"Un sistema se vuelve inseguro simplemente con el mero hecho de encenderlo. El único sistema totalmente seguro sería uno que estuviese apagado, desconectado de cualquier red, metido dentro de una caja fuerte de titanio, rodeado de gas y vigilado por unos guardias armados insobornables. Aún así yo no apostaría mi vida por él"

Gene Spafford, experto en seguridad

VPN SOBRE LINUX

ANÁLISIS DE CIPE Y PPTP

Estableciendo Túneles

Dollceys Mestre Ruiz
Karol Medrano Medina

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
Facultad de Ingeniería de Sistemas

2004

Cartagena, Bolívar.

VPN SOBRE LINUX

ANÁLISIS DE CIPE Y PPTP

Estableciendo Túneles

Mestre R. Dollceys
Medrano M, Karol

Monografía presentada para optar el título de Ingeniero de Sistemas

Asesor

Giovanni Vásquez
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

Facultad de Ingeniería de Sistemas

2004

Cartagena, Bolívar.

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Cartagena, Julio 21-2004

Cartagena, Julio 21 de 2004

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente nos permitimos informarles que la monografía titulada "**VPN SOBRE LINUX"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

DOLLCEYS MESTRE RUIZ	**KAROL MEDRANO MEDINA**
Código	Código

Cartagena, Julio 21 de 2004

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente me permito informarles que la monografía titulada "**VPN SOBRE LINUX"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como director considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

Giovanni Vásquez

Magíster en Ciencias Computacionales

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Julio 21 de 2004

Yo DOLLCEYS MESTRE RUIZ, identificado con la cédula de ciudadanía número 73.140.830 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

DOLLCEYS MESTRE RUIZ

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Julio 21 de 2004

Yo KAROL MEDRANO MEDINA identificado con la cédula de ciudadanía número 33.334.441 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

KAROL MEDRANO MEDINA

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no pueden ser explotados comercialmente sin autorización.

Dedicado a:

A Dios, a mi familia, luz de mi camino, en especial a ti Loli.

Dollceys Mestre Ruiz.

A DIOS,
Y a mi Familia, que siempre me apoyó.

Karol Medrano Medina.

CONTENIDO

INTRODUCCIÓN

El desarrollo de las comunicaciones ha permitido que las empresas a nivel mundial, expandan la cantidad y calidad de los servicios que prestan a través de sus redes, pero los costos que implica mantener enlaces permanentes entre las diferentes sedes, ha motivado la generación de nuevas y más baratas alternativas de comunicación. Las VPNs se presentan como una alternativa de bajo costo, que permite cubrir de forma segura las necesidades de grandes y pequeñas empresas, con unos costos mínimos en infraestructura y tiempos muy cortos para la implementación de soluciones. Adicionalmente la aparición y desarrollo de software como LINUX ha generado una reacción del mercado, que acostumbrado a manejar solo soluciones de tipo propietario, encuentra particularmente atractiva la idea minimizar los costos en la adquisición de software, especialmente cuando este permite mayor integración y ventajas realmente competitivas a nivel de comunicaciones. La unión de estas dos corrientes es la razón del siguiente estudio, que pretende mostrar de forma practica la implementación de dos alternativas de VPN sobre LINUX, utilizando los protocolos **CIPE** y **PPTP,** pretendiendo ser al final una guía para la selección objetiva de alguno de estos desarrollos, como solución de bajo costo para la industria.

JUSTIFICACIÓN

La empresa moderna es conciente de que el mundo de las comunicaciones, es cada vez mas relevante para el buen desarrollo de su economía, sin embargo, es común que las empresas no tengan la información necesaria o el personal capacitado en las diferentes alternativas del mercado, sobre todo, de tecnologías nuevas. Siendo la universidad el estadio natural para la investigación y el desarrollo, este documento se desarrolla teniendo en cuenta la necesidad de la industria y del estudiantado, interesado en conocer sobre alternativas seguras y económicas para la transferencia de información a través de redes públicas como Internet.

OBJETIVOS

Analizar las principales características de las VPN

Mostrar por medio de un ejemplo la Implementación de VPNs con CIPE sobre LINUX

Mostrar por medio de un ejemplo la Implementación de VPNs con PPTP sobre LINUX

Brindar un documento de apoyo, a los estudiantes y profesores de la Universidad interesados en la Seguridad en redes.

1. QUE ES VPN?

1.1 ACCESO REMOTO SEGURO

1.1.1 ¿CUÁL ES EL PROPÓSITO DE LOS ACCESOS REMOTOS SEGUROS?

Con los accesos remotos seguros, las conexiones vía Modem telefónico pueden transferir datos seguros vía un proveedor de servicios Internet o vía una red corporativa. Los datos se encriptan en el cliente antes de que sean transmitidos y se desencriptan en la puerta de la firewall. El software proporcionado, habilita a los usuarios remotos a que se pueden conectar a la red corporativa como si ellos estuvieran detrás de la firewall.
La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

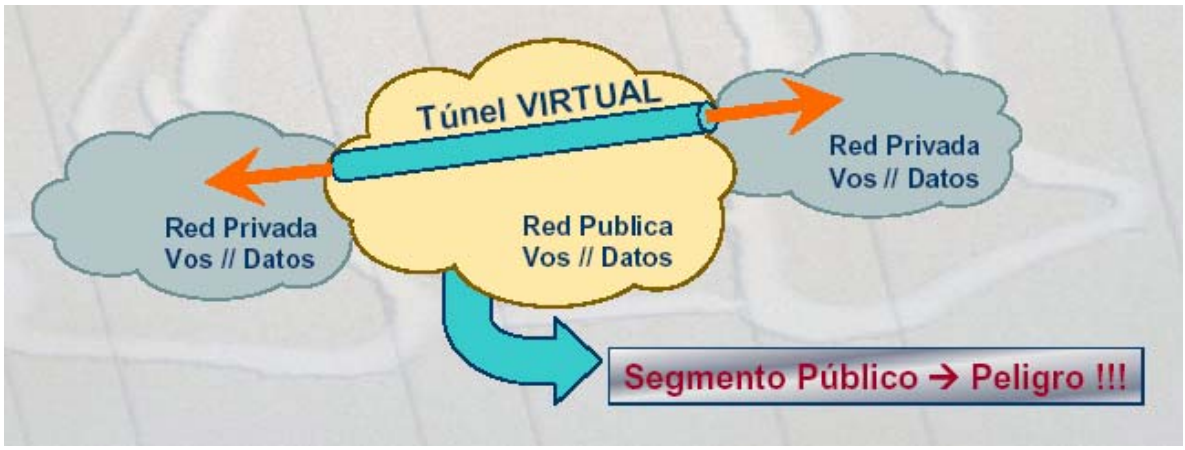
1.1.2 ¿QUÉ ES UNA RED SEGURA, PRIVADA Y VIRTUAL?

Una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia. Para

lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas. Primero, deben poder pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública. Segundo, la solución debe agregar encripción, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado. Finalmente, la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

1.2 DEFINICIÓN.

Una VPN es un grupo de dos o más computadores, en muchas ocasiones conectados a una red privada, que tienen una salida hacia Internet y se comunican de manera segura sobre esta red pública. Para realizar esta transferencia se utilizan métodos de seguridad, que garantizan la privacidad de los datos que se intercambian a través de túneles. Esta forma de comunicación permite extender las capacidades de las redes internas a las oficinas distantes, sin tener que realizar costosas llamadas de larga distancia.



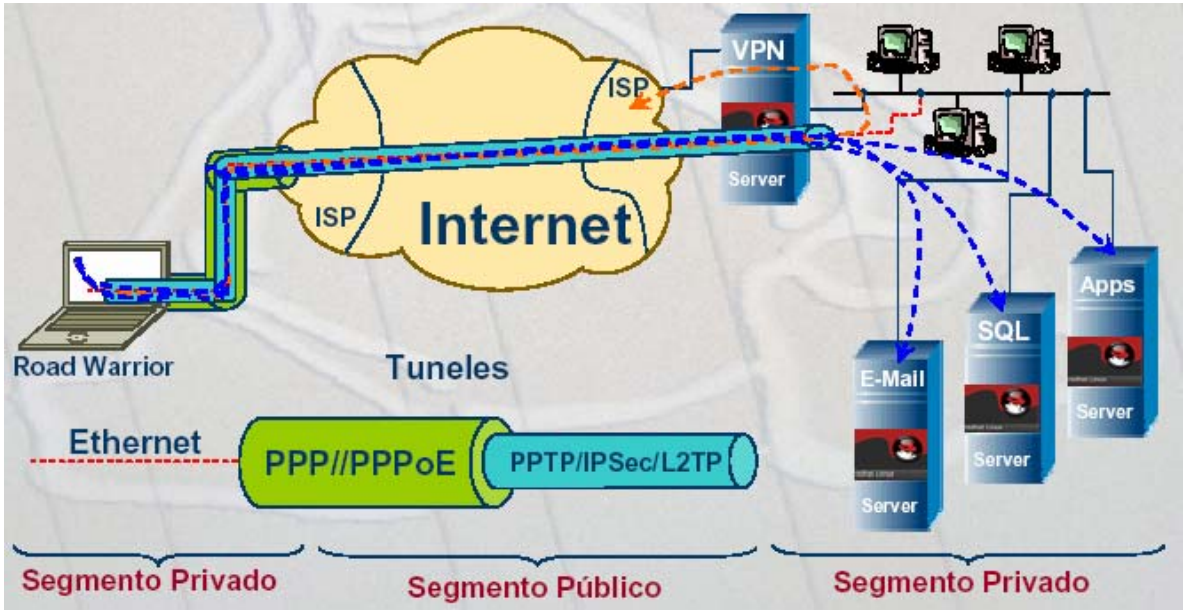
Las VPNs son capaces de transferir la información utilizando la técnica de Tunneling.

¿Cómo trabaja la tecnología de túneles de una Red Privada Virtual?

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos. La tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.
Los proveedores de varias firewall incluyen redes privadas virtuales como una característica segura en sus productos.

Algunas de las tecnologías de tunneling son:

DLSW- Data Link Switching (SNA over IP)
IPX for Novell Netware over IP
GRE – Generic Routing Encapsulation (rfc 1701/2)
ATMP – Ascend Tunnel Management Protocol
IPSec – Internet Protocol Security Tunnel Mode
PPTP - Point-to-Point Tunneling Protocol
L2F – Layer 2 Forwarding
L2TP – Layer 2 Tunneling Protocol



Para que la información transmitida pueda ser protegida, esta es encriptada en tiempo real, asegurando la **confidencialidad e integridad** de los datos transmitidos.

1.3 REQUERIMIENTOS

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puede obviarse algunos.

Autentificación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.

Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.

Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.

Administración de claves, debe proveer un mecanismo de claves de encriptación para los clientes y los servidores.

Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando la red pública, por ejemplo IPX, IP, etc...

2. CARACTERÍSTICAS

2.1 TIPOS

Los tipos de VPN se pueden clasificar así:

Sistemas Basados en Hardware: Son sistemas que utilizan Routers que encriptan, su ventaja consiste en que son muy fáciles de usar e instalar, tan solo se conectan y listo. Su desventaja consiste en que se deben adquirir los equipos en vez de usar una CPU de la empresa, adicionalmente se trata de equipos muy delicados.

Sistemas Basados en Cortafuego: Estos sistemas se implementan a través del software Firewall. Su ventaja consiste en que se mantienen los mecanismos de seguridad que usan los Firewall, permiten NAT y otros servicios útiles para las VPN. Su desventaja consiste en que, al no tener hardware especializado para la encriptación, el rendimiento es menor.

Sistemas Basados en Software:

Son los sistemas más flexibles, permiten enrutar la información en función de las direcciones o de los protocolos, a diferencia de

los basados en hardware, en los cuales el tráfico es enrutado por túnel.

2.2 PROTOCOLOS

Si la tunelación ("Tunneling") es el método para crear la red virtual, el túnel es el camino lógico por el que los datos son encaminados desde un extremo a otro del circuito que se crea. Para que pueda establecerse un túnel es necesario que los extremos implicados utilicen los mismos protocolos de tunelación.

MPPE *(Microsoft Point-to-Point Encryption, descrito en el RFC 3078):* Es un protocolo que se basa en encriptar los datos de PPP (Point to Point Protocolo). El algoritmo de cifrado que emplea es el RSA RC4 para proporcionar la confidencialidad de los datos. La longitud de la clave para la sesión puede ser negociada, actualmente soporta claves de sesión de 40 bits y 128 bits.

IPIP *(IP in IP Tunneling, descrito en el RFC 1853):* La encapsulación IP en IP ha sido empleada por bridges que tienen diferentes capacidades o políticas. Pero también se puede emplear para implementar técnicas de Tunneling. La técnica de encapsulación es muy simple. Una cabecera IP exterior es añadida antes que la cabecera IP original. Entre ellas hay otras cabeceras para la ruta, por ejemplo cabeceras de seguridad que configuran el túnel.

L2TP (Layer 2 Tunneling Protocol, descrito en el RFC 2661) : Es una extensión del PPTP (Point-to-Point Protocol), mezclando lo mejor de los protocolos PPTP de Microsoft y L2F de Cisco. Los dos componentes principales del L2TP son:

El LAC (L2TP Access Concentrator), que es el dispositivo que físicamente termina una llamada; y el LNS (L2TP Network

Server), que es el dispositivo que autentifica y termina el enlace PPP. L2TP utiliza redes conmutadas de paquetes para hacer posible que los extremos de la conexión estén ubicados en distintas computadoras. El usuario tiene una conexión L2 al LAC, el cual crea el túnel de paquetes PPP. Así, los paquetes pueden ser procesados en el otro extremo de la conexión, o bien, terminar la conexión desde un extremo.

IPSec *(IP Seguro, descrito en el RFC 2411)* : protocolo que sirve para establecer una sesión segura entre dos hosts que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red.

IPSec trata de remediar algunas carencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.
Define nuevos formatos de paquete: la cabecera de autentificación (AH), que permite asegurar la integridad de los datos y el ESP (Encapsulating Security Payload), que permite asegurar la privacidad e integridad de los datos. AH protege la integridad y autenticidad de los datos, incluyendo los campos invariantes de la cabecera IP. Esta cabecera no proporciona confidencialidad, mientras que ESP protege tanto la confidencialidad como la integridad y la autenticidad de los datos. Cuando se usa para comprobar la integridad de los datos no incluye los invariantes de la cabecera IP.

MS-CHAP (descrito en el RFC 2433): Microsoft creó MS-CHAP para autentificar estaciones remotas Windows. Proporciona la funcionalidad a la cual los usuarios Lan están acostumbrados, integrando algoritmos de cifrado y hash sobre redes Windows.

En general la elección del protocolo determina el tipo de implementación que se desea, en este caso en particular, se utilizará los siguientes protocolos CIPE Y PPTP, los cuales, se describirán a continuación

2.2.1 CIPE (CRYPTO IP ENCAPSULATION)

CIPE es un protocolo que permite transferir información entre subredes, utilizando la encapsulación IP sobre paquetes UDP (Análogo a Ipsec, el cual usa TCP para la encapsulacion en vez de UDP), como herramienta para proteger los datos que son enviados a través de una red pública como lo es Internet. Para esto, encripta los datos a nivel de red, es decir, los paquetes que viajan entre hosts por la red están encriptados. El motor de encriptación se sitúa cerca del controlador que envía y recibe los paquetes. El protocolo CIPE consta de dos partes: encriptación y suma de verificación de los paquetes de datos e intercambio de claves dinámico.

Blowfish es uno de los algoritmos de encriptación utilizados para proteger los datos, este algoritmo es seleccionado en el momento de la instalación del software, lo cual permite una implementación mas sencilla, consumir menos recursos y tener latencia mas baja y la posibilidad de usarlo bajo Firewall tipo Socks.

Para que los paquetes puedan ser transferidos sobre IP como paquetes UDP, CIPE crea un dispositivo de red virtual (Cipcbx) que coloca los paquetes sobre la red transportadora al nodo remoto destinado. La encriptación de nivel bajo tiene la ventaja de que puede hacerse funcionar de forma transparente entre las dos redes conectadas en la VPN, sin ningún cambio en el software de aplicación.

Cada datagrama IP se toma como un todo, incluyendo la cabecera. Se rellena al final con cero a siete octetos aleatorios, de tal forma, que la longitud total en octetos es congruente a tres módulo ocho.

Al paquete rellenado se le adiciona un octeto del valor P y el CRC-32 al paquete construido hasta el momento e incluyendo P. Esto hace que la longitud del paquete completo sea un

múltiplo de ocho octetos. El valor P se da así: los bits 6, 5, 4 indican la longitud del relleno entre el final del paquete original y P. Los bits 2 y 1 son un tipo de código e indican la clase de paquete. Los bits sobrantes 7, 3 y 0 están reservados y deben ser cero.

Los tipos de código son:
00 - dato
01 - intercambio de clave
10 - reservado
11 – reservado

Los paquetes que se transmiten no llevan ninguna información relativa al datagrama IP original aparte de su longitud, rellenada a un múltiplo de ocho. Esto debería prevenir efectivamente contra la mayoría de los aspectos de análisis de tráfico.

Existen diferentes razones para seleccionar CIPE como protocolo base para creación de VPNs:

En las distintas distribuciones de linux se encuentra incluido el software CIPE además de los diferentes sistemas de encripción soportados por CIPE.

CIPE utiliza los algoritmos de encripción BLOWFISH e IDEA. Dependiendo la regulación en los países, se puede utilizar el algoritmo por defecto BLOWFISH para encriptar todo el tráfico de la Intranet.

Debido a que CIPE es basado en software, cualquier computador capaz de correr LINUX se puede convertir en un gateway CIPE, ahorrándole a cualquier organización la necesidad de gastar grandes sumas de dinero en la compra de hardware exclusivo para VPN.

CIPE es actualmente desarrollado para trabajar en conjunto con *iptables, ipchains*, y otros Firewall basados en reglas. Que el

destinatario acepte los paquetes UDP CIPE es todo lo que se necesita para coexistir con los Firewall basados en reglas.

La configuración de CIPE esta basada en archivos de texto, permitiendo a los administradores configurar los servidores y clientes CIPE remotamente sin necesidad de utilizar herramientas graficas que funcionan pobremente sobre una red.

2.2.2 PPTP (POINT-TO-POINT TUNNELING PROTOCOL)

El protocolo fue originalmente designado como un mecanismo de encapsulamiento, para permitir el transporte de protocolos diferentes del TCP/IP, como por ejemplo IPX sobre la red Internet. La especificación es bastante genérica, y permite una variedad de mecanismos de autentificación y algoritmos de encriptación.

PPTP es una especificación de protocolo desarrollada por varias compañías: Ascend Communications, Microsoft Corporation, 3 Com/Primary Access, ECI Telematics, and U.S. Robotics. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo.

El Protocolo de Túnel Punto-a-Punto es un protocolo que permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN.

El principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Generalmente hay tres computadores involucrados en el uso del PPTP. Hay un cliente PPTP, un servidor de acceso a la red y un servidor de PPTP. En el caso de una LAN, el servidor de acceso a

la red no es necesario, porque ya esta en la misma red. La comunicación segura creada usando el protocolo PPTP conlleva tres fases, cada una de los cuales requiere la finalización correcta de las anteriores. Estas son: PPP conexión y comunicación, PPTP control de conexión, PPTP data tunneling.

PPP conexión y comunicación

Primero el cliente necesita una conexión a Internet, conectando con un Servidor de Acceso a Red (NAS Network Access Server) vía un Proveedor de Servicios de Internet (ISP). Un cliente PPTP usa el PPP para establecer esta conexión. La conexión requerida por un cliente consiste en unas credenciales de acceso (usuario, password) y un protocolo de autentificación para que el servidor de PPTP pueda autentificar al cliente. Una vez conectado el cliente puede enviar y recibir paquetes sobre Internet.

PPTP control de conexión

Cuando el cliente tiene establecida la conexión PPP con el ISP, se realiza un segundo establecimiento de llamada, sobre la conexión PPP existente. Esto crea la conexión VPN (conexión de control) a un servidor PPTP de una LAN privada a una empresa y actúa como un túnel a través de la cual fluyen los paquetes de red. Un set de ocho mensajes de control establecerá, mantendrán y finalizaran el túnel PPTP. Los mensajes son los siguientes:

- PPTP_START_SESSION_REQUEST Starts Session
- PPTP_START_SESSION_REPLY Replies to Start Session Request
- PPTP_ECHO_REQUEST Maintains Session
- PPTP_ECHO_REPLY Replies to Maintain Session Request
- PPTP_WAN_ERROR_NOTIFY Reports an error in the PPP connection
- PPTP_SET_LINK_INFO Configures PPTP Client/Server Connection
- PPTP_STOP_SESSION_REQUEST Ends Session

- PPTP_STOP_SESSION_REPLY Replies to End Session Request
- PPTP Data Tunneling

Después de establecer el túnel PPTP, los datos son transmitidos entre el cliente y el servidor PPTP. Los datos son enviados en formato de datagramas IP que contienen paquetes PPP, a los que referimos normalmente como paquetes PPP encapsulados. Los datagramas IP contienen paquetes IPX, NetBEUI, o TCP/IP y tiene el siguiente formato:

PPP encabezado de entrega	IP Encabezado	GRE Encabezado	PPP Encabezado	IP Encabezado	TCP Encabezado	DATOS

El encabezado IP de entrega proporciona la información necesaria para que el datagrama atraviese la red Internet. El encabezado GRE se usa para encapsular el paquete PPP dentro de un datagrama IP. La zona ensombrecida representa los datos encriptados.
Después de que la conexión VPN esta establecida, el usuario remoto (cliente) puede realizar cualquier operación como si fuera un usuario local.

Una de las características de este protocolo es la característica disponible de seguridad. Hay tres áreas en la seguridad PPTP que lo hace más atrayente. Son la autentificación, encriptación de datos y filtrado de paquetes PPTP.

Autentificación
La autentificación de un cliente PPTP remoto se hacen de la misma manera que la autentificación PPP usado por cualquier cliente RAS (Remote Access Service). Las cuentas de usuarios son configuradas para que solo los usuarios específicos tengan acceso a la red a través del domino de confianza. El uso de contraseñas seguras es uno de las mejores formas de utilización exitosa del PPTP.

Encriptación de Datos

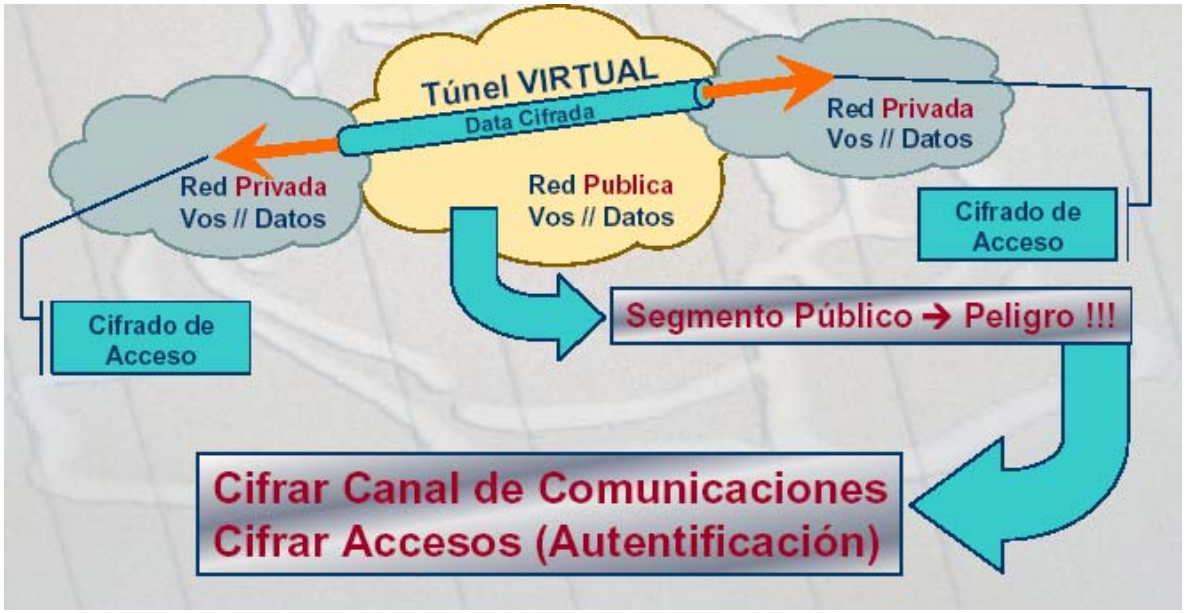
Los datos enviados por el túnel PPTP en los dos sentidos son encriptados. Los paquetes de red son encriptados en la fuente (cliente o servidor), viajan a través del túnel, y son desencriptados en el destino. Como todos los datos en una conexión PPTP fluyen dentro del túnel, los datos son invisibles al resto del mundo. La encriptación de datos dentro del túnel da un nivel adicional de seguridad.

Filtrado de Paquetes PPTP

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si está activada en el servidor PPTP. Cuando está activa acepta y enruta solo los paquetes PPTP de los usuarios autorizados. Esto prevé que el resto de paquetes entren en la red privada y en el servidor de PPTP.

2.3 SEGURIDAD

El aspecto importante en las VPN o cualquier tecnología que comprometa la naturaleza típicamente restrictiva de una red privada es la seguridad. Los primeros detractores de las VPN fueron ágiles en demostrar la vulnerabilidad de la tecnología y muchos críticos señalaron a los protocolos mismos.



La importancia del problema de la seguridad exclusivamente en relación a las VPN ha llevado a que muchas compañías implementen normas estrictas en el uso de Internet y de las aplicaciones de software para los usuarios de las VPN.

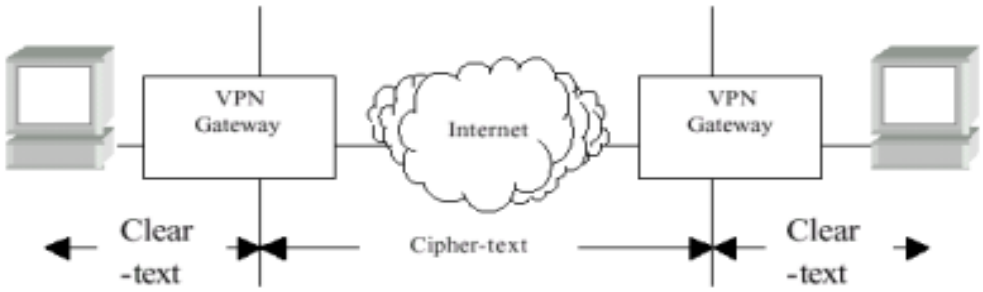
Internet es una red pública, donde los datos en tránsito pueden ser "leídos por cualquier equipo". La seguridad en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión no puedan ser descifrados. Los datos transitan codificados por Internet en " Túneles Virtuales" creados por dispositivos VPN que utilizan criptografía; y esos dispositivos que son capaces de "entender" los datos codificados forman, una " red virtual" sobre la red pública.

2.3.1 ENCRIPCIÓN

Las redes privadas virtuales garantizan la privacidad y la confidencialidad de la información haciendo uso de la encripción. Encripción es una técnica que codifica la información de un modo que hace difícil o imposible su lectura,

y la decodifica de modo que pueda ser leída nuevamente. A la información codificada se la llama cipher-text y a la información sin codificar, clear-text.

Cuando en una VPN se transmite información de un punto a otro, el Gateway de la VPN del punto de origen encripta la información en cipher-text antes de enviarla. En el otro punto, el Gateway receptor desencripta la información, es decir se vuelve clear-text, y luego la envía a la LAN.



Un algoritmo de encripción es una técnica reproducible de cifrado y descifrado de información que puede ser realizada por personas o computadoras. Un ejemplo sencillo de un algoritmo de encripción sería reemplazar cada letra en una oración por la letra que le sigue inmediatamente a ésta en el alfabeto, obteniendo el cipher-text. Para leer la oración original, simplemente reemplazaríamos cada letra del cipher-text por la letra que la precede en el alfabeto.

En el pasado, la encripción permanecía segura manteniendo el algoritmo como un secreto. De este modo, no se podía leer un mensaje encriptado ya que se desconocía cómo había sido creado. El principal problema es que una vez que el algoritmo ha sido descubierto, se tiene acceso a toda la información que haya sido encriptada con el mismo. Peor aún, dado que la técnica de encripción es un secreto, resulta imposible determinar cuán buena es su calidad ya que muy poca gente puede probarla.

Actualmente, los mejores métodos de encripción son públicos de modo tal que todo el mundo sepa cómo funcionan. De hecho, se sabe exactamente cómo es encriptada la información. Estos métodos están disponibles para cualquiera y están muy probados.

2.3.2 CLAVES

Ahora, dado que el método no es secreto, se evita que alguien acceda a la información mediante el uso de keys (claves). Una clave es un código secreto utilizado por el algoritmo de encripción para crear una versión única de cipher-text. Esta clave podría compararse con la combinación utilizada en una caja fuerte.

De este modo, la seguridad no depende de que el algoritmo de encripción sea un secreto. Actualmente, la mayoría de los estándares de seguridad de Internet (como DES y 3DES) toman esta postura de exponer su algoritmo ante cualquiera para que sea examinado y usado, brindando seguridad a través de la generación de claves únicas y con alta dificultad de ser conocidas. El nivel de seguridad generalmente depende en buena parte del largo de la clave (key lenght).

2.3.3 KEY LENGHT

Utilizando algoritmos de encripción conocidos, la seguridad depende del largo de la clave. Una clave de 8 bits implica 2^8 combinaciones, mientras que una clave de 16 bits implica 2^{16} (65536) combinaciones posibles.

Con una clave de 16 bits, alguien podría realizar 65536 intentos antes de adivinar la clave que brinda acceso al *cipher-text*. Para una persona esto sería bastante difícil, pero para una

computadora no sería un gran desafío y no tomaría demasiado tiempo recorrer todas las posibilidades.

Key length(bits)	Combinaciones posibles
8	256
16	65.536
56	72.057.594.037.927.900
112	5.192.296.858.534.830.000.000.000.000.000.000
168	374.144.419.156.711.000.000.000.000.000.000.000.000.000.000.000

Generar claves seguras es sólo una parte de la ecuación. Para garantizar una seguridad continua, lo deseable es que las claves cambien constantemente cada breve periodo de tiempo. Del mismo modo en que los algoritmos que basan su seguridad en mantenerse secretos, sucede con las claves. Si se logra adivinar una clave, se tiene acceso a toda la información encriptada con ella. Por este motivo, en una buena implementación nuevas claves son generadas cada vez que un túnel VPN es establecido, y las claves son regeneradas cada cierto tiempo, generalmente cada dos horas.

2.3.4 CLAVES SIMÉTRICAS Y ASIMÉTRICAS

Cuando la misma clave es utilizada para encriptar y desencriptar la información, esta es denominada simétrica. Esto requiere que los puntos comunicados a través de la VPN posean la misma clave.

Otra técnica utilizada permite que la información sea encriptada con una clave, pero desencriptada con otra. La información

encriptada con una clave no puede ser desencriptada con la misma y viceversa. Dos claves son requeridas, una para encriptar y otra para desencriptar, y estas no pueden ser intercambiadas. Estos pares de claves son denominadas claves asimétricas.

Con las claves asimétricas, a una clave se la denomina clave pública y a la otra clave privada. La clave pública en general no se mantiene en secreto. Si A desea enviarle un mensaje a B de modo tal que nadie más pueda verlo, entonces A encripta el mensaje usando la clave pública de B. B es el único capaz de desencriptar el mensaje, utilizando su clave privada. En otro ejemplo, si A envía un mensaje a B y desea que B pueda corroborar que efectivamente el mensaje proviene de A y no está falsificado, entonces A puede encriptar el mensaje utilizando su clave privada, y B puede desencriptar el mensaje con la clave pública de A. Si de este modo B logra desencriptar el mensaje correctamente, entonces el mensaje tiene que haber provenido de A.
Las claves asimétricas suelen ser muy largas - por ej. 1024 o 2048 bits -. El procesamiento de encripción requiere bastante potencia computacional y toma mucho tiempo. Por esto, las claves asimétricas son utilizadas para eventos que no ocurren frecuentemente, como establecer un túnel VPN. Las claves simétricas suelen ser mucho más cortas - por ej. 56, 112 o 168 bits-, por lo que el procesamiento de encripción utilizando claves simétricas es considerablemente mas rápido que con las asimétricas. Las claves simétricas se utilizan para transacciones de alta frecuencia, especialmente para la encripción de datos transmitidos sobre una VPN.

2.3.5 AUTENTICACIÓN

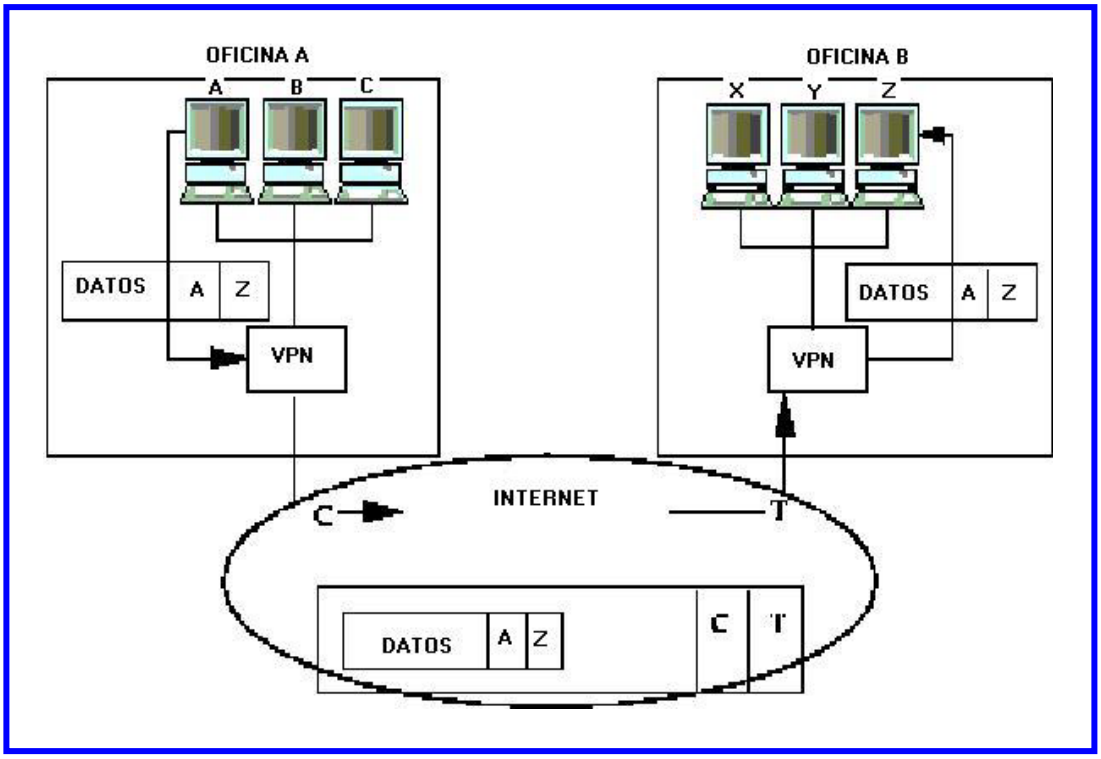
La tecnología de encripción garantiza la privacidad de la información al atravesar Internet. La tecnología de autenticación garantiza:

1. La identidad de los participantes de la VPN (los *gateways* y clientes son quienes dicen ser)
2. La integridad de la información recibida (no ha sido alterada en el camino)

Existen diversos modos de autenticación, siendo el más común el uso de usuario y contraseña. El problema con este método en particular es que es un tanto inseguro: una de sus debilidades es que los usuarios deben elegir contraseñas que puedan recordar fácilmente. Esto significa que pueden ser adivinadas.
Una de las tecnologías mas utilizadas es la de certificados digitales, lo que permite autenticar e identificar tanto a personas como a sistemas sin el uso de usuarios y contraseñas. Un certificado digital es un registro que incluye varios datos, como el nombre de una persona, su dirección, su clave pública, y fechas de expiración del certificado que indican cuando éste deja de ser válido. En una VPN, los certificados digitales se utilizan para identificar a quien (persona o sistema) intenta conectarse a la VPN, y como medio de distribución de claves públicas.

2.3.6 ENCAPSULAMIENTO

Encripción, claves, certificados y firmas digitales son las tecnologías de seguridad que garantizan la privacidad en una VPN. Ahora, generalmente, el envío de información en una VPN se realiza entre direcciones privadas. Es decir, entre direcciones no routeables vía Internet.



Veamos este ejemplo. En la oficina A la maquina con dirección 'a' puede comunicarse con 'c' al enviar paquetes con encabezados que digan dirección-origen: a, dirección-destino: b. Esto funciona perfectamente dentro de la Lan.

El problema se presenta cuando la máquina 'a' de la oficina A quiere enviar información a la máquina 'z' en la oficina B. Como ambas direcciones son privadas, no hay modo de routear paquetes a través de Internet, que es la red pública que une a ambas oficinas. Entonces, para realizar esta conexión, se requiere encapsulamiento.

El *gateway* de la oficina A, con dirección C, sabe que las direcciones privadas 'x', 'y' y 'z' se encuentran en la oficina B; y también sabe que el *gateway* de la oficina B tiene dirección T. Entonces, cuando 'a' envía un paquete a 'z', el gateway de la oficina A lo recibe y prepara para su envío. El paquete inicial que dice dirección-origen: a, dirección-destino: b, es encriptado y puesto dentro de un segundo paquete que dice dirección-origen: C, dirección-destino: T. Como estas direcciones son

Routeables en Internet, este paquete es enviado a la oficina B, en donde el *gateway* de esta oficina extrae el primer paquete y lo envía a la LAN.

Este proceso de poner un paquete dentro de otro es denominado encapsulamiento, y es la base del **tunneling**.

2.4 VENTAJAS

El uso de VPNs tiene las siguientes ventajas:

Costos: La principal motivación para la implantación de las VPN es la financiera: los enlaces dedicados son demasiados caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un coste mas bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

Seguridad: Los datos son encriptados y Encapsulados de manera que hace que estos viajen codificados y a través de un túnel.

Mejor administración: Se puede asignar una IP fija a cada usuario que se conecta, de manera administrativa o de forma dinámica, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente.

Facilidad para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

3. POR QUE LINUX?

La solución VPN basada en Linux que es una tecnología con un alto crecimiento en el mercado presenta beneficios importantes ya que esta plataforma hereda las características principales de los sistemas UNIX: robustez, alta performance y seguridad, además de no necesitar ningún tipo de licenciamiento, ya que está basada en software de libre distribución.

Linux es un sistema operativo que comenzó su desarrollo en el año 1991 por Linus Torvals mientras era estudiante en la universidad de Helsinki en Finlandia. **Linus Torvalds** después de realizar la primera versión estable libera el código a Internet. Desde ese día este sistema operativo creció sin precedentes.

El objetivo ha sido crear un clon de UNIX, libre de cualquier software con derechos de autor comercialmente registrado, que cualquier persona pudiera utilizar.

3.1 CARACTERÍSTICAS DE LINUX

- **Velocidad**
  Su velocidad se debe a la eficiente administración de los recursos, como memoria, CPU y File Systems

- **Estabilidad**
  Su estabilidad es una de las armas fuertes de Linux esto se ve reflejado en el uso de Linux por ejemplo en los ISP

(Internet Service Provider) que lo utilizan para servicios 7 x 24

- **Portabilidad**
  Linux es el sistema operativo que se ejecuta en más plataformas, Intel, Motorola, PowerPC, Alpha

- **Escalabilidad**
  Las aplicaciones podrán correr en una 386, Pentium III, PowerPC, etc.

Linux se basa en estándares más precisamente POSIX y se tiene acceso a todos los fuentes de los programas y herramientas con el derecho de poder modificarlos.

El crecimiento de Linux se ve reflejado en la utilización del mismo. Hoy se puede encontrar en Universidades, Gobiernos, Empresas, etc. Este crecimiento tiene una explicación y son las características que llevaron a este sistema operativo a lo más alto en tecnología: robustez y estabilidad.

3.2 OPEN SOURCE

El Software Libre es una forma novedosa y diferente de producir y distribuir software, que crece día a día. Para definir lo que es el software libre hay que conocer sus cuatro premisas fundamentales que son: usar el software como uno lo requiera, redistribuirlo a quien lo desee, modificarlo y mejorarlo según nuestras necesidades.

Para que las premisas se cumplan realmente se debe cumplir que el propietario del software disponga del código fuente a terceros y libere el software bajo licencia de software libre como puede ser GPL.

El software libre tiene beneficios inigualables con respecto al software propietario. En el Software propietario el licenciamiento nos limita por usuarios así como también el uso

del mismo y son pagas, estas licencias restringen las libertades de los usuarios a usar, modificar, copiar y distribuir el software. Es por ello que el desarrollo, programación y actualización del software lo realiza la empresa que tiene los derechos.

A continuación se detalla tres características que se suman a las anteriores del software propietario:

- En el software propietario se suele ocultar los avances y descubrimientos tecnológicos entre las empresas que lo desarrollan

- El futuro del software que compra una empresa o usuario final solo depende de una compañía comercial

- Muchas veces con estrategias comerciales se suele inducir a los usuarios a que actualicen su software comercial, sin que exista una necesidad verdadera de ello, consiguiendo de esta forma hacer que el usuario invierta en nuevas licencias, la mayoría de las veces innecesarias.

En el Software Libre la licencia es la GPL, esta licencia fue creada por la Free Software Foundation http://www.gnu.org/. Esta licencia no esta limitada por usuarios y garantiza a los usuarios a usar, modificar, copiar, y distribuir el software.

En el desarrollo de software open source puede intervenir cualquier persona, empresa u organización del mundo. Lo cual genera una avalancha de ideas innovadoras, posibilitando grandes avances tecnológicos en estos productos.

A continuación se detalla tres características que se suman a las anteriores del software libre:

- El usuario no depende una sola empresa, ya que el software que implemente puede ser mantenido y modificado por cualquiera en el mundo, esto lo garantiza la licencia GPL.

- Los avances y descubrimientos tecnológicos son diarios, y se encuentran en Internet de forma gratuita. La principal meta de software libre es compartir los avances tecnológicos con los demás.

- El software libre tiene la costumbre de seguir siendo compatible hacia atrás, tanto en software como en hardware, no obliga al usuario a cambiar de tecnología, ya que no persigue los mismos fines económicos que el software comercial.

El caso de éxito más grande del Software Libre es Linux, este sistema operativo fue desarrollado en 1991 por Linus Torvalds en desarrollo colectivo con miles de programadores de todo el mundo, es 100% libre y su filosofía permitió que creciera en forma continua convirtiéndose hoy en uno de los sistemas operativos más estables y robusto que existen.

3.3 REDUCIR COSTOS

Hoy día las empresas necesitan reducir costos para adaptarse al contexto actual y de esa forma lograr mayor eficiencia y productividad.

Reducir costos hoy es real, mediante tecnologías de última generación como es Linux.

Linux es hoy un mercado en constante crecimiento, con soluciones que van desde Mailserver's, Webserver's, hasta servidores de Alta disponibilidad.

Linux crece más allá de su beneficio en costo, por factores que son fundamentales en equipos de producción: confiabilidad y robustez.

Otras de las características de Linux son sus libertades:

- Libertad para correr el software con cualquier propósito
- Libertad de adaptar el software según nuestras necesidades
- Libertad de distribuir copias

3. LABORATORIO: IMPLEMENTACION

Para demostrar como se realiza la configuración de CIPE y PPTP, se asumirá que durante o posteriormente a la instalación de LINUX se incluyo el paquete CIPE y PPTP.

4.1 CONFIGURACION DE CIPE

En el caso de CIPE, para establecer un enlace VPN se necesita que al menos, uno de los extremos del túnel tenga una dirección IP valida fija.

Los archivos de configuración de cipe son archivos planos y son:

1./etc/cipe/options.cipcb0: En el cual se encuentran las definiciones básicas del enlace.

2./etc/rc.d/init.d/ciped.cipcb0: En el cual se establece las reglas de enrutado

La configuración de estos archivos depende de en que extremo del túnel se encuentran

CONFIGURACIÓN DEL LADO DEL CLIENTE

1. /etc/cipe/options.cipcb0

/etc/cipe/options.cipcb0

Surprise, this file allows comments (but only on a line by themselves)
This is probably the minimal set of options that has to be set
Without a "device" line, the device is picked dynamically
the peer's IP address

device=cipcb0

ptpaddr 192.9.200.94

our CIPE device's IP address

ipaddr 192.168.38.100

my UDP address. Note: if you set port 0 here, the system will pick
one and tell it to you via the ip-up script. Same holds for IP 0.0.0.0.

me 0.0.0.0:7638

...and the UDP address we connect to. Of course no wildcards here.

peer 200.69.106.194:9860

The static key. Keep this file secret!
The key is 128 bits in hexadecimal notation.

key 3248fd20adf9c00ccf9ecc2393bbb3e4

En este archivo se definen los siguientes parámetros del enlace:

Device: Determina el nombre del dispositivo virtual cipcb0

Ptpaddr: Determina la dirección IP privada del servidor

Ipaddr: Determina la dirección IP privada del cliente

Me: Determina la dirección IP pública (Dinámica) del cliente y el puerto UDP donde se recibirá la información

Peer: Determina la dirección IP pública (Estática) del servidor y el puerto UDP donde se recibirá la información

Key: Determina la clave de 128 bits que utiliza el algoritmo de encriptación

2. /etc/rc.d/init.d/ciped.cipcb0

```
#!/bin/sh
#  This shell script takes care of starting and stopping ciped.
[ -f /etc/cipe/options ] || exit 0
prog="ciped"
start() {
   # Start daemons.
   echo -n $"Starting $prog: "
   /sbin/modprobe cipcb
   ##### Definicion de las rutas por cada sucursal #######
   /usr/sbin/ciped-cb -o /etc/cipe/options.cipcb0
   /sbin/route add -net 192.9.200.0 netmask 255.255.255.0 gw
    192.168.38.100 dev cipcb0
   echo
}
stop() {
   # Stop daemons.
   echo -n $"Shutting down $prog: "
   killall ciped-cb
   echo
}
# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart|reload)
        stop
        start
        RETVAL=$?
        ;;
  status)
        ;;
  *)
        echo $"Usage: $0 {start|stop|restart|condrestart|status}"
```

En este archivo se inicializa el demonio de CIPE y se definen las reglas de enrutado.

Por último se debe crear un script que se encargue de llamar a cipe cuando sea necesario o al iniciar el sistema.

CARGUECIPE

```
#Para verificar si hay conexion a internet
contadorpppd=`ps xa|grep pppd|grep -v grep|grep -v
carguecipe|wc -l`

#Para Verificar si el ciped esta cargado
contadorcipe=`ps xa|grep $1|grep -v grep|grep -v carguecipe|wc
-l`

#Carga internet
if ( test $contadorpppd = "0" ) then
 /usr/sbin/pppd call internet
 sleep 45
#fi

#Vuelve a verificar si hay conexion a internet
#contadorpppd=`ps xa|grep pppd|grep -v grep|grep -v
carguecipe|wc -l`
#if ( test $contadorpppd != "0" ) then
 if ( test $contadorcipe = "0" ) then
#Carga cipe si no esta arriba
    service ciped.$1 start
    /etc/cipe/firewall start eth1 eth0
 fi
#fi
```

CONFIGURACIÓN DEL LADO DEL SERVIDOR

1. /etc/cipe/options.cipcb0

/etc/cipe/options.cipcb0

Surprise, this file allows comments (but only on a line by themselves)
This is probably the minimal set of options that has to be set
Without a "device" line, the device is picked dynamically
the peer's IP address

device=cipcb0

ptpaddr 192.168.38.100

our CIPE device's IP address

ipaddr 192.9.200.94

my UDP address. Note: if you set port 0 here, the system will pick
one and tell it to you via the ip-up script. Same holds for IP 0.0.0.0.

me 200.69.106.194:9860

...and the UDP address we connect to. Of course no wildcards here.

peer 0.0.0.0:7638

The static key. Keep this file secret!
The key is 128 bits in hexadecimal notation.

key 3248fd20adf9c00ccf9ecc2393bbb3e4

2. /etc/rc.d/init.d/ciped.cipcb0

```
#!/bin/sh
#  This shell script takes care of starting and stopping ciped.
[ -f /etc/cipe/options ] || exit 0
prog="ciped"
start() {
   # Start daemons.
   echo -n $"Starting $prog: "
   /sbin/modprobe cipcb
   ##### Definicion de las rutas por cada sucursal #######
   /usr/sbin/ciped-cb -o /etc/cipe/options.cipcb0
   /sbin/route add -net 192.168.38.0 netmask 255.255.255.0 gw
    192.9.200.94 dev cipcb0
   echo
}
stop() {
   # Stop daemons.
   echo -n $"Shutting down $prog: "
   killall ciped-cb
   echo
}
# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart|reload)
        stop
        start
        RETVAL=$?
        ;;
  status)
        ;;
  *)
        echo $"Usage: $0 {start|stop|restart|condrestart|status}"
```

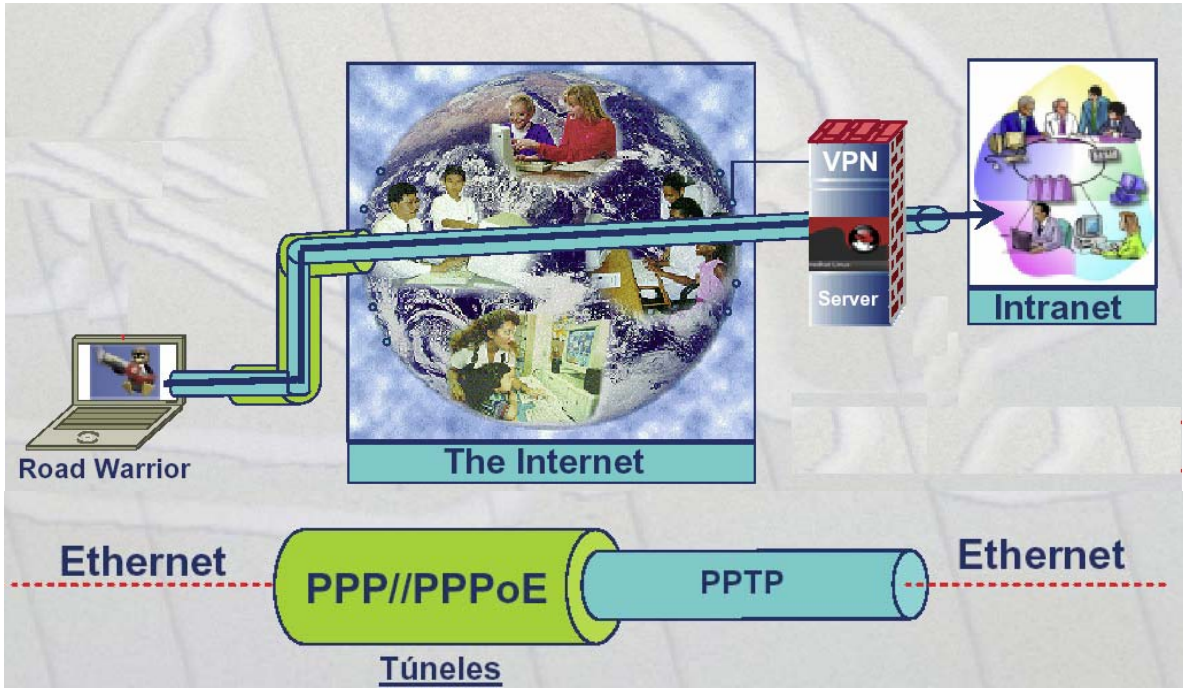
Se debe destacar que para que, el intercambio de información tenga lugar, se debe colocar en los archivos de configuración options.cipcb0, tanto del lado del cliente como del servidor, la misma clave de 128 bits.

Estas claves pueden ser generadas de la siguiente forma:

ps -auxw | md5sum

4.2 CONFIGURACION DE PPTP

ESCENARIO



ELECCIONES Y DECISIONES

- Server VPN/Protocolo Túnel VPN

  - PPTPD (PoPToP) // PPTP

- Plataforma de Trabajo Server: Red Hat Linux 9.0

- Cifrado de Datos MPPE (40/128 Bits)
- Autentificación MS-CHAP/MS-CHAPv2
- Accesos a Internet

  - Server, dedicado a Internet con IP Publica/Fija Servicio DNS proporcionado por Server Privado

  - Cliente, accesos a Internet PPP/PPPoE, con IP de ISP vía DHCP

ELECCIONES Y DECISIONES ¿Por qué?

- Server VPN/Protocolo Túnel VPN

  - Decisión escogida por el sistema operativo del cliente, el que casi por defecto será de la línea de sistemas operativos de Microsoft y por lo tanto será compatible con PPTP/MPPE/MS-CHAP
  - Ahora la implementación del Server VPN, Red Hat Linux 9.0, por el ahorro en costos, seguridad, estabilidad, posibilidad de firewall en la misma maquina, LOG…etc.

- Cifrado de Datos MPPE (40/128 Bits)

  - Decisión escogida por el sistema operativo del cliente, el que casi por defecto será de la línea de sistemas operativos de Microsoft y por lo tanto será compatible con PPTP/MPPE/MS-CHAP

- Autentificación MS-CHAP/MS-CHAPv2

  - Decisión escogida por el sistema operativo del cliente, el que casi por defecto será de la línea de sistemas operativos de Microsoft y por lo tanto será compatible con PPTP/MPPE/MS-CHAP

- Accesos a Internet

  - Se plantea una posible futura necesidad:
    - Acceso VPN tras NAT Routing en el extremo Cliente VPN

REQUERIMIENTOS DE SOFTWARE

- Elección de Versiones para el Server/Cliente VPN

  - Distribución a usar → Red Hat Linux 9.0

  - PPTP → pptp –1.1.3-1.i386.rpm

  - PPP → ppp -2.4.1-3 mppe. I386.rmp

  - KERNEL → Linux -2.5.5.tar.bz2

  -PATH (MPPE) → **Linux-2.5.5-openssl-0.9.6b-mppe.patch**

  - CLIENTE VPN → Windows ’98 // windows XP

REQUERIMIENTOS DE HARDWARE

- SERVER VPN

  - Plataforma Intel P4, 512 MRAM, 30 GHDD, NIC’s 3 COM // D-Link

- CLIENTE VPN

  - cualquier computador que se conecte a Internet Vía PPP/PPPoE. Se probó la implementación con portátil Sony VAIO (P4, 512 MRAM, 30 GHDD), Windows 98/ Windows XP (Profesional).

Procedimiento de Instalación del Server VPN (Paso a Paso)

Primero:
Instalar en el Server VPN, **Red Hat Linux 9.0**, se propone Instalación personalizada, con la idea de asegurar la instalación de los componentes de Firewall (Iptable) e Interfaz Grafica por si el usuario lo necesite, cliente FTP y configuradores de Networking para conexión a Internet y descarga de los Software necesarios para la implementación.

Nota:
Desde este momento y en adelante se proponen modos de instalación y formas de prueba según implementación de VPN efectuada. Se argumentarán las decisiones tomadas de versiones y afines, pero la variabilidad de versiones hace que la implementación de Server VPN sea muy dinámica tanto en procedimientos de instalación como requerimientos Software

Segundo: Parche, Compilación e Instalación de Kernel
Sobre la Instalación de Red Hat Linux 9.0 efectuada en el punto anterior, descomprimir las fuentes del Kernel, se recomienda trabajar en: "/usr/src"

#tar –jxvf linux-2.5.5.tar.bz2
#gunzip linux-2.5.5-openssl-0.9.6b-mppe.patch

Crear y asociar Links (por posibles problemas de apuntamiento a la hora del PATCH)
#ln –s –d linux-2.5.5 linux-2.4
#ln –s –d linux-2.4 linux

Segundo: Compilación e Instalación de Kernel

Aplicación del PATCH a las Fuentes del Kernel 2.5.5
#patch –p1 < linux-2.5.5-openssl-0.9.6b-mppe.patch

Recompilación del Kernel Linux-2.5.5, trabaja en "/usr/src/linux-2.5.5"

Respaldo de Makefile
#cp Makefiel Makefile.org

Editar Makefile (Linea 4)
EXTARVERSION = PoPToP+MPPE

Reconfigurar Kernel para Recompilación, la opción recomendada es "make menuconfig"

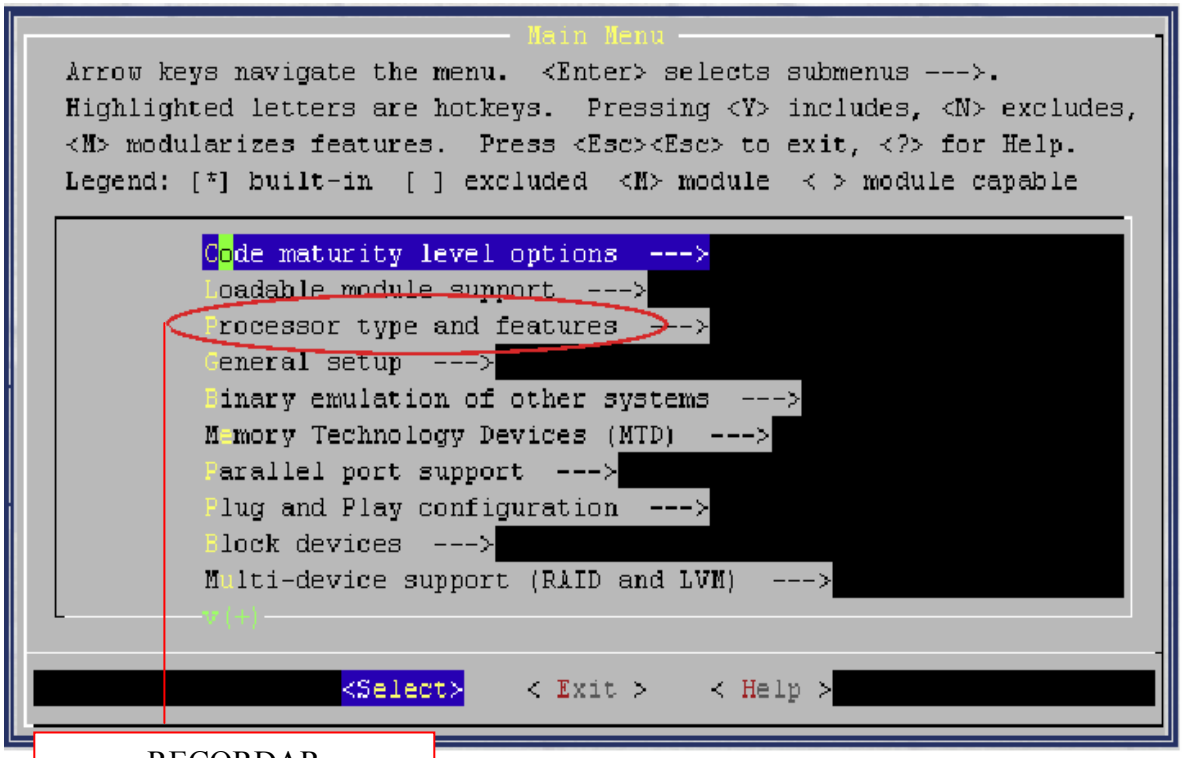
Segundo: Compilación e Instalación de Kernel
#make config
ó
#make menuconfig
ó
#make xconfig

Para la preparación del archivo de configuración de la compilación del Kernel se recomienda tener previamente bien claro el hardware de la maquina en cuestión, y las opciones especiales que no se deben dejar de por lo menos modularizar en el Kernel nuevo.

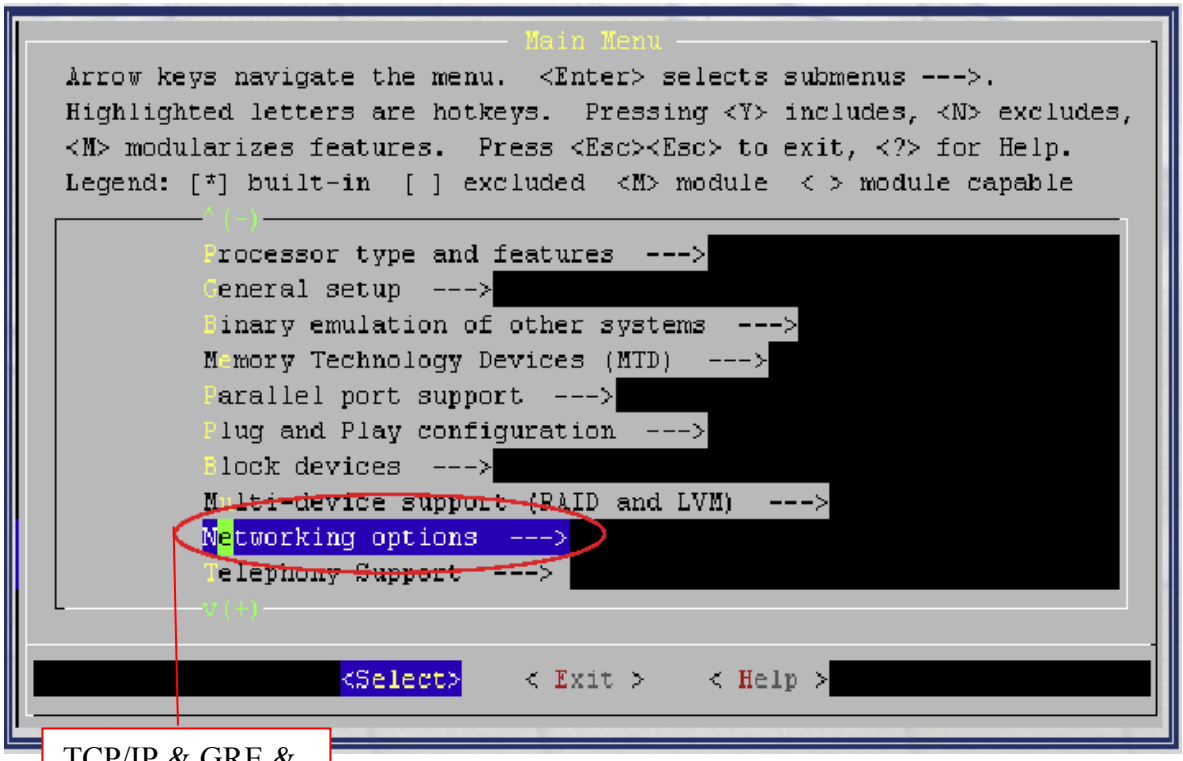
Argumento de uso de Linux-2.5.5
Se uso esta versión del kernel por cuestiones de compatibilidad de hardware (NIC's) y ello depende de los PATCH existentes para el soporte de MPPE:

linux-2.4.16-openssl-0.9.6b-mppe.patch
linux-2.5.5-openssl-0.9.6b-mppe.patch
linux-2.5.10-openssl-0.9.6b-mppe.patch
linux-2.4.19-openssl-0.9.6b-mppe.patch

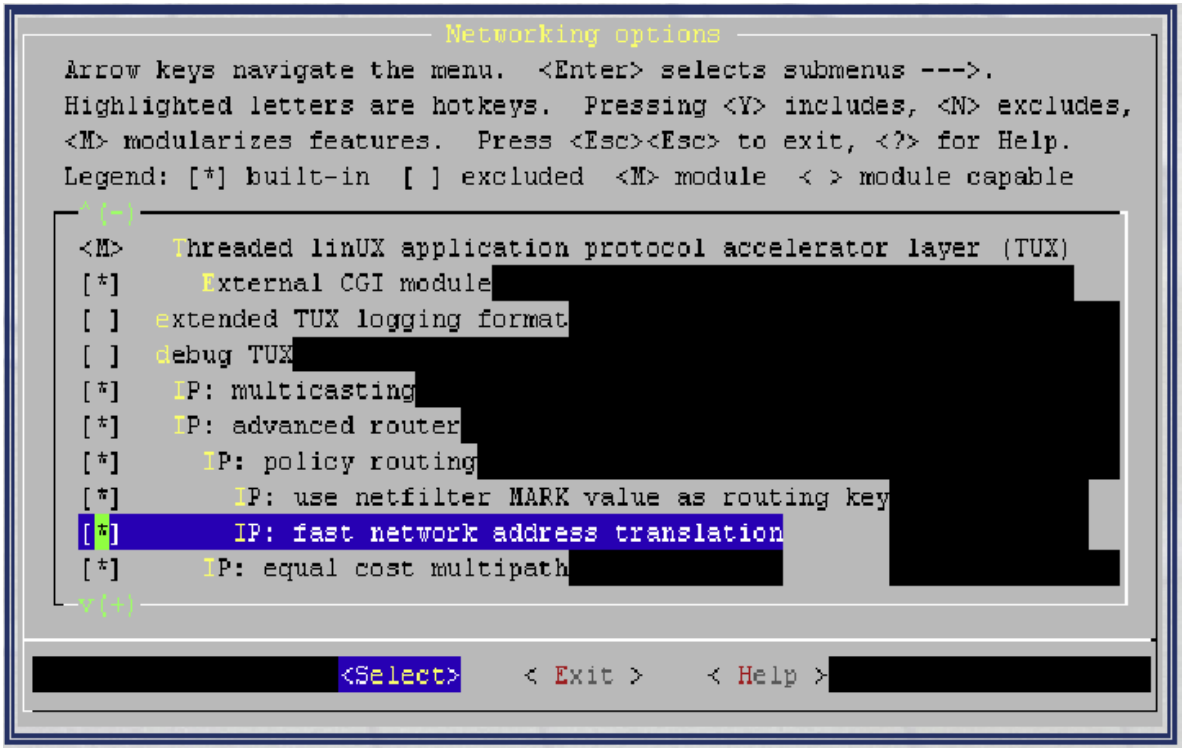
Segundo: Compilación e Instalación de Kernel
Vista rápida a la preparación del archivo de compilación del Kernel

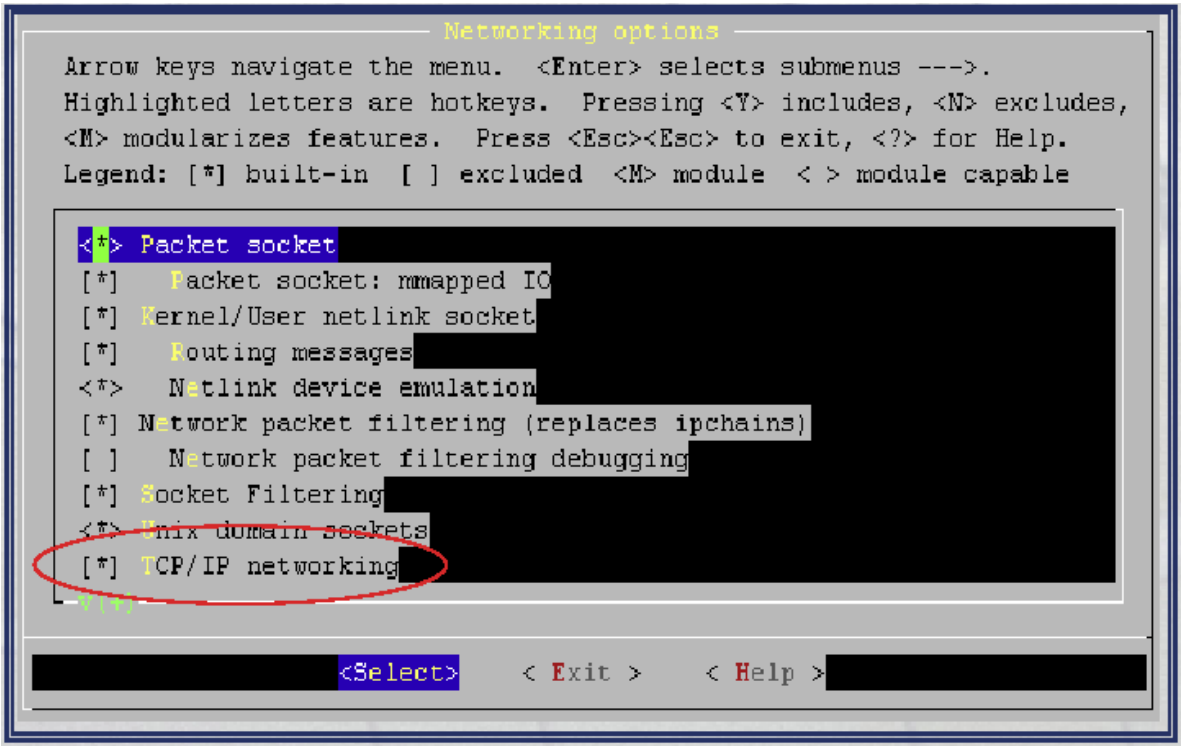


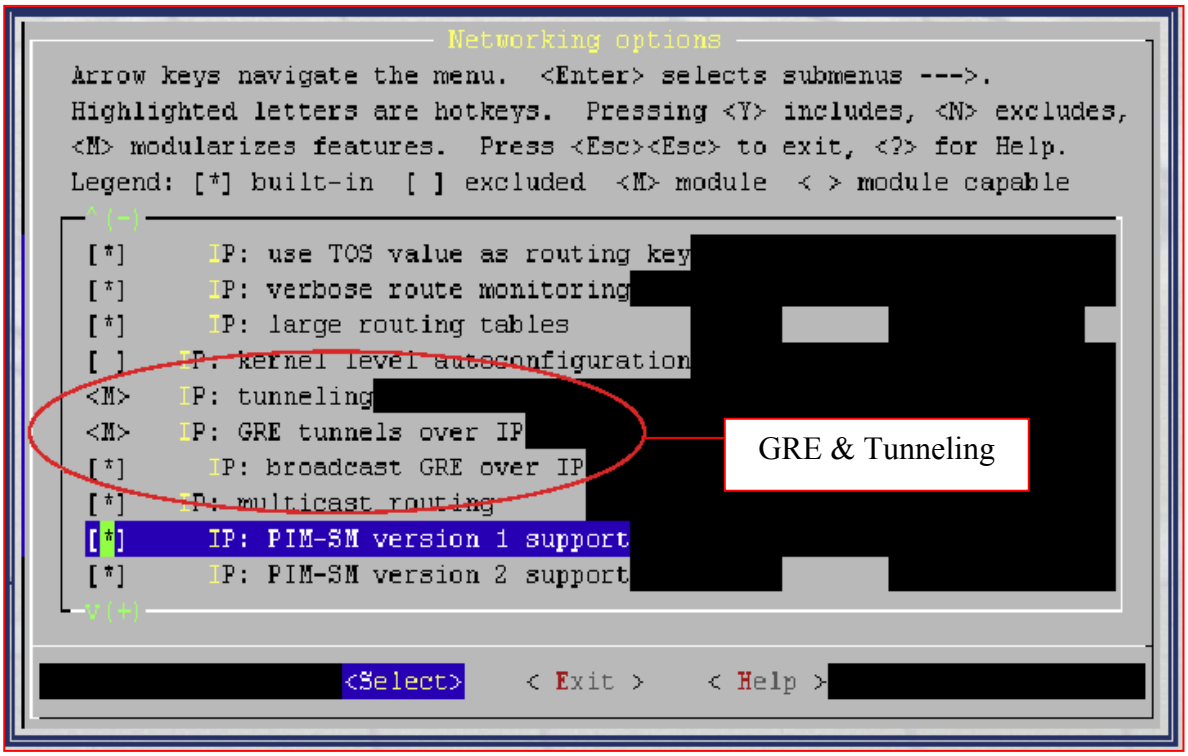
RECORDAR
PROBLEMA PORTATIL

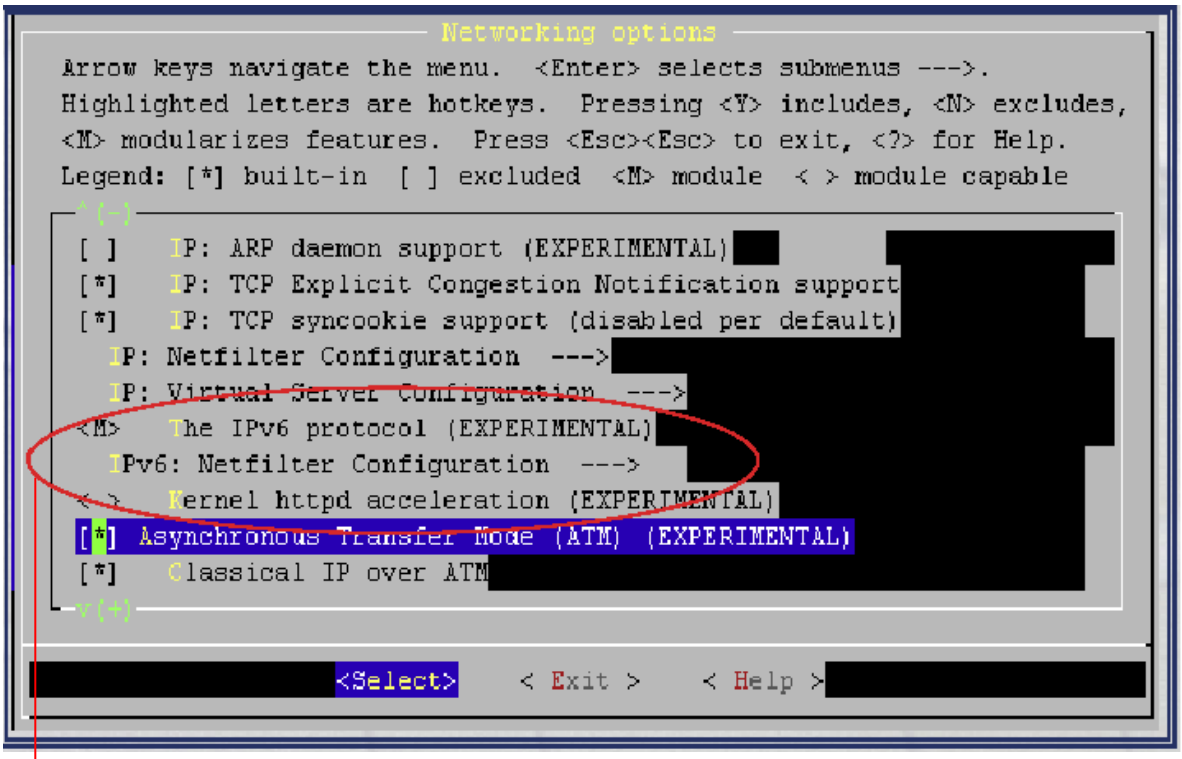


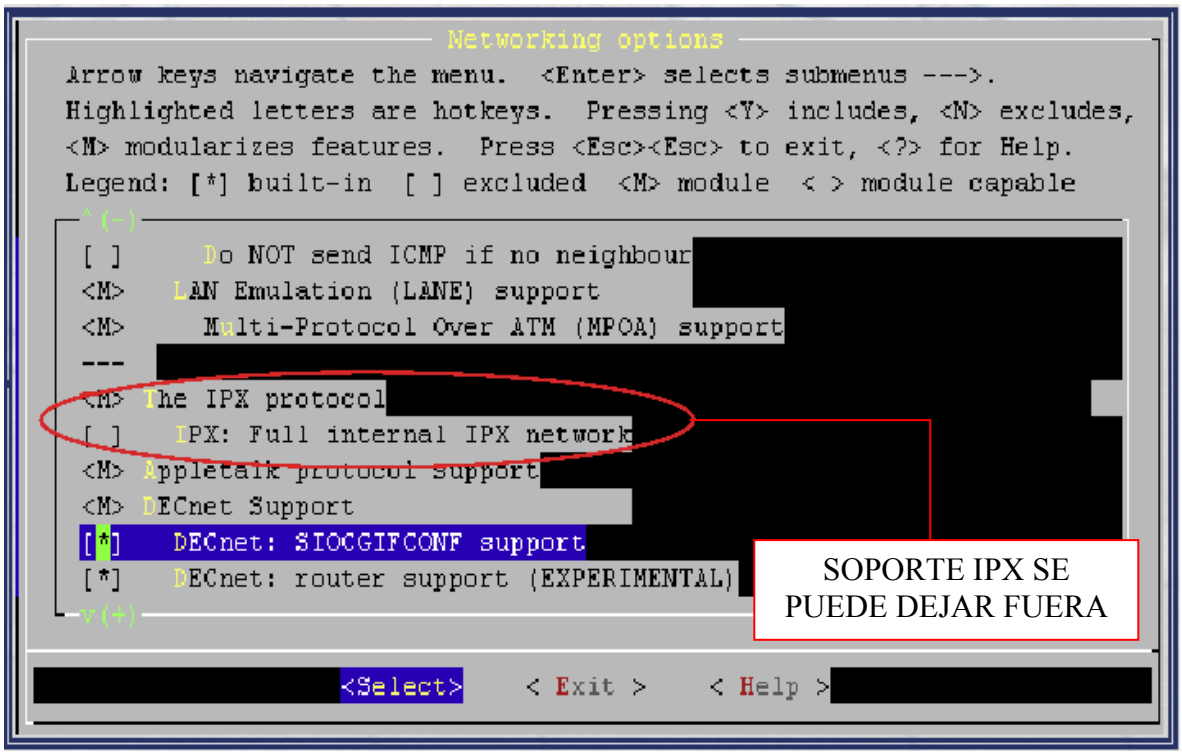
TCP/IP & GRE &
Tunneling


Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
<M> Threaded linUX application protocol accelerator layer (TUX)
[*] External CGI module
[ ] extended TUX logging format
[ ] debug TUX
[*] IP: multicasting
[*] IP: advanced router
[*] IP: policy routing
[*] IP: use netfilter MARK value as routing key
[*] IP: fast network address translation
[*] IP: equal cost multipath
<Select> < Exit > < Help >

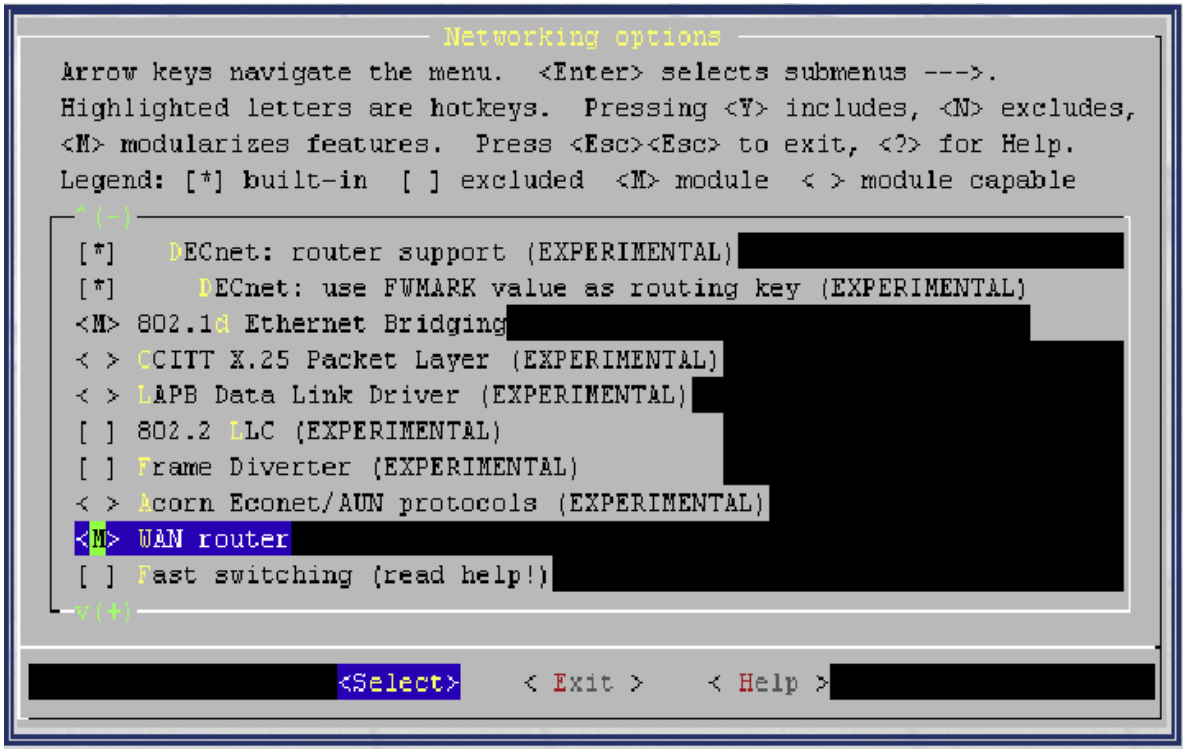

Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
<*> Packet socket
[*] Packet socket: mmapped IO
[*] Kernel/User netlink socket
[*] Routing messages
<*> Netlink device emulation
[*] Network packet filtering (replaces ipchains)
[ ] Network packet filtering debugging
[*] Socket Filtering
<*> Unix domain sockets
[*] TCP/IP networking
<Select> < Exit > < Help >

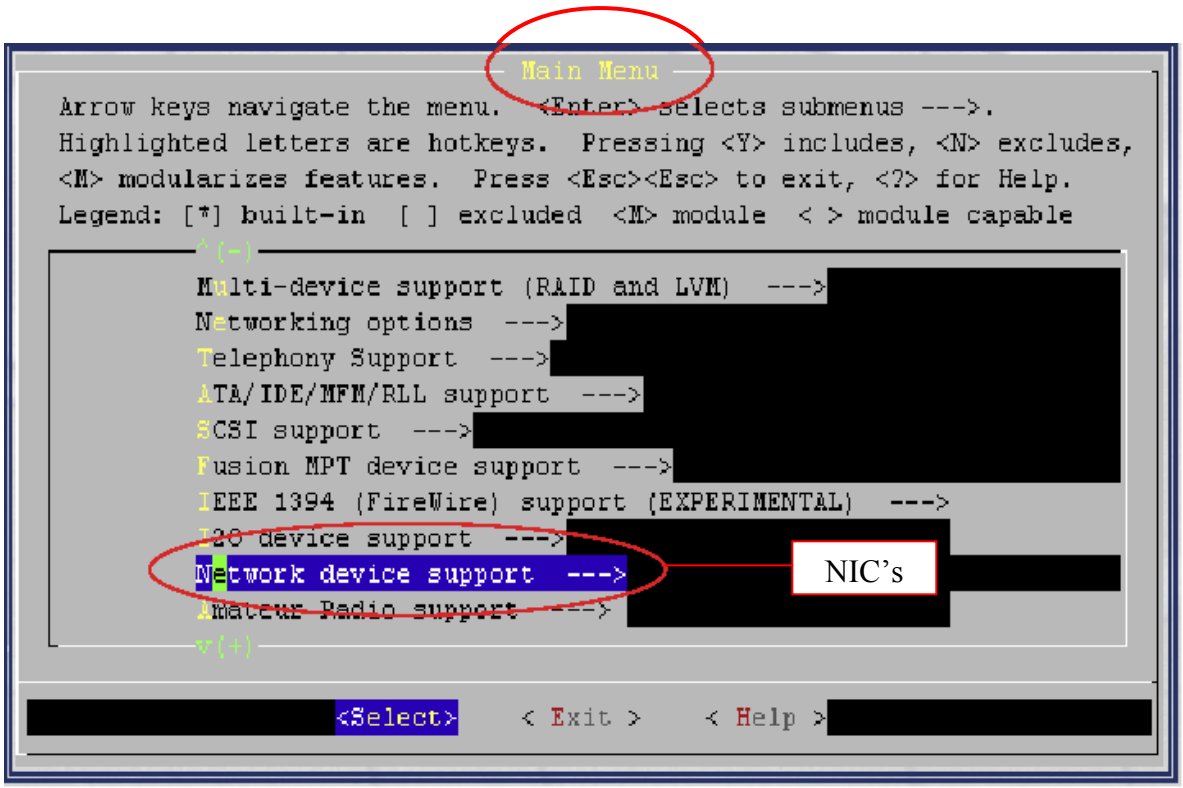

Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
[*] IP: use TOS value as routing key
[*] IP: verbose route monitoring
[*] IP: large routing tables
[ ] IP: kernel level autoconfiguration
<M> IP: tunneling
<M> IP: GRE tunnels over IP
[*] IP: broadcast GRE over IP
[*] IP: multicast routing
[*] IP: PIM-SM version 1 support
[*] IP: PIM-SM version 2 support
<Select>
< Exit >
< Help >
GRE & Tunneling

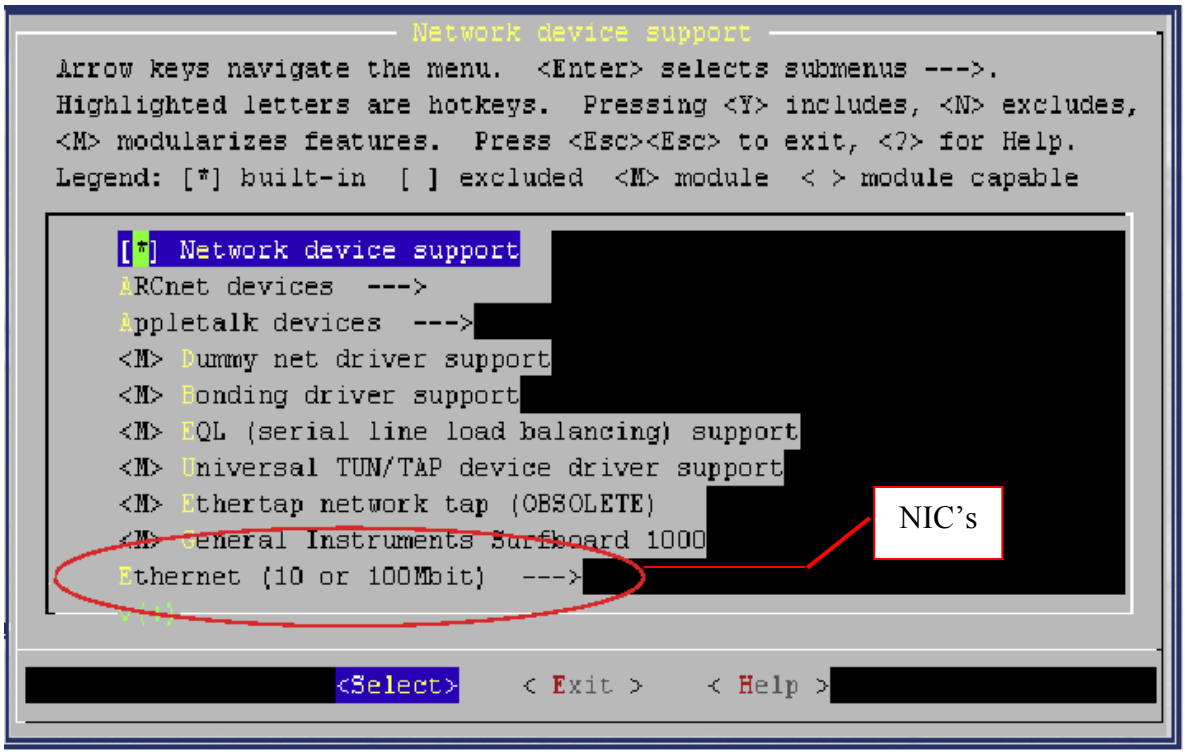

Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
[ ] IP: ARP daemon support (EXPERIMENTAL)
[*] IP: TCP Explicit Congestion Notification support
[*] IP: TCP syncookie support (disabled per default)
IP: Netfilter Configuration --->
IP: Virtual Server Configuration --->
<M> The IPv6 protocol (EXPERIMENTAL)
IPv6: Netfilter Configuration --->
< > Kernel httpd acceleration (EXPERIMENTAL)
[*] Asynchronous Transfer Mode (ATM) (EXPERIMENTAL)
[*] Classical IP over ATM
<Select>
< Exit >
< Help >
SOPORTE IPv6 SE
PUEDE DEJAR FUERA

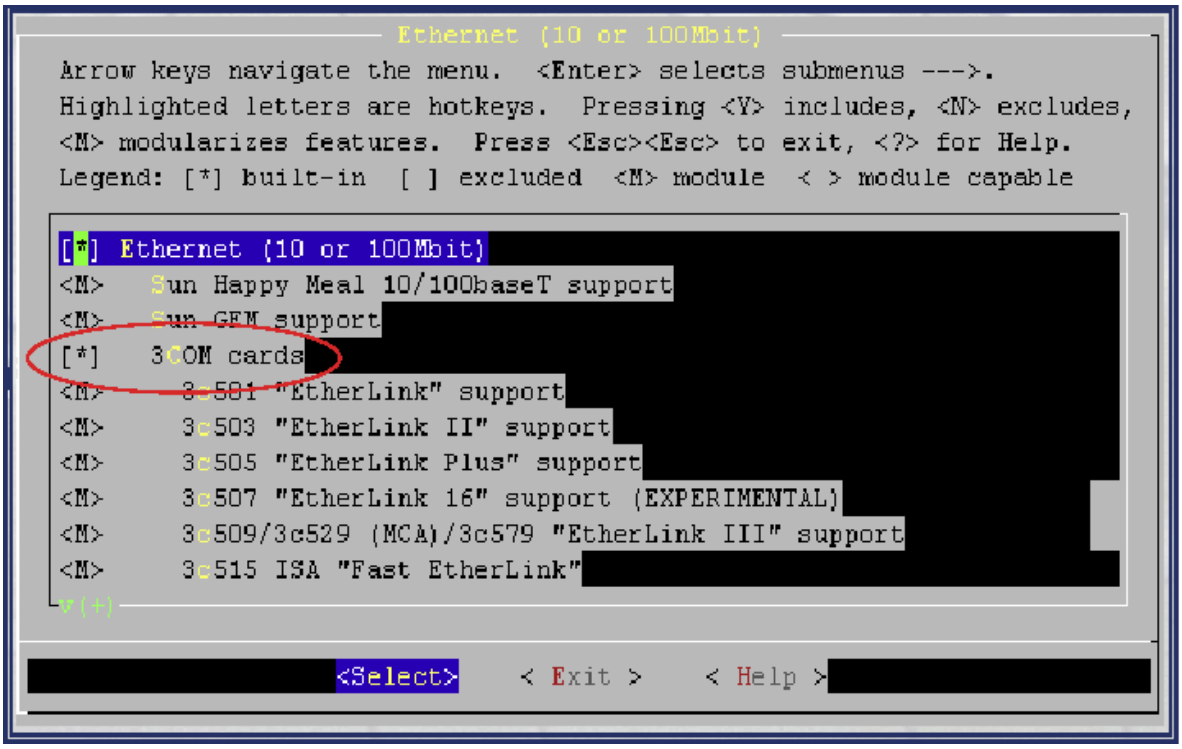

Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
[ ] Do NOT send ICMP if no neighbour
<M> LAN Emulation (LANE) support
<M> Multi-Protocol Over ATM (MPOA) support

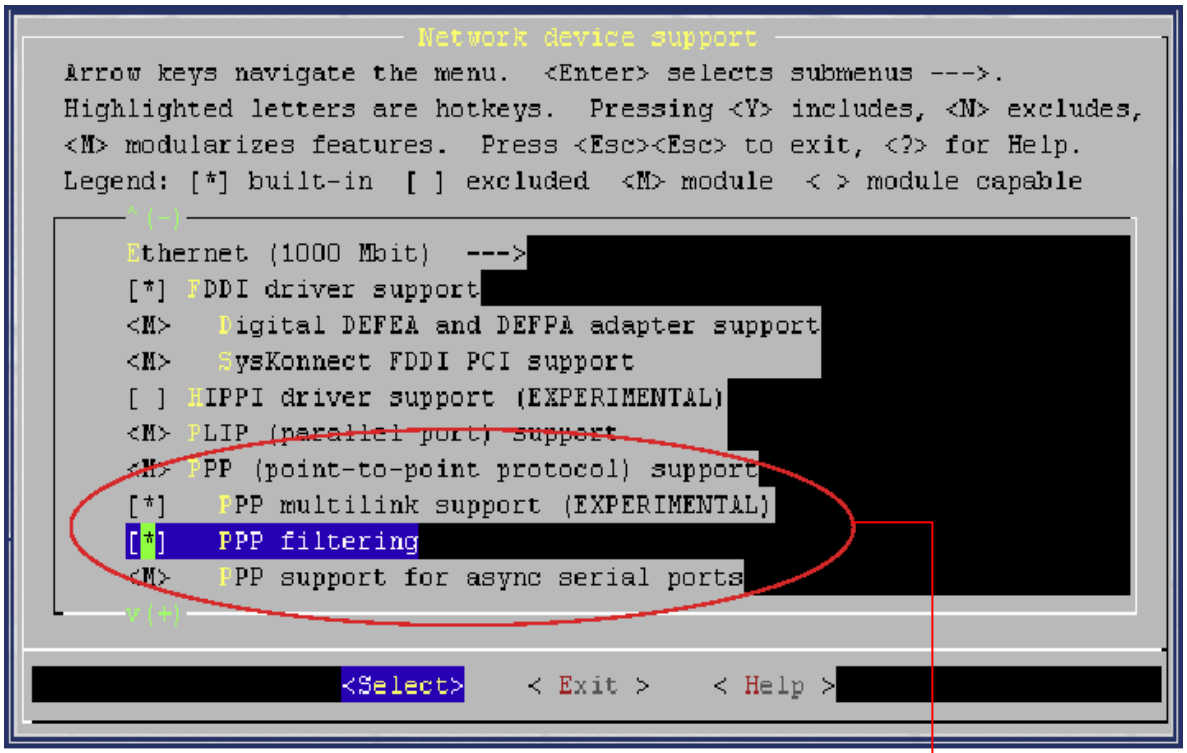
<M> The IPX protocol
[ ] IPX: Full internal IPX network
<M> Appletalk protocol support
<M> DECnet Support
[*] DECnet: SIOCGIFCONF support
[*] DECnet: router support (EXPERIMENTAL)
<Select> < Exit > < Help >
SOPORTE IPX SE
PUEDE DEJAR FUERA


Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
[*] DECnet: router support (EXPERIMENTAL)
[*] DECnet: use FWMARK value as routing key (EXPERIMENTAL)
<M> 802.1d Ethernet Bridging
< > CCITT X.25 Packet Layer (EXPERIMENTAL)
< > LAPB Data Link Driver (EXPERIMENTAL)
[ ] 802.2 LLC (EXPERIMENTAL)
[ ] Frame Diverter (EXPERIMENTAL)
< > Acorn Econet/AUN protocols (EXPERIMENTAL)
<M> WAN router
[ ] Fast switching (read help!)
<Select> < Exit > < Help >

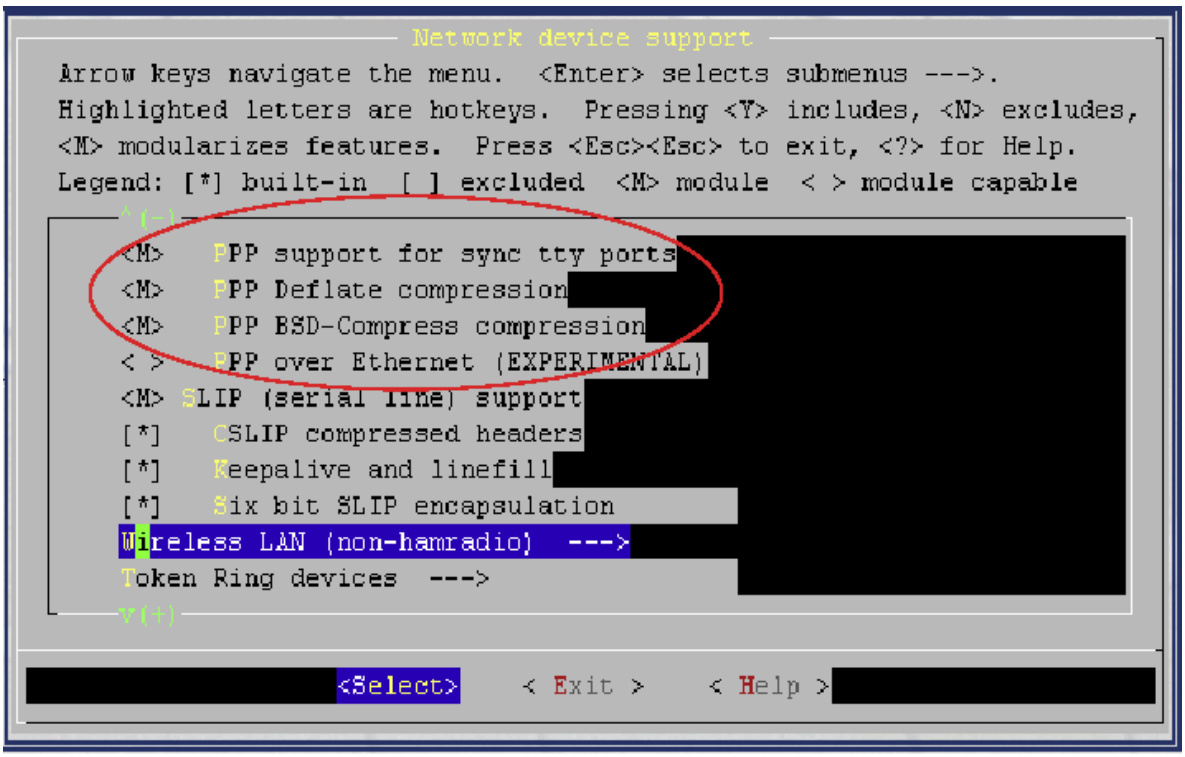

Main Menu
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
Multi-device support (RAID and LVM) --->
Networking options --->
Telephony Support --->
ATA/IDE/MFM/RLL support --->
SCSI support --->
Fusion MPT device support --->
IEEE 1394 (FireWire) support (EXPERIMENTAL) --->
I2O device support --->
Network device support --->
Amateur Radio support --->
<Select> < Exit > < Help >
NIC's


Network device support
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help.
Legend: [*] built-in [ ] excluded <M> module < > module capable
[*] Network device support
ARCnet devices --->
Appletalk devices --->
<M> Dummy net driver support
<M> Bonding driver support
<M> EQL (serial line load balancing) support
<M> Universal TUN/TAP device driver support
<M> Ethertap network tap (OBSOLETE)
<M> General Instruments Surfboard 1000
Ethernet (10 or 100Mbit) --->
<Select> < Exit > < Help >
NIC's

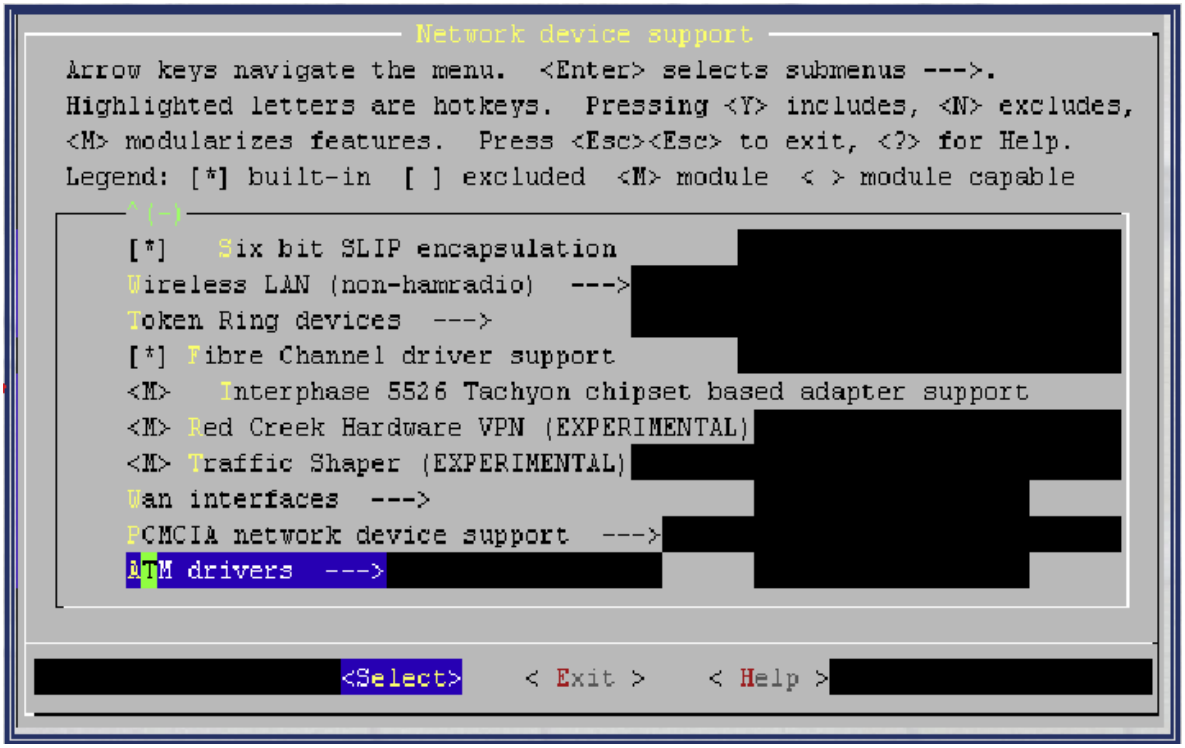




PPP & PPP ASYNC &
PPP SYNCTTY



Recordar el resto de las cosas



Creación del Makefile respectivo, el que ya modificamos y creara a la hora de la compilación todos los archivos y el mismo Kernel con extensiones de nombre "PoPToP+MMPE"

#make dep (1 min)
#make clean (3 seg)
#make bzImage (10 a 30 min)
#make modules (3 min)
#make modules_install (3 min)
Resultando "arch/i386/boot/"
bzImage
System.map

Segundo: Instalación de Kernel
En "arch/i386/boot"
cp bzImage /boot/vmlinuz-2.5.5-PoPToP+MPPE
cp System.map /boot/System.map-2.5.5-PoPToP+MPPE
#mkinitrd/boot/initrd-2.5.5PoPToP+MPPE.img 2.5.5.PoPToP+MPPE
A continuación configurar Grub Linux Loader !!!

Segundo: Instalación de Kernel
Algo como esto debe ser el grub.conf en la maquina
grub.conf generated by anaconda
#
Note that you do not have to rerun grub after making changes to this file
NOTICE: You have a /boot partition. This means that
all kernel and initrd paths are relative to /boot/, eg.
root (hd0,0)
kernel /vmlinuz-version ro root=/dev/hda2

```
#         initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz

title Red Hat Linux 9.0 (2.4.18-14)
        root (hd0,1)
        kernel /vmlinuz-2.4.18-14 ro root=/
        initrd /initrd-2.4.18-14.img

title Red Hat Linux 9.0 (2.5.5-poptop+mpp)
root (hd0,1)
kernel /vmlinuz-2.5.5-poptop+mppe ro root=/dev/hda3
LABEL=/initrd /initrd-25.5-poptop+mppe.img
```

Segundo: Instalación de Kernel
Para probar el correcto funcionamiento:
shutdown –r now
Y al bootear elegir el Kernel nuevo

Tercero: Instalación de PPP Nuevo (Upgrade)
Con atributos de root en la maquina:
#rpm –qa ppp (Para enterarnos de la versión de PPP instalada)
#ppp-2.4.1-7 (O algo por el estilo)
#rpm –e --nodeps ppp
#rpm –Uvh ppp-2.4.1-3mppe.i386.rpm
Nota: En Red Hat Linux 9.0 no debe ser más que esto

Cuarto: Instalación de PoPToP (PPTPD)
Con atributos de root en la maquina:
#rpm –Uvh pptpd-1.1.3-1.i386
Nota: En Red Hat Linux 9.0 no debe ser más que esto

Quinto: Configuración de PoPToP (PPTPD)
Con atributos de root en la maquina, revisar
"/etc/modules.conf"
Debe ser al menos algo como esto:

alias char-major-108 ppp_generic
alias tty-ldisc-3 ppp_async
alias tty-ldisc-14 ppp_synctty
alias ppp-compress-18 ppp_mppe
alias ppp-compress-21 bsd_comp
alias ppp-compress-24 ppp_defalte
alias ppp-compress-26 ppp_defalte

Quinto: Configuración de PoPToP (PPTPD)
Archivos de configuración de PPTPD:
/etc/ppp/chap-secrets
/etc/ppp/options.pptp (options.pptpd)
/etc/pptpd.conf

A continuación una mirada a estos archivos de Configuración...

Quinto: Configuración de PoPToP (PPTPD)
/etc/ppp/chap-secrets

Client	Server	Secret	IP addresses
Jperez	*	**Jperez-passwd**	*
NTDOMINIO\\jgonsalez	*	**Jgonsalez-passwd**	*

NOTA: Como enterarse de la configuración de la columna "Client", mas adelante en el debug del Servidor

Quinto: Configuración de PoPToP (PPTPD)
/etc/options.pptp

CHANGE TO SUIT YOUR SYSTEM
lock
turn pppd syslog debugging on
debug
change 'pptpd' to whatever you specify as your server name in chap-secrets

#name pptpd
proxyarp
This option applies if you use ppp with chapms-strip-domain patch
#chapms-strip-domain
+chap
These options apply if you use ppp with mppe patch
NB! You should also apply the ChapMS-V2 patch
-chap
+chapms
+chapms-v2
mppe-40
mppe-128
mppe-stateless
These options will tell ppp to pass on these to your clients
To use ms-dns or ms-dns in options.pptpd it must exist in /etc/resolv.conf
#ms-wins your.server.here
#ms-dns your.server.here

Quinto: Configuración de PoPToP (PPTPD)
/etc/pptpd.conf

```
##################################################
##
# Sample PoPToP configuration file # # for PoPToP version 1.1.3
#
##################################################
##
# TAG: speed
# Specifies the speed for the PPP daemon to talk at
#speed 115200
# TAG: option
# Specifies the location of the PPP options file.
# By default PPP looks in '/etc/ppp/options‘
option /etc/ppp/options.pptp
# TAG: debug
# Turns on (more) debugging to syslog#
```

```
#debug
# TAG: localip
# TAG: remoteip
## Specifies the local and remote IP address ranges.
## You can specify single IP addresses separated by commas or
you can
# specify ranges, or both. For example:
## 192.168.0.234,192.168.0.245-249,192.168.0.254
## IMPORTANT RESTRICTIONS:
## 1. No spaces are permitted between commas or within
addresses.
## 2. If you give more IP addresses than MAX_CONNECTIONS,
it will
# start at the beginning of the list and go until it gets
# MAX_CONNECTIONS IPs. Others will be ignored.
## 3. No shortcuts in ranges! ie. 234-8 does not mean 234 to
238,
# you must type 234-238 if you mean this.
## 4. If you give a single localIP, that's ok - all local IPs will
# be set to the given one. You MUST still give at least one
remote
# IP for each simultaneous client.
#
localip 192.168.0.234-238,192.168.0.245
remoteip 192.168.1.234-238,192.168.1.245
```

Sexto: Arranque de PoPToP (PPTPD), debug del Servidor VPN

```
# /etc/init.d/pptpd restart
```

Ó

```
# service pptpd restart
```

Si presenta problema con módulos:

- ppp_async
- ppp_generic
- ppp_mppe
- slhc

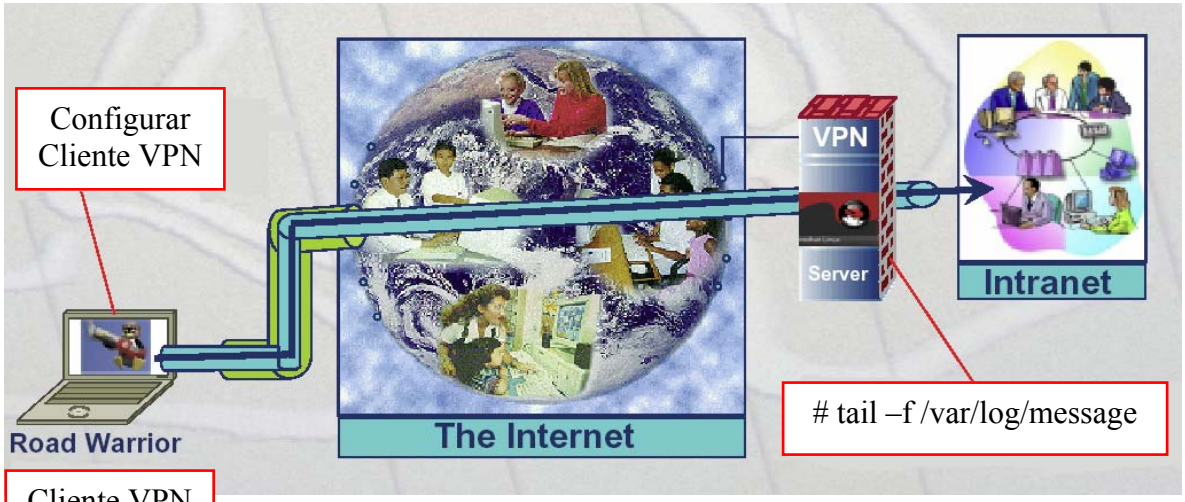
cargar:

```
modprobe ppp_async
modprobe ppp_generic
modprobe ppp_mppe
modprobe slhc
```

Además poner en el /etc/rc.local (para el próximo boot)

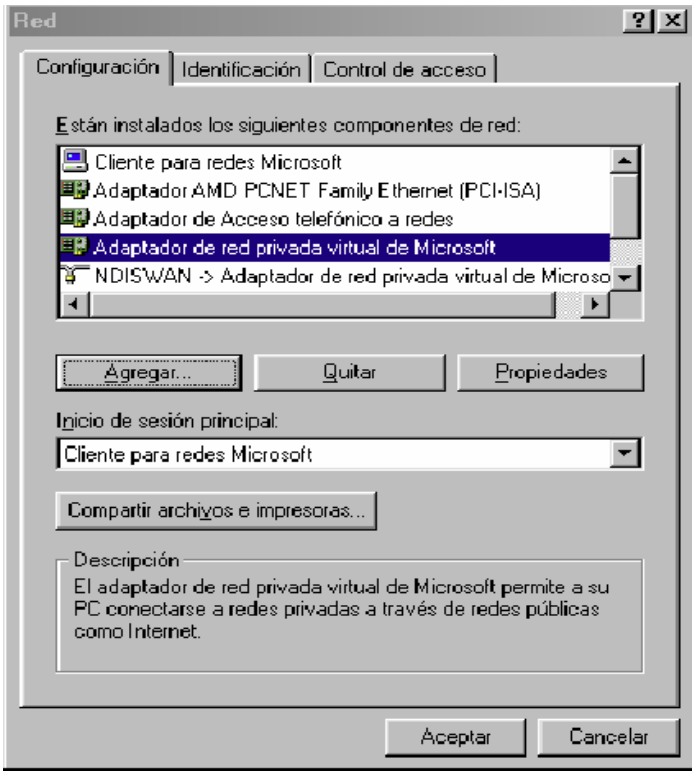
Además sería conveniente en este momento arrancar el reenvio de paquetes IPv4
#echo 1 > /proc/sys/net/ipv4/ip_forward

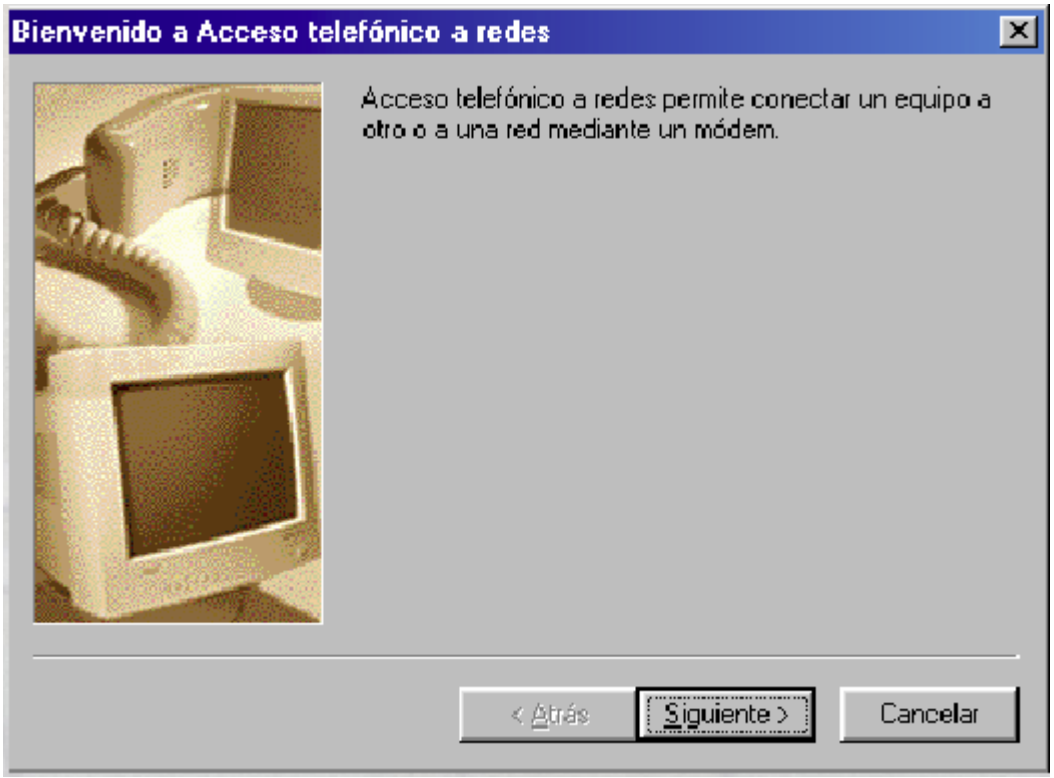
Sexto: Debug del Servidor VPN
Recordar el Escenario:



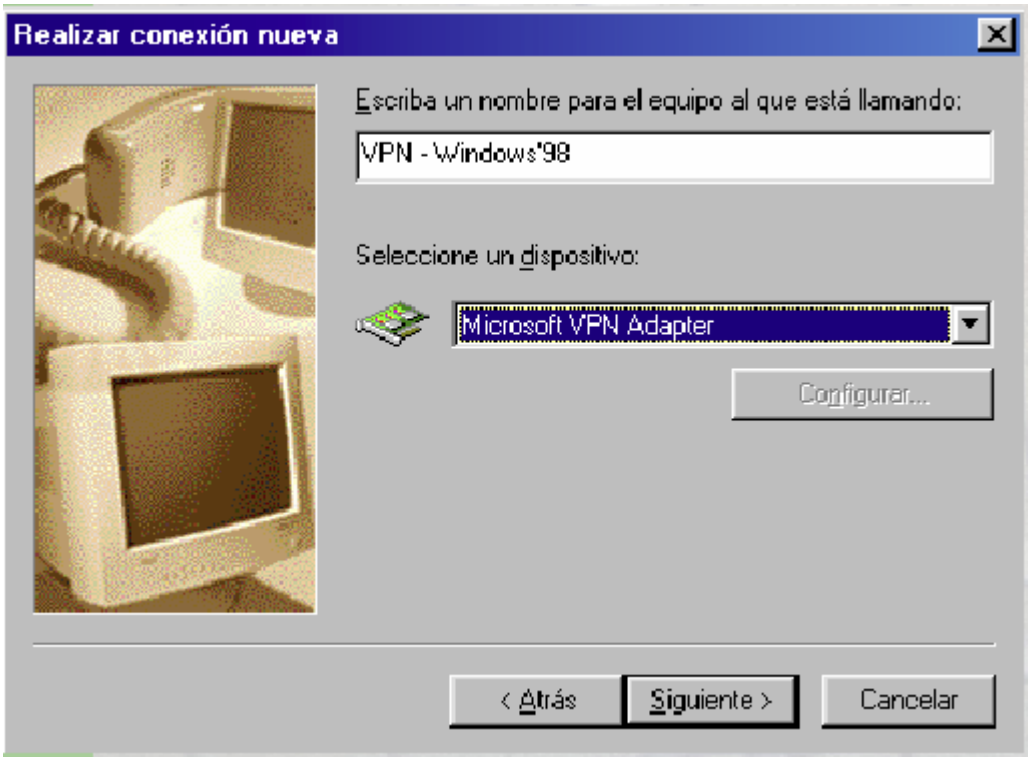
Sexto: Debug del Servidor VPN

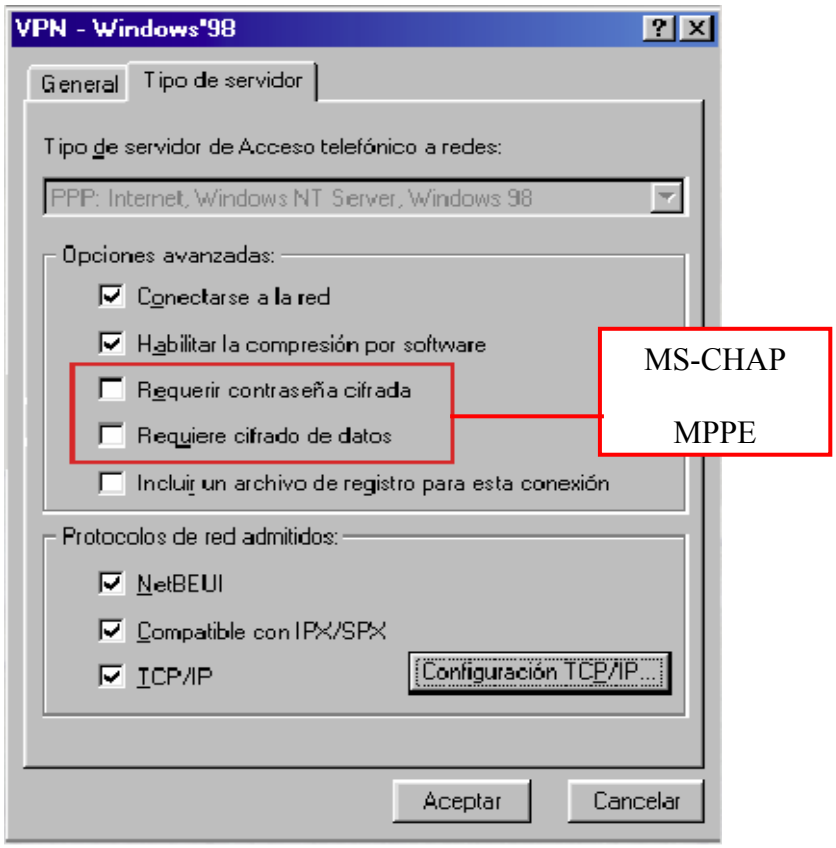
Configuración del Cliente para Windows 98:

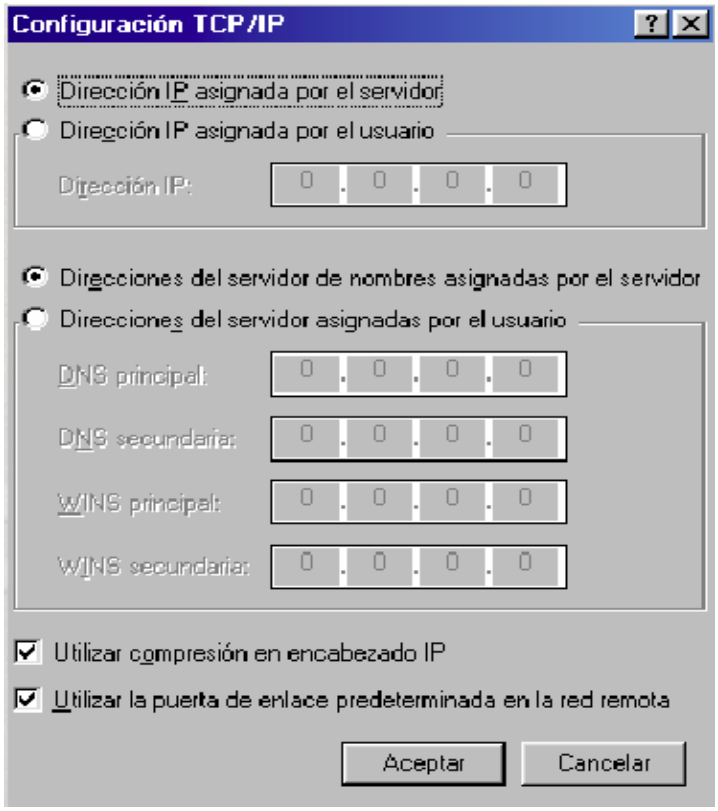





Realizar conexión nueva
Escriba el nombre o la dirección del servidor VPN:
Nombre del host o dirección IP:
vpn.ejemplo.cl
< Atrás
Siguiente >
Cancelar


Realizar conexión nueva
Escriba un nombre para el equipo al que está llamando:
VPN - Windows'98
Seleccione un dispositivo:
Microsoft VPN Adapter
Configurar...
< Atrás
Siguiente >
Cancelar


VPN - Windows'98
General
Tipo de servidor
Tipo de servidor de Acceso telefónico a redes:
PPP: Internet, Windows NT Server, Windows 98
Opciones avanzadas:
Conectarse a la red
Habilitar la compresión por software
Requerir contraseña cifrada
Requiere cifrado de datos
Incluir un archivo de registro para esta conexión
MS-CHAP
MPPE
Protocolos de red admitidos:
NetBEUI
Compatible con IPX/SPX
TCP/IP
Configuración TCP/IP...
Aceptar
Cancelar


Configuración TCP/IP
Dirección IP asignada por el servidor
Dirección IP asignada por el usuario
Dirección IP:
0 . 0 . 0 . 0
Direcciones del servidor de nombres asignadas por el servidor
Direcciones del servidor asignadas por el usuario
DNS principal:
DNS secundaria:
WINS principal:
WINS secundaria:
Utilizar compresión en encabezado IP
Utilizar la puerta de enlace predeterminada en la red remota
Aceptar
Cancelar

NOTAS

- Establecer conexión con tail –f al /var/log/message, como en /etc/ppp/options.pptp esta activa la acción “debug”, el pptpd enviará al archivo de log todos los eventos, así podemos ver las conexiones y en caso de problemas revisar la causa y resolver.

- Una vez el cliente Win98 está configurado, probar con un cliente WinXP, para asegurar el correcto funcionamiento de MPPE-128 y MSCHAPv2.

- Probar con más de un cliente a la vez, y con comando “top” verificar la carga de la maquina.

- Finalmente deshabilitar “debug” en options.pptp

5. CONCLUSION

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y Prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias.

Los innegables beneficios en infraestructura y costos que ofrece la implantación de Redes Privadas Virtuales como soporte de las comunicaciones corporativas necesitan de una fuerte garantía de seguridad que haga factible su empleo, máxime cuando el medio sobre el que se montan es totalmente abierto y, para determinados propósitos incluso hostil. El factor crítico en la operación de las VPN no está en el túnel de conexión, sino en los mecanismos de seguridad que preservan la intimidad e integridad de la comunicación.

VENTAJAS:

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere

totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un computador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el computador cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.

Aparte de esta se encuentran dos importantes ventajas:

Bajo Costo:
Una forma de reducir costo en las VPN es eliminando la necesidad de largas líneas de costo elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio.

Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada metropolitana.

Además la implementación de VPN con un sistema operativo con licencia libre como LINUX permite aun mas bajar el presupuesto.

Escalabilidad:
La implementación y configuración de la VPN es sencilla y rápida, permitiendo un crecimiento escalable en cantidad de puntos. De esta manera se evita el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet, se deriva simplemente en accesos distribuidos geográficamente.

INCONVENIENTES:

Mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor relentización de la mayoría de conexiones.

Mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones a lo largo del desarrollo.

Las redes VPN dependen de un área externa a la organización, en concreto de Internet, y por lo que depende de factores externos al control de la organización.

Las diferentes tecnologías de VPN podrían no trabajar bien juntas.

Las redes VPN necesitan diferentes protocolos que los de IP.

APLICACIONES:

Entre las aplicaciones más frecuentes de las VPN podemos encontrar:

- **Teletrabajo**: Es la solución ideal, por su efectividad y sus bajos costos, para aquellas organizaciones que necesiten que sus empleados accedan a la red corporativa, independientemente de su ubicación geográfica.

- **VPN Empresa**: Solución de conectividad entre sucursales de la empresa o entre la empresa y sus socios, proveedores, etc. Gracias a su flexibilidad se adapta al tamaño y necesidades de la organización.

RECOMENDACIÓNES

La razón de este documento, es la de ser una guía para las empresas y para el estudiantado en general, interesado en conocer las formas de implementar una VPN de bajo costo y con las características necesarias, para ser una solución segura y eficaz.

Se abordan dos protocolos, cada uno con características que los hacen atractivos en diferentes ambientes de trabajo, sin que esto signifique que otras soluciones no puedan implementarse.

La intención final de este documento es ser un punto de partida, para futuras investigaciones en la implementación de VPNs, por lo cual se insta al estudiantado a que se realicen mejoras en las áreas críticas de seguridad, como la selección del algoritmo de encriptación y actualizar las implementaciones de autenticación, basadas en las políticas que fabricantes como Microsoft desarrollan para sus productos.

Todo esto permitirá que se desarrollen nuevas estrategias para la selección de soluciones de conectividad, permitiendo que las empresas vean con nuevos ojos las características del software Open Source.

ANEXOS

COMPARACIÓN DE LAS VPN CON LAS TECNOLOGÍAS CONVENCIONALES

Otra forma de aproximarse a las VPN es comparándolas directamente con otras tecnologías. En las secciones siguientes compararemos las VPN con RAS y con las líneas alquiladas.

LAS VPN FRENTE A RAS

Actualmente, muchas empresas están intentando ser flexibles en lo que se refieren a los organigramas de personal. Poder trabajar desde casa es una opción muy atractiva para mucha gente, especialmente si son padres solos o viven a gran distancia de la oficina. Además, muchas empresas necesitan una fuerza de trabajo móvil. El personal de ventas y los ingenieros de mantenimiento necesitan viajar para realizar su actividad.

Tradicionalmente, sólo hay dos opciones posibles: abrir los recursos de la Intranet al mundo exterior o mantener un grupo de módems a través de los cuales puedan conectarse los usuarios. Ambas soluciones tiene desventajas importantes.

Proporcionar recursos por Internet significa que dichos recursos están disponibles para todas las personas que están en Internet, no sólo para los usuarios a los que están dirigidos. Esto puede significar riesgos de seguridad serios. Si los recursos están comprometidos, podríamos vernos afectados por la revelación no autorizada de secretos comerciales, de información registrada y de la propiedad industrial. No sólo eso, si hay relaciones de confianza entre servidores, un servidor comprometido puede infectar a los demás. Desde un perspectiva empresarial, esto se traduce en pérdidas financieras exponenciales.

Si al contrario optamos por mantener un grupo de módems, nuestros costes se pueden disparar rápidamente. Los servidores PPP, los módems, las placas multipuerto, las líneas telefónicas, las llamadas a larga distancia y los costes de administración aumentarán. Además, podríamos ser víctimas de una guerra de marcación telefónica, un método que todavía está en práctica que podría comprometer nuestra red interna. Nuevamente esto podría constituir pérdidas financieras para nuestra empresa.

LAS VPN FRENTE A LAS LINEAS DEDICADAS

Cuando conectamos redes geográficamente distantes, lo normal es utilizar líneas dedicadas. Aunque el nombre puede llevar a cierta confusión, las líneas dedicadas pueden ser cualquier cosa, desde las tradicionales T (T1, T3 o análogas europeas, E), líneas OC (OC3, OC12, OC48, OC192) o enlaces inalámbricos (microondas, RF o satélite). Las líneas están “dedicadas” porque el ancho de banda que proporcionan es de su propietario.

Las líneas dedicadas son buenas para algunas aplicaciones. Si tenemos una base de datos esencial para el funcionamiento del negocio que necesita mucho rendimiento, una línea dedicada podría ser una buena elección porque ofrece un ancho de banda garantizado. Además podemos negociar líneas dedicadas según el rendimiento que necesitemos. Si estuviéramos en Nueva

York, probablemente no nos daríamos cuenta de que el servidor de bases de datos está en San Francisco, si utilizamos una OC-3.

Otra ventaja de la líneas dedicadas es que siempre están (o deberían estar) disponibles. Como controlamos el equipo que mantiene la conexión, tenemos un control razonable sobre ella. Esto no siempre es así, porque estas líneas normalmente pasan por una nube WAN; sin embargo, la nube WAN está muy controlada y normalmente tiene enlaces redundantes con capacidad de recuperación automática ante fallos. La probabilidad de que experimentemos una caída como resultado de un fallo de una nube WAN es relativamente baja. Si nuestra base de datos se replica regularmente, necesitará consultas constantes o actualizaciones cada 24 horas, por lo que probablemente deberíamos optar por una línea dedicada.

Aunque una línea dedicada tiene ventajas en determinadas situaciones, puede ser muy costosa. Dependiendo de donde estemos, una simple T1 puede constar más de 5000 dólares por la instalación, 2500 dólares al mes por el servicio y 5000 por el CPE (Customer Premise Equipment, equipo terminal del cliente). Sólo el primer año, podría llegar a 40000 dólares, y esto sin contar los costes de personal, de equipo, etc. A todo esto hay que añadir el coste de la conexión a Internet. Recordemos que este cálculo sólo tiene en cuenta la conectividad entre dos redes. Más redes equivalen a más costes.

Confiamos en los ISP y en las empresas de telecomunicaciones en lo que respecta a nuestra conexión a Internet, pero no deberíamos hacerlo. Ellos tienen un acceso completo a los datos que atraviesan sus líneas. ¿Qué evita que uno de sus empelados haga sniffing de los datos? Muchos proveedores de servicios tienen sniffers en sus redes a efectos de solucionar problemas, pero ¿operan los sniffers éticamente, teniendo la confidencialidad de los clientes como una de sus prioridades principales? Si necesitamos confianza absoluta en las

comunicaciones entre dos puntos, nuestro proveedor de servicios no es una buena solución.

Con la utilización de una solución VPN, podemos reducir el coste del primer año de unos 5000 dólares, y limitándonos sólo a los costes administrativos en los años subsiguientes. Además con una VPN no tendremos que invertir en otras líneas dedicadas en caso de futuras migraciones o esfuerzos de expansión.

BIBLIOGRAFIA

ANONIMO. LINUX Máxima Seguridad. Madrid. Prentice Hall, 2000.

Kolesnikov, Olef & Hatch, Brian. Redes Privadas Virtuales con Linux". Prentice Hall. Primera Edición 2002.

Douglas E. Comer. "Internetworking with TCP/IP Principes, protocols & architectures". Volumen 1 Prentice Hall, 1995

Brown, Steven. Implantación de Redes Privadas Virtuales. McGraw-Hill, 2003

Maxwell, Steve. Red Hat Linux – Herramientas Para La Administración de Redes. McGraw-Hill, 2003

Seven. Red Hat Linux – Guía Del Usuario. Anaya Multimedia, 2003

Para la realización de este proyecto se han consultado las siguientes páginas de Internet, con el fin de obtener la suficiente información:

- http://www.linux.com, http://www.linux.org
- http://www.gulp.org.mx/articulos/vpn.html
- http://www.xtech.com.ar/html/NuevasSoluciones.htm
- http://www.pcworld.com/
- http://adslnet.ws/vpn.htm
- http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml
- http://www.sans.org/infosecFAQ/encryption/understanding_VPN.htm
- http://www.europe.redhat.com/documentation/rhl9/rhl-sg-en-9/index.php3
- http://www.uv.es/ciuv/cas/vpn/vpnw98.html
- http://www.uv.es/ciuv/cas/vpn/vpnw2000.html
- http://www.uv.es/ciuv/cas/vpn/vpnwxp.html
- http://www.latinsud.com/vpn/#intro
- http://www.redlibre.net/pipermail/linuxap/2003-January/000190.html
- http://www.cyclades.com.pe/Documentacion/Articulos/SiteToSite_VPN.htm