.805: Serial0/0: HDLC myseq 4, mineseen 4*, yourseen 5, line up
17:21:59.837: Serial0/0: HDLC myseq 5, mineseen 5*, yourseen 6, line up
17:22:09.865: Serial0/0: HDLC myseq 6, mineseen 6*, yourseen 7, line up

[80] **ETHERNET:** Es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de *ether*. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

17:22:19.905: Serial0/0: HDLC myseq 7, mineseen 7*, yourseen 8, line up
17:22:29.945: Serial0/0: HDLC myseq 8, mineseen 8*, yourseen 9, line up
Router1 (config-if)#shut
17:22:39.965: Serial0/0: HDLC myseq 9, mineseen 9*, yourseen 10, line up
17:22:42.225: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
17:22:43.245: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down

Tabla V-2: Ejemplo de keepalives enviados y recibidos por el Router 1**. [A]**

Router 2
***Sep 24 17:21:04.929: Serial2/0: HDLC myseq 0, mineseen 0, yourseen 0, line up**
***Sep 24 17:21:14.941: Serial2/0: HDLC myseq 1, mineseen 1*, yourseen 1, line up**
***Sep 24 17:21:24.961: Serial2/0: HDLC myseq 2, mineseen 2*, yourseen 2, line up**
***Sep 24 17:21:34.981: Serial2/0: HDLC myseq 3, mineseen 3*, yourseen 3, line up**
***Sep 24 17:21:45.001: Serial2/0: HDLC myseq 4, mineseen 4*, yourseen 4, line up**
***Sep 24 17:21:55.021: Serial2/0: HDLC myseq 5, mineseen 5*, yourseen 5, line up**
***Sep 24 17:22:05.041: Serial2/0: HDLC myseq 6, mineseen 6*, yourseen 6, line up**
***Sep 24 17:22:15.061: Serial2/0: HDLC myseq 7, mineseen 7*, yourseen 7, line up**
***Sep 24 17:22:25.081: Serial2/0: HDLC myseq 8, mineseen 8*, yourseen 8, line up**
***Sep 24 17:22:35.101: Serial2/0: HDLC myseq 9, mineseen 9*, yourseen 9, line up**
***Sep 24 17:22:45.113: Serial2/0: HDLC myseq 10, mineseen 10*, yourseen 10, line up**
***Sep 24 17:22:55.133: Serial2/0: HDLC myseq 11, mineseen 10, yourseen 10, line up**
***Sep 24 17:23:05.153: HD(0): Reset from 0x203758**
***Sep 24 17:23:05.153: HD(0): Asserting DTR**
***Sep 24 17:23:05.153: HD(0): Asserting DTR and RTS**
***Sep 24 17:23:05.153: Serial2/0: HDLC myseq 12, mineseen 10, yourseen 10, line up**
***Sep 24 17:23:15.173: HD(0): Reset from 0x203758**
***Sep 24 17:23:15.173: HD(0): Asserting DTR**
***Sep 24 17:23:15.173: HD(0): Asserting DTR and RTS**
***Sep 24 17:23:15.173: Serial2/0: HDLC myseq 13, mineseen 10, yourseen 10, line**

down
17:23:16.201: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
Router2#
17:23:25.193: Serial2/0: HDLC myseq 14, mineseen 10, yourseen 10, line down

Tabla V-3: Ejemplo de keepalives enviados y recibidos por el Router 2**. [A]**

5.7. TÚNEL GRE KEEPALIVES

El túnel GRE KeepAlive es un mecanismo que es ligeramente diferente a la de Ethernet o interfaces seriales. Da la capacidad para enviar y recibir paquetes desde y hacia un router remoto incluso si el mando a distancia del router no es compatible con GRE keepalives. Esto significa que el paquete GRE KeepAlive no se ve afectado por cualquier salida de funciones de la interfaz de túnel.

Otro atributo que tiene el túnel GRE keepalive es que el tiempo en cada lado es independiente y no tiene que coincidir. El problema con la configuración de keepalives sólo en un lado del túnel es que sólo un router tiene configurado el keepalive.

El túnel puede convertirse en un agujero negro para los paquetes dirigidos en el túnel desde el lado que no se ha configurado los keepalives.

5.7.1. Túnel de trabajo

Un túnel GRE es una interfaz lógica de un router de Cisco que ofrece una forma de encapsular los paquetes dentro de un protocolo de transporte. Se trata de una arquitectura diseñada para proporcionar los servicios para la aplicación de punto a punto en un sistema de encapsulado.

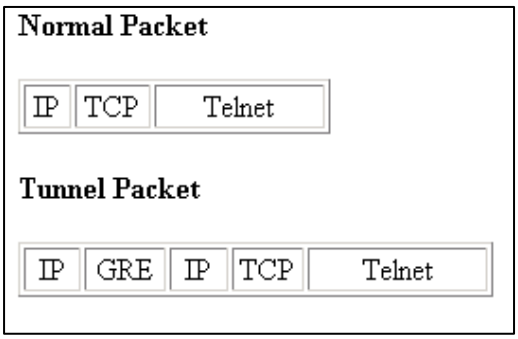

Figura V-7: Comparación entre un paquete normal y un paquete usando GRE. **[1]**

- IP es el protocolo de transporte.
- GRE es el protocolo de encapsulado.
- IP es el protocolo de pasajeros.

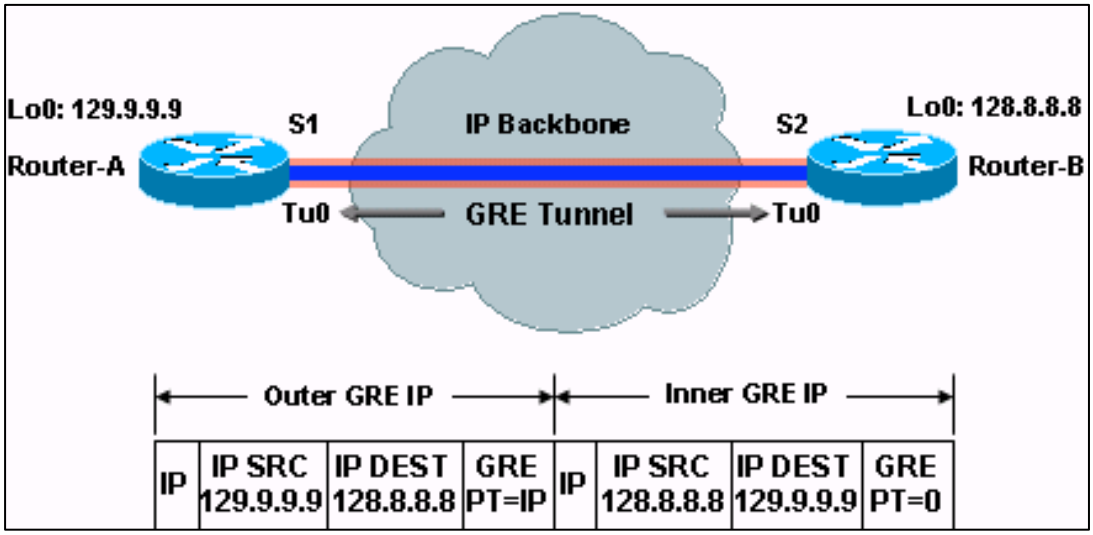

Figura V-8: Aplicación grafica de un túnel GRE entre dos routers. **[2]**

Esta salida muestra los comandos que uso para configurar keepalives sobre túneles GRE.

```
Router # configure terminal
Router (config) # interfaz tunnel0
Router (config-si) # 5 4 KeepAlive
  ! --- La sintaxis de este comando es KeepAlive [segundos
[reintentos]].
  ! --- Los keepalives se envían cada 5 segundos y 4 reintentos.
```

```
  ! --- Los keepalives deben perderse antes de que el túnel está
apagado.
  ! --- Los valores por defecto son 10 segundos para el intervalo
de reintentos y 3.
```

Figura V-9: Keepalives . **[5]**

Esta tabla muestra la configuración del router A y B con túnel KeepAlive configurado en ambos routers.

Hostname Router-A	Hostname Router-B
interface loopback 0	interface loopback 0
ip address 129.9.9.9 255.255.255.255	ip address 128.8.8.8 255.255.255.255
interface tunnel 0	interface tunnel 0
ip address 1.1.1.1 255.255.255.240	ip address 1.1.1.2 255.255.255.240
tunnel source loopback0	tunnel source loopback0
tunnel destination 128.8.8.8	tunnel destination 129.9.9.9
keepalive 5 4	keepalive 5 4

Tabla V-4: Configuración del router A y B usando Keepalive. **[A]**

Este diagrama muestra un ejemplo de escenario de lo que ocurre cuando un router A envía GRE KeepAlive a un router B:

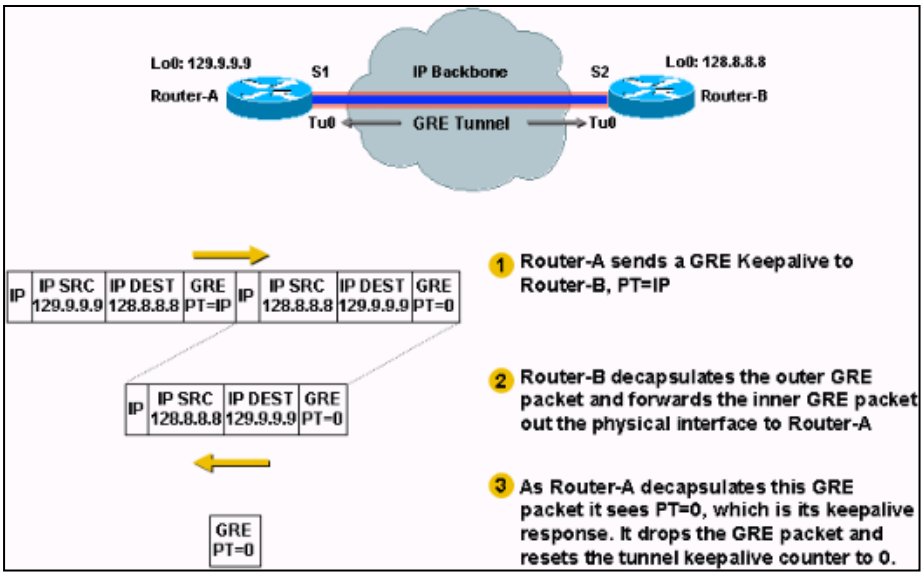

Figura V-10: GRE keepalive enviado del router A al B. **[5]**

Este diagrama muestra un ejemplo de escenario de lo que ocurre cuando el router B envía una GRE KeepAlive a un router:

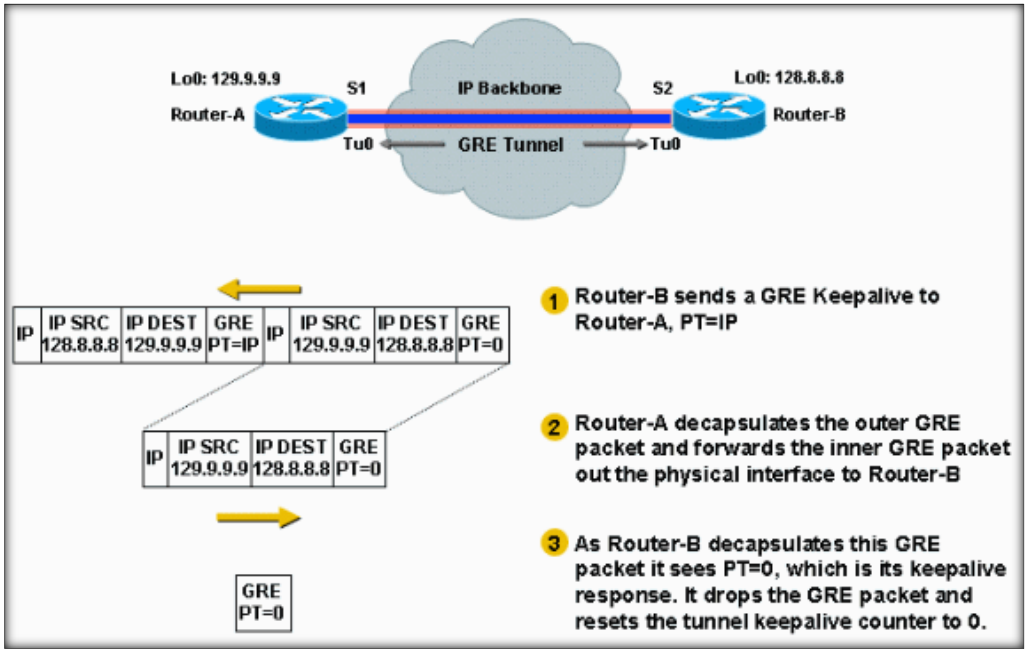

Figura V-11: GRE keepalive enviado del router B al A. **[1]**

5.8. Túneles GRE con IPSec

Los Túneles GRE en ocasiones se combinan con IPSec, porque no es compatible en algunos paquetes de multidifusión IP. Esto evita que los protocolos de enrutamiento dinámico se ejecute con éxito a través de una red VPN IPSec. Desde que los túneles GRE apoyan con la multidifusión IP, un protocolo de enrutamiento dinámico se puede ejecutar en un túnel GRE. Entonces, usted puede cifrar los paquetes GRE IP unicast por IPSec.

Hay dos maneras diferentes que IPSec puede cifrar los paquetes GRE. Una forma es con el uso de un cripto-mapa y la otra es usar protección túnel. Ambos métodos de cifrado IPSec se especifica cuando se realiza la adición de la encapsulación GRE. Cuando un cripto-mapa se usa, se aplica a la interfaz física de salida para el túnel. Cuando se utiliza la protección del túnel, se configura en la interfaz de túnel GRE.

Este diagrama muestra los paquetes que vienen codificados en un router a través de una interfaz de túnel GRE. El router tiene un cripto-mapa se aplicará sobre la interfaz física. Una vez que los paquetes son de encriptado y de encapsulado, que siguen a su propiedad intelectual como destino de texto.

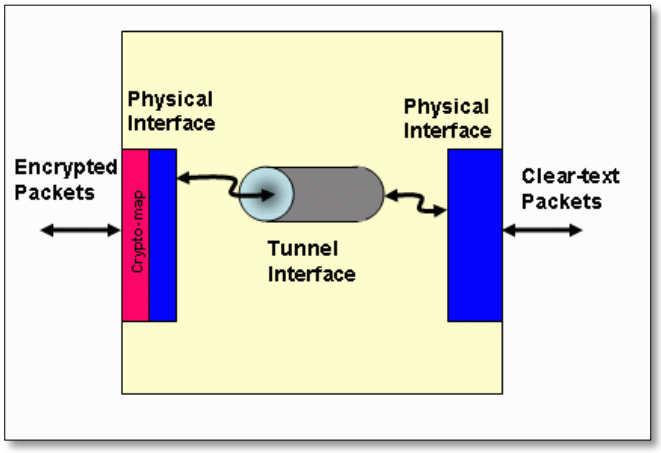

Figura V-12: IPsec sobre GRE usando cripto mapas. **[1]**

Este diagrama muestra lo que ocurre cuando se configura la protección en el túnel GRE interfaz de túnel. Los paquetes vienen codificados en el router a través de la interfaz de túnel, encriptado y encapsulado antes de continuar hacia su destino como texto.

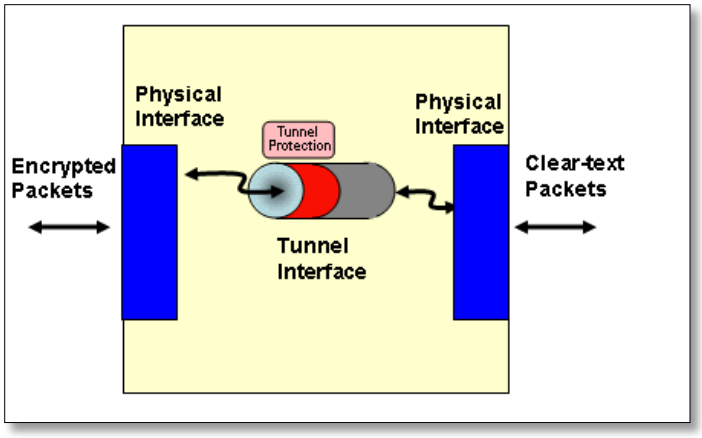

Figura V-13: IPsec sobre GRE usando protección del túnel. **[1]**

CAPÍTULO VI. EJERCICIO PRÁCTICO

6. APLICACIÓN PRÁCTICA

Packet Tracer 5.2 es la versión más reciente de Cisco Reding Academy en la completa tecnología de redes de enseñanza y aprendizaje del software. Características innovadoras de Packet Tracer 5.2, incluyendo potentes de simulación, visualización, autoría, la evaluación, y capacidades de colaboración, ayudará a los estudiantes y profesores colaborar, resolver problemas y aprender conceptos en un atractivo y dinámico entorno social.

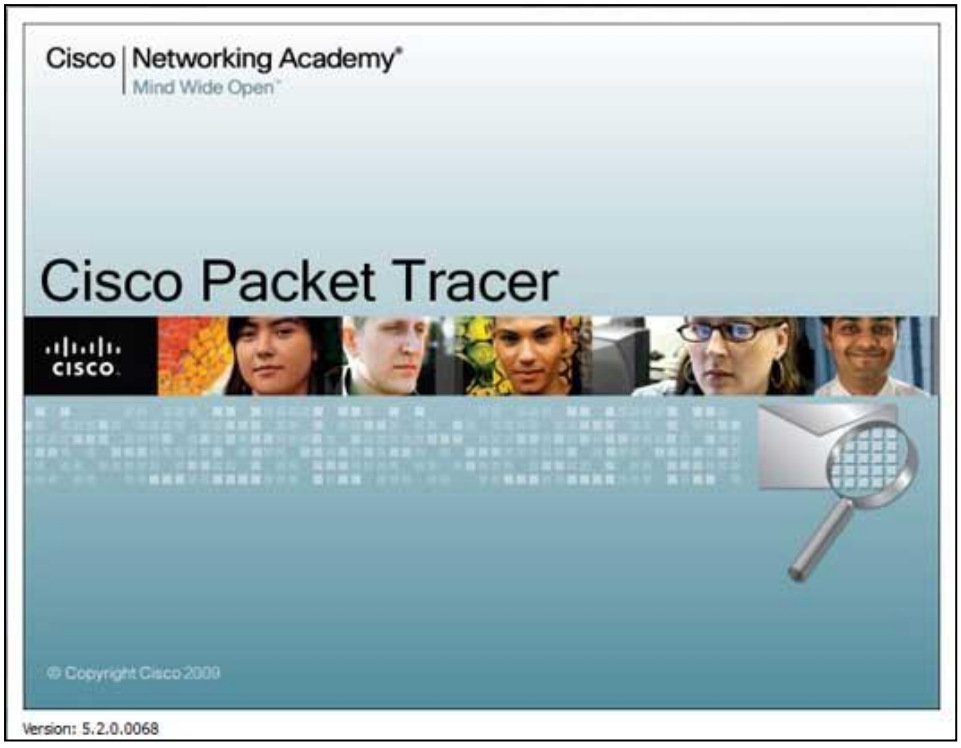

Figura VI-1: Packet Tracer 5.2. **[1]**

Packet Tracer hace tanto la enseñanza y el aprendizaje más fácil - instructores y los estudiantes pueden crear sus propios virtual "red mundos" para la exploración, la experimentación, y la explicación de conceptos y tecnologías de redes.

- Los instructores pueden demostrar las tecnologías y configuraciones utilizando paquetes Tracer para enseñar CCNA compleja red a nivel conceptos, por lo que es extremadamente útil para conferencias, laboratorios de grupo e individuales, evaluaciones, solución de problemas y modelado de tareas, tareas, juegos y concursos.

- Los estudiantes pueden diseñar, configurar y solucionar problemas de redes de paquetes utilizando la Tracer versátil entorno de simulación y visualización, que también proporciona la oportunidad y la flexibilidad adicional para la práctica fuera del aula.

Tracer proporciona a los estudiantes oportunidades de aprendizaje complementarias que no son físicamente posibles crear en el aula o laboratorio. Además, complementa los paquetes Tracer CCNA planes de estudio y las actividades de rastreo de paquetes están integradas tanto en CCNA Discovery y CCNA Exploración para ofrecer experiencias de aprendizaje de tecnología de redes.

Packet Tracer 5.1 ofrece una combinación única de simulación y visualización realista de experiencias, evaluación y compleja actividad de autoría de las capacidades y las oportunidades de colaboración multiusuario y la competencia, y está disponible de forma gratuita a todos los instructores de Reding Academy, estudiantes y ex alumnos.

6.1. Configuración y verificación sitio a sitio usando IPsec sobre VPN con línea de comandos

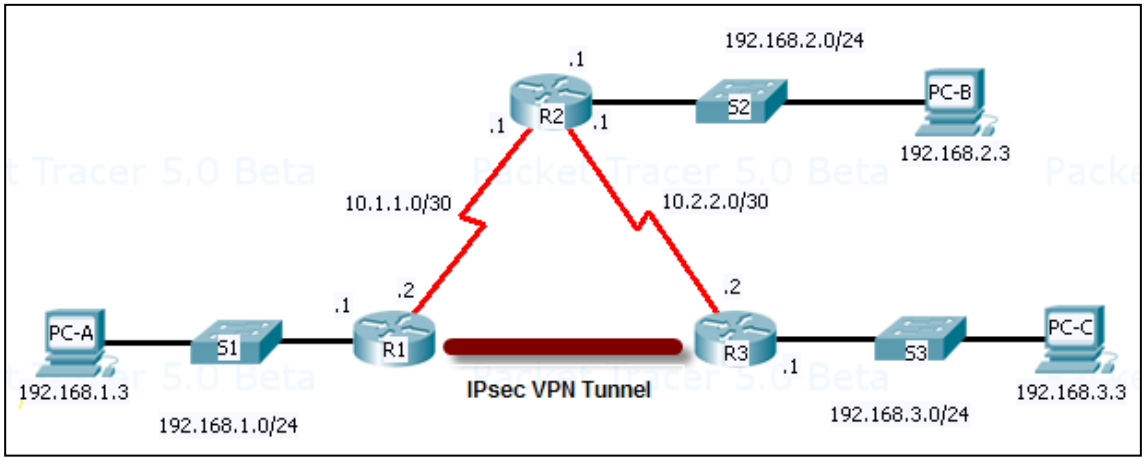

Figura VI-2: Red IPSEC VPN. **[1]**

6.2. TABLA DE DIRECCIONES

Dispositivo	Interface	Dirección IP	Mascara
R1	Fa0/0	192.168.1.1	**255.255.255.0**
	S0/0/0	10.1.1.2	**255.255.255.252**
R2	S0/0/0	10.1.1.1	**255.255.255.252**
	Fa0/0	192.168.2.1	**255.255.255.0**
	S0/0/1	10.2.2.1	**255.255.255.252**
R3	S0/0/1	10.2.2.2	**255.255.255.252**
	Fa0/0	192.168.3.1	**255.255.255.0**
PC-A	NIC	192.168.1.3	**255.255.255.0**
PC-B	NIC	192.168.2.3	**255.255.255.0**
PC-C	NIC	192.168.3.3	255.255.255.0

Tabla VI-1: Tabla de direcciones. **[A]**

6.3. OBJETIVOS:

- Compruebe la conectividad en toda la red.
- Configurar el router R1 para apoyar sitio a sitio el IPsec sobre VPN con el router R3.

6.4. INTRODUCCION:

La topología de la red muestra tres routers. La tarea consiste en configurar dos routers R1 y R3 para apoyar de sitio a sitio usando IPsec sobre VPN cuando el tráfico fluye de sus respectivas redes de área local. El túnel IPSec VPN va desde R1 a R3 router a través de R2. R2 actúa como punto de paso y no tiene conocimiento de la VPN. IPsec proporciona la transmisión segura de información sensible a través de redes desprotegidas como Internet. IPsec actúa en la capa de red, la protección y autenticación de los paquetes IP entre los que participan los dispositivos de IPsec, como los enrutadores de Cisco.

Parámetros		Router R1	Router R3
Método de distribución de claves	Manual ó ISAKMP	ISAKMP	ISAKMP
Algoritmo de cifrado	DES, 3DES, or AES	AES	AES
Algoritmo de hash	MD5 or SHA-1	SHA-1	SHA-1
Método de autentificación	Claves pre-compartidas ó RSA	pre-compartido	pre-compartido
Intercambio de claves	DH Group 1, 2, or 5	DH 2	DH 2
Tiempo de vida de IKE SA	86400 segundos ó menos	86400	86400
Clave ISAKMP		vpnpa55	vpnpa55

Tabla VI-2: Parámetros de Configuración. **[A]**

6.5. POLÍTICA DE PARÁMETROS DE IPSEC

Parámetros	Router R1	Router R3
Transform Set	VPN-SET	**VPN-SET**
Peer Hostname	R3	**R1**
Peer IP Address	10.2.2.2	**10.1.1.2**
Red to be encrypted	192.168.1.0/24	**192.168.3.0/24**
Crypto Map name	VPN-MAP	**VPN-MAP**
SA Establishment	**IPsec-isakmp**	**IPsec-isakmp**

Tabla VI-3: Parámetros IPSEC. **[A]**

Los routers han sido pre-configurado con el texto siguiente:

- Contraseña de la línea de la consola: **ciscoconpa55**
- Contraseña para las líneas vty: **ciscovtypa55**
- Habilitar contraseña: **ciscoenpa55**
- RIP versión 2

6.6. Configurar los parámetros de IPsec en R1

- **Ping** desde el PC-A a la PC-C.

6.7. Identificar el tráfico en R1.

- Configurar las listas de control de acceso (ACL) **110** para identificar el tráfico de la LAN en la R1 a la LAN en R3. Este tráfico desencadenará la VPN IPSec que deberá realizarse cada vez que hay tráfico entre R1 y R3. El resto del tráfico procedente de las redes de área local no serán encriptado.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

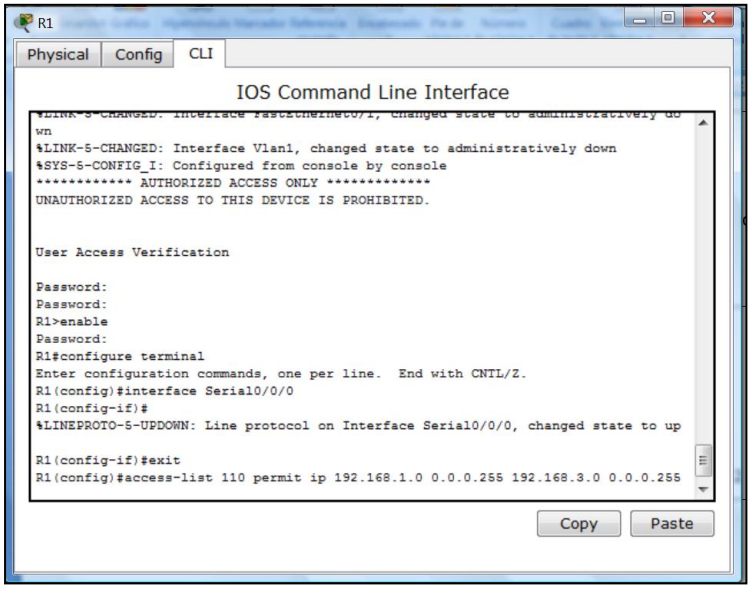

Figura VI-3: Identificación del trafico. **[A]**

6.8. Configurar ISAKMP Fase 1 en R1.

- Configurar la directiva de ISAKMP en R1 junto con la clave de cifrado compartida **vpnpa55.**

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

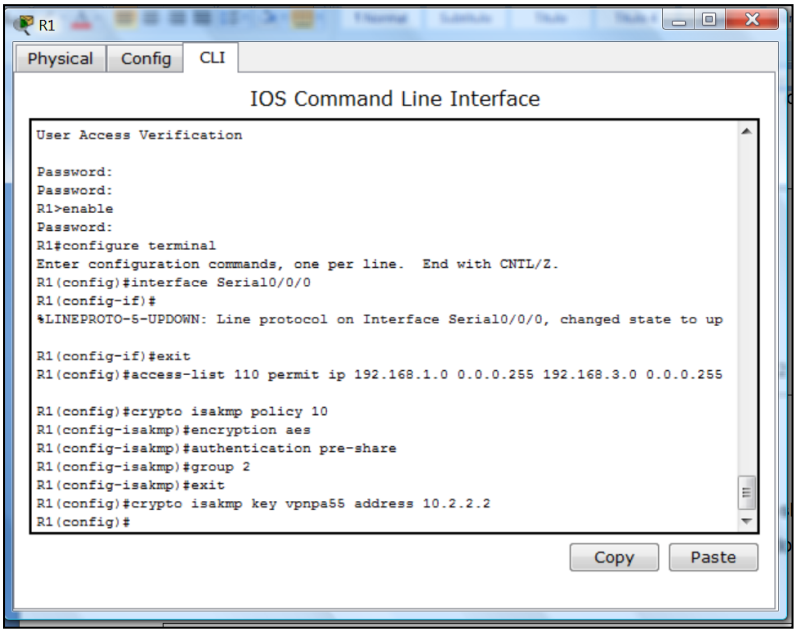

Figura VI-4: Configuracion ISAKMP Fase1. **[A]**

6.9. Configurar ISAKMP Fase 2 en R1.

- Creo la transform-set VPN para utilizar ESP-3DES y esp-sha-HMAC.
- Luego, creo el mapa de cifrado VPN-MAP que une a todos los de la Fase 2.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

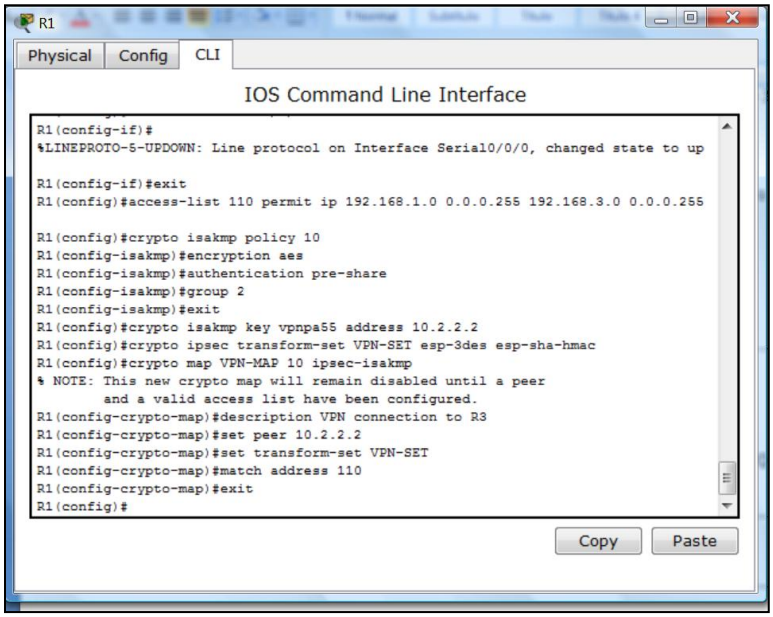

Figura VI-5: Configuracion ISAKMP Fase 2. **[A]**

6.10. Configurar el mapa de cifrado en la interfaz de salida.

- Por último, el enlace **VPN-MAP** a la salida de interfaz serial 0/0/0.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

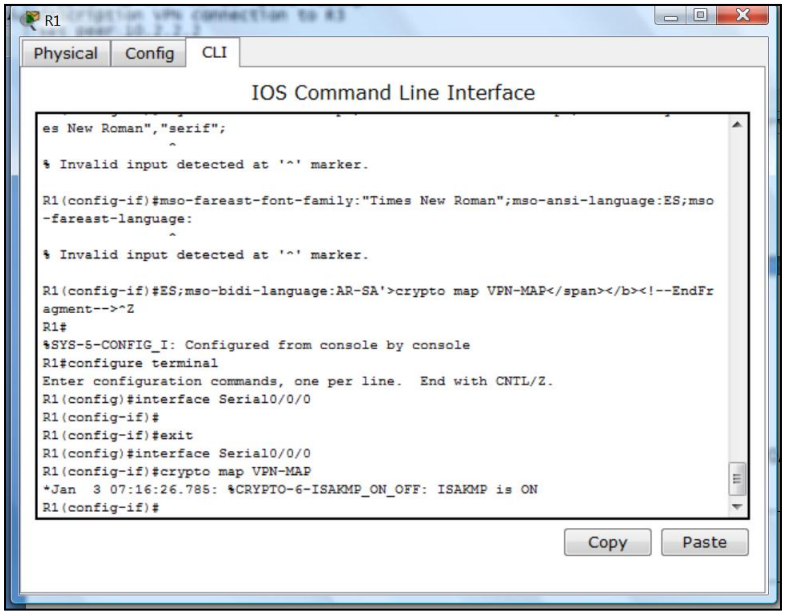

Figura VI-6: Configuración del mapa de cifrado. **[A]**

6.11. Configurar los parámetros de IPsec en R3

- Ahora configuro los parámetros de movimiento alternativo en R3

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
```

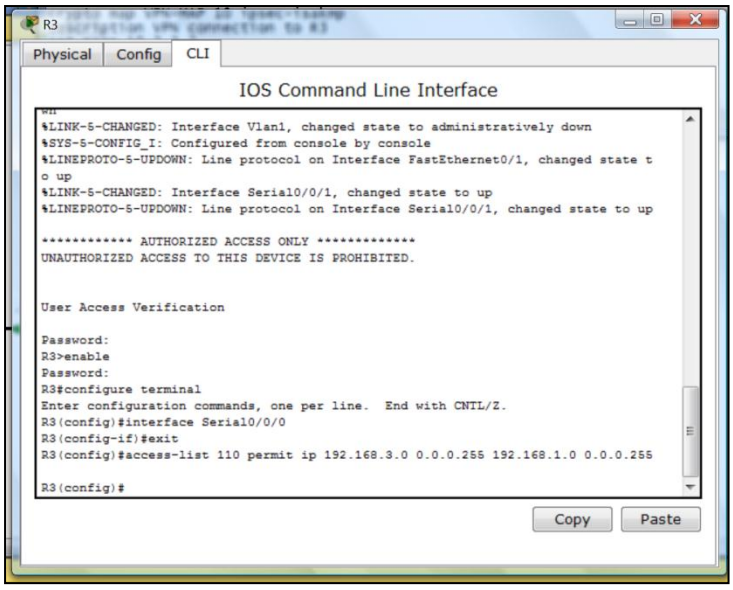

Figura VI-7: Configuración de parâmetros IPSEC. **[A]**

6.12. Configurar ISAKMP Fase 1 en R3.

- Configurar la política de ISAKMP en R3, junto con la criptografía de clave compartida **vpnpa55**

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

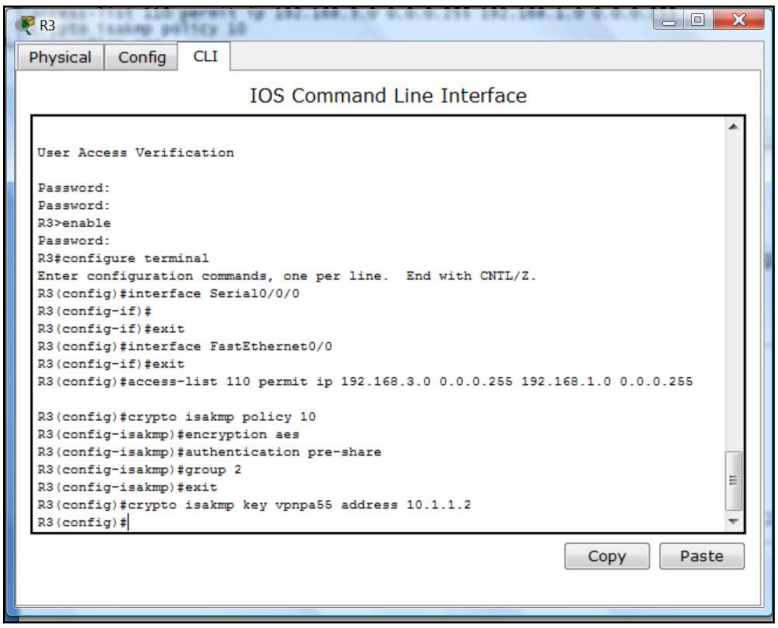

Figura VI-8: Configuración de ISAKMP. **[A]**

6.13. Configurar ISAKMP Fase 2 en R3.

- Realizó algo parecido, como lo hecho en R1.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-
hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
```

```
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

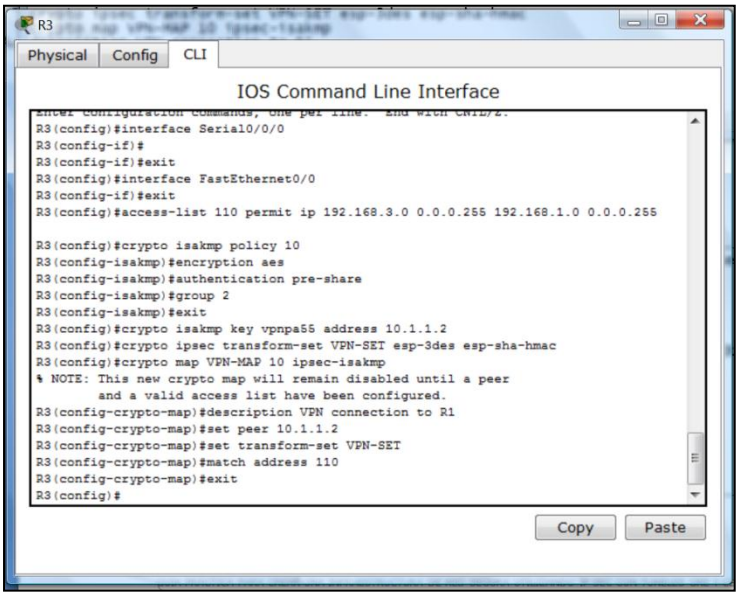

Figura VI-9: Configuracion de ISAKMP parte 2. **[A]**

6.14. Configurar el mapa de cifrado en la interfaz de salida.

- Por último, el enlace VPN-MAP

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

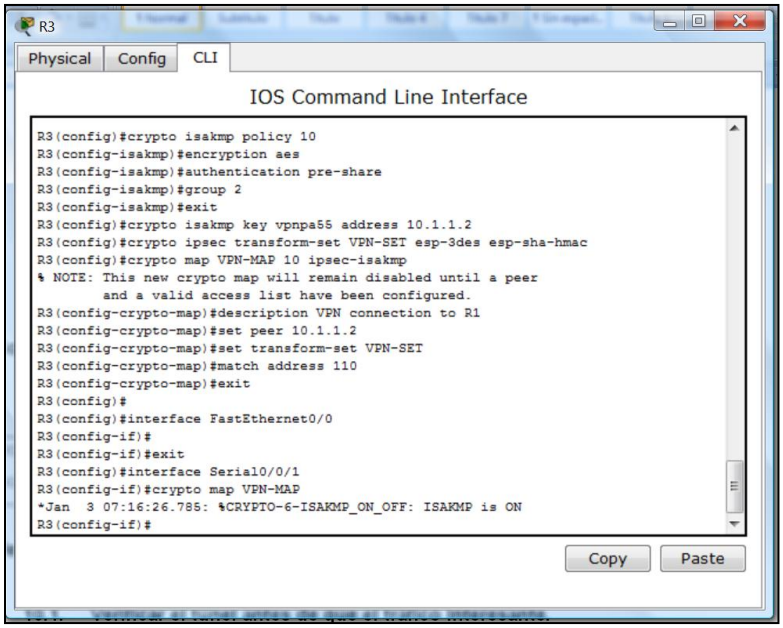

Figura VI-10: Configuracion VPN-MAP. **[A]**

6.15. Verificar la VPN IPSec

- Observo que el número de paquetes encapsulados, cifrados y descifrados decapsulado se ajustan a 0.

6.16. Crear tráfico interesante.

- Realizo ping desde la PC-A a la PC-C

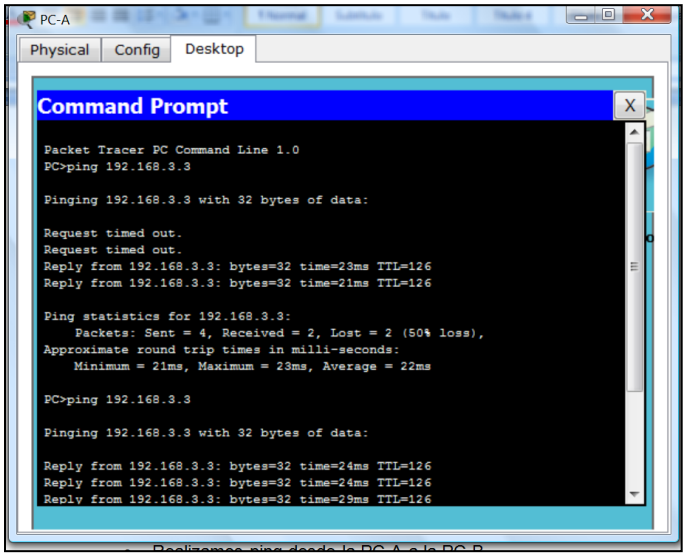

Figura VI-11: Creación de tráfico. **[A]**

6.17. Verificar el túnel después del tráfico

- En R1, uso **show crypto ipsec sa**

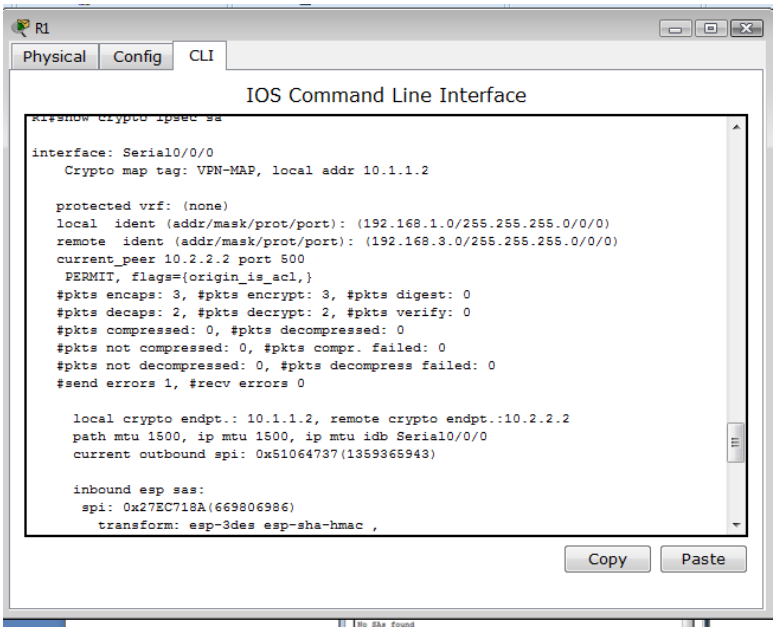

Figura VI-12: Verificación del Túnel. **[A]**

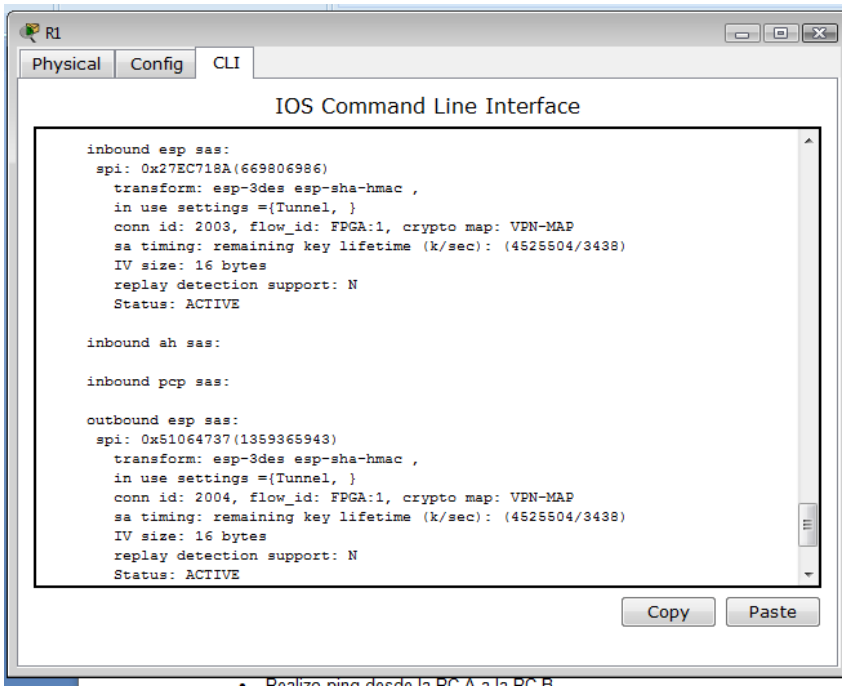

Figura VI-13: Verificación del Túnel. **[A]**

6.18. Crear el tráfico de interés.

- Realizo ping desde la PC-A a la PC-B

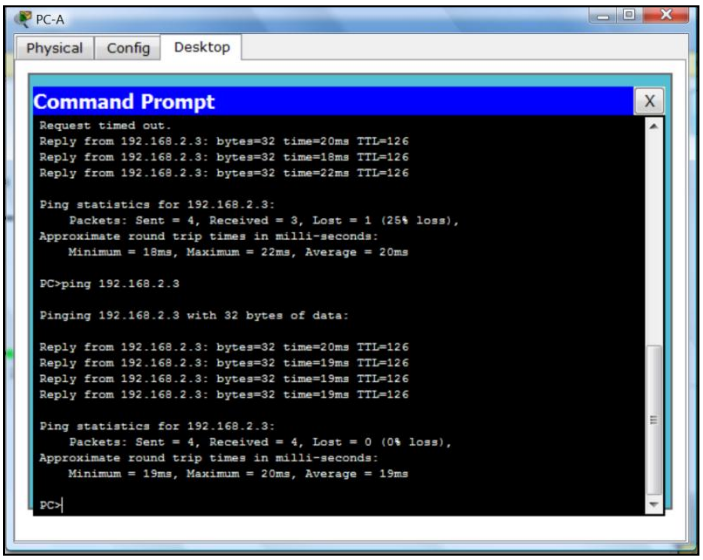

Figura VI-14: Creación de Trafico. **[A]**

6.19. Verificar el túnel.

- En R3, usamos **show crypto ipsec sa**

6.20. Comprobación de resultados

- Su porcentaje de finalización debe ser del 100%. Haga clic en Buscar para ver los resultados de votos y la verificación de que los componentes requeridos han sido completados.

7. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- Para mejorar la seguridad, se debería fomentar temas de disertación como el presentado, ya que se podría fortalecer las vulnerabilidades de ciertos sistemas o infraestructuras.
- La creación de túneles es un modo de utilizar una infraestructura de redes de un protocolo para transferir una carga.
- Para soportar la transferencia de guardar y enviar se requiere una gran cantidad de trabajo con el búfer.
- X.25 y TCP/IP son similares en la medida en que utilizan protocolos de conmutación de paquetes. Sin embargo, existen algunas diferencias entre ellos:
- TCP/IP sólo tiene comprobación de errores y control de flujo extremo a extremo.
- X.25 tienen control de errores nodo a nodo.
- Para compensar el hecho de que una red TCP/IP sea completamente pasiva, TCP/IP tiene un control de flujo y un mecanismo de ventana más complicado que el de X.25.
- X.25 tiene unos niveles de enlace y eléctricos muy concretos; TCP/IP está diseñado para trabajar con distintos tipos de medios, y con servicios de enlace muy variados.
- El software Cisco IOS usa como método de identidad la dirección IP por default.
- En Cisco IOS, se configura el nombre o IP del host remoto.
- IPSec es un conjunto de estándares abiertos desarrollados por el Internet Engineering Task Force (IETF).
- IPSec ofrece protección en la transmisión de información sensible sobre redes inseguras tal como es la propia Internet.
- IPSec actúa en la capa de red, protegiendo y autentificando paquetes IP entre los dispositivos participantes.
- Antes del modelo de referencia OSI se escribieron muchos protocolos. Por tanto, no es extraño encontrar jerarquías de protocolos que no se correspondan directamente con el modelo OSI.
- Cada IDS implementa la arquitectura de manera diferente.

- Este proyecto se puede implementar en medianas y grandes empresas, Instituciones gubernamentales, militares, campus universitarios y toda empresa donde se requiera seguridad y confidencialidad.
- La filosofía de distribución de código libre, busca que el conocimiento del desarrollo de las aplicaciones, sea libre para quien quiera emplearlas, de esta forma si el usuario llegase a encontrar algún problema de seguridad o de otra índole en la aplicación, podrá editar directamente el código fuente o informar al desarrollador de la aplicación, para que en una futura versión se corrija el problema.
- Mientras más mecanismos de seguridad se empleen en sistemas de control de acceso, el sistema será más seguro, aun cuando un sistema con seguridad absoluta no exista, el hecho de implementar un mayor número de mecanismos de control ayudará a que el sistema sea menos vulnerable.
- La identificación de cada uno de los procesos y las tareas asociadas a cada organización, permitirán que se pueda realizar una implementación, reduciendo los riesgos de interrupciones de la organización y ayudando en una más rápida adopción de la nueva tecnología.
- Las crypto ACL identifican el flujo del tráfico que va a ser protegido.
- El tráfico que coincide con la ACL es protegido y cifrado.
- Las tendencias futuras de la implantación de túneles de seguridad dan cabida a que se elimine la infraestructura física, lo cual abarataría costos y fomentaría su uso en algunos campos.

7.2. RECOMENDACIONES

- Se recomienda profundizar este estudio presentado, en otras disertaciones, como enfocándolo a la parte de software propiamente dicho.
- Recomiendo que se realicen temas de disertación partiendo de este como: Implementación de Túneles GRE Y CET en Internet, IPSEC en wireless, Vulnerabilidades de IPSEC, entre otros.
- Se debería incluir una breve explicación de los túneles de seguridad en la Cátedra de Redes, lo cual fomentaría tener mayor capacidad ante ciertos problemas de la vida práctica.

- Además se recomienda que la Facultad, cree cursos de Ethical Hacking y de Túneles de Seguridad, lo cual nos permitirá conocer ciertas pautas que nos ayudará a ser más precavidos en la implantación de una red.
- IPSEC se recomienda para proteger el canal de comunicación entre dos servidores y restringir los equipos que se pueden comunicar entre sí. Por ejemplo, puede ayudar a proteger un servidor de base de datos si establece una directiva que permita solicitudes provenientes sólo de un equipo cliente de confianza como, por ejemplo, un servidor de aplicaciones o un servidor web. También puede restringir la comunicación a protocolos IP y puertos TCP o UDP específicos.
- Se recomienda que las contraseñas tengan un periodo corto de duración y el administrador del túnel las cambie periódicamente, de esta manera se evita que algún usuario no autorizado acceda al túnel.
- Si se emplea mecanismos de autenticación con nombres de usuario y clave, es necesario concientizar a los usuarios de la importancia de mantener sus claves seguras con normas básicas como que no deben anotarlas en ningún lugar como recordatorio o que no deben facilitárselas a otras personas.

8. REFERENCIAS

8.1. BIBLIOGRAFÍA:

[A] AGUAS BUCHELI, Luis Fernando, "*Guía práctica para crear una infraestructura de red segura utilizando IPSEC con túneles GRE y CET*", Noviembre 2009

[B] B. W, Lampson. *"A note on the Connement Problem. Communications of the ACM"*, Octubre 2004.

[C] BLACK, D. P, *"Managing Switched Local Area Reds", A Practical Guide.* Addison-Wesley, 1998

[D] J.C. Laprie, *" Dependability: Basic concepts and terminology"*, Springer-Verlag, 2006.

[E] J.C.Wray, *"An analysis of covert timing channels. In Proceedings of the 2000 Symposium on Research in Security and Privacy"*, ieee Computer Society, Mayo 2000.

[F] J.W. Wray, *"Toward a mathematical foundation for information own security. In Proceedings of the 2002 Symposium on Research in Security and Privacy",*2002

[G] LAMPORT, Leslie , *"Password authentication with insecure communication"*. Communications of the ACM, Noviembre 2000

[H] LANDWHER, Carl E, BULL, Alan R, MCDERMOTT, John P, CHOI, William S, *" A taxonomy of computer program security aws, with examples. ACM Computing Surveys"*, Septiembre 1994.

[I] LEW, Kim, H. y otros, *"Interconectividad Manual para la Resolución de problemas",* Cisco Press, 2000.

[J] LIPNER, Steven B, *"A note on the Connement Problem. Operating Systems Review"*, Noviembre 2005

[K] LISTER, Justin Jay,*"Intrusion Detection Systems: an Introduction to the detection and prevention of computer abuse"*. PhD thesis, University of Wollongong,2005.

[L] LUNT, Teresa, *"A real time intrusion detection expert system (ides)"*,2002.

[M] M. J. Williamson. *"Non Secret encryption using a Technical report"*, CESG, Enero 2004

[N] M. J. Williamson. *"Thoughts of Secret encryption using a Technical report"*, CESG, Enero 2007

[O] MAIMON, Uriel, *"Port Scanning without the synag. Phrack Magazine"*, 2005

[P] MANGER, Jason, *"Unix: The complete book"*, Sigma Press, 2003.

[Q] MARKHOW, John, *"Author of computer `virus' is son of U.S. electronic security expert"*, The New York Times, 5 Noviembre 2006

[R] MICROSOFT, Corporation, "Biblioteca de Consulta Encarta", 2009

[S] MICROSOFT, Corporation, "Galería de Imágenes Office", 2009

[T] SANDEEP, Kumar, "*Classification and Detection of Computer Intrusions*". PhD thesis, Purdue University, Agosto 2005.

[U] TANENBAUM, Andrew S, "Computer Reds", *4th Ed.* Prentice-Hall, 2003

[V] TATU, Ylonen, *"ssh Secure login connetions over the Internet. In Proceedings of the 6th usenix Security Symposium"*, The usenix Association, Julio 2006.

[W] U. Manber, *"A simple scheme to make passwords based on One-Way functions muchharder to crack"*, Computers & Security, 2006

[X] WINKLER, Ira S, DEALY, Brian, *"Information security technology?...Don't rely on it. A case study in social engineering. In Proceedings of the 5th usenix Unix Security Symposium"*, The usenix Association, Junio 2005.

[Y] WONG, Chris, *"HP-UX 11i Security"*, Prentice Hall, Septiembre 2001

[Z] WRESKI, Dave, *"Linux Security Administrator's Guide"*,2005

[AA] ZIEGLER, Robert L, *"Linux Firewalls. New Riders"*, 2nd edition, 2001.

8.2. INTERNET:

[1] http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/797/4/T10140CAP3.pdf

[2] http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/989/5/10762CAP1.pdf

[3] http://cisco.netacad.net/cnams/search/SearchResultContainer.jsp?keyword=GRE

[4] http://dhobsd.pasosdejesus.org/?id=Utilizaci%F3n+de+IPSEC

[5] http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf

[6] http://es.wikipedia.org/wiki/ADSL2

[7] http://es.wikipedia.org/wiki/FTTH

[8] http://es.wikipedia.org/wiki/GRE

[9] http://es.wikipedia.org/wiki/Red_de_computadoras

[10] http://linuxsilo.net/articles/vpn.html

[11] http://nic.com/~dave/Security/

[12] http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/04_conceptosBasicos2.pdf

[13] http://www.arcert.gov.ar/ncursos/material/Tutorial_IPSec_1.2.pdf

[14] http://www.bulma.net/body.phtml?nIdNoticia=2269

[15] http://www.cisco.com/web/LA/docs/pdf/Seguridad.pdf

[16] http://www.monografias.com//

[17] http://www.scribd.com/doc/2926337/El-Protocolo-IPv6-y-sus-extensiones-de-seguridad-IPSec#

[18] http://www.securityfocus.com/infocus/1859

[19] http://www.utpl.edu.ec/seguridad/wp-content/uploads/seguridad/proyectosEjecutados/document.pdf

[20] https://cisco.netacad.net/cnams/dispatch

9. GLOSARIO

- **802.11a:** Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.
- **802.11b:** Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.
- **802.11g:** Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.
- **Actualizar:** Sustituir el software o firmware existente con una versión más moderna.
- **Adaptador:** Dispositivo que añada funcionalidad de red a su equipo.
- **Ad-hoc:** Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.
- **AES:** (Estándar avanzado de cifrado) Técnica de cifrado de datos simétrica de bloque de 256 bits.
- **Ancho de banda:** Capacidad de transmisión de un dispositivo o red determinado.
- **Banda ancha:** Conexión a Internet de alta velocidad y siempre activa.
- **Banda ISM:** Banda de radio utilizada en las transmisiones de redes inalámbricas.
- **Base de datos:** Recopilación de datos que puede organizarse de forma que pueda sus contenidos puedan accederse, gestionarse y actualizarse fácilmente.
- **Bit:** (dígito binario). La unidad más pequeña de información de una máquina.
- **Byte:** Una unidad de datos que suele ser de ocho bits.
- **Cargar:** Transmitir un archivo a través de una red.
- **CSMA/CA:** (Acceso múltiple de detección de portadora) Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.
- **Cifrado:** Cifrado es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.
- **Conmutador:**

  1. Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.

2. Dispositivo para realizar, interrumpir o modificar las conexiones de un circuito eléctrico.

- **CTS:** (Limpiar para enviar) Señal enviada por un dispositivo para indicar que está preparado para recibir datos.
- **DDNS:** (Sistema dinámico de nombres de dominio) Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.
- **Descargar:** Recibir un archivo transmitido a través de una red.
- **DHCP:** (Protocolo de configuración dinámica de host) Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.
- **Dirección IP:** Dirección que se utiliza para identificar un equipo o dispositivo en una red.
- **Dirección IP dinámica:** Dirección IP temporal que asigna un servidor DHCP.
- **Dirección IP estática:** Dirección fija asignada a un equipo o dispositivo conectado a una red.
- **Dispersión de secuencia:** Técnica de frecuencia de radio de banda ancha que se utiliza para la transmisión más fiable y segura de datos.
- **DMZ:** (Zona desmilitarizada) Suprime la protección de servidor de seguridad del enrutador de un equipo, permitiéndole que pueda “verse” desde Internet.
- **DNS:** (Servidor de nombres de dominio) La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.
- **DSL:** (Línea de suscriptor digital) Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.
- **DSSS:** (Espectro de dispersión de secuencia directa). Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.
- **DTIM:** (Mensaje de indicación de tráfico de entrega). Mensaje incluido en paquetes de datos que puede aumentar la eficacia inalámbrica.
- **Dúplex completo:** La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.
- **Dúplex medio:** Transmisión de datos que puede producirse en dos direcciones a través de una única línea, pero sólo en una dirección cada vez.

- **EAP:** (Protocolo de autenticación extensible). Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.
- **EAP-PEAP:** (Protocolo de autenticación extensible-Protocolo de autenticación extensible protegido). Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.
- **EAP-TLS:** (Protocolo de autenticación extensible-Seguridad de la capa de transporte) Método de autenticación mutua que utiliza certificados digitales.
- **Encadenamiento de periféricos:** Método utilizado para conectar dispositivos en serie, uno tras otro.
- **Enrutador:** Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.
- **Enrutamiento estático:** Reenvío de datos de una red a través de una ruta fija.
- **Ethernet:** Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.
- **Finger:** Programa que le facilita el nombre asociado con una dirección de correo electrónico.
- **Firmware:** El código de la programación que ejecuta un dispositivo de red.
- **Fragmentación:** Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.
- **Frase secreta:** Se utiliza con mucha frecuencia como una contraseña, ya que una frase secreta simplifica el proceso de cifrado WEP generando de forma automática las claves del cifrado WEP para los productos Linksys.
- **FTP:** (Protocolo de transferencia de archivos) Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.
- **Hardware:** El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.
- **HTTP:** (Protocolo de transferencia de hipertexto) Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.
- **IEEE:** (Instituto de ingenieros eléctricos y electrónicos) Instituto independiente que desarrolla estándares de redes.
- **Infraestructura:** Equipo de red e informático actualmente instalado.
- **Inicio:** Iniciar un dispositivo y provocar que comience a ejecutar instrucciones.

- **Intervalo de indicador:** El intervalo de frecuencia del indicador, que es una emisión de paquetes de un enrutador para sincronizar una red inalámbrica.
- **IP:** (Protocolo Internet) Protocolo utilizado para enviar datos a través de una red.
- **IPCONFIG:** Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.
- **IPSEC:** (Seguridad del protocolo Internet) Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP.
- **ISIP:** (Proveedor de servicios de Internet) Compañía que proporciona acceso a Internet.
- **Itinerancia:** Capacidad de transportar un dispositivo inalámbrico desde el alcance de un punto de acceso hasta otro sin perder la conexión.
- **LAN:** (Red de área local) Los equipos y productos de red que componen la red doméstica o de oficina.
- **LEAP:** (Protocolo de autenticación extensible ligero) Método de autenticación mutua que utiliza un sistema de usuario y contraseña.
- **MAC:** (Dirección de control de acceso al medio) Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.
- **Máscara de subred:** Código de dirección que determina el tamaño de la red.
- **Mbps:** (Megabits por segundo) Un millón de bits por segundo, unidad de medida de transmisión de datos.
- **mIRC:** Programa de Internet Relay Chat que se ejecuta bajo Windows.
- **Módem de cable:** Un dispositivo que conecta una equipo a la red de la televisión por cable que a su vez se conecta a Internet.
- **Modo infraestructura:** Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.
- **Multidifusión:** Envío de datos a un grupo de destinos a la vez.
- **NAT:** (Traducción de direcciones de red) La tecnología NAT traduce direcciones IP de la red de área local a una dirección IP diferente para Internet.
- **Navegador:** Programa de aplicación que proporciona una forma de consultar e interactuar con la información de la World Wide Web.
- **NNTP:** (Protocolo de transferencia de noticias a través de la red) Protocolo utilizado para conectar a los grupos Usenet de Internet.

- **Nodo:** Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.
- **OFDM:** (Multiplexado por división de frecuencia ortogonal) La transmisión de frecuencia que separa la corriente de datos en un número de corrientes de datos de velocidad inferior que se transmiten en paralelo para prevenir que se pierda información durante la transmisión.
- **Paquete:** Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.
- **PEAP:** (Protocolo de autenticación extensible protegido) Protocolo para la transmisión de de datos de autenticación, incluyendo contraseñas, a través de redes inalámbricas 802.11.
- **Ping:** (Buscador de paquetes de Internet) Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.
- **Pirata informático**: Un término de jerga para un entusiasta informático. También hace referencia a los individuos que obtienen acceso no autorizado a sistemas informáticos con el fin de robar y corromper datos.
- **PoE:** (Alimentación a través de Ethernet) Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.
- **POP3:** (Protocolo de oficina de correo 3) Protocolo estándar utilizado para recuperar correo electrónico almacenado en un servidor de correo.
- **PPPoE:** (Protocolo a través de Ethernet punto a punto) Tipo de conexión de banda ancha que proporciona autenticación (usuario y contraseña) además de transporte de datos.
- **PPTP:** (Protocolo de túnel punto a punto) Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.
- **Preámbulo:** Parte de la señal inalámbrica que sincroniza el tráfico de red.
- **Puente:** Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.
- **Puerta de enlace:** Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.
- **Puerta de enlace predeterminada:** Dispositivo que re direcciona tráfico de Internet desde su red de área local.

- **Puerto:** Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.
- **Punto de acceso:** Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.
- **RADIUS:** (Servicio de usuario de marcado con autenticación remota) Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.
- **Red:** Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.
- **Red troncal:** Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.
- **Rendimiento:** Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.
- **RJ-45:** (Toma registrada 45) Conector Ethernet que alberga hasta ocho hilos.
- **RTP:** (Protocolo de tiempo real) Un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.
- **RTS:** (Solicitud para enviar) Método de red para la coordinación de paquetes grandes a través de la configuración Umbral de solicitud de envío (RTS).
- **Servidor:** Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.
- **Servidor de seguridad:** Un servidor de seguridad es cualquiera de los esquemas de seguridad que evitan a los usuarios no autorizados obtener acceso a una red de equipos o que supervisa la transferencia de información hacia y desde la red.
- **Servidor de seguridad SPI:** (Inspección de paquetes de datos) Una tecnología que inspecciona los paquetes de información entrantes antes de permitirles que entren en la red.
- **SMTP:** (Protocolo simple de transferencia de correo) Protocolo de correo electrónico estándar de Internet.
- **SNMP:** (Protocolo simple de administración de redes) Protocolo de control y supervisión de redes ampliamente extendido.
- **Software:** Instrucciones para el equipo. Se denomina “programa” al conjunto de instrucciones que realizan una tarea determinada.

- **SOHO:** (Oficina pequeña/oficina doméstica) El segmento de mercado de profesionales que trabajan en casa o en pequeñas oficinas.
- **SSID:** (Identificador de conjunto de servicio) Nombre de su red inalámbrica.
- **Tasa TX:** Tasa de transferencia.
- **TCP:** (Protocolo de control de transporte) Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.
- **TCP/IP:** (Protocolo de control de transporte/Protocolo Internet) Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.
- **Telnet:** Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.
- **TFTP:** (Protocolo trivial de transferencia de archivos) Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.
- **TKIP:** (Protocolo de integridad de clave temporal) Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.
- **TLS:** (Seguridad de capa de transporte) Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.
- **Topología:** Distribución física de una red.
- **UDP:** (Protocolo de datagramas de usuario) Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.
- **URL:** (Localizador uniforme de recursos) Dirección de un archivo situado en Internet.
- **VPN:** (Red privada virtual) Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.
- **WAN:** (Red de área extensa) Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.
- **WEP:** (Protocolo de equivalencia con cable) WEP es un protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.

- **WINIPCFG:** Utilidad de Windows 98 y Millenium que muestra la dirección IP de un dispositivo de red concreto.
- **WLAN:** (Red de área local inalámbrica) Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.
- **WPA:** (Acceso protegido WiFi) Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.
- **WPA2:** (Acceso protegido Wi-Fi 2) WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.
- **WPA-Enterprise:** Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.
- **WPA-Personal:** Versión de WPA

10. ANEXOS:

A. PLAN DE DISERTACIÓN

B. REDES

C. PROTOCOLOS

D. SEGURIDAD

E. OTROS