ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ESTUDIO DE LA TECNOLOGÍA MPLS, PARA PROPONER GUÍA DE MEJORAS EN SEGURIDAD PARA SERVICIO DE VPN"

TESIS DE GRADO

Previa la obtención del título de:

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

EDGAR DANIEL ZURITA GALLEGOS

RIOBAMBA – ECUADOR

2012

AGRADECIMIENTO

A Dios por permitirme ser, a mis padres por inculcarme la importancia de estudiar, a mi familia y amigos por toda su ayuda, a la Escuela Superior Politécnica de Chimborazo y a todos los profesores de la EIE-TC por la formación académica recibida.

DEDICATORIA

Dedico este trabajo a mi hijo que es el pilar primordial y fuente de motivación para la consecución de mis objetivos en la vida.

FIRMAS DE RESPONSABLES Y NOTAS

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes	…….	…….

DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

Ing. Pedro Infante	…….	…….

DIRECTOR DE LA ESCUELA DE INGENIERIA ELECTRONICA EN TELECOMUNIACIONES Y REDES

Ing. Alberto Arellano	…….	…….

DIRECTOR DE TESIS

Ing. Diego Ávila	…….	…….

MIEMBRO TESIS

Lc. Carlos Rodríguez	…….	…….

DIRECTOR CENTRO DOCUMENTACION

NOTA DE LA TESIS **…….**

"Yo, EDGAR DANIEL ZURITA GALLEGOS soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

Edgar Daniel Zurita Gallegos

INDICE DE ABREVIATURAS

AS	Autonomous System
ATM	Asynchronous Transfer Mode
ACL	Access Control List
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
CEF	Cisco Express Forwarding
CPU	Central Processing Unit
CPE	Equipo Local del Cliente
CR-LDP	Constraint-based Label Distribution Protocol
CoS	Class of Service
CIR	Committed Information Rate
CE	Customer Edge
DNS	Domain Name System
DoS	Denial of Service

DDoS Denegación Distribuida de Servicio

DES Data Encryption Standard

DLCI Data Link Connection Identifier

DWDM Dense Wavelength Division Multiplexing

ER-LSP Explicitly-Routed Label Switched Path

EIGRP Enhanced Interior Gateway Routing Protocol

FR Frame Relay

FEC Forward Error Correction

GTSM Security Mechanism

HDLC High-Level Data Link Control

IP Internet Protocol

ISO International Organization for Standardization

ISP Internet Service Provider

ICMP Internet Control Message Protocol

IPSec Internet Protocol Security

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IETF	Internet Engineering Task Force
iBGP	Internal Border Gateway Protocol
IPsec	Internet Protocol security
IPX/SPX	Internetwork Packet Exchange/Sequenced Packet Exchange
MPLS	Multiprotocol Label Switching
MD2	Message-Digest Algorithm 2
MD5	Message-Digest Algorithm 5
MP-BGP	Multiprotocol BGP
Nmap	Network Mapper
NAT	Network Address Translation
NSP	Network Service Provider
LAN	Local Area Network
LSR	Label Switch Router
LSP	Label-switched Paths
LDP	Label Distribution Protocol
LER	Label Edge Router
OSI	Open System Interconnection

OSPF	Open Shortest Path First
P	Provider
PE	Provider Edge
PDU	Protocol Data Units
PPP	Point-to-Point Protocol
PPVPN	Security for Provider Provisions VPN
PHP	Hypertext Pre-processor
POP	Post Office Protocol
ATM PNNI	ATM Signaling Private Network-to-Network Interface
QoS	Quality of Service
OSPF	Open Shortest Path First
RFC	Request For Comments
RIP	Routing Information Protocol
RR	Route reflectors
RIB	Routing Information Base
RSVP	Resource reservation protocol
RD	Route Distinguisher
SHA	Secure Hash Algorithm

SSH	Secure SHell
SSL	Secure Sockets Layer
SSL/TLS	Secure Sockets Layer Transport Layer Security
SLA	Service Level Agreement
TTL	Time To Live
TCP	Transmission Control Protocol
TDP	Tag Distribution Protocol
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
VPN	Virtual Private Network
VoIP	Voice over IP
VRF	Virtual Routing and Forwarding
WAP	Wireless Application Protocol
Web	Wired Equivalent Privacy
WWW	Web World Wide

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I

Marco Referencial

1.1. Introducción

La evolución de las redes backbones a mediados de los 90 supuso el primer gran paso hacia la Internet del siglo XXI: una red común para todos los servicios y aplicaciones. Y que supuso pasar de ATM, una tecnología sólida y muy consolidada en las redes de los proveedores, a una tecnología de etiquetaje denominada MPLS, que debía aportar más velocidad y mayor versatilidad. Este documento nace de la duda de las grandes compañías de servicios y de los grandes clientes, de la seguridad de una arquitectura de red que surge con la idea de sustituir ATM. Durante años, ATM les había proporcionado niveles de velocidad, robustez y seguridad que superaban anteriores soluciones. Las grandes compañías necesitan estar seguras de

que la información que transmiten de una compañía a otra o a sus propias sucursales, no corre peligro. ATM, en este aspecto les aportaba eso que añoraban en décadas anteriores, y la idea de cambiar de ATM, a una tecnología basada en IP, no convencía a nadie. Como se podrá observar, es uno de los principales puntos de investigación para todos aquellos que han optado por MPLS en detrimento de ATM. Durante los primeros capítulos se atacará el tema de la seguridad en nuestras redes, para tener una visión más directa de los peligros de los que debe defenderse MPLS. Durante los siguientes puntos, y como principal objetivo, se explicaran las soluciones que se adoptan para que las grandes redes de proveedores no sucumban frente a los ataques de los hackers.

A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de conmutación, encabezadas por la tecnología ATM. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red.

De aquí derivan los siguientes problemas: el paradigma del Routing está muy extendido en todos los entornos. El rediseño total del software existente hacia la conmutación supondría un enorme gasto de tiempo y dinero. Igualmente sucede con el hardware que está funcionando hoy día.

1.2. Justificación Del Proyecto De Tesis

La reducción en los costes de operación se explica porque MPLS permite ofrecer múltiples servicios de transporte de manera virtual (Ethernet, ATM, FR, HDLC, PPP, etc.) con una única red, por lo que ya no es necesario mantener equipamiento y configurar distintas redes, con la correspondiente reducción en personal especialista que esto implica. No obstante, en la actualidad su mayor auge viene de la mano de otro servicio, el de redes privadas virtuales (VPN).

La tecnología MPLS está siendo adoptada por la mayoría de los proveedores de servicios de Internet (ISP) ya que les permite reducir costes en la operación de la red y ofrecer a sus clientes SLAs con compromisos reales de QoS, lo cual se está convirtiendo en una auténtica necesidad con la introducción en las empresas de la VoIP.

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Se identificará las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red de acuerdo a los requerimientos del negocio. Se busca también identificar las herramientas o productos tecnológicos que apoyen los controles que permiten mitigar el riesgo y mejorar de esta manera la seguridad en la red.

La seguridad en redes cubre también aspectos como: disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, de tal forma que se propondrá un enfoque integral de acercamiento a la seguridad de la información que viaja por la red. De tal manera que se

pueda combinar efectivamente la seguridad de la información en la tecnología MPLS para servicio de VPN. Todo lo anterior conforma una estrategia integrada para la seguridad en la red.

Con el estudio mencionado se pretende reducir los riesgos de posibles vulnerabilidades que pueden tener la tecnología MPLS para servicio de VPN por medio de una guía propuesta.

1.3. Objetivos

1.3.1. Objetivo General

Analizar la tecnología MPLS, para proponer guía de mejoras de seguridad para servicio de VPN.

1.3.2. Objetivos Específicos

Analizar las alternativas de las VPNs en capa 2 y de capa 3 para tecnología MPLS para la creación de servicios de eje troncal VPN.

Analizar la arquitectura MPLS para ver el modelo topológico de MPLS con VPNs y poder dar posibles soluciones en cuanto a seguridades.

Implementar un prototipo de pruebas para identificar posibles vulnerabilidades de seguridad en la tecnología MPLS para servicio de VPN utilizando software GNS3 para la emulación.

Crear una guía de mejoras de seguridad de la tecnología MPLS para servicio de VPN.

1.4. Hipótesis

Mediante el estudio de la tecnología MPLS se permitirá proponer una guía de mejoras de seguridad para servicio de VPN.

1.5. Métodos Y Técnicas

1.5.1. Métodos

1.5.1.1. Método Científico

Para poder tener un conocimiento correcto de la lógica utilizada debemos tener una descripción de lo que ocurre como su correspondiente explicación del funcionamiento de la tecnología MPLS con servicio de VPN, que es un elemento crucial en la realización de este estudio.

1.5.1.2. Método Experimental

Se fundamenta en el método científico, comprueba en forma objetiva una ley o una verdad científica, enriquece la calidad de información, datos y vivencias que contribuyen a interpretar la realidad y a actuar sobre ella conscientemente. En la práctica se experimentará en un escenario en el cual se configurará la tecnología MPLS con servicio de VPN y se podrá aceptar o rechazar la hipótesis formulada.

1.5.2. Técnicas

Revisión de la Documentación Se utilizara esta técnica para la recolección de la información más importante para el análisis y configuración del servicio VPN en tecnología MPLS.

Consultas Bibliográficas Se utilizará para la recolección de la información.

Pruebas Prácticas Se utilizara para determinar la funcionalidad en tiempo real del entorno de trabajo de la VPN en tecnología MPLS.

CAPÍTULO II

Marco Teórico

2.1. Seguridades

2.1.1. Qué es la Seguridad?

Hoy en día todos dependemos de la información que radica y generamos en nuestras computadoras; estos objetos ya no se encuentran aislados como en los 80´s y principios de los 90´s, si no por el contrario, hoy dependemos de una conexión física para podernos comunicar, el avance que se ha tenido con las redes nos ha permitido solucionar problemas y hacer provecho de sistemas que nos ayudan a manipular la información.

Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o

a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers. Es por eso que tenemos que tener una serie de precauciones para evitar que alguien no deseado busque en nuestra información y seamos presa fácil de extorsiones, fraudes y pérdidas irreparables.

La **seguridad informática** consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

2.1.2. Servicios para la seguridad

Podemos entender como seguridad un estado de cualquier tipo de información o la (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.

- **Confidencialidad**: La información sólo debe ser legible para los autorizados.

- **Disponibilidad**: Debe estar disponible cuando se necesita.

- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

- **Autenticación:** La autenticación no es más que la confirmación de que el emisor es quien dice ser. También es la manera de asegurar que el mensaje no ha sido interceptado y reenviado a su destino original. Este proceso se puede llevar a cabo a través del uso de claves, firmas digitales, PINs; según el protocolo de autenticación utilizado.

- **Control de acceso:** Es la habilidad de limitar y controlar el acceso a una aplicación o a un dispositivo-ordenador. Para ello, en primer lugar se autentica o identifica al usuario. Si ha tenido éxito, se procede a su autorización para poder utilizar los servicios de la aplicación o del dispositivo.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea comprometida.

2.1.3. Términos relacionados con la seguridad informática

- **Activo**: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

- **Amenaza**: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- **Impacto**: Medir la consecuencia al materializarse una amenaza.

- **Riesgo**: Es la probabilidad de que suceda la amenaza o evento no deseado.

- **Vulnerabilidad**: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

- **Ataque**: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

- **Desastre o Contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la vulnerabilidad está ligada a una Amenaza y el riesgo a un Impacto.

La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. Una persona no autorizada podría: Clasificar y desclasificar los datos, filtrar información, alterar la información, borrar la información, usurpar datos, hojear información clasificada.

2.1.4. Las causas de inseguridad

Generalmente, la inseguridad puede dividirse en dos categorías:

- Un **estado de inseguridad activo**, es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita).
- Un **estado pasivo de inseguridad**; es decir, cuando el administrador (o el usuario) de un sistema no está familiarizado con los mecanismos de seguridad presentes en el sistema.

2.1.5. Tipo de atacantes

Hackers

Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico, pero no pretenden provocar daños en estos sistemas.

Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

Crackers ("blackhats")

Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etc.

Los atacantes pueden tener muchos motivos:

- La atracción hacia lo prohibido.
- El deseo de obtener dinero (por ejemplo, violando el sistema de un banco).
- La reputación (impresionar a sus amigos).
- El deseo de hacer daño (destruir datos, hacer que un sistema no funcione).

2.1.6. Identificación de las Amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption**: la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS)**: servicios que deberían estar disponibles no lo están.
- **Leakage**: los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

La Tabla detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

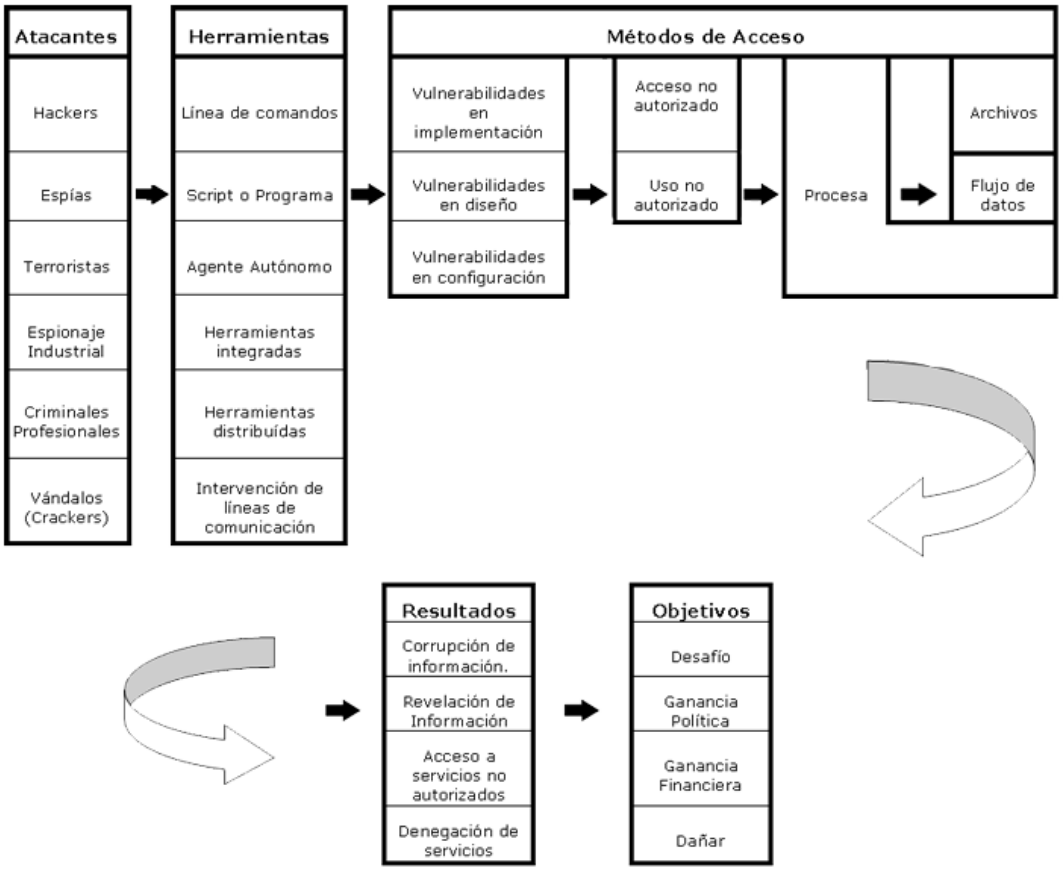


Figura II.1:Identificación de las Amenazas

Fuente: "http://www.cert.org.Capítulo 6- Página 71"

Cualquier adolescente sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Los números que siguen no pretenden alarmar a nadie ni sembrar la semilla del futuro Hacker. Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

2.1.7. Amenazas y contramedidas

Todo elemento de red, ordenador o dispositivo con sistema operativo, es susceptible de padecer intrusiones, virus u otros elementos indeseables. En la década de las comunicaciones incluso los móviles comienzan a ser parte de la carnaza para los "phreackers" ("hackers" de los sistemas telefónicos). Este mundo, tiene muchas ramificaciones, pero lo más importante es que cada día tiene más adeptos, y las grandes empresas de seguridad están haciendo el agosto.

En esta sección, únicamente daremos un vistazo a las amenazas más comunes y genéricas en el mundo de las redes, y que por lo tanto, son más probables en ambientes de MPLS.

2.1.7.1. Planear

Cualquier atacante que se precie, utiliza la técnica del espionaje para averiguar información sobre su objetivo. A través de las informaciones que recopila al respecto, puede conseguir planear un ataque mejor.

A nivel de red, en algunos tipos de ataques, se deben conocer las direcciones IP de las máquinas y los puertos abiertos, los sistemas operativos que se utilizan y servicios que ofertan. Por lo tanto, podemos llamar planear a la recopilación de información sobre una red o un sistema.

Esta recopilación se puede llevar a cabo a través de intentos de envíos ping (si contesta afirmativamente quiere decir que la IP existe). En el caso de

querer averiguar los puertos abiertos, se puede hacer un "escaneado de puertos",

Programas como el Nmap tienen este objetivo. Su funcionamiento es muy simple, y sólo consiste en ir preguntando secuencialmente a los números de puerto en una máquina y esperar la respuesta. Con esta técnica se puede averiguar tanto los servicios que presta la máquina como las puertas abiertas que deja.

Muchos de los firewalls actuales tienen la capacidad de poder descubrir este tipo de ataques, y acto seguido avisar al administrador de las peticiones que se hacen desde el exterior.

2.1.7.2. Sniffing de paquetes

Un sniffer de paquetes es un programa que se ejecuta en un dispositivo asociado a la red. Como se muestra en la figura con él los administradores pueden conocer todos los movimientos de la red, con el fin de gestionar y monitorizar la red.

Por otro lado, para los hackers es una gran manera de obtener información. El llamado eavesdropping puede facilitar información privada de los usuarios de la red. Con la lectura ilegal de los payloads, pueden obtener tanto información de la red como de direcciones de red, el tipo de aplicaciones-servicios que se ejecutan, pero sobre todo identificadores y contraseñas.

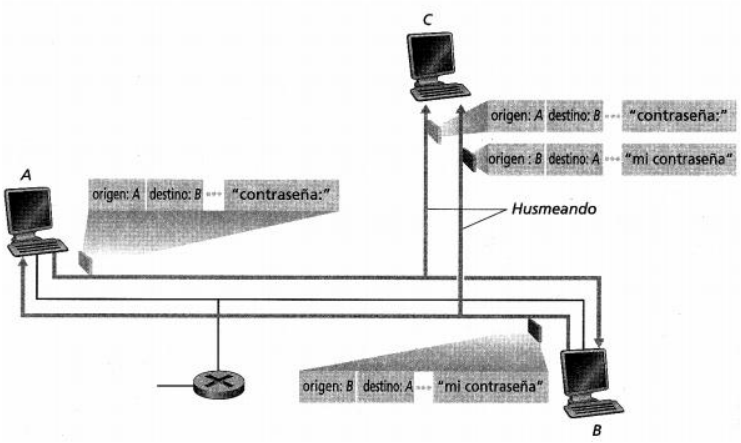


Figura II.2: Ejemplo de Eavesdropping

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

2.1.7.3. Spoofing

Éste, es utilizado en los ataques de denegación de servicio. El spoofing o falsificación es hacer creer al agredido que la web, la IP, el e-mail o cualquier tipo de tráfico de red, es real cuando en realidad una tercera persona es la que lo está generando.

Este tipo de ataques tiene muchas alternativas: podemos encontrar spoofing IP, ARP, Web, DNS e incluso e-mail. Posiblemente el más típico es el que se ilustra en la figura. Se trata del ataque de spooging IP, y es muy sencillo de ejecutar porque cualquier administrador puede cambiar la IP (192.168.0.5) de su interfaz por otra (172.16.0.6), para, por ejemplo, intentar entrar en una red restringida a un conjunto de IPs, o como en el caso de la figura, hacer recibir al agredido una información que no había pedido.

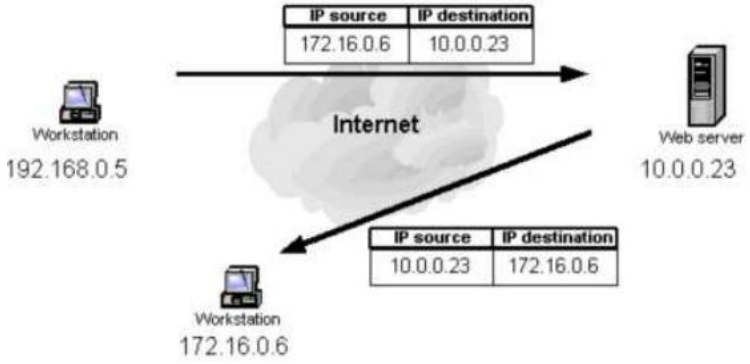


Figura II.3:Ejemplo de IP Spoofing

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

Cada vez más, se están buscando maneras para evitar este tipo de ataques y la denegación de servicios que normalmente viene asociada. Estas contramedidas pasan por autenticar que los datos recibidos son verdaderos-originales (como por ejemplo para los e-mails, o para las DNS), como también denegando la entrada a cualquier tipo de tráfico broadcast.

En el RFC 2267 se indica que este tipo de tráfico se puede evitar si los ISPs filtran los ataques desde su origen. Se alega que toda interfaz conectada a un ISP (Internet Service Provider) tiene asociada una IP (estática o dinámica) que no puede ser cambiada por el usuario. Por lo tanto, en el momento en que el usuario intente enviar una paquete con otra dirección que no corresponda la suya, se puede filtrar y el ataque quedará neutralizado. Pero la única pega de esta idea es que los ISPs tienen que querer hacerlo.

2.1.7.4. Denegación de servicio (DoS)

La denegación de servicio o DoS (Denial of Service) tiene por objetivo inutilizar a un elemento de red, un host o una red completa. Este tipo de ataques, consisten en incrementar mucho la carga de trabajo de la infraestructura atacada de modo que no pueda realizar las tareas que tiene encomendadas.

Por ejemplo, en el ataque de inundación SYN, el atacante inunda un servidor con paquetes TCP SYN cada uno con una dirección IP origen falsificada (spoofing). El servidor, al ser incapaz de diferenciar un SYN legítimo de otro falso, reserva el tamaño apropiado para los búferes (de transmisión-recepción) y las variables de conexión, y envía un segmento de concesión de conexión.

Pero el atacante por su parte, no contesta a este segmento, dejando al host a la espera con las conexiones abiertas, con lo que el servidor sobrecarga su memoria y finalmente se rinde y cae.

Otro ataque parecido puede ser, enviar fragmentos IP pero nunca los suficientes como para poder completar el datagrama. De tal manera que el servidor va acumulando los fragmentos IP sin poder llegar a procesarlos y llena su memoria.

También existe otro tipo de ataque a terceros, llamado smurf. Este ataque consiste en hacer que un gran número de host inocentes respondan a los paquetes ICMP de solicitud de eco (ping), con una dirección IP origen falsa.

Esto produce que un gran número de paquetes ICMP de respuesta inundaran al host cuya dirección ha sido robada.

2.1.7.5. Denegación distribuida de servicio (DDoS)

Éste es un tipo de ataque mucho más potente que el DoS y a su vez más complicado de evitar y de gestar. En este caso el atacante debe instalar y ejecutar un programa esclavo en un conjunto de host sin que los usuarios sean conscientes.

Con un programa maestro, el atacante puede indicar a todos los programas que ha distribuido que ejecuten unos comandos o un ataque preestablecido. La suma de todos los ataques originados desde distintos puntos de la red, siempre tiene resultados devastadores.

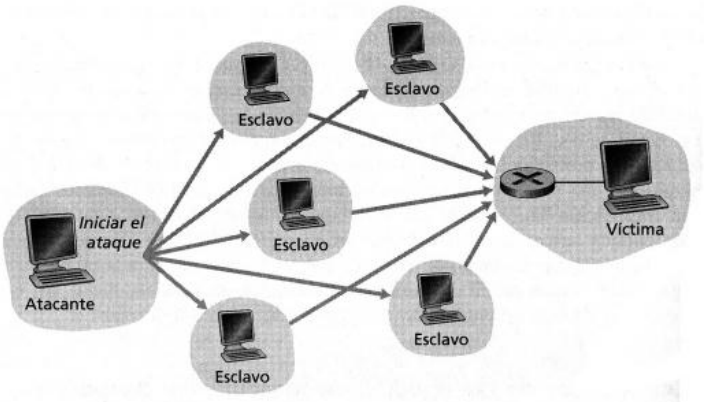


Figura II.4:Ejemplo de Ataque DDoS

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

Un ataque como el presentado en la figura puede llegar a hacer caer portales de Internet como eBay, Yahoo o el de la CNN, incluso servidores DNS o de correo electrónico.

Las soluciones ante este tipo de ataques (tanto DoS como DDoS) pasa por filtrar todos los paquetes broadcast, tener actualizados los servidores y simples ordenadores de toda la red (Internet), y también seguir las indicaciones del RFC 2267 como ya se ha comentado.

2.1.7.6. Secuestro

Como la misma palabra indica, este tipo de ataques consiste en secuestrar una conexión entre dos puntos finales, de tal manera que el atacante (copiando los datos de ACK, SYN, IP, puertos, etc.) pueda hacerse pasar por uno de los dos puntos finales sin que el otro se de cuenta.

El atacante, en algunas ocasiones, actúa como una pasarela de aplicación, enviando información falsa a los usuarios reales de la conexión sin que ellos puedan notarlo.

2.1.8. Los peligros de nuestras redes

Después de este pequeño repaso a las distintas amenazas de la red y a algunas de sus contramedidas, sólo cabe listar algunos de los peligros más comunes en infraestructuras MPLS, y en tecnologías como VPN y BGP.

• En plano de usuario:

- Observación no autorizada de tráfico de usuarios

- Modificación de tráfico de usuario

- Inserción de tráfico no auténtico

- Suplantación de usuario o conexión

- DoS del plano de usuario

- Falsificación de VPNs

• En plano de control:

- DoS del plano de control

- Ataques a infraestructuras

- Desconfiguración de dispositivos

- Suplantación de servidores para la difusión de información falsa

- Ataques a protocolos de control (BGP, RIP, etc.)

- Observación no autorizada de tráfico de control

Para acabar, una frase que resume de la mejor manera este capítulo:

"Lo mejor que podemos hacer es resistir a un cierto conjunto de ataques que conocemos y con los cuales estamos familiarizados. No hay nada en el mundo que pueda protegernos contra nuevos tipos de ataques"

2.2. Red privada virtual (VPN)

Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del

equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

2.2.1. Medios

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación:

- Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

- Integridad: De que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

- Confidencialidad: Dado que solo puede ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

- No repudio: Es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

2.2.2. Requerimientos básicos

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

- Codificación de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.

- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

2.2.3. Tipos de VPN

Arquitecturas de conexión VPN:

2.2.3.1. VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etc) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

2.2.3.2. VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

2.2.3.3. Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

2.2.3.4. VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que

sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAcaddress, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna.

2.2.4. Redes Privadas Virtuales (VPNs de capa 2 y capa 3)

El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables.

La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en

la gestión (y los mayores costos asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs. (Algo similar a la solución IP sobre ATM).

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3 (OSI/TCP), mediante el protocolo IPSec del IETF
- En el nivel 2 (OSI/TCP), mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP

En las VPNs basadas en tuneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los

paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen características comunes que las hacen menos eficientes frente a la solución MPLS:

- Están basadas en conexiones punto a punto (PVCs o túneles)

- La configuración es manual
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones (como se hace en ATM)
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales
- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos.

Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS.

Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada rutas MPLS sino que ve un internet privado (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

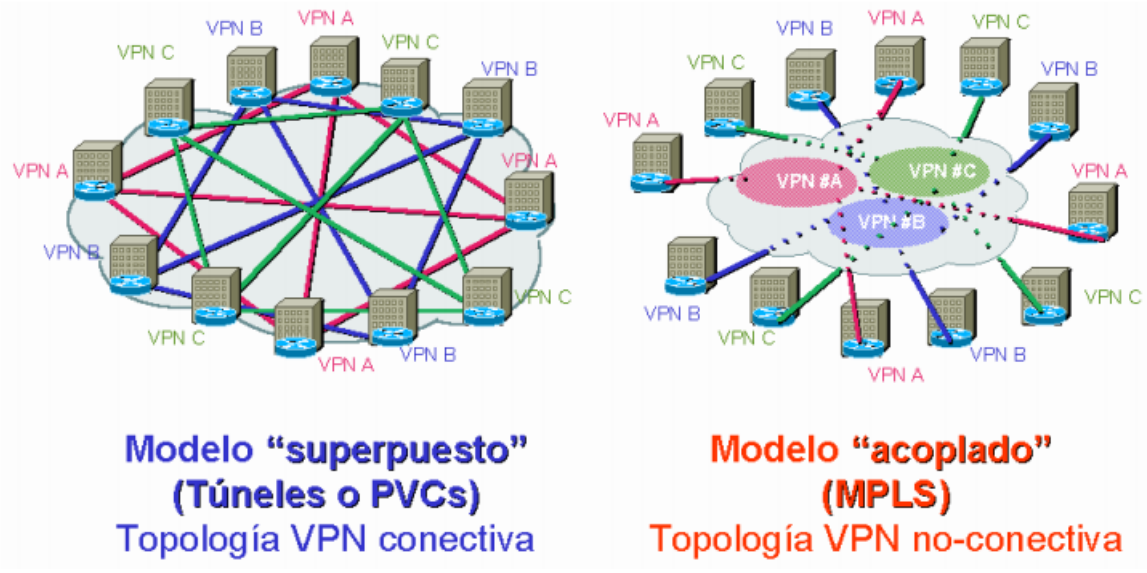


Figura II.5:Modelo "superpuesto" (túneles/PVCs) vs. modelo "acoplado" (MPLS)

Fuente: "http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml"

En la figura se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs)

- Evita la complejidad de los túneles y PVCs

- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router

- Tiene mayores opciones de crecimiento modular

- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

2.2.5. Alternativas de Capa 2 y de capa 3

Las VPN pueden ser creadas en redes de Capa 2 y de Capa 3. En la Figura se puede observar la jerarquía de las variantes para construir ambos tipos de redes.

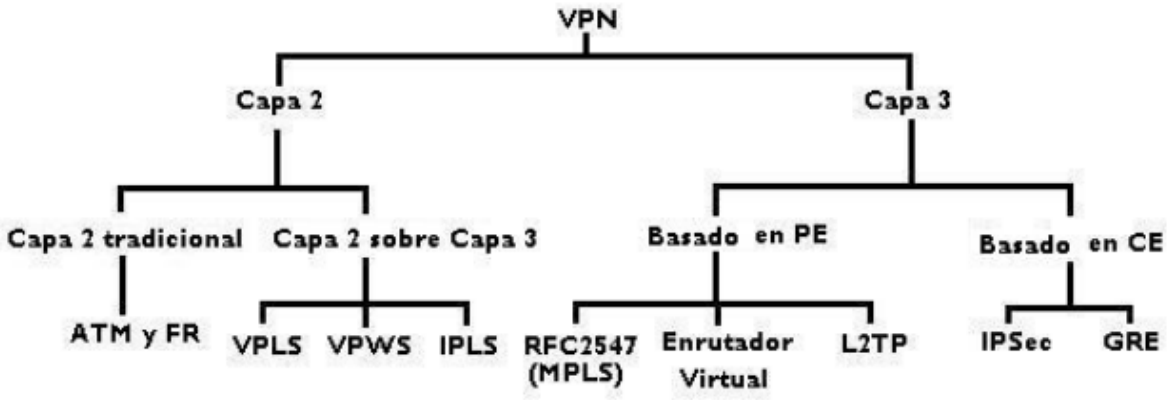


Figura II.6:Jerarquía VPN

Fuente: "http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo3.pdf"

2.3. Multiprotocol Label Switching

MPLS (siglas de Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MPLS es una tecnología híbrida que intenta combinar las mejores características de las técnicas conocidas para hacer llegar un paquete de un origen a un destino, tanto de capa 2 (switching) como de capa 3 (routing), a través de una red de interconexión.

Las principales funciones de MPLS son:

- Especificar mecanismos para gestionar flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente hardware, diferentes máquinas,...).

- Quedar independiente de los protocolos de la capa de enlace y la capa de red.

- Disponer de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.

- Ofrecer interfaces para diferentes protocolos de routing y señalización.

- Soportar los protocolos de la capa de enlace de IP, ATM2 y Frame Relay.

En MPLS la transmisión ocurre en caminos de etiquetas conmutadas LSP, que son secuencias de etiquetas en cada nodo del camino desde el emisor al receptor. Hay dos formas de requerir los LSPs:

1. Antes de la transmisión de datos (control-driven).

2. Una vez detectado un cierto flujo de datos (data-driven).

Las etiquetas se distribuyen utilizando un protocolo de señalización como LDP o RSVP, o también, añadidas a protocolos de routing como BGP u OSPF.

Las etiquetas son insertadas al comienzo del paquete en la entrada de la red MPLS. En cada salto el paquete es encaminado según el valor de la etiqueta y sale por la interfaz correspondiente con otra etiqueta. Se obtiene una gran rapidez en la conmutación gracias a que las etiquetas son insertadas al principio del paquete y son de longitud fija, lo que hace que pueda hacerse una conmutación vía hardware.

2.3.1. Orígenes de MPLS

Para poder crear los circuitos virtuales como en ATM, se pensó en la utilización de etiquetas añadidas a los paquetes. Estas etiquetas definen el circuito virtual por toda la red.

- Estos circuitos virtuales están asociados con una QoS determinada, según el SLA.

- Inicialmente se plantearon dos métodos diferentes de etiquetamiento, o en capa 3 o en capa 2.

- La opción de capa 2 es más interesante, porque es independiente de la capa de red o capa 3 y además permite una conmutación más rápida, dado que la cabecera de capa 2 está antes de capa 3.

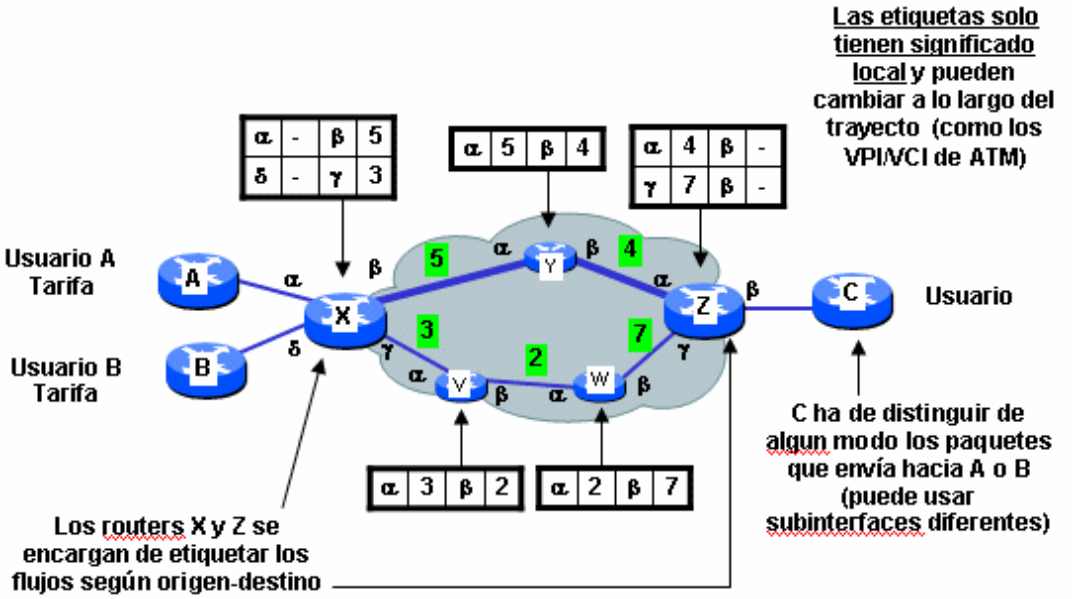


Figura II.7:Arquitectura MPLS

Fuente: "http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml"

2.3.2. MPLS y pila de etiquetas

Jerarquía MPLS

- MPLS funciona sobre multitud de tecnologías de nivel de enlace.
- La etiqueta MPLS se coloca delante del paquete de red y detrás de la cabecera de nivel de enlace.
- Las etiquetas pueden anidarse, formando una pila con funcionamiento LIFO (Last In, First Out). Esto permite ir agregando (o segregando) flujos. El mecanismo es escalable.

- Cada nivel de la pila de etiquetas define un nivel de LSP Túneles MPLS

- Así dentro de una red MPLS se establece una jerarquía de LSPs.

- En ATM y Frame Relay la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente.

2.3.2.1. Elementos

- **LER (Label Edge Router)**: elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como **Ingress Router** y uno de salida como **Egress Router**. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.

- **LSR (Label Switching Router)**: elemento que conmuta etiquetas.

- **LSP (Label Switched Path)**: nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

- **LDP (Label Distribution Protocol)**: un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

- **FEC (Forwarding Equivalence Class)**: nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

2.3.2.2. Cabecera MPLS

Figura II.8:Cabecera MPLS

Fuente: "http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching"

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "stack".

Las etiquetas identifican el camino que un paquete puede atravesar. La etiqueta es encapsulada en la cabecera de la capa de enlace. Una vez el paquete ha sido etiquetado viajará a través del backbone mediante conmutación de etiquetas, es decir, cada router examinará la etiqueta, consultará en sus tablas de envío para saber con qué etiqueta y por qué interfaz debe salir, intercambiará las etiquetas y lo enviará por el interfaz correspondiente.

Pasos para la asignación de etiquetas:

1. Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.

2. Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 (DLCIs, VPIs/VCIs y longitud de onda DWDM, respectivamente) pueden servir como etiquetas. Para redes como Ethernet

y PPP, a la etiqueta se le añade una cabecera shim entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campo TTL.

Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío como encaminamiento unicast, multicast, ingeniería de tráfico, VPN y QoS.

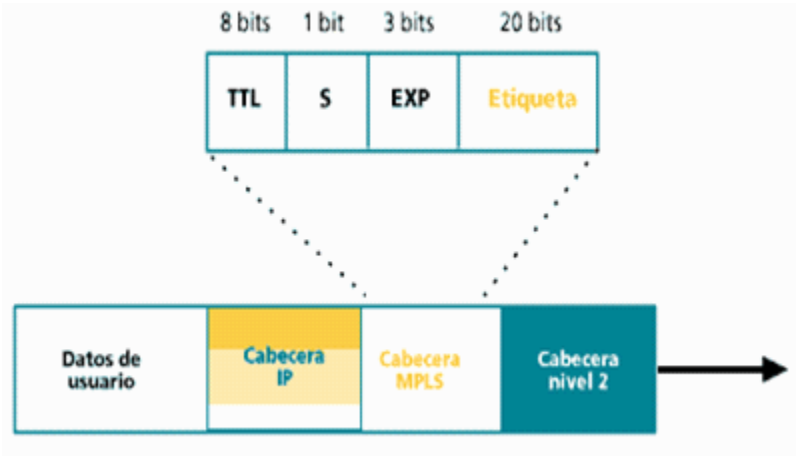


Figura II.9:Etiqueta MPLS

Fuente: "http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml"

Cada etiqueta consiste en cuatro campos:

Donde:

- Label (20 bits): Es la identificación de la etiqueta.
- Exp (3 bits): Llamado también bits experimentales, también aparece como QoS en otros textos, afecta al encolado y descarte de paquetes.
- S (1 bit): Del inglés stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay mas etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.

- TTL (8 bits): Time-to-Live, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado. Generalmente sustituye el campo TTL de la cabecera IP.

Estos paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP. De esta manera, cuando MPLS fue concebido, la búsqueda de etiquetas y el envío por etiquetas eran más rápido que una búsqueda RIB (Base de información de Ruteo), porque las búsquedas eran realizadas en el switch fabric y no en la CPU.

2.3.3. Situación de la etiqueta MPLS

En la siguiente figura podemos observar la posición en la que se ubica la pila de etiquetas MPLS en los distintos protocolos de comunicación.

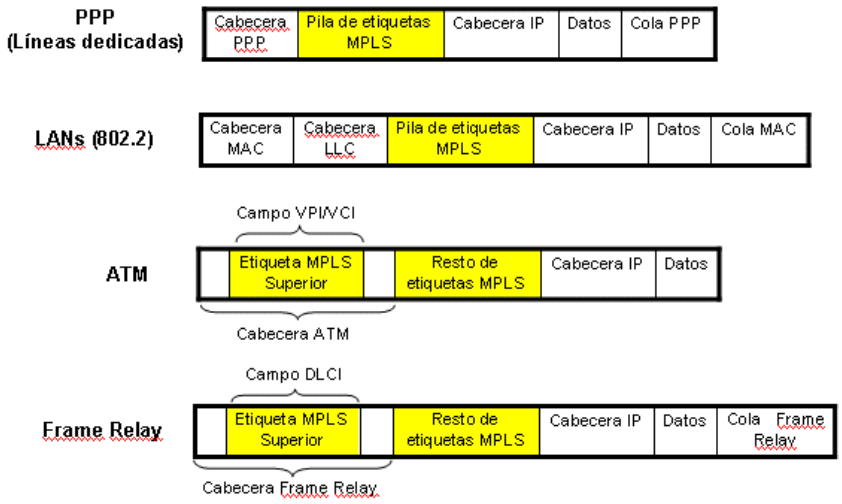


Figura II.10:Situación de la etiqueta MPLS

Fuente: "http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml"

2.3.4. Funcionamiento de MPLS

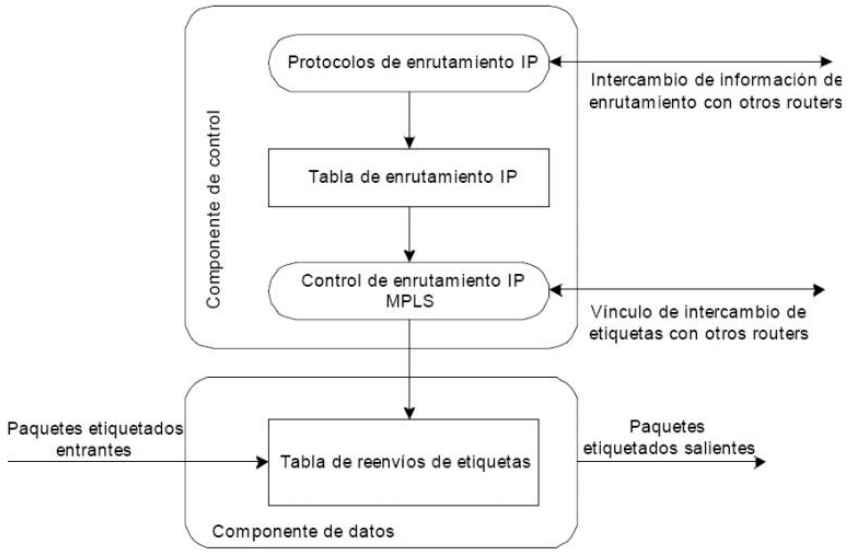


Figura II.11:Funcionamiento de MPLS

Fuente: "http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml"

Conmutación de etiquetas en un LSR a la llegada de un paquete:

- Examina la etiqueta del paquete entrante y la interfaz por donde llega
- Consulta la tabla de etiquetas
- Determina la nueva etiqueta y la interfaz de salida para el paquete.

2.3.5. Routing MPLS

- Los paquetes se envían en función de las etiquetas.
  - No se examina la cabecera de red completa

- El direccionamiento es más rápido

- Cada paquete es clasificado en unas clases de tráfico denominadas FEC (Forwarding Equivalence Class)

- Los LSPs por tanto definen las asociaciones FEC-etiqueta.

2.3.6. Arquitectura MPLS

La arquitectura MPLS básicamente está conformada por dos bloques:

Plano de Control: Lleva a cabo tares destinadas a determinar la disponibilidad del acceso hacia una red destino. Por lo tanto el plano de control contiene toda la información de direccionamiento de la capa tres. Algunos ejemplos comunes acerca de las funciones de la capa de control es el intercambio de información por parte de los protocolos de enrutamiento tales como OSPF y BGP.

Por lo tanto el intercambio de información acerca del direccionamiento IP es una función del plano de control, además de todas las funciones que cumplen aquellos protocolos responsables del intercambio de etiquetas entre routers vecinos tal como el protocolo de distribución de etiquetas (LDP).

Plano de Datos: Lleva a cabo tareas relacionadas con el forwarding o envío de paquetes en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen del plano de control.

Tabla II.IBloques Arquitectónicos de MPLS

Fuente: "http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf"

2.3.7. Distribución De Etiquetas

MPLS permite varios protocolos de señalización para la distribución de etiquetas entre LSRs, el uso de cada uno de ellos dependerá del hardware de la red MPLS y de las políticas de administración de ésta.

Protocolos de routing como BGP permiten llevar piggybacked información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en VPNs. Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas, a éste se le han añadido extensiones para soportar, también, requerimientos de QoS y CoS , así tenemos CR-LDP.

RSVP y CR-LDP se utilizan para la ingeniería de tráfico y reserva de recursos.

Para direcciones multicast tenemos PIM.

2.3.8. Label Switched Path

Cuando un paquete entra en la red MPLS se examina para determinar qué LSP debe asociársele y, a partir de aquí, qué etiqueta asignarle. Esta decisión se debe a factores como la dirección de destino, QoS y el actual estado de la red.

Dominio MPLS: conjunto de dispositivos habilitados en MPLS.

Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP:

Encaminamiento salto a salto: cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la metodología utilizada en redes IP). El LSR utiliza cualquier protocolo de routing disponible como OSPF, ATM PNNI,etc.

Encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícita desde la entrada hasta la salida (ER-LSP). Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos (Nodo Abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permite que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

Puede clasificarse como estricto (strict), aquel camino que incluye todos los nodos, nodos abstractos y Sistemas Autónomos por los que pasa y el orden establecido; o como tolerante (loose), aquél que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto específico.

El camino puede que no sea óptimo puesto que deben tenerse en cuenta los parámetros del servicio. Los recursos serán reservados a lo largo del camino para asegurar QoS.

Esto facilita la ingeniería de tráfico y el poder tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red.

El establecimiento de un LSP para un FEC es unidireccional. El tráfico de vuelta debe tomar otro LSP.

Cuando se detecte un fallo en la red o la topología cambie se debe de proporcionar un nuevo LSP para re-encaminar el tráfico. En una ruta explícita estricta sólo se puede re-encaminar el tráfico en el LER de entrada que es quien decide la ruta, con lo que debe ser informado del error para proporcionar una ruta alternativa. En una ruta explícita tolerante cualquier LSP puede tomar un camino alternativo si es capaz de detectar el fallo del vecino, si la ruta ya está disponible o si un LSP de mayor prioridad requiere esos recursos reservados.

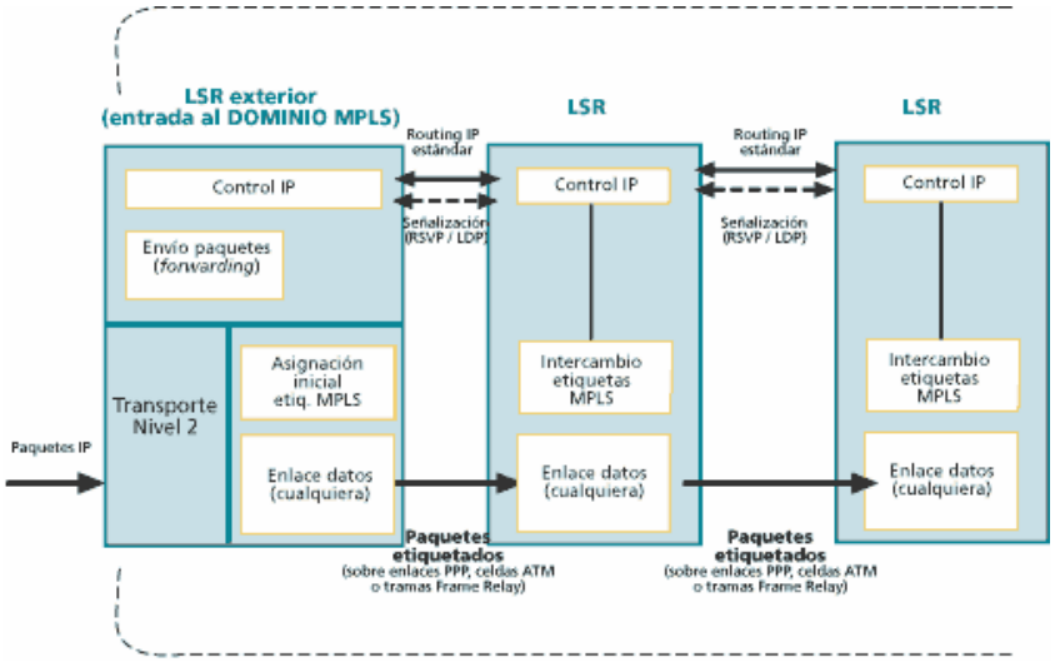


Figura II.12:Label Switched Path

Fuente: "http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html"

2.3.9. Label Distribution Protocol

El protocolo LDP es el protocolo más recomendado por el IETF y ha sido creado específicamente para la asignación de etiquetas a FEC dentro de una red MPLS, este protocolo se ejecuta sobre TCP, lo cual significa que éste asegura la fiabilidad en el envío de mensajes.

Éste no es el único protocolo de enrutamiento capaz de llevar la información de la etiqueta, también está el BGP42 (Border Gateway Protocol), sin embargo, LDP ha sido la solución más adoptada para la redes MPLS. El protocolo LDP tiene como función mapear las FECs, las cuales al ser mapeadas indican la ruta que deben seguir los paquetes para llegar a su destino final armando así los LSPs.

2.3.10. Características básicas y funcionamiento

La tecnología IP ofrece un servicio no orientado a conexión mediante el transporte de datagramas:

- No mantiene un «estado» de la comunicación entre dos nodos.
- No ofrece circuitos virtuales.
- Trabaja bajo la única política de mejor esfuerzo (Best Effort).

2.3.11. Aplicaciones de MPLS

La diversidad de servicios con los que puede trabajar, y las tecnologías que puede soportar, propicia que existan una gran cantidad de aplicaciones en las que se puede involucrar. Entre ellas:

• Ingeniería de Tráfico

• Integración de IP con: ATM, Frame Relay, SONET/SDH, Ethernet, redes ópticas

• VPN (con protocolos como BGP)

• Diferenciación de niveles de servicio (CoS)

• Soporte multiprotocolo

De entre estas aplicaciones, la diferenciación de niveles de servicio y una buena ingeniería de tráfico ayudan a conseguir el objetivo de proporcionar QoS y eficiencia en redes compartidas. Con esta presentación, son muchas

las propuestas nuevas que pueden surgir ya que se dispone de la tecnología adecuada, y de niveles de servicio elevados.

2.3.12. Beneficios de VPN/MPLS

La gran eclosión de MPLS comenzó al unirse al grupo de soluciones beneficiarias de las redes virtuales. ATM no acaba de aportar los niveles de QoS, eficiencia y robustez que tanto se reclamaban. Se podrá ver a continuación los beneficios que presenta VPN/MPLS:

• Integración:

- Sencilla con clientes de intranets.

- No se requiere el soporte de MPLS por parte de los clientes, ni de cambios en la intranet.

• Escalabilidad:

- Posibilidad de soportar miles de "sites" por VPN y centenares de miles de VPNs por proveedor de servicio.

- Los routers P no mantienen ninguna información de rutas de las VPN, lo que incrementa la escalabilidad y evita cuellos de botella.

- La incorporación de un nuevo cliente, sólo supone configurar la entrada en el PE, no la re-configuración de todos los elementos involucrados como en ATM.

- Los clientes no deben preocuparse por la duplicidad de direcciones.

Por lo tanto no es necesario el uso de NAT, excepto en el caso de duplicidad en la misma VPN.

- CoS:

  - Soporta múltiples clases de servicios.

  - El cliente elige las clases de servicios que quiere para sus envíos, y éstas se implementan por parte del proveedor o ambos.

  - Se pueden definir distintas políticas de actuación como la probabilidad de descarte o el retardo.

- Simplicidad de uso:

  - Las VPNs las gestiona el proveedor de servicios.

  - Soporte transparente para direcciones IP privadas.

  - Múltiples clases de QoS para implementar las exigencias de la empresa.

- Bajo coste:

  - Independencia de los equipos del cliente al servicio.

  - La implementación de la VPN no requiere un hardware específico ni costoso para ser instalado.

  - Se pueden integrar distintos servicios y aplicaciones sobre una misma plataforma: voz, datos y video.

• Independencia:

- Una VPN puede soportar distintos protocolos de acceso/transporte: dial, xDSL, ATM, etc.

- El servicio de envío es independiente de la tecnología de transporte o de acceso.

• Rápida recuperación a fallos de conexiones

• Seguridad:

- No es necesario el uso de protocolos o aplicaciones adicionales para soportar niveles de seguridad comparables a ATM.

- Los tráficos VPN se mantienen separados.

- La distribución de rutas VPN se restringe sólo a los miembros de la propia VPN.

Estos son los beneficios más importantes de esta unión.

Evidentemente, es una pequeña síntesis de lo que se puede explicar en un sin fin de páginas. Pero aporta la suficiente información como para poder ver el poder integrador de esta unión, y el abanico de posibilidades que se abren para la aparición de nuevas aplicaciones-servicios.

2.3.13. Creación de una Red MPLS VPN

En el contexto de las Redes Privadas Virtuales, los enrutadores que funcionan como ingreso o regreso a la red son frecuentemente llamados

enrutadores a la Orilla del Proveedor (enrutadores PE), los dispositivos que sirven solo de tránsito son llamados similarmente enrutadores de Proveedor (enrutadores P). Véase el RFC2547.

En MPLS el camino que se sigue está prefijado desde el origen (se conocen todos los saltos de antemano), se pueden utilizar etiquetas para identificar cada comunicación y en cada salto se puede cambiar de etiqueta (mismo principio de funcionamiento que VPI/VCI en ATM, o que DLCI en Frame Relay).

El DLCI identifica una conexión virtual particular sobre un interfaz, por lo que tiene solamente una significación local para un abonado o un nodo.

- Paquetes destinados a diferentes IPs pueden usar el mismo camino LSP (pertenecer al mismo FEC).

- Las etiquetas con el mismo destino y tratamiento se agrupan en una misma etiqueta: los nodos mantienen mucha menos información de estado que por ejemplo ATM. Las etiquetas se pueden apilar, de modo que se puede encaminar de manera jerárquica.

2.3.14. MPLS-VPN: Estructura

Por mucho que exista un etiquetaje, la estructura de la red es una parte fundamental ya que, en parte, acaba determinado el funcionamiento de la misma.

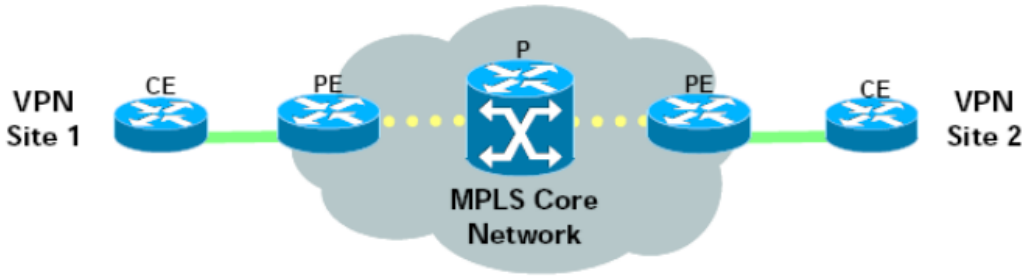


Figura II.13: Estructura de la red

Fuente: "http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html"

- **CE (Customer Edge):** Como se puede observar en la figura, es el dispositivo frontera de la red del cliente. Gracias al valor de integración que aporta el uso de etiquetas, este dispositivo no necesita conocer todos los elementos de la red, ni utilizar MPLS.

- **PE (Provider Edge):** El LSR frontera trabaja como elemento puente entre la red del cliente y la backbone. Es el punto donde se lee la cabecera del paquete que entra y se etiqueta según su destino, las preferencias de CoS del cliente, la VPN a la que pertenece, y otros elementos distintivos.

Si el paquete sale, este router debe eliminar la o las etiquetas que se hayan añadido al paquete, para acto seguido encaminarlo al CE destino.

- **Router P:** Provider (core) router; no tiene conocimientos de las VPNs.

- **Core Network:** Como son los PEs los encargados de la inteligencia de la red, los Ps (Providers) o nodos del core, deben leer la etiqueta e encaminarla convenientemente. Esta ligereza, ayuda a que puedan tratarse

los paquetes de manera más individualizada al poder ejecutar con mayor plenitud una ingeniería de tráfico que se adapte al tiempo.

- **Sitio:** Un sitio se conecta al backbone MPLS a través de uno o más enlaces PE/CE.

- **VRF (Virtual Routing and Forwarding)**

Tabla de rutas más su tabla de forwarding

- **LDP (label Distribution Protocol):** Este es el protocolo encargado de la distribución de la información de la etiquetas entre dispositivos. Para esta tarea, puede asociarse con el BGP.

2.3.15. MPLS VPN: Modelo de conexión

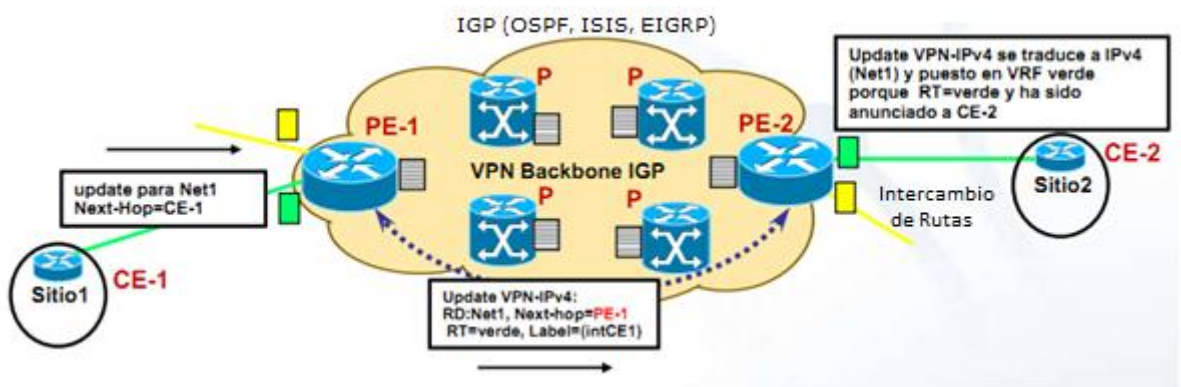


Figura II.14: Modelo de conexión MPLS-VPN

Fuente: "http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf"

• Backbone VPN = conjunto de LSRs MPLS

• PEs hablan con CEs y propagan información de VPN con MP-BGP a otros PEs.

Direcciones VPN-IPv4, Extended Community, Label

- Routers P no corren BGP ni conocen VPNs
- PEs y CEs intercambian rutas
- CEs corren un software IP tradicional
- PEs mantienen tablas de rutas separadas
    - Tabla de rutas global

        Contiene a todos los P y Pes, contiene el "mapa" del backbone.

    - VRF (VPN Routing and Forwarding)

        -Tabla de Routing y Forwarding asociada a uno o más sitios directamente conectados (CEs).

        -VRF son asociadas con interfaces conectadas a los CEs

        -Interfaces pueden compartir la misma VRF si los sitios conectados pueden compartir la misma información de rutas

        -Sitios diferentes que comparten la misma información, pueden compartir la misma VRF

        -Las interfaces que conectan a estos sitios usarán la misma VRF

        -Sitios que pertenecen a la misma VPN "podrían" usar la misma VRF

• Las rutas que el PE recibe de los CEs las ubica en una VRF apropiada.

• Las rutas que el PE recibe desde el IGP del backbone las pone en la tabla IP “tradicional”.

• Las direcciones de las VPNs no tienen que ser mutuamente exclusivas, ya que son ubicadas en diferentes VPNs.

• PEs y Ps comparten un IGP (OSPF, ISIS, EIGRP).

• PEs arman sesiones MP-iBGP entre ellos.

• PEs usan MP-BGP para informar sobre sitios y VPNs conectadas.

Direcciones VPN-IPv4, Extended Community, Label

• Dirección VPN-IPV4: es la unión de las siguientes estructuras de datos

1- Route Distinguisher

64 bits

Le da unicidad global al prefijo IPv4

RD es configurado en el PE para cada VRF

RD puede estar (o no) relacionado a un sitio o una VPN

2 - Direcciones IPv4 (32bits)

• Route Target (dato de 64 bits)

Identitifica al conjunto de sitios a los que la ruta les debe llegar anunciada.

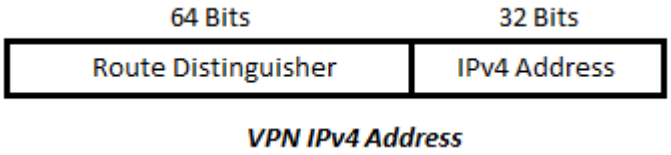


Figura II.15: Representación de la dirección de VPN IPv4

Autor: "Edgar Zurita"

- Otros atributos BGP tradicionales
    - Local Preference

        MED

        Next-hop

        AS_PATH

- Un Label, que identifica:

    La VRF a la cual pertenece el anuncio (label de la VPN).

- PEs reciben updates IPv4s
- PEs traducen el update a formato VPN-IPv4

    Asignan un SOO y RT según lo configurado.

    Re-escriben el atributo Next-Hop.

    Asignan un label basándose en la VRF y/o la interfaz.

Envían anuncio MP-iBGP a sus vecinos PE.

• PEs receptores traducen nuevamente a IPv4

Insertan la ruta en la VRF identificada por el atributo RT (de acuerdo a cómo haya sido configurado el PE)

• El label asociado a la dirección VPN-IPv4 será impuesto en los paquetes enviados hacia su respectivo destino

• Distribución de rutas a los sitios se basa en el atributo llamado "route-target".

-Es una "Community" (atributo) del protocolo BGP.

-En el sitio receptor, se instalarán rutas en la VRF que "reclame" rutas que coincidan con atributo "route-target" de los anuncios que llegan desde otros extremos del backbone.

-Controlado a través de configuración en el PE.

• Un PE que conecta sites de VPN distintas instala la ruta en la VRF del sitio si el atributo "route-target" contiene una o más VPNs al cual el sitio está asociado.

2.3.16. MPLS: Forwarding de paquetes

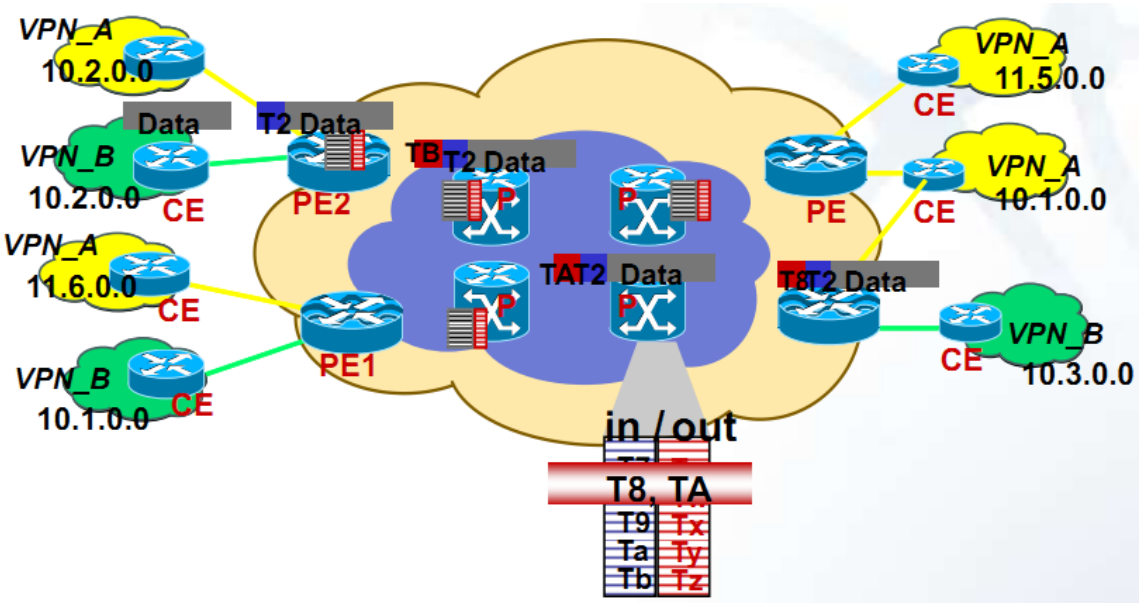


Figura II.16: Forwarding de paquetes

Fuente: "http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf"

• Los valores "next-hop" anunciados por el BPG de los PEs deben ser visibles por el IGP.

• Labels se distribuyen con LDP (hop-by-hop), con el fin de lograr llegar a los Next-Hops de BGP.

• Stack de labels para el forwarding de paquetes

-Top label indica el next-hop BGP (label interior)

-Label de 2do nivel indica la interfaz saliente o VRF (label exterior).

• Los nodos MPLS conmutan con el label externo.

• P no saben nada de BGP ni de VPNs.

• Los P rutean usando el label interior.

• El PE de egreso quita el label interior.

• El PE de egreso usa el label exterior para decidir la VPN a la cual entregar el paquete.

• Se saca el label exterior y se envía el paquete al router CE

2.3.17. Penultimate Hop Popping

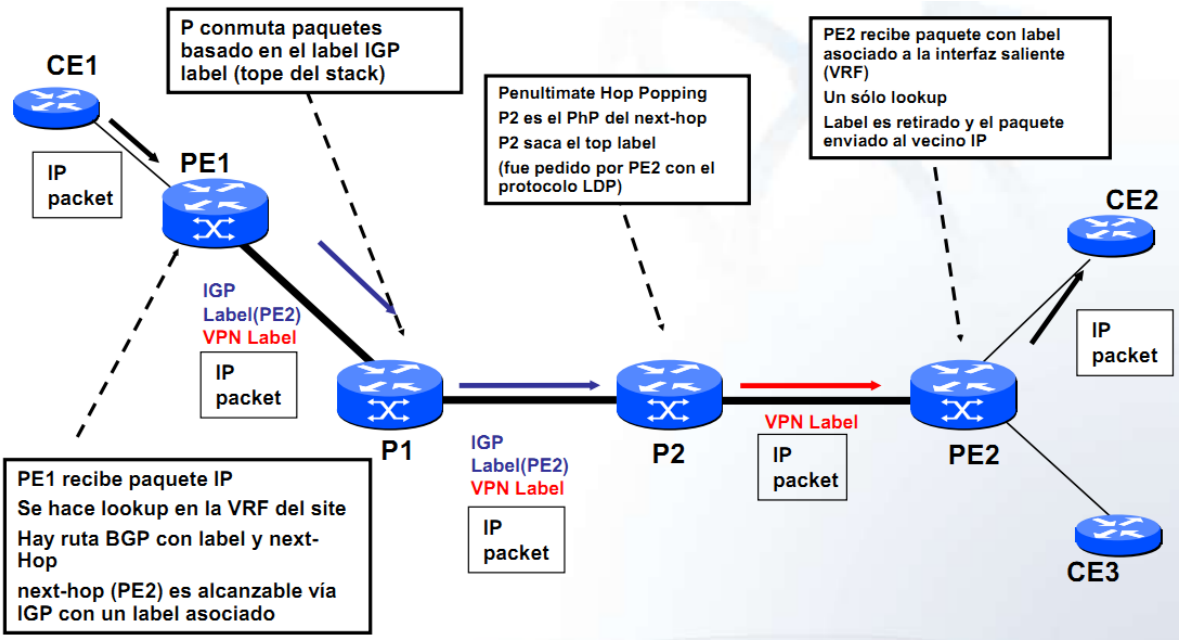


Figura II.17: Penultimate Hop Popping

Fuente: "http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf"

• El router upstream LDP del next-hop de BGP (PE) descartará la etiqueta externa. "Penultimate hop popping".

• Es solicitado con el protocolo LDP.

• El PE de egreso conmutará el paquete en base a la info de la etiqueta de 2do nivel (que explica la interfaz y/o la VPN de salida).

2.4. Seguridad En Mpls

Llegado este punto del trabajo, todos vemos claro que MPLS surgió como gran alternativa de futuro para hacer de las backbones redes más flexibles y eficaces. Ante él, existía (y aún existe) un arduo camino hasta que sea considerado por TODOS como un tecnología solvente y adecuada.

ATM dejó el listón muy alto. Todos los que habían trabajado con esta tecnología eran reacios a tener que cambiar a una tecnología que trabajaba con IP. Y la idea de que en el corazón de la red se trabajara a nivel 3 no les gustaba ya que entendían que así el corazón de la red (core) dejaba de ser seguro.

Durante este capítulo se mostrará el modelo con el que trabaja MPLS, pero esta vez guiando más la vista hacia el aspecto de la seguridad. Con ello, pasaremos a conocer las grandes amenazas de MPLS para posteriormente, explicar si son una amenaza real, y si realmente lo son, como se puede proteger la red.

2.4.1. El modelo de seguridad de MPLS

Cualquier institución, proveedor de servicios o empresa que contenga una red de ordenadores u otros dispositivos, debe procurar aplicar a la red una buena protección contra las amenazas. Para ello debe instalar antivirus, firewalls y cualquier otro tipo de software o hardware acorde con sus

necesidades: todo depende de si tiene una intranet, una extranet, o por ejemplo acceso a Internet.

De todos modos, los proveedores de servicios tienen la desgracia de tener que pensar en todo ello, y adaptarlo para que miles de dispositivos conectados a sus redes puedan disfrutar de una buena protección.

Tanto MPLS como cualquier otra tecnología debe (o debería) asegurar que sus redes pueden ofrecer una serie de servicios básicos como confidencialidad, disponibilidad, integridad y un rápido restablecimiento de las conexiones en caso de fallo. Para aplicar todo esto, es necesario crear una buena política de seguridad y plasmarla en un modelo acorde con los servicios que le gustaría ofrecer.

El modelo utilizado para MPLS VPN surge de las especificaciones formuladas en el RFC 4111 ("Security for Provider Provisions VPNs – PPVPN"). En él se tratan las características fundamentales que deben seguir las redes de servicios para poder afrontar con solvencia los peligros de las redes compartidas.

2.4.1.1. Modelo de seguridad básico

En la figura se puede observar el modelo de seguridad básico utilizado en las redes MPLS VPN. Se pueden denotar la existencia de tres "módulos" diferenciados: las VPNs de los usuarios, las VPN de la red MPLS VPN y el core de la red MPLS VPN (como se ilustra en la figura).

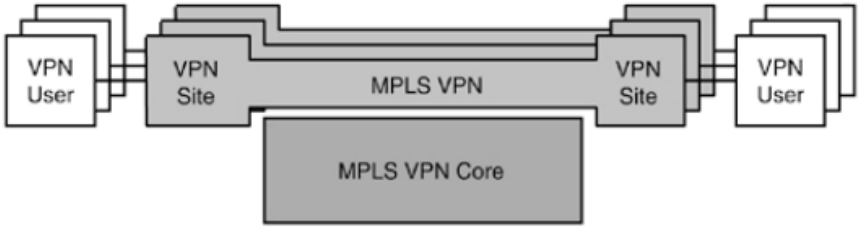


Figura II.18: Modelo de referencia de seguridad base

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

Si concretizamos un poco más, se puede observar que no existe ninguna conexión con ninguna red externa (Internet o extranet). Las únicas conexiones que existen, son las que unen las VPN de los usuarios con su respectiva VPN.

No existe por lo tanto ninguna conectividad entre VPNs distintas. El otro punto a tener en cuenta, es la inexistencia de vínculo entre el core y las VPN existentes.

Por lo tanto, en este modelo básico se puede observar que existe una gran independencia de las VPNs con respecto al resto de VPNs y la red core.

2.4.1.2. Modelo de seguridad con extranet o Internet

El modelo básico no ofrecer ningún tipo de servicio alternativo. Algo que aporte más versatilidad a las "simples" conexiones entre sedes de la misma empresa.

Pongamos por caso que una empresa de apartamentos con diferentes sedes repartidas por distintas ciudades, contrata un servicio de domótica a una empresa especializada. Tal vez, les saldría a cuenta conectar sus redes para

poder crear un servicio más personalizado, y donde se pudieran controlar mejor las instalaciones. A esta interconexión se le llamaría extranet, y es lo que se representa en la siguiente figura.

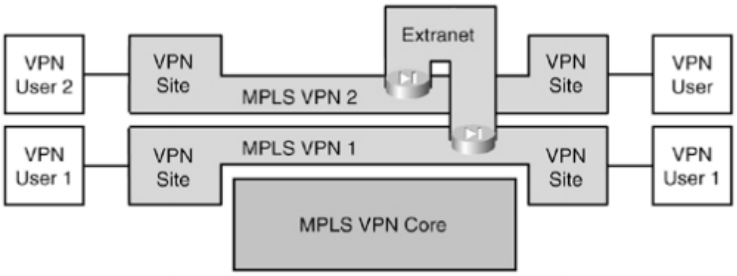


Figura II.19:Modelo con extranet

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

Esta vinculación, desde el punto de vista de MPLS, supone la unión de dos (o más) VPNs para formar sólo una. En cualquier caso, el resto de conexiones permanecen igual (el core no tiene ninguna vinculación con las VPNs). Como detalle, denotar que en las conexiones de cada empresa (user 1 y user 2) con la extranet, se sitúa un firewall/NAT para asegurar la privacidad y evitar solapamientos de direcciones entre redes.

Otro caso muy común, es la vinculación de una empresa a Internet. En la figura se muestra este tipo de conexión que, como en los casos anteriores, no representa ningún tipo de amenaza para la seguridad del core, al menos en su modelo más simple.

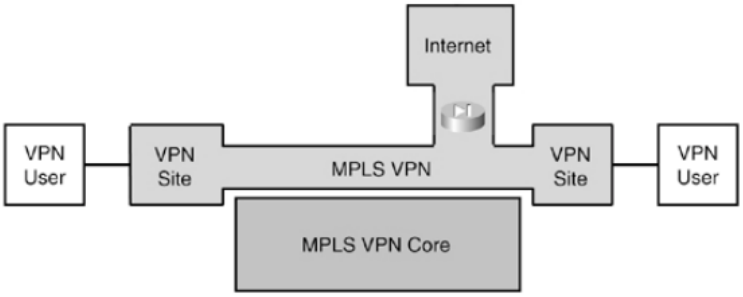


Figura II.20:Modelo con Internet

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

2.4.1.3. Modelo de seguridad con diversos proveedores MPLS

Hasta el momento se han tratado los casos en que las diferentes VPNs viajaban a través de una única red backbone.

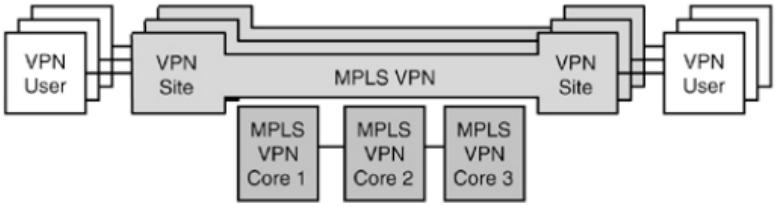


Figura II.21:Modelo con diversos Proveedores MPLS

Fuente: "http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf"

En este caso se puede observar en la figura, que a veces se necesita vincular diferentes redes de proveedores para poder ofrecer el servicio VPN a usuarios de distintas "cores". Como en los casos anteriores, las redes "base" siguen siendo invisibles para las VPNs, ya que no existe relación con los "cores". En realidad, para los usuarios no supone ningún cambio que sus

datos atraviesen una o múltiples backbones. Aunque sí supone cierto riesgo entre las diferentes redes core.

Tanto en los casos tratados, como en el resto de posibles e imaginables, debe existir cierta confianza en que los bloques-módulos vecinos son seguros. De todos modos, se deben tomar precauciones para evitar que se cuelen ataques de DoS de una red core a otra. Por la misma razón por la que se coloca un firewall/NAT en las conexiones con extranets. Aunque entre módulos no vinculados no existe ningún tipo de peligro, entre aquellos que sí lo están se deben tomar las precauciones pertinentes.

CAPÍTULO III

Implementación

3.1. Amenazas a MPLS VPN

Para cualquier red existe un gran surtido de amenazas que pueden hacer temblar los cimientos de su infraestructura.

Para MPLS también existen muchos puntos peligrosos, puntos calientes, por donde los "hackers" pueden tener alguna posibilidad de entrar. Las amenazas son prácticamente las mismas. Así pues, podemos decir que las mayores amenazas son las siguientes:

• Observación de las conexiones para envíos de rutas y etiquetas, entre el PE y CE, y cores diferentes.

• Ataque DoS y DDoS a los PEs

• Falsificación de etiquetas y direcciones IP

• Lectura de la información de los mensajes internos del core

• Ataques entre VPNs conectadas a través de una extranet

• Ataques desde Internet

Como en el caso de ATM, los ataques de spoofing y DoS son los más comunes. Y, por lo tanto, serán los tipos de ataques que más se referenciarán durante la siguiente sección, dónde se observarán las soluciones intrínsecas MPLS y las soluciones a los problemas que se presentan.

3.2. Escenario Propuesto

3.2.1. Seguridad en MPLS

La mayoría de los análisis sobre seguridad que corren por las bibliotecas e Internet, tienen como objetivo comparar puntos concretos de MPLS con ATM.

Estos requisitos que se revisan a MPLS son:

• Separación de espacio de direcciones

• Separación entre VPNs

• Resistencia a los ataques

• Ocultación del core

• Resistencia a ataques spoofing

Abriremos aquellas puertas que los investigadores de esta tecnología no habían abierto hasta hace poco. En él se tratarán características del RFC 2547bis y se intentará dar una valoración más cercana a la realidad, el escenario propuesto se encuentran dos VPNs en la cual no existe conexión de alguna Extranet ni Internet.

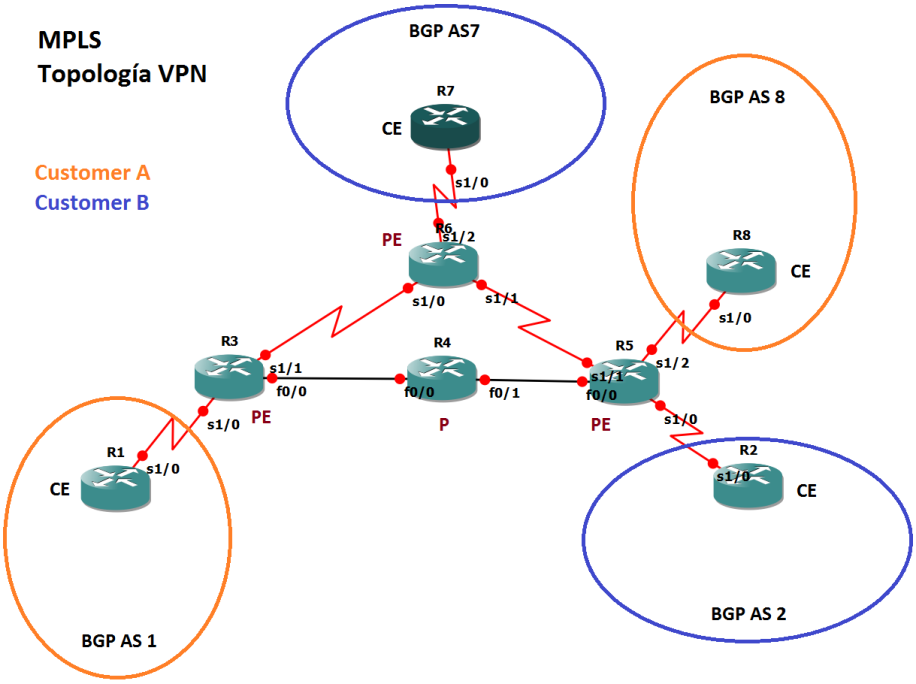


Figura III.22:Escenario Propuesto MPLS VPN

Autor: "Edgar Zurita"

3.2.1.1. Separación entre VPNs

Una de las facilidades que aporta MPLS a los clientes de las redes backbones, es que pueden seguir utilizando su rango de direcciones sin ningún problema. MPLS, mantiene separados los rangos de direcciones de las VPNs y el core a través de un formato de empaquetamiento llamado VPN-IPv4.

Este estándar permite la distinción de direcciones entre VPNs añadiendo a los 4 bytes de las direcciones de IPv4 (o los 16 de IPv6), 8 bytes llamados Route Distinguisher (RD). Lo que permite una gran cantidad de repeticiones de direcciones sin solapamientos. Estos identificadores, son difundidos y asignados por el multiprotocolo BGP (MP-BGP), que es el único que realiza esta tarea. De esta manera, se asegura que no existen dos identificadores RD idénticos en toda la red.

```
R5#sh ip bgp vpnv4 all
BGP table version is 24, local router ID is 150.1.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf CustB)
*>i150.1.1.1/32     150.1.3.3                0    100      0 1 ?
*> 150.1.8.8/32     192.168.58.2             0             0 8 ?
*>i172.31.1.0/24    150.1.3.3                0    100      0 1 ?
*> 172.31.8.0/24    192.168.58.2             0             0 8 ?
*>i192.168.13.0/30  150.1.3.3                0    100      0 1 ?
r> 192.168.58.0/30  192.168.58.2             0             0 8 ?
Route Distinguisher: 2:1 (default for vrf CustA)
*> 150.1.2.2/32     192.168.25.2             0             0 2 ?
*>i150.1.7.7/32     150.1.6.6                0    100      0 7 ?
*> 172.31.2.0/24    192.168.25.2             0             0 2 ?
*>i172.31.8.0/24    150.1.6.6                0    100      0 7 ?
r> 192.168.25.0/30  192.168.25.2             0             0 2 ?
*>i192.168.67.0/30  150.1.6.6                0    100      0 7 ?
```

Tabla III.II VRF R5

Autor: "Edgar Zurita"

Por otro lado, a cada VPN se le asigna una instancia o tabla VRF (Virtual Routing and Forwarding) VRF CustA y VRF CustB. Por su parte, cada PE mantiene estas tablas separadas las unas de las otras, con lo que la información sobre las direcciones de cada VPN y las direcciones de los PEs conectados a los CEs de su misma VPN, permanecen ocultas. Únicamente la PE de cada VPN tiene conocimiento de las direcciones que la forman, y ningún otro dispositivo de la red u otras VPNs tienen acceso a esa información.

3.2.1.2. Separación de tráfico

Una simple demostración de que las VPNs se mantienen separadas, es la prueba que comenta Holly Xiao en su trabajo "Security Measurement on MPLS-VPN". Con ellas se formaban dos VPNs (VPN-A, VPN-B). La prueba es muy simple: enviar un ping de un terminal a otro.

El tráfico de una VPN se divide en tráfico de plano de control y tráfico de plano de datos. El plano de control es el tráfico originado y terminado en el mismo core; y por su parte, el plano de datos contiene el tráfico enviado desde las diferentes VPNs. Este tráfico es encapsulado y enviado de PE a PE añadiendo una etiqueta llamada LSP (Label-switched Paths).

Como se puede observar en el escenario propuesto, los diferentes tráficos quedan separados los unos de los otros. Por ello, todo el tráfico entre CEs resta oculto para el core.

En la siguiente figura se muestra un ping realizado de R7 a R2, ambos router pertenecen a la misma VNP CustB.

```
R7#ping 172.31.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/72/112 ms
```

Figura III.23: Ping de R7 a R2 Interface Fashethernet 0/0

Autor: "Edgar Zurita"

En la figura se muestra un ping realizado de R7 a R1, en el cual R7 pertenece a la VPN CustB y R1 a la VPN CustA, se debe tomar en cuenta que tanto R7 como R8 tienen la misma dirección IP en la interface Fashethernet 0/0 y como veremos a continuación el tráfico se mantiene separado entre VPNs.

```
R7#ping 172.31.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura III.24: Ping de R7 a R1 Interface Fashethernet 0/0

Autor: "Edgar Zurita"

En la figura se muestra un ping realizado de R1 a R8, en el cual ambos router pertenecen a la VPN CustA.

```
R1#ping 172.31.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 800/984/1204 ms
```

Figura III.25: Ping de R1 a R8 Interface Fashethernet 0/0

Autor: "Edgar Zurita"

En la figura se demuestra que incluso habiendo utilizado el mismo rango y las mismas direcciones, los paquetes ICMP llegan a su destino real.

Conociendo esto, podemos concretizar más y observar que la separación del tráfico, recibe diferente trato dependiendo del tipo de interfaz utilizada:

• Interfaz no-VRF: Este tipo de interfaz está asociada con una tabla de enrutado global. Por ello la decisión de envío se toma a partir de esta tabla y el paquete es tratado como un paquete IP normal. Este tipo de interfaz se encuentra en el core y en casos de vinculación de la red de servicios con Internet.

• Interfaz VRF: En este caso la decisión se basa en la información de la tabla de encaminamiento de la VRF. La separación de varias VPNs viene creada por la encapsulación de los paquetes con la cabecera VPN que le pertenece.

Con todo esto queda claro que:

• Con MPLS se consigue la separación de direcciones, tráficos y VPNs.

• Se consigue tanto escalabilidad como seguridad ya que ni el core ni las diversas VPN son alcanzables entre sí.

• Es imposible introducirse en otra VPNs que no sea la que se tiene asignada.

• No se puede acceder desde el exterior al core a menos que se autorice a ello.

3.2.1.3. Ocultación del Core

Éste es uno de los requisitos de seguridad más exigidos por los detractores de MPLS. ATM consigue ocultar el core, porque trabaja a nivel 2, mientras que MPLS lo hace a nivel 3. Sin lugar a dudas, la ocultación es un gran beneficio en la lucha contra los atacantes de redes. Poder ocultar la red, significa que los atacantes no tienen posibilidad de conocer direcciones internas que puedan ser atacadas.

```
R1#traceroute 172.31.8.1

Type escape sequence to abort.
Tracing the route to 172.31.8.1

  1 192.168.13.1 576 msec 628 msec 184 msec
  2 192.168.58.1 [AS 8] [MPLS: Label 20 Exp 0] 692 msec 448 msec 452 msec
  3 192.168.58.2 [AS 8] 1520 msec 592 msec 632 msec
```

Tabla III.IIITraceroute de R1 a R8 Interface Fashethernet 0/0

Autor: "Edgar Zurita"

Para poder atacar un elemento interno de una red, primero se debe conocer su dirección. Y MPLS no rebela ninguna información sobre el core al exterior.

```
C:\Users\DAN>tracert 172.31.8.1

Traza a 172.31.8.1 sobre caminos de 30 saltos como máximo.

  1    113 ms    103 ms     59 ms  172.31.1.1
  2    406 ms    327 ms    274 ms  192.168.13.1
  3    661 ms    357 ms    636 ms  192.168.58.1
  4    182 ms    118 ms     64 ms  172.31.8.1

Traza completa.
```

Tabla III.IV Tracert del PC (conectado al R1) a R8 Interface Fashethernet 0/0

Autor: "Edgar Zurita"

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.45.0/30 is subnetted, 1 subnets
C       192.168.45.0 is directly connected, FastEthernet0/1
     192.168.56.0/30 is subnetted, 1 subnets
O       192.168.56.0 [110/74] via 192.168.45.1, 00:41:55, FastEthernet0/1
     192.168.36.0/30 is subnetted, 1 subnets
O       192.168.36.0 [110/74] via 192.168.34.1, 00:41:55, FastEthernet0/0
     192.168.34.0/30 is subnetted, 1 subnets
C       192.168.34.0 is directly connected, FastEthernet0/0
     150.1.0.0/32 is subnetted, 4 subnets
O       150.1.6.6 [110/75] via 192.168.45.1, 00:41:55, FastEthernet0/1
                  [110/75] via 192.168.34.1, 00:41:55, FastEthernet0/0
O       150.1.5.5 [110/11] via 192.168.45.1, 00:41:55, FastEthernet0/1
C       150.1.4.4 is directly connected, Loopback0
O       150.1.3.3 [110/11] via 192.168.34.1, 00:42:08, FastEthernet0/0
```

Tabla III.VRutas de R4

Autor: "Edgar Zurita"

El único elemento del que se puede poseer esa dirección es del PE (tratado un poco más abajo). Incluso conociendo o intuyendo la dirección de alguno de los elementos interiores de la red, MPLS trata a todos los mensajes llegados por una VPN como mensajes de esa VPN, y por lo tanto no circulan a otro lugar (ni a las direcciones internas del core, ni a otras VPN). Por lo que un ataque desde el exterior a cualquier elemento interno de la red es muy difícil de conseguir también en redes MPLS.

Como se ha podido notar, me he referido a la anterior opción de ataque desde una perspectiva exterior. En cuanto un ataque desde el interior, no existe capa o protocolo en particular que garantice la protección contra ataques internos.

De alguna manera se podrán encriptar los datos, pero incluso en ATM es posible este tipo de ataques.

```
R8#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/30 is subnetted, 1 subnets
B       192.168.13.0 [20/0] via 192.168.58.1, 00:48:15
     192.168.58.0/30 is subnetted, 1 subnets
C       192.168.58.0 is directly connected, Serial1/0
     172.31.0.0/24 is subnetted, 2 subnets
B       172.31.1.0 [20/0] via 192.168.58.1, 00:48:15
C       172.31.8.0 is directly connected, FastEthernet0/0
     150.1.0.0/32 is subnetted, 2 subnets
C       150.1.8.8 is directly connected, Loopback0
B       150.1.1.1 [20/0] via 192.168.58.1, 00:48:15
```

Tabla III.VI: Rutas de R8

Autor: "Edgar Zurita"

En cuanto a la revelación de información de las redes de los clientes a las PEs, ya hemos visto que la información únicamente queda almacenada en cada VRF con lo que ninguna otra VPN tendrá acceso a esa información. Anunciar esa información no compromete la seguridad de la red del cliente, porque la información conocida por el core es sobre rutas de la red y no información de host específicos.

Por lo que se ha explicado hasta el momento, existen dos maneras de atacar el core:

- Atacado directamente los routers PE

- Atacando los mecanismos de señalización

Es posible atacar a los routers frontera (PE) porque es la única dirección revelada al exterior. Esta información es revelada por el enrutado entre el CE y el PE. Esta operación puede ser ejecutada de dos maneras:

• Por enrutado estático: En este caso los routers PE son configurados estáticamente con la información de la red del CE; y los CEs son configurados también estáticamente apuntando hacia el PE u otras partes de la VPN (normalmente un router por defecto). La ruta estática puede apuntar a la dirección IP del router PE, o a la interfaz del router CE (por ejemplo, serial0).

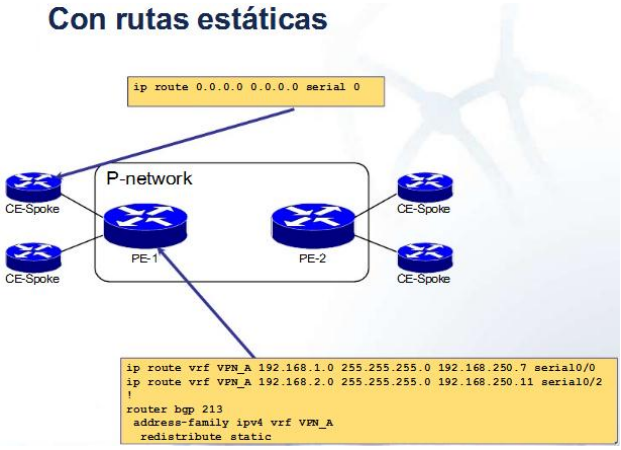


Figura III.26: VRF con Rutas Estáticas

Fuente: http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf

En la segunda de las opciones, el CE no necesita conocer ninguna de las direcciones IP en la red core, ni tan solo las direcciones del PE. Aunque esta opción tiene la desventaja de requerir una configuración estática más extensa, es ideal desde una perspectiva de red segura. En este caso es posible configurar un ACL (Acces Control List) en el PE. Con ello se puede bloquear todo el tráfico hacia su interfaz.

• Por enrutado dinámico: En todos los casos donde se utilizan protocolos dinámicos de enrutado (RIP, BGP, OSPF), cada CE necesita conocer por lo menos la identificación del router del PE, y por lo tanto almacena una destinación potencial para un ataque. En la práctica, los proveedores de servicio pueden limitar el acceso al PE aprovechándose del protocolo de encaminamiento, de las siguientes maneras:

- Usar ACLs para limitar el acceso sólo a paquetes de enrutado y al puerto (o los puertos) del protocolo, enviados desde el CE.

- Cuando sea posible, configurar la autenticación Message Digest MD-5 para protocolos de enrutado. La autenticación MD-5 está disponible para BGP (RFC 2385), OSPF (RFC 2154) y RIP2 (RFC 2082). Esto previene el spoofing desde elementos del interior de la red del cliente que no sea el CE.

- Cuando sea posible, se podría configurar parámetros del protocolo de enrutado para fortalecer la seguridad. Por ejemplo, se debería limitar el número de interacciones de enrutado. También se podría configurar un máximo nombre de rutas aceptadas por VRF. Esto ayudaría a asegurar que una VPN no pueda inundar el provider-edge router con demasiadas rutas. La utilización de Generalized TTL (Time-to-Live) Security Mechanism (GTSM, RFC 3682), en su caso sería una buena baza de seguridad que debería utilizarse en todos lo protocolos que lo soporten (incluso con el protocolo interno LDP (Label Distribution Protocol).

En resumen; no es posible introducirse de una VPN a otra. Y aunque el core revelase direcciones de sus PE a sus respectivos CEs, hemos podido ver que

existen recursos para poder evitar un ataque. De todas maneras, y como veremos en la sección de ataques de spoofing y DoS, sigue siendo posible un ataque DoS aunque se reduzcan las posibilidades.

Al menos en lo que respecta al objetivo de este punto (ocultación del core), queda claro que se consigue, aunque en opciones de uso de Internet, se deberá trabajar algo más para poder evitar intrusiones. En este caso, el uso de NAT ayudaría a asegurar la privacidad de los usuarios de las VPNs.

3.2.1.4. Resistencia a ataques

Para resistir a los ataques, MPLS utiliza filtrado de paquetes y no revelación de información del core. De esta manera, los ataques son mucho más complicados y obligan a los hackers a buscar alternativas.

Se ha podido ver hasta ahora que MPLS ofrece ocultación de las direcciones internas y del acceso a la tabla de enrutado global. Con la ayuda de los filtrajes a través de inclusión de ACL en los routers PE y la aplicación de diferentes configuraciones de seguridad en protocolos dinámicos de enrutado, se consigue una seguridad igualable a ATM y FR. En ambientes con acceso a Internet, la información revelada al exterior, si se siguen unos requisitos mínimos de seguridad, MPLS también puede estar a la altura.

Con la ayuda de la separación de VPNs, en caso de que se produjera un ataque, éste perjudicaría únicamente a los miembros de la VPN y no al resto de VPNs establecidas o al core. El único problema llegaría de la mano de ataques DoS que reducirían la capacidad de gestión de las PE, peligrando así los valores mínimos de QoS.

3.2.1.5. Spoofing

Este tipo de ataques puede afectar tanto a redes de nivel 2 como de nivel 3.

Por ello todas las redes-backbones deben protegerse contra este tipo de ataques. Particularmente para MPLS se presentan dos alternativas de ataque para los hackers:

• IP spoofing: MPLS permite a sus clientes utilizar todo el rango de direcciones (de 0.0.0.0 a 255.255.255.255). Esto permite un gran margen de maniobra a los atacantes con este tipo de armas. La utilización de VRF, permite a MPLS retener este tipo de ataques en la VPN. Con ello se evita que puedan "saltar" a otras VPNs de la red. De todas formas, para este tipo de ataques, los investigadores consultados (normalmente de Cisco), piden a los administradores de las redes Cliente que utilicen refuerzos de seguridad, ya que sólo les afectará a ellos.

• Label spoofing: Dentro del core, los paquetes de diferentes VPNs se distinguen por la inserción de etiquetas. Un usuario malicioso de una VPN podría intentar crear su propia etiqueta (falsa) para entrar en el core. De esta manera podría infiltrarse en el tráfico de otra VPN. Por esta razón, cualquier paquete con etiqueta llegado de un CE es descartado por los PEs. Eso hace de este tipo de ataques simplemente imposibles.

• No es posible que un atacante "inyecte" etiquetas (en el borde no existe soporte del protocolo LDP).

• En el borde, se deben tomar las mismas precauciones que para una arquitectura IP¨(spoofing, DoS, etc).

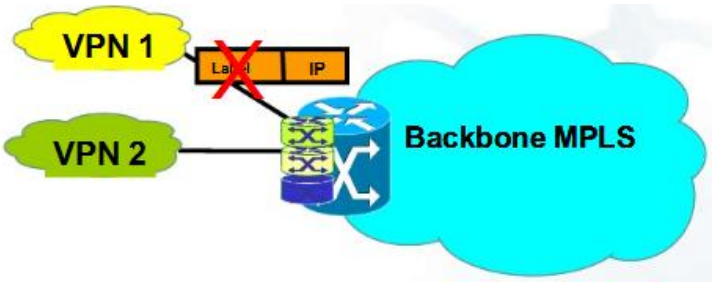


Figura III.27:Etiqueta (falsa)

Fuente: "http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf"

Como MPLS dispone de la separación de VPNs este tipo de ataques quedan contenidos en las propias VPNs. Con lo que se puede decir que los usuarios de las VPNs (maliciosos o no), sólo se pueden atacar a ellos mismos. Con lo que no hay ningún riesgo para el core, ni el resto de VPNs.

3.2.1.6. DoS

Este tipo de agresiones son los más difíciles de contener. Cualquier protección existente hoy en día no asegura un 100% de fiabilidad, ya que es difícil encontrar una solución con las tecnologías actuales.

Este tipo de ataques pueden intentar afectar a MPLS sobreutilizando los siguientes recursos:

• Sobrecargando la línea en una red

• Excediendo la capacidad de envío de paquetes de un router

• Excediendo la capacidad de proceso de paquetes de un servidor

En general los ataques DoS están dirigidos a agotar uno de los siguientes recursos:

- Ancho de banda
- CPU
- Memoria

Este tipo de ataques suelen llegar desde Internet, aunque también se pueden colar por las VPNs. Entre la conexión de Internet y la de VPN, existe una gran diferencia de ancho de banda. Al consumir más ancho de banda Internet, en casos de repetición de paquetes, como en un ataque DoS, las VPNs reducen su capacidad, incluso llegando a la desconexión.

La única manera para el proveedor de solventar este tipo de ataques es sobretodo, disponiendo de un correcto posicionamiento de dispositivos, para poder solventar la demanda de recursos de ciertas zonas de la red. También es positivo hacer una correcta planificación de los anchos de banda y disponer de una buena política de QoS. A todo esto, se le debe añadir algunas de las opciones que ofrece MPLS para poder solventar este tipo de problemas.

3.2.2. Routers resistentes a DoS

Tecnológicamente estamos distantes de poder tener la capacidad de poder solventar con creces los efectos de un ataque DoS o DDoS. Existe un router de Cisco llamado CRS-1 que da el primer paso. Este router tiene la peculiaridad de permitir separación de CPU y memoria completa. Con ello,

la capacidad de procesamiento en un ataque se solventa con mayor facilidad. Puede que de aquí a un tiempo lo podamos saber.

3.2.3. Seguridad obligatoria

Durante todo este capítulo, hemos podido observar la gran variedad de soluciones que presenta MPLS. De cada una de las expuestas aquí, se han extraído algunos puntos conflictivos.

Un punto en cuanto a seguridad que no se ha tratado aquí, es que relaciona el cliente con la proveedora de servicios. Siempre debe establecerse una relación entre clientes o entre clientes y proveedores. Y tener en cuenta aspectos como: la autenticación, la seguridad a la entrada de sus redes, etc.

Estos aspectos, son a veces olvidados por los clientes. Estos, no deben dejar agujeros que puedan implicar a la VPN que tienen creada en la red MPLS. Por ejemplo, la mala gestión de seguridad en el acceso wireless, puede causar la entrada de los "hackers". Esto, evidentemente, no es problema del proveedor de servicios. Como no es culpa del cliente, las desconfiguraciones de las rutas de los routers. Por ello, y haciendo referencia a una frase de Michael H. Behringer: no se pueden cerrar las puertas a cal y canto, y dejar las ventanas abiertas. Con lo que, cada administrador de red, debería crear una buena política de seguridad adaptada a su red. A partir de ahí, deberían cumplirse los objetivos marcados, y en el momento de compartir información con otras redes, conocer sus niveles de seguridad. Porque, aunque una red tenga un gran

nivel de seguridad, si su homónima no lo tiene, pueden producirse situaciones desagradables.

CAPÍTULO IV

Análisis de Resultados

4.1. Introducción

En este capítulo se pone a consideración el análisis de los resultados obtenidos a través del desarrollo del proyecto de tesis, los mismos que sirven también para la comprobación de la hipótesis. Para esto se trabajó en el escenario desarrollado, los resultados se obtuvieron a partir de los programas whireshark para analizar el tráfico de la red y Nmap para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

4.1.1. Utilización de Nmap en la Red MPLS VPN

Con Nmapse puede evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Se realizó un escaneo de puertos a distintas Interfaces de los Routers de la Red MPLS VPN, el siguiente gráfico muestra los resultados obtenidos del escaneo realizado al Router CE-R1 de la red en la interface Serial 1/0 desde la red del cliente AS1.

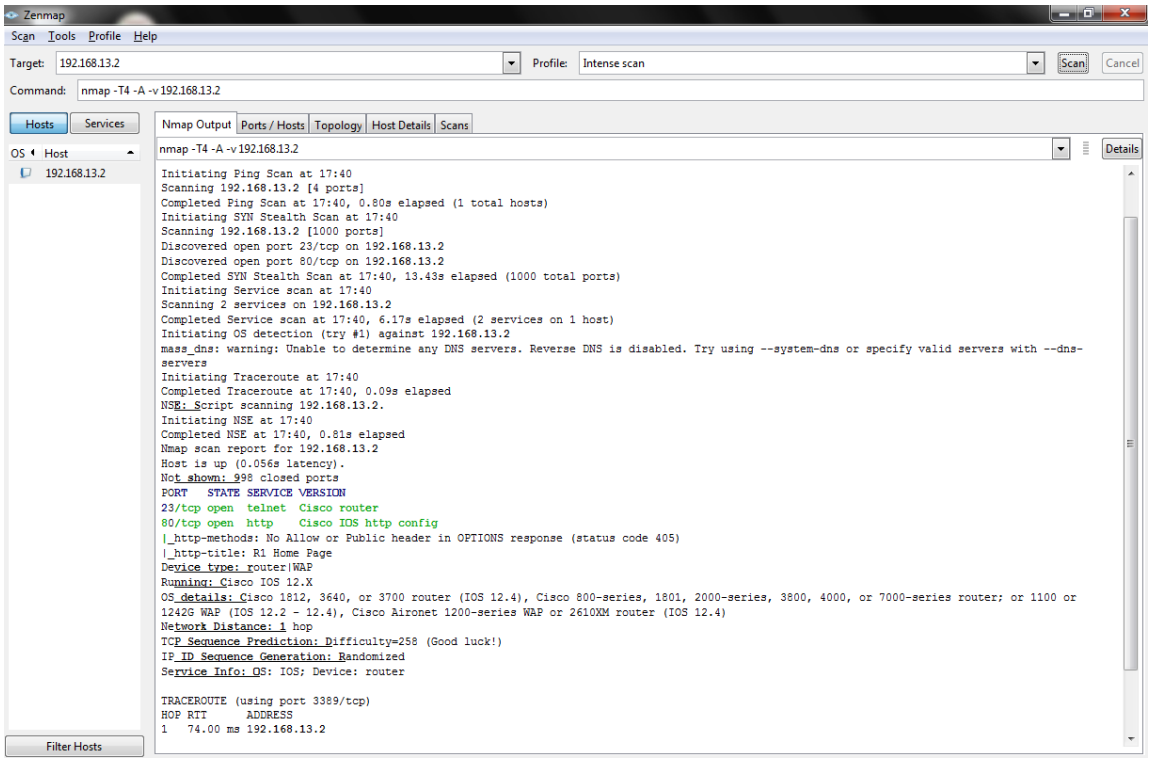


Figura IV.28Escaneo de Puertos a R1 Interface Serial 1/0

Autor: "Edgar Zurita"

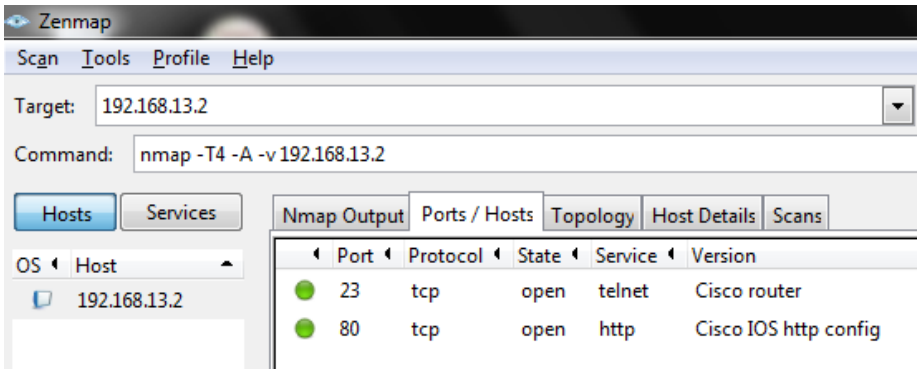


Figura IV.29:Puertos encontrados CE-R1

Autor: "Edgar Zurita"

Como podemos observar en la imagen se encontraron dos puertos pertenecientes al Router CE-R1 (puertos 23 y 80).

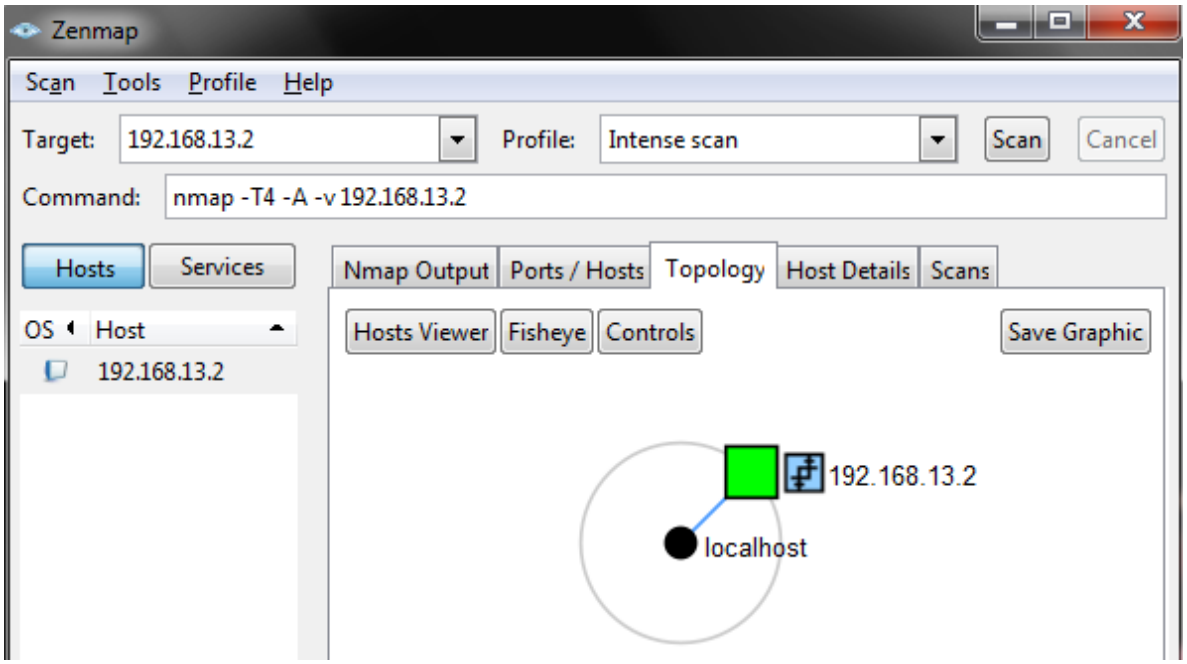


Figura IV.30:Topología Red hasta R1

Autor: "Edgar Zurita"

En la siguiente figura se muestra los resultados obtenidos en el Router PE-R3 el cual está configurado ACLs (Lista de Control de Acceso) y está habilitado la autenticación en el intercambio de rutas para el protocolo BGP.

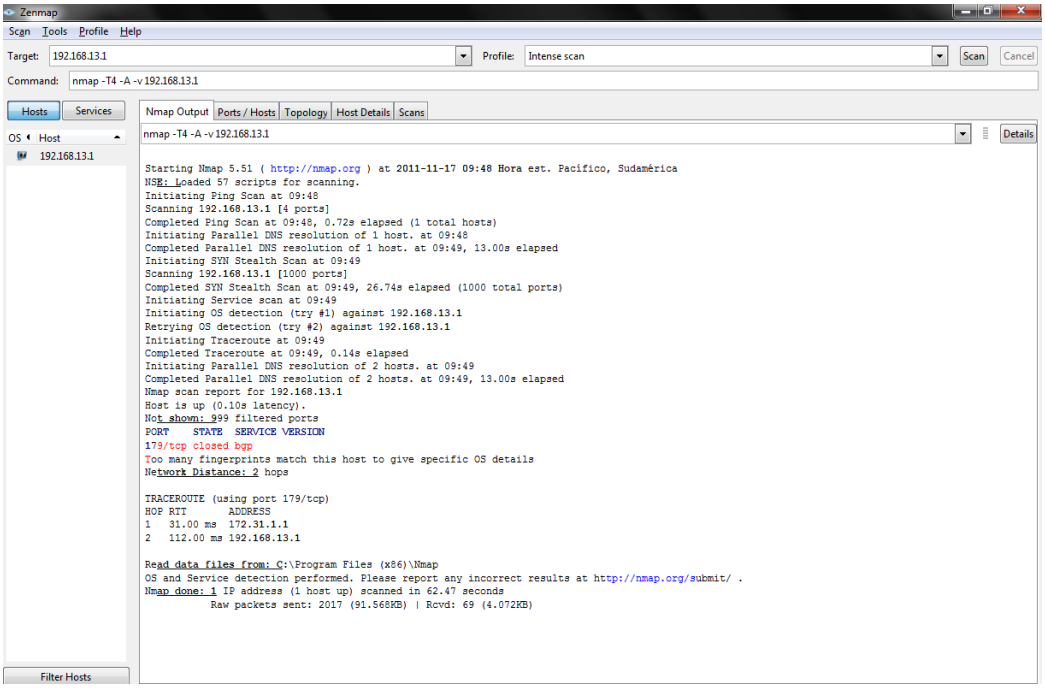


Figura IV.31:Escaneo de Puertos a R3 Interface Serial 1/0

Autor: "Edgar Zurita"

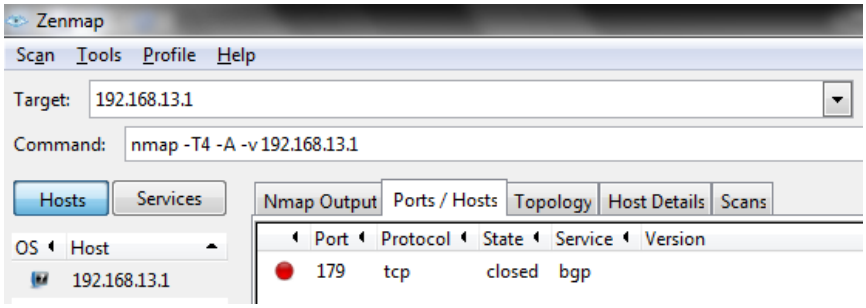


Figura IV.32: Puertos encontrados PE-R3

Autor: "Edgar Zurita"

En dicha imagen podemos observar que se encontró el puerto perteneciente al protocolo BGP.

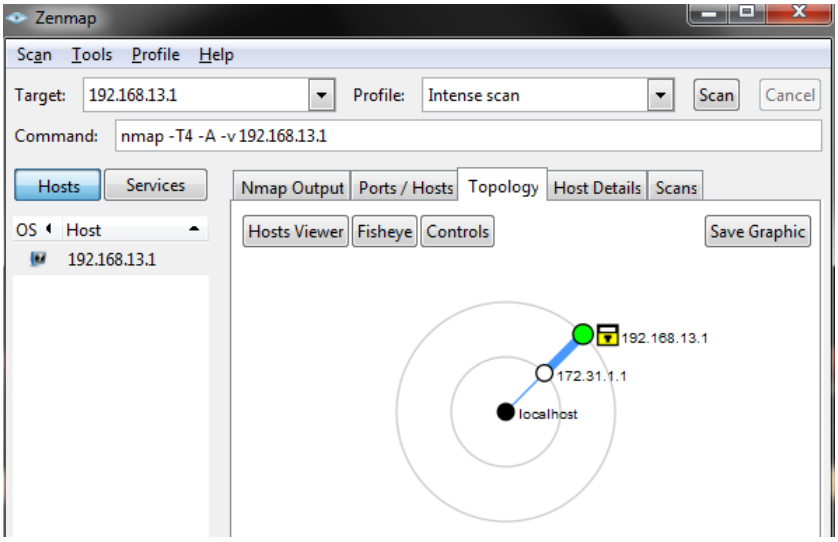


Figura IV.33:Topología Red hasta R3

Autor: "Edgar Zurita"

A continuación se realizó un escaneo de puertos al mismo Router PE-R3 pero esta vez se utilizó la interface Fastethernet 0/0 que pertenece ya al núcleo MPLS.

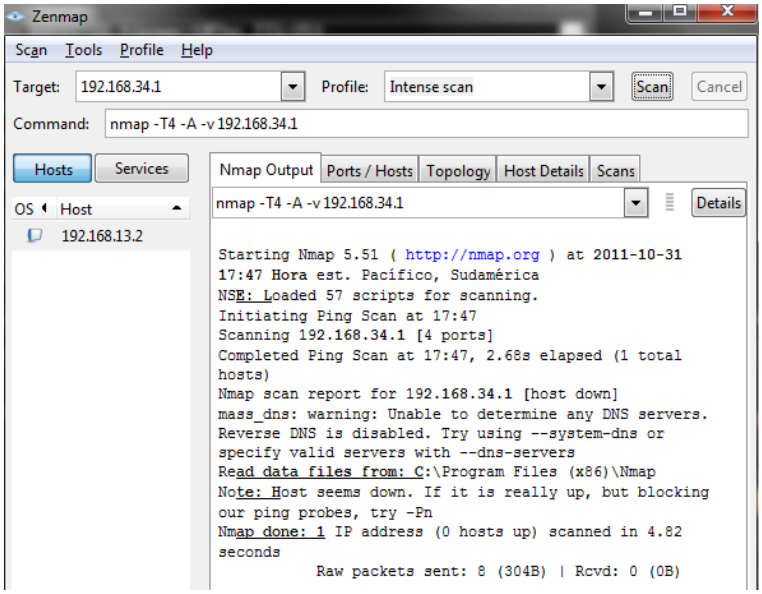


Figura IV.34:Escaneo de Puertos R3 Interface Fastethernet 0/0

Autor: "Edgar Zurita"

En dicho escaneo no se encontraron resultados, con esto podemos confirmar que el núcleo MPLS permanece oculto ante los usuarios de las VPN y es inaccesible desde el exterior.

4.1.2. Captura de Paquetes en la Red MPLS VPN

Con el analizador de tráfico WireShark se realizó la captura de paquetes que circulan dentro del core MPLS VPN en el que se puede observar los distintos protocolos aplicados que conforman la Red.

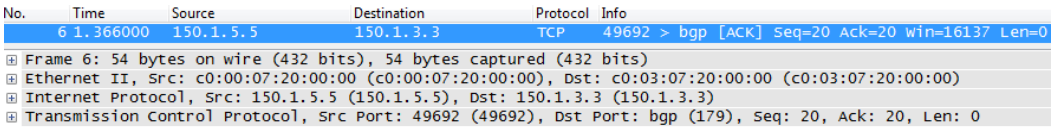


Figura IV.35: Captura de paquetes TCP

Autor: "Edgar Zurita"

BGP

En la imagen siguiente podemos observar la captura del paquete BGP, esta captura se la realizo sin autenticación.

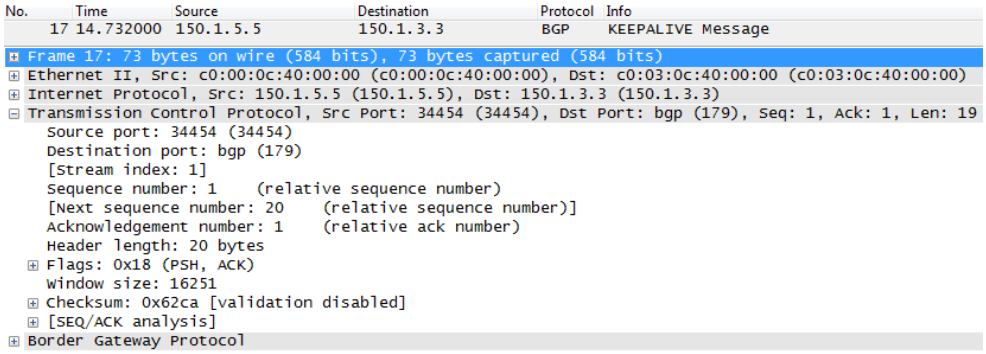
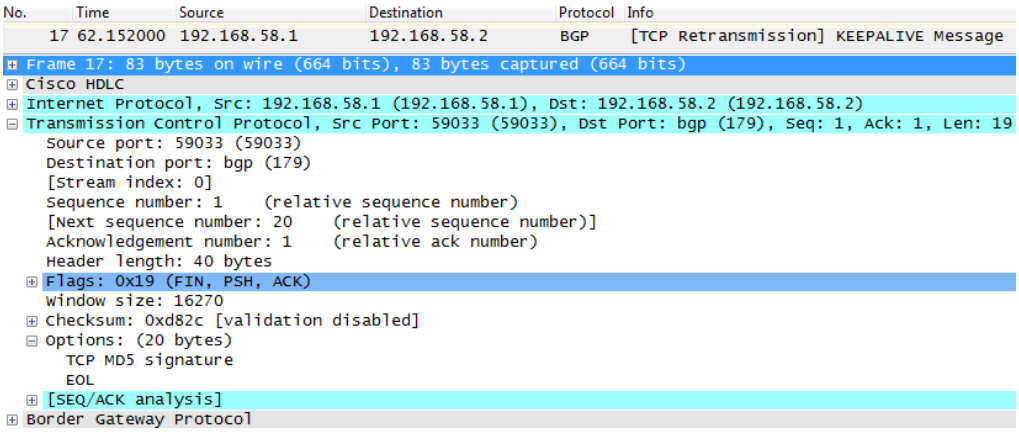


Figura IV.36:Captura de Paquetes BGP

Autor: "Edgar Zurita"

En la imagen siguiente podemos observar la captura del paquete BGP en el cual está incluido MD5, nótese que en TCP aparece un nuevo campo "Options" en la cual se indica dicha autenticación.



FiguraIV.37:Captura de Paquetes BGP con MD5

Autor: "Edgar Zurita"

LDP

Los mensajes MPLS LDP (descubrimiento, sesión, publicidad y los mensajes de notificación) se intercambian entre compañeros del LDP a través de dos canales:

•LDP "mensajes de descubrimiento" son transmitidos como User Datagram Protocol (UDP) al puerto conocido LDP.

•Mensajes de Sesión, publicidad, y la notificación se intercambian a través de una conexión TCP establecida entre dos pares LDP. Estos mensajes pueden ser protegidos contra falsos segmentos TCP con la opción firma TCP MD5.

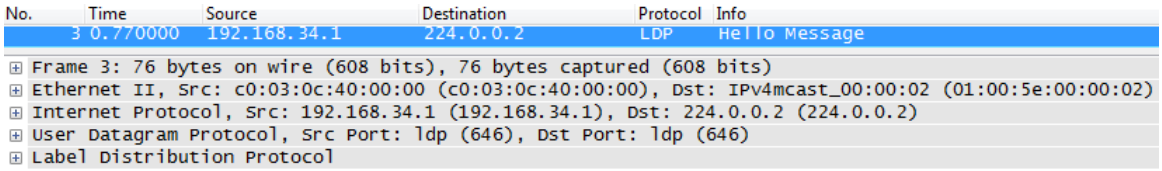


Figura IV.38:Captura de Paquetes LDP

Autor: "Edgar Zurita"

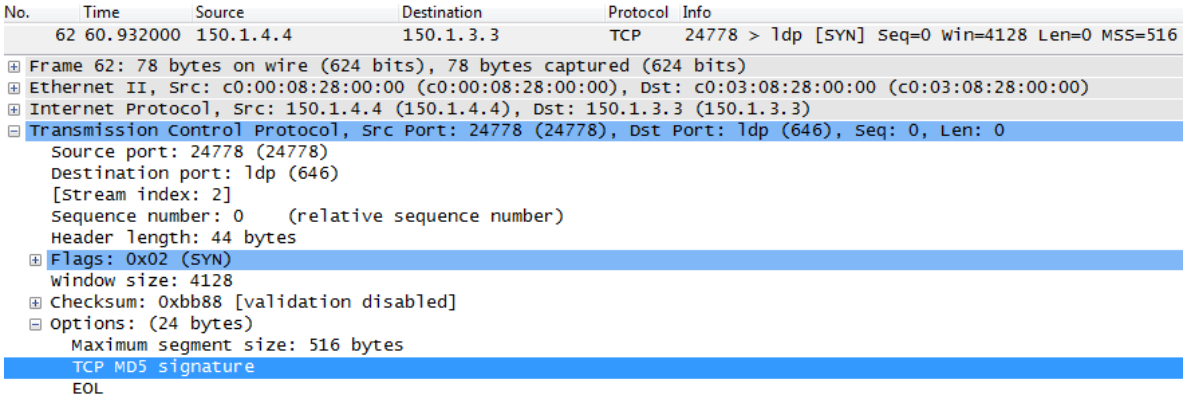


Figura IV.39:Captura de Paquetes LDP con MD5

Autor: "Edgar Zurita"

OSPF

Captura del paquete de OSPF sin autenticación.

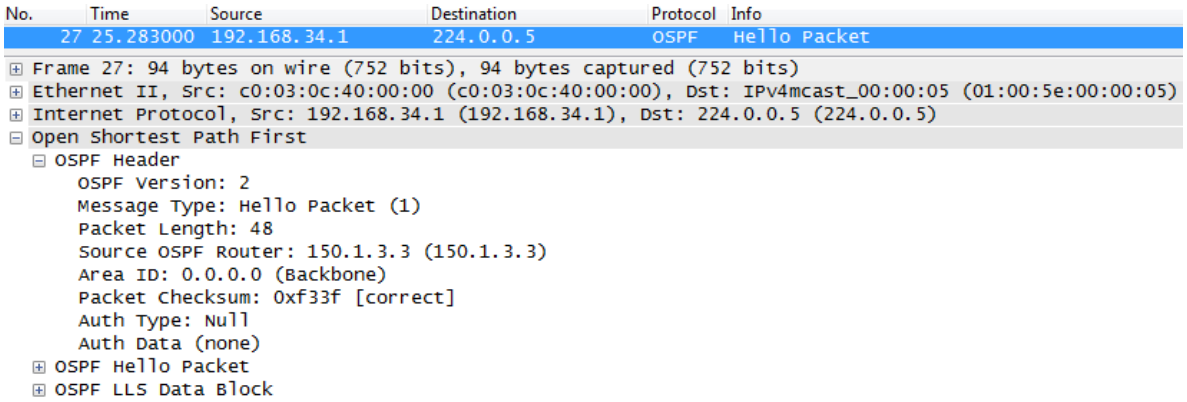


Figura IV.40:Captura de Paquetes OSPF

Autor: "Edgar Zurita"

Se habilito la autenticación de OSPF para intercambiar información de enrutamiento de actualización de una manera segura. La autenticación de OSPF puede ser ninguna (o nulo), simple, o MD5. El método de autenticación "no" significa que no se utiliza la autenticación de OSPF y es el método por defecto. Con la autenticación simple, la contraseña va en texto claro por la red. Con la autenticación MD5, la contraseña no pasa por la red. Cuando se configura la autenticación, debe configurar un área completa por el mismo tipo de autenticación.

En la imagen podemos observar que en la cabecera está habilitada la autenticación MD5.

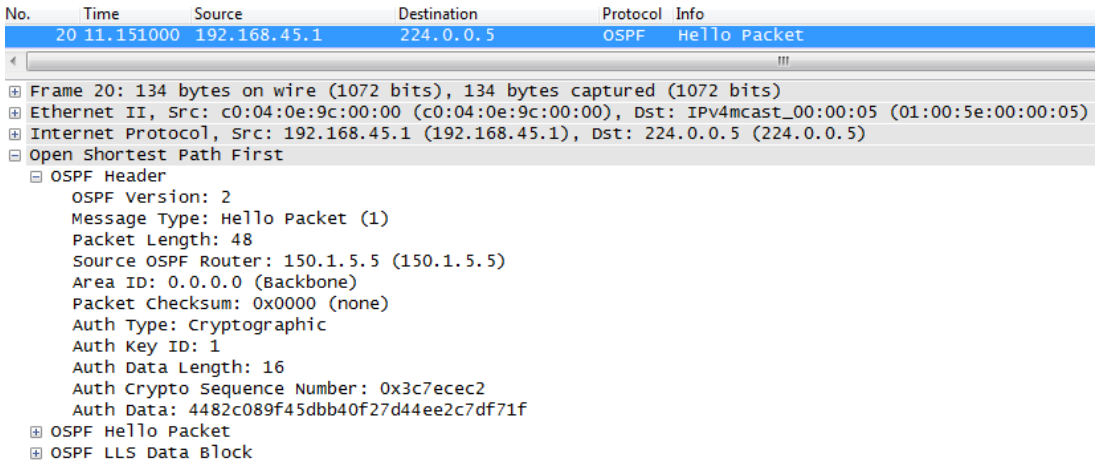


Figura IV.41:Captura de Paquetes OSFP con MD5

Autor: "Edgar Zurita"

IPsec

IPSec es una herramienta que los clientes pueden utilizar, para configurar IPSec basados en VPNs entre los dispositivos de sitio a sitio. Encapsula el

tráfico con cabeceras de los paquetes nuevos, lo que ayuda a garantizar la entrega a destinos específicos. La red es privada porque el tráfico puede entrar en un túnel sólo en un extremo. Además, IPSec proporciona confidencialidad de verdad (encriptación de la información) y puede llevar el tráfico cifrado.

En la captura podemos observar los paquetes de como inicializa el túnel entre los Routers CE-R1 y CE-R8 de los clientes.

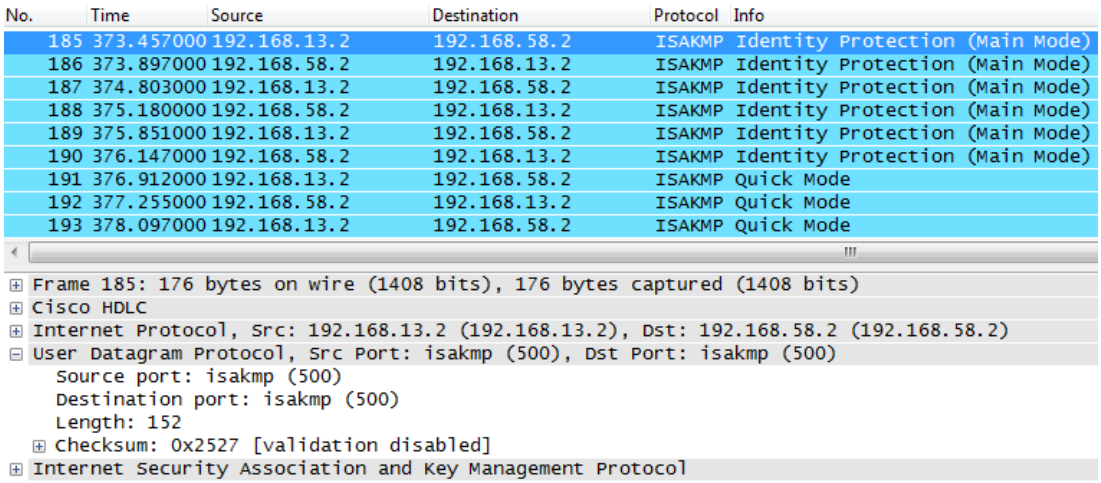


Figura IV.42:Captura de Paquetes IPsec

Autor: "Edgar Zurita"

CAPÍTULO V

GUÍA DE SEGURIDADES CON TECNOLOGÍA MPLS PARA SERVICIO VPN

5.1. Introducción

MPLS permite ofrecer múltiples servicios de transporte de manera virtual (Ethernet, ATM, FR, HDLC, PPP, etc.) con una única red, por lo que ya no es necesario mantener equipamiento y configurar distintas redes. No obstante, en la actualidad su mayor auge viene de la mano de otro servicio, el de redes privadas virtuales (VPN).

La tecnología MPLS está siendo adoptada por la mayoría de los proveedores de servicios de Internet (ISP) ya que les permite reducir costes en la operación de la red y ofrecer a sus clientes SLAs con compromisos reales de

QoS, lo cual se está convirtiendo en una auténtica necesidad con la introducción en las empresas de la VoIP.

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Esta guía cubrirá las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red de acuerdo a los requerimientos del negocio. Se busca también identificar las herramientas o productos tecnológicos que apoyen los controles que permiten mitigar el riesgo y mejorar de esta manera la seguridad en la red.

La seguridad en redes cubre también aspectos como: disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, de tal forma que se propondrá un enfoque integral de acercamiento a la seguridad de la información que viaja por la red. De tal manera que se pueda combinar efectivamente la seguridad de la información en la tecnología MPLS para servicio de VPN. Todo lo anterior conforma una estrategia integrada para la seguridad en la red.

Una empresa que necesita seguridad y gran cantidad de servicios en su red, (voz, datos y video) podría utilizar las dos tecnologías al mismo tiempo, obteniendo una VPN segura y con gran cantidad de servicios. Debido a la gran cantidad de topologías de red, y estructuras internas de cada empresa, la guía de usuario es solamente eso, una guía, no se debe tomar como un manual absoluto, por lo que se recomienda que se busque documentación y ejemplos de configuración del fabricante del equipo a utilizar, como por ejemplo en este caso, cisco.

Como último punto, cabe destacar que ninguna de las tecnologías basadas en VPN puede evitar un ataque desde el interior.

Índice

5.2. Desarrollo de una red VPN MPLS

5.2.1. Configuración del núcleo MPLS: LDP (Label Discovery Protocol)

Cubriremos el protocolo LDP (Label Discovery Protocol) y su interoperación con el protocolo de enrutamiento interior OSPF (que usaremos en el núcleo MPLS).

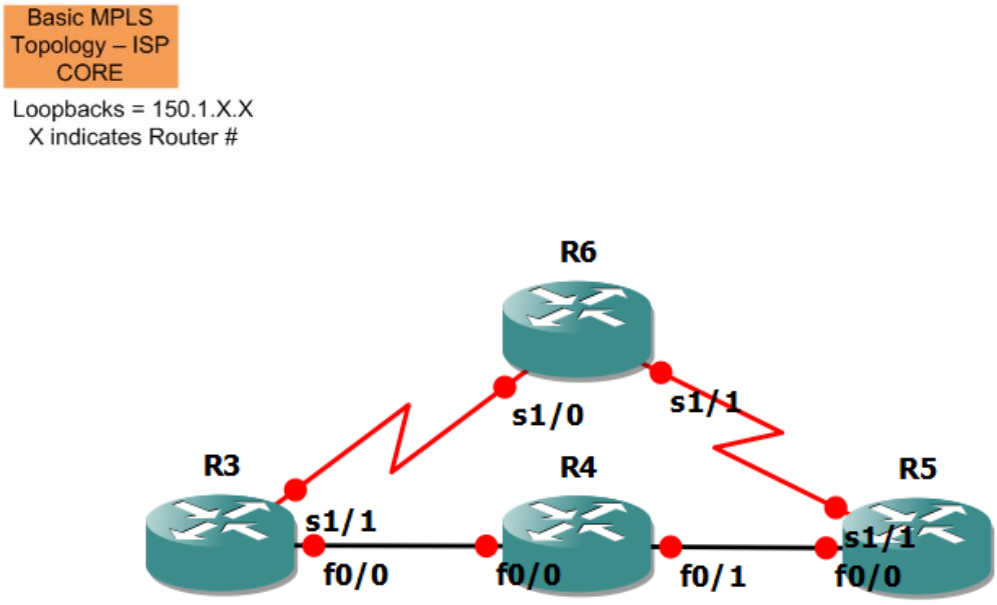


Figura V.43: Topología Básica del Core MPLS de un ISP.

Autor: "Edgar Zurita"

Topología básica del núcleo MPLS de un ISP que identifica cada uno de los puertos usados.

Antes de empezar la configuración de MPLS, debemos acordar cómo va a estar configurado inicialmente nuestro ISP hipotético. El ISP inicialmente estará ejecutando el protocolo de enrutamiento OSPF (IGP) en una sola

área (área 0) y no transportará tráfico de usuario. Con esto pretendemos que dicho ISP apenas está iniciando su operación y que aún no tiene usuarios conectados, por ahora el tráfico es completamente interno. La configuración de los enrutadores es:

R3:

```
hostname R3
        !
ip cef
!
interface Loopback0
ip address 150.1.3.3 255.255.255.255
        !
mpls ip
        !
interface Serial1/1
ip address 192.168.36.1 255.255.255.252
mpls ip
serial restart-delay 0
        !
interface Fa0/0
ip address 192.168.34.1 255.255.255.252
mpls ip
        !
router ospf 100
log-adjacency-changes
```

network 150.1.0.0 0.0.255.255 area 0

network 192.168.36.0 0.0.0.255 area 0

network 192.168.34.0 0.0.0.255 area 0

R4:

hostname R4

!

ip cef

!

interface Loopback0

ip address 150.1.4.4 255.255.255.255

!

mpls ip

!

interface Fa0/0

ip address 192.168.34.2 255.255.255.252

mpls ip

!

interface Fa0/1

ip address 192.168.45.2 255.255.255.252

mpls ip

!

router ospf 100

log-adjacency-changes

network 150.1.0.0 0.0.255.255 area 0

network 192.168.34.0 0.0.0.255 area 0

network 192.168.45.0 0.0.0.255 area 0

R5:

```
hostname R5
 !
ip cef
 !
interface Loopback0
ip address 150.1.5.5 255.255.255.255
 !
mpls ip
 !
interface Fa0/0
ip address 192.168.45.1 255.255.255.252
mpls ip
 !
interface Serial1/1
ip address 192.168.56.1 255.255.255.252
mpls ip
serial restart-delay 0
 !
router ospf 100
log-adjacency-changes
network 150.1.0.0 0.0.255.255 area 0
network 192.168.45.0 0.0.0.255 area 0
network 192.168.56.0 0.0.0.255 area 0
```

R6:

```
hostname R6
 !
ip cef
!
interface Loopback0
ip address 150.1.6.6 255.255.255.255
        !
mpls ip
        !
interface Serial1/0
ip address 192.168.36.2 255.255.255.252
mpls ip
serial restart-delay 0
        !
interface Serial1/1
ip address 192.168.56.2 255.255.255.252
mpls ip
serial restart-delay 0
        !
router ospf 100
log-adjacency-changes
network 150.1.0.0 0.0.255.255 area 0
network 192.168.36.0 0.0.0.255 area 0
network 192.168.56.0 0.0.0.255 area 0
```

Una vez configurado OSPF, podemos revisar la tabla de enrutamiento de R6 para tener una idea del estado de la red.

```
R6#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.45.0/30 is subnetted, 1 subnets
O       192.168.45.0 [110/74] via 192.168.56.1, 00:00:29, Serial1/1
     192.168.56.0/30 is subnetted, 1 subnets
C       192.168.56.0 is directly connected, Serial1/1
     192.168.36.0/30 is subnetted, 1 subnets
C       192.168.36.0 is directly connected, Serial1/0
     192.168.34.0/30 is subnetted, 1 subnets
O       192.168.34.0 [110/74] via 192.168.36.1, 00:00:29, Serial1/0
     150.1.0.0/32 is subnetted, 4 subnets
C       150.1.6.6 is directly connected, Loopback0
O       150.1.5.5 [110/65] via 192.168.56.1, 00:00:29, Serial1/1
O       150.1.4.4 [110/75] via 192.168.56.1, 00:00:29, Serial1/1
                  [110/75] via 192.168.36.1, 00:00:29, Serial1/0
O       150.1.3.3 [110/65] via 192.168.36.1, 00:01:43, Serial1/0
```

Tabla V.V Rutas de R6

Autor: "Edgar Zurita"

En la tabla de enrutamiento podemos verificar que los enrutadores han aprendido sobre la existencia de todas las redes conectadas al núcleo MPLS (incluyendo las direcciones de Loopback) por medio de OSPF, excepto para los enlaces que se conectaran a futuros usuarios. Note también que R6 tiene dos caminos de igual costo hacia la dirección de loopback de R4 (150.1.4.4). Esto pronto tendrá consecuencias.

Para habilitar MPLS en los enrutadores se realizan tres pasos. Primero, MPLS no funcionará si no se habilita CEF, se requiere ejecutar el comando global ip cef en cada enrutador sobre el cual se planee implementar MPLS. Segundo, se requiere habilitar MPLS de manera global por medio del comando mpls ip. Finalmente, se configura el protocolo de distribución de

etiquetas sobre las interfaces conectadas al núcleo MPLS con el fin de habilitar el intercambio de etiquetas entre los enrutadores, esto se hace a través del comando mpls ip pero por cada interface (en el modo de configuración de cada interface). En la mayoría de las redes, se usa LDP como protocolo de distribución de etiquetas. Cisco soporta un viejo propietario denominado TDP (Tag Distribution Protocol), pero es considerado un protocolo heredado (legacy). LDP es el protocolo por defecto en la versión 12.4 o posterior del IOS. De tal suerte que con la configuración anterior hemos habilitado MPLS en todos los enrutadores e interfaces que se conectan al núcleo MPLS. Para verificar la configuración en R6, se usa el comando sh mpls interfaces.

```
R6#show mpls interfaces
Interface              IP            Tunnel   Operational
Serial1/0              Yes (ldp)     No       Yes
Serial1/1              Yes (ldp)     No       Yes
```

Tabla V.VI MPLS interfaces en R6

Autor: "Edgar Zurita"

Una vez completada la configuración de todos los enrutadores conectados al núcleo, podemos verificar que se han establecido las sesiones LDP y que se están comunicando. Usaremos para ello un par de comandos:

```
R6#show mpls ldp discovery
 Local LDP Identifier:
    150.1.6.6:0
    Discovery Sources:
    Interfaces:
        Serial1/0 (ldp): xmit/recv
            LDP Id: 150.1.3.3:0
        Serial1/1 (ldp): xmit/recv
            LDP Id: 150.1.5.5:0
```

Tabla V.VII MPLS ldp discovery en R6

Autor: "Edgar Zurita"

```
R6#show mpls ldp neighbor
    Peer LDP Ident: 150.1.3.3:0; Local LDP Ident 150.1.6.6:0
        TCP connection: 150.1.3.3.646 - 150.1.6.6.46726
        State: Oper; Msgs sent/rcvd: 61/61; Downstream
        Up time: 00:42:09
        LDP discovery sources:
          Serial1/0, Src IP addr: 192.168.36.1
        Addresses bound to peer LDP Ident:
          150.1.3.3       192.168.34.1    192.168.36.1
    Peer LDP Ident: 150.1.5.5:0; Local LDP Ident 150.1.6.6:0
        TCP connection: 150.1.5.5.646 - 150.1.6.6.30329
        State: Oper; Msgs sent/rcvd: 19/19; Downstream
        Up time: 00:07:23
        LDP discovery sources:
          Serial1/1, Src IP addr: 192.168.56.1
        Addresses bound to peer LDP Ident:
          192.168.45.1    150.1.5.5       192.168.56.1
```

Tabla V.VIII MPLS ldp neighbor en R6

Autor: "Edgar Zurita"

Un par de aspectos claves para mencionar. Primero, note el LDP Id en la salida del comando show mpls ldp discovery. Dicha dirección ha sido escogida de manera similar a como se escoge el router-id en la mayoría de protocolos: Se escoge la dirección más alta de la interface de Loopback del enrutador, y si no se tiene ni una interface de Loopback, entonces se escoge la dirección más alta de las interfaces físicas. Lo importante es saber que si dicha dirección no es alcanzable (is not reachable), no se podrá formar la adyacencia LDP. Es decir, hay que asegurarse que dichas direcciones se puedan alcanzar desde los otros equipos vecinos de la red.

Algo más para resaltar es que LDP se comunica usando TCP usando el puerto 646. Esto es importante de recordar en caso de que se tenga alguna medida de seguridad implementada entre enlaces (ACLs, firewalls, etcétera).

Revisemos la LIB y la correspondiente LFIB sobre el enrutador R6:

```
R6#show mpls ip binding
  150.1.3.3/32
        in label:     18
        out label:    imp-null  lsr: 150.1.3.3:0      inuse
        out label:    17        lsr: 150.1.5.5:0
  150.1.4.4/32
        in label:     19
        out label:    16        lsr: 150.1.3.3:0      inuse
        out label:    18        lsr: 150.1.5.5:0      inuse
  150.1.5.5/32
        in label:     20
        out label:    18        lsr: 150.1.3.3:0
        out label:    imp-null  lsr: 150.1.5.5:0      inuse
  150.1.6.6/32
        in label:     imp-null
        out label:    19        lsr: 150.1.3.3:0
        out label:    20        lsr: 150.1.5.5:0
  192.168.34.0/30
        in label:     16
        out label:    imp-null  lsr: 150.1.3.3:0      inuse
        out label:    16        lsr: 150.1.5.5:0
  192.168.36.0/30
        in label:     imp-null
        out label:    imp-null  lsr: 150.1.3.3:0
        out label:    19        lsr: 150.1.5.5:0
  192.168.45.0/30
        in label:     17
        out label:    17        lsr: 150.1.3.3:0
        out label:    imp-null  lsr: 150.1.5.5:0      inuse
  192.168.56.0/30
        in label:     imp-null
        out label:    imp-null  lsr: 150.1.5.5:0
        out label:    20        lsr: 150.1.3.3:0
```

Tabla V.IX MPLS ip binding en R6

Autor: "Edgar Zurita"

```
R6#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     192.168.34.0/30  0          Se1/0       point2point
17     Pop tag     192.168.45.0/30  0          Se1/1       point2point
18     Pop tag     150.1.3.3/32     0          Se1/0       point2point
19     18          150.1.4.4/32     0          Se1/1       point2point
       16          150.1.4.4/32     0          Se1/0       point2point
20     Pop tag     150.1.5.5/32     0          Se1/1       point2point
```

Tabla V.X MPLS forwarding-table en R6

Autor: "Edgar Zurita"

Se han resaltado un par de rutas para ilustrar lo que muestran las tablas. Primero observamos la ruta 192.168.45.0/30. La LIB muestra que los paquetes enviados con destino hacia 192.168.45.0/30, llegaran con una etiqueta (label) marcada con el número 16. Hay dos posibles caminos de salida para dichos paquetes: a través de R3 (LSR Id 150.1.3.3) o a través de R5 (LSR Id 150.1.5.5). R5 ha sido escogido, como lo muestra la notación "in-use". Esto es porque es el mejor camino de acuerdo al protocolo IGP (OSPF). La etiqueta saliente (outgoing tag) es "Imp-null", lo cual significa un valor NULL implícito.

Esto se refiere al hecho de que R6 realmente elimina (POP) la etiqueta antes de enviar el paquete a R5. Esto es llamado eliminación de la etiqueta en el penúltimo salto "Penultimate Hop Popping (PHP)" y es una función habilitada por defecto en los enrutadores Cisco.

En esencia, el enrutador R6 evita que el enrutador R5 tenga que hacer un procesamiento extra (eliminar la etiqueta 16) puesto que la red 192.168.45.0 está directamente conectada a R5. R5 no tendrá que gastar tiempo precioso de CPU para buscar la etiqueta; este solamente recibe el paquete como un paquete normal de nivel 3. Esto también es indicado en la LFIB con "16 Pop tag" como la etiqueta saliente.

También es de interés observar el camino hacia 150.1.4.4/32. Como se puede ver, hay dos caminos hacia la dirección de loopback de R4 con igual costo. Entonces, la LFIB opera de manera similar a la FIB cuando se habilita CEF y permite el balanceo de carga por dichos caminos.

Hasta ahora se ha habilitado MPLS en el núcleo de la red del ISP. Esto es todo respecto a la configuración básica de MPLS. MPLS en si misma solo se torna interesante cuando se corren aplicaciones sobre ella. Una vez se configuran VPNs e Ingeniería de tráfico (Trafic Engineering), se puede ver su poder. Por ahora, se puede pasar a implementar esta red. Experimente con diferentes comandos y logrará mayor entendimiento de cómo opera MPLS.

5.2.2. Configuración de dos VPN MPLS

Hay muchas formas de conseguir que las rutas que conoce el enrutador CE de un usuario específico lleguen a la respectiva tabla VRF del enrutador PE (con el cual se conecta directamente el enrutador CE). Para intercambiar rutas entre un PE y los enrutadores CE que él reciba, podemos usar rutas estáticas, OSPF, RIP, etcétera,. Usaremos BGP puesto que en la vida real dicho protocolo es el de uso más común en las conexiones entre el PE y el CE. Esto también nos evitará tener que redistribuir rutas hacia MP-BGP (MP-BGP va a ser usado posteriormente entre PEs), debido a que cada conexión PE-a-CE es esencialmente una conexión eBGP.

Como primer paso ha que configurar los VRFs en cada enrutador PE. Puesto que cada sucursal tiene su propio número de sistema autónomo o AS. Más exactamente, el usuario B tiene al BGP AS 1 para una de sus sucursales y al BGP AS 8 para la otra sucursal (ver figura). De acuerdo a lo anterior, la convención escogida en el presente ejemplo es usar el valor más bajo de los AS usados por cada usuario para asignarlo a su respectivo RD (1 para el Customer B y 2 para el Customer A).

Con ello la configuración de los VRFs en los enrutadores PE R3, R5 y R6 queda (R4 no requiere de una configuración adicional puesto que desempeña el papel de un equipo P):

R3:

```
ip vrf CustB
description Customer B
rd 1:1
route-target export 1:1
route-target import 1:1
```

R5:

```
ip vrf CustA
description Customer A
rd 2:1
route-target export 2:1
route-target import 2:1
      !
ip vrf CustB
description Customer B
rd 1:1
route-target export 1:1
route-target import 1:1
```

R6:

```
ip vrf CustA
description Customer A
```

rd 2:1

route-target export 2:1

route-target import 2:1

Ahora que se tienen configurados los VRFs en los enrutadores PE, estos VRFs se aplican a las interfaces de cada enrutador PE que esté recibiendo a un enrutador CE, pero teniendo en cuenta al respectivo usuario recibido por cada interface. Algo de notar es que si previamente se ha configurado la dirección IP en estas interfaces, al realizar la aplicación de los VRF sobre ellas, borrará sus direcciones IP y por lo tanto se tendrán que volver a configurar dichos valores. La aplicación de los VRFs y la configuración de las direcciones IP (teniendo en cuenta las figuras) en las interfaces queda:

R3:

interface Serial1/0

ip vrf forwarding CustB

ip address 192.168.13.1 255.255.255.252

R5:

interface Serial1/0

ip vrf forwarding CustA

ip address 192.168.25.1 255.255.255.252

interface Serial1/2

ip vrf forwarding CustB

ip address 192.168.58.1 255.255.255.252

R6:

interface Serial1/2

ip vrf forwarding CustA

ip address 192.168.67.1 255.255.255.252

Podemos verificar que los VRF han sido aplicados de forma correcta de la siguiente manera (en R3 como ejemplo):

```
R3#sh ip vrf CustB
  Name                             Default RD          Interfaces
  CustB                            1:1                 Se1/0
```

Tabla V.XI IP vrf CustB en R3

Autor: "Edgar Zurita"

Después de tener los VRFs configurados y activos, es momento de realizar la configuración BGP.

Empezaremos con la configuración básica de BGP en los enrutadores CE, es decir, en todos los equipos de borde del usuario (R1- con AS 1, R2– con AS 2, R7– con AS 7 y R8– con AS 8.). Note que el núcleo MPLS va a operar internamente con MP-BGP- con AS 101. En nuestro ejemplo, con el objetivo de simplificar la obtención de las redes de los diferentes usuarios por parte de cada PE (un usuario puede tener muchas redes detrás de su equipo CE), tan solo vamos a redistribuir hacia BGP (en cada CE) las rutas de las redes directamente conectadas a los enrutadores CE (esencialmente la red local de cada usuario):

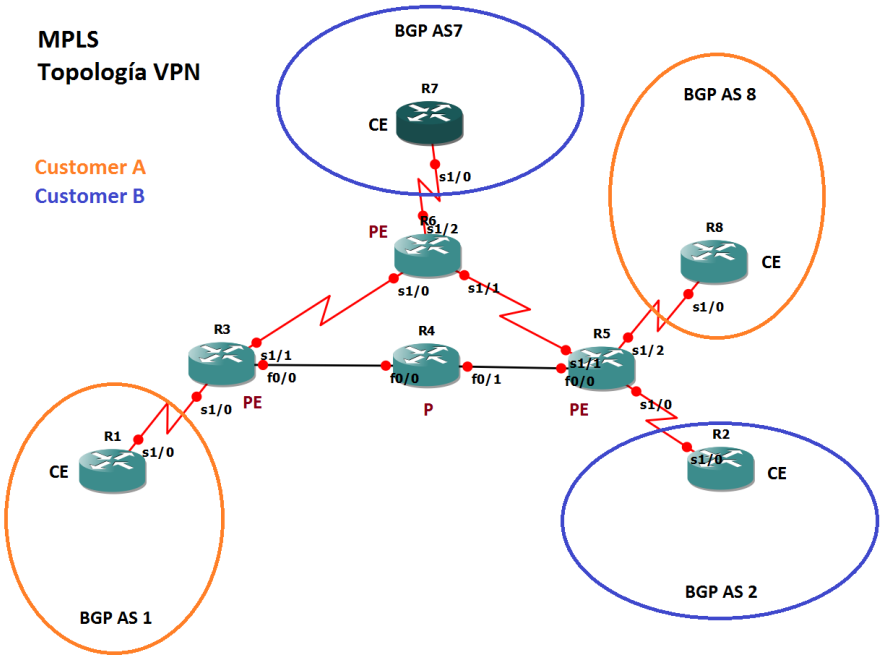


Figura V.44: Topología VPN MPLS que identifica los puertos usados.

Autor: "Edgar Zurita"

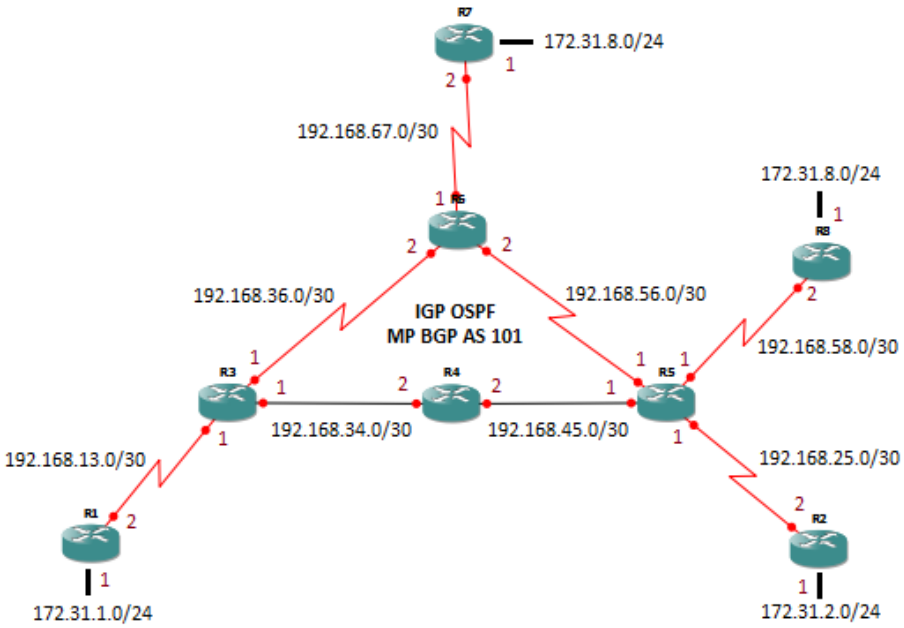


Figura V.45: Topología VPN MPLS que identifica las direcciones IP de las Interfaces.

Autor: "Edgar Zurita"

R1:

```
interface loopback 0
ip address 150.1.1.1 255.255.255.255
interface fastEthernet 0/0
ip address 172.31.1.1 255.255.255.0
interface Serie 1/0
ip address 192.168.13.2 255.255.255.252
router bgp 1
bgp router-id 150.1.1.1
redistribute connected
neighbor 192.168.13.1 remote-as 101
no auto-summary
```

R8:

```
interface loopback 0
ip address 150.1.8.8 255.255.255.255
interface fastEthernet 0/0
ip address 172.31.8.1 255.255.255.0
interface Serie 1/0
ip address 192.168.58.2 255.255.255.252
router bgp 8
bgp router-id 150.1.8.8
redistribute connected
neighbor 192.168.58.1 remote-as 101
no auto-summary
```

R2:

interface loopback 0

ip address 150.1.2.2 255.255.255.255

interface fastEthernet 0/0

ip address 172.31.2.1 255.255.255.0

interface Serie 1/0

ip address 192.168.25.2 255.255.255.252

router bgp 2

bgp router-id 150.1.2.2

redistribute connected

neighbor 192.168.25.1 remote-as 101

no auto-summary

R7:

interface loopback 0

ip address 150.1.7.7 255.255.255.255

interface fastEthernet 0/0

ip address 172.31.8.1 255.255.255.0

interface Serie 1/0

ip address 192.168.67.2 255.255.255.252

router bgp 7

bgp router-id 150.1.7.7

redistribute connected

neighbor 192.168.67.1 remote-as 101

no auto-summary

Lo que sigue es configurar los enrutadores PE para que formen adyacencias BGP con los enrutadores CE. Pondremos la configuración PE-a-PE y PE-a-CE bajo un solo proceso BGP, de tal manera

que haya un solo aspecto por abordar. Cuando se configura MP-BGP, se requiere modificar la familia-de-direcciones que es IPv4 por defecto (address-family). Lo anterior porque el proceso BGP de los enrutadores PE ahora tendrá que tratar con familias-de-direcciones IPv4 y VPNv4, para ello se requiere aplicar el comando no bgp default ipv4-unicast bajo el modo de configuración de BGP:

R3:

```
router bgp 101
bgp router-id 150.1.3.3
no bgp default ipv4-unicast
neighbor 192.168.13.2 remote-as 1
        !
address-family ipv4 vrf CustB
neighbor 192.168.13.2 remote-as 1
neighbor 192.168.13.2 activate
exit-address-family
```

R5:

```
router bgp 101
bgp router-id 150.1.5.5
no bgp default ipv4-unicast
neighbor 192.168.25.2 remote-as 2
neighbor 192.168.58.2 remote-as 8
        !
address-family ipv4 vrf CustA
neighbor 192.168.25.2 remote-as 2
```

```
neighbor 192.168.25.2 activate
exit-address-family
        !
address-family ipv4 vrf CustB
neighbor 192.168.58.2 remote-as 8
neighbor 192.168.58.2 activate
exit-address-family
```

R6:

```
router bgp 101
bgp router-id 150.1.6.6
no bgp default ipv4-unicast
neighbor 192.168.67.2 remote-as 7
        !
address-family ipv4 vrf CustA
neighbor 192.168.67.2 remote-as 7
neighbor 192.168.67.2 activate
exit-address-family
```

Como se puede ver, la configuración anterior es un poco diferente que la configuración BGP estándar. En primer lugar, se requiere configurar un vecino (neighbor) bajo la configuración general de BGP para establecer la adyacencia con el CE. En segundo lugar, se crea una familia-de-direcciones IPV4 por cada VRF. Bajo cada familia-de-direcciones, se requiere usar de nuevo el comando neighbor para configurar el CE como vecino.

Para verificar que R5 (un enrutador PE) está recibiendo información de sus vecinos R2 y R8 (enrutadores CE) a través de BGP, se usa el comando sh ip bgp vpnv4 all:

```
R5# sh ip bgp vpnv4 all
     BGP table version is 4, local router ID is 150.1.5.5
     Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
     Origin codes: i - IGP, e - EGP, ? - incomplete

          Network          Next Hop            Metric LocPrf Weight Path
     Route Distinguisher: 1:1 (default for vrf CustB)
     *> 150.1.8.8/32      192.168.58.2             0         0      8 ?
     *> 172.31.8.0/24     192.168.58.2             0         0      8 ?
     r> 192.168.58.0/30   192.168.58.2             0         0      8 ?
     Route Distinguisher: 2:1 (default for vrf CustA)
*> 150.1.2.2/32      192.168.25.2             0         0      2 ?
     *> 172.31.2.0/24     192.168.25.2             0         0      2 ?
     r> 192.168.25.0/30   192.168.25.2             0         0      2 ?
```

De la salida anterior observamos que R5 está recibiendo rutas de los usuarios por medio del protocolo eBGP y que dichas rutas están siendo

asociadas con los respectivos VRFs previamente configurados. Mediante el comando sh ip route vrf CustA podemos observar las tablas VRF, usando al usuario A como ejemplo:

```
R5# sh ip route vrf CustA

      Routing Table: CustA

      Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

      E1 - OSPF external type 1, E2 - OSPF external type 2

      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

      o - ODR, P - periodic downloaded static route

      Gateway of last resort is not set

            192.168.25.0/30 is subnetted, 1 subnets

      C        192.168.25.0 is directly connected, Serial1/0

            172.31.0.0/24 is subnetted, 1 subnets

      B        172.31.2.0 [20/0] via 192.168.25.2, 00:10:22

            150.1.0.0/32 is subnetted, 1 subnets
```

B 150.1.2.2 [20/0] via 192.168.25.2, 00:10:22

Como se puede ver, dentro del enrutador R5 las redes de cada usuario están separadas a nivel lógico de las redes de otros usuarios.

Hasta ahora todo pudo resultar muy bien, pero no será de mucha utilidad hasta que se logre que las sucursales de cada usuario del ISP se puedan comunicar mutuamente. Vamos a configurar parejas VPNv4 (VPNv4 peerings) entre los enrutadores PE con el fin de que entre ellos se intercambien rutas VPNv4. Para simplificar las cosas, se creará una malla completa "full mesh" entre todos los enrutadores PE y de esa manera no habrá que preocuparse del reflector de rutas "route reflectors (RR)". Para nuestro caso de ejemplo, esto no será un problema mayor; pero un ISP real definitivamente tendrá que usar reflectores de rutas (RRs). Observe que simplemente por razones de redundancia, en la configuración se está estableciendo la vecindad "peering" a la dirección de loopback0 de cada PE:

R3:

```
router bgp 101
neighbor 150.1.5.5 remote-as 101
neighbor 150.1.5.5 update-source lo0
neighbor 150.1.6.6 remote-as 101
neighbor 150.1.6.6 update-source lo0
        !
address-family vpnv4
neighbor 150.1.5.5 activate
```

neighbor 150.1.5.5 send-community extended

neighbor 150.1.6.6 activate

neighbor 150.1.6.6 send-community extended

exit-address-family

R5:

router bgp 101

neighbor 150.1.3.3 remote-as 101

neighbor 150.1.3.3 update-source lo0

neighbor 150.1.6.6 remote-as 101

neighbor 150.1.6.6 update-source lo0

!

address-family vpnv4

neighbor 150.1.3.3 activate

neighbor 150.1.3.3 send-community extended

neighbor 150.1.6.6 activate

neighbor 150.1.6.6 send-community extended

exit-address-family

R6:

router bgp 101

neighbor 150.1.3.3 remote-as 101

neighbor 150.1.3.3 update-source lo0

neighbor 150.1.5.5 remote-as 101

neighbor 150.1.5.5 update-source lo0

!

address-family vpnv4

neighbor 150.1.3.3 activate

neighbor 150.1.3.3 send-community extended

neighbor 150.1.5.5 activate

neighbor 150.1.5.5 send-community extended

exit-address-family

Con la configuración anterior hemos pretendido formar adyacencias entre enrutadores PE y adicionado la familia-de-direcciones VPNv4. Además de activar la familia-de-direcciones, nos debemos asegurar que la configuración incluya el comando send-community extended. Esto es debido a que como ya lo anotamos, los RT (route targets) se envían dentro de BGP como una comunidad extendida. A continuación tenemos un ejemplo que muestra esto:

```
R5#show ip bgp vpnv4 vrf CustB 150.1.1.1
BGP routing table entry for 1:1:150.1.1.1/32, version 20
Paths: (1 available, best #1, table CustB)
  Advertised to update-groups:
     2
  1
    150.1.3.3 (metric 21) from 150.1.3.3 (150.1.3.3)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/23
```

Tabla V.XII IP bgp vpnv4 vrf CustB 150.1.1.1 en R5

Autor: "Edgar Zurita"

En este punto, se debe tener completa conectividad extremo-a-extremo (end-to-end) entre las redes de cada usuario del ISP. En el siguiente ejemplo, podemos ver las redes del sitio "AS 1" (R1) que pertenecen al usuario B, desde la tabla de enrutamiento del sitio "AS 8" (R8), sitio que también pertenece al usuario B:

```
R8#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/30 is subnetted, 1 subnets
B       192.168.13.0 [20/0] via 192.168.58.1, 00:07:28
     192.168.58.0/30 is subnetted, 1 subnets
C       192.168.58.0 is directly connected, Serial1/0
     172.31.0.0/24 is subnetted, 2 subnets
B       172.31.1.0 [20/0] via 192.168.58.1, 00:07:28
C       172.31.8.0 is directly connected, FastEthernet0/0
     150.1.0.0/32 is subnetted, 2 subnets
C       150.1.8.8 is directly connected, Loopback0
B       150.1.1.1 [20/0] via 192.168.58.1, 00:07:28
```

Tabla V.XIII IP route en R8

Autor: "Edgar Zurita"

5.2.3. Configuraciones Adicionales para mejorar la Seguridad

Propagar el TTL

El tracerouter ya no es una herramienta útil para los clientes, algunos vendors permiten deshabilitar propagar el TTL, se recomienda hacerlo.

```
R1#traceroute 172.31.8.1

Type escape sequence to abort.
Tracing the route to 172.31.8.1

  1 192.168.13.1 360 msec 728 msec 420 msec
  2 192.168.34.2 [MPLS: Labels 17/20 Exp 0] 2728 msec 2576 msec 2816 msec
  3 192.168.58.1 [AS 8] [MPLS: Label 20 Exp 0] 1636 msec 1300 msec 1904 msec
  4 192.168.58.2 [AS 8] 1492 msec 496 msec 516 msec
```

Tabla V.IX Traceroute en R1

Autor: "Edgar Zurita"

R3(config)#no mpls ip propagate-ttl forwarded

R5(config)#no mpls ip propagate-ttl forwarded

R6(config)#no mpls ip propagate-ttl forwarded

```
R1#traceroute 172.31.8.1

Type escape sequence to abort.
Tracing the route to 172.31.8.1

  1 192.168.13.1 576 msec 628 msec 184 msec
  2 192.168.58.1 [AS 8] [MPLS: Label 20 Exp 0] 692 msec 448 msec 452 msec
  3 192.168.58.2 [AS 8] 1520 msec 592 msec 632 msec
```

Tabla V.XV Traceroute en R1 sin propagate-ttl forwarded

Autor: "Edgar Zurita"

LDP

Si los ISP requieren proteger a sus sesiones LDP con una contraseña. Las sesiones LDP no tienen que ser reajustadas. Se utilizará la protección MD5.

R3(config)#mpls ldp neighbor 150.1.4.4 password c1sc0

R3(config)#mpls ldp neighbor 150.1.6.6 password c1sc0

R4(config)#mpls ldp neighbor 150.1.3.3 password c1sc0

R4(config)#mpls ldp neighbor 150.1.5.5 password c1sc0

R5(config)#mpls ldp neighbor 150.1.4.4 password c1sc0

R5(config)#mpls ldp neighbor 150.1.6.6 password c1sc0

R6(config)#mpls ldp neighbor 150.1.3.3 password c1sc0

R6(config)#mpls ldp neighbor 150.1.5.5 password c1sc0

```
R3#show mpls ldp neighbor detail
    Peer LDP Ident: 150.1.6.6:0; Local LDP Ident 150.1.3.3:0
        TCP connection: 150.1.6.6.32935 - 150.1.3.3.646; MD5 on
        State: Oper; Msgs sent/rcvd: 22/21; Downstream; Last TIB rev sent 19
        Up time: 00:09:08; UID: 5; Peer Id 0;
        LDP discovery sources:
          Serial1/1; Src IP addr: 192.168.36.2
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          192.168.36.2    150.1.6.6       192.168.56.2
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 150.1.4.4:0; Local LDP Ident 150.1.3.3:0
        TCP connection: 150.1.4.4.55501 - 150.1.3.3.646; MD5 on
        State: Oper; Msgs sent/rcvd: 11/12; Downstream; Last TIB rev sent 19
        Up time: 00:00:53; UID: 6; Peer Id 1;
        LDP discovery sources:
          FastEthernet0/0; Src IP addr: 192.168.34.2
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          192.168.34.2    150.1.4.4       192.168.45.2
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Tabla V.XVI MPLS ldp neighbor detail en R3

Autor: "Edgar Zurita"

OSPF

Estos son los tres diferentes tipos de autenticación compatibles con OSPF.

Null Authentication Esto también se llama del tipo 0ysignifica que no hay información de autenticación se incluye en la cabecera del paquete. Es el valor por defecto.

Plain Text Authentication Esto también se llama de tipo 1 y usa simples contraseñas de texto claro.

MD5 Authentication Esto también se llama de tipo 2 y utiliza contraseñas MD5 criptográficos.

La autenticación no es necesario establecer. Sin embargo, si se fija, todos los routers de parecen el mismo segmento debe tenerla misma contraseña y el método de autenticación.

Autenticación MD5 ofrece mayor seguridad que la autenticación de texto plano. Este método utiliza el algoritmo MD5 para calcular un valor hash a partir de los contenidos de los paquetes OSPF y una contraseña (o clave). Este valor hash se transmite en el paquete, junto con un identificador de clave y un número de secuencia no decreciente. El receptor, que conoce la misma contraseña, calcula su valor propio hash. Si no hay nada en el mensaje cambia, el valor hash del receptor debe coincidir con el valor hash del remitente que se transmite con el mensaje.

El ID de la llave permite que los routers de referencia múltiples contraseñas. Esto hace la migración de contraseñas fácil y más seguro. Por ejemplo, para migrar de una clave a otra, configurar una contraseña en un identificador de clave diferente y eliminar la primera clave. El número de secuencia previene los ataques de repetición, en el que los paquetes OSPF son capturados, modificada, y se retransmite a un router. Al igual que con la autenticación de texto plano, las contraseñas MD5, no tienen por qué ser el mismo en toda la zona. Sin embargo, es necesario que la misma entre los vecinos.

R3

interface Serial 1/1

ip ospf message-digest-key 1 md5 AREA63

!--- Message digest key with ID "1" and Key value (password) is set as " AREA63".

!

interface fastEthernet 0/0

ip ospf message-digest-key 2 md5 AREA43

!--- Message digest key with ID "1" and Key value (password) is set as " AREA43".

!

router ospf 100

area 0 authentication message-digest -->

!--- MD5 authentication is enabled for all interfaces in Area 0.

R4

interface fastEthernet 0/0

ip ospf message-digest-key 2 md5 AREA43

!--- Message digest key with ID "1" and Key value (password) is set as " AREA43*".*

!

interface fastEthernet 0/1

ip ospf message-digest-key 1 md5 AREA45

!--- Message digest key with ID "2" and Key value (password) is set as " AREA45*".*

!

router ospf 100

area 0 authentication message-digest -->

!--- MD5 authentication is enabled for all interfaces in Area 0.

R5

interface Serial 1/1

ip ospf message-digest-key 2 md5 AREA65

!--- Message digest key with ID "2" and Key value (password) is set as " AREA65*".*

!

interface fastEthernet 0/0

ip ospf message-digest-key 1 md5 AREA45

!--- Message digest key with ID "2" and Key value (password) is set as " AREA45*".*

!

router ospf 100

area 0 authentication message-digest -->

!--- MD5 authentication is enabled for all interfaces in Area 0.

R6

interface Serial 1/0

ip ospf message-digest-key 1 md5 AREA63

!--- Message digest key with ID "1" and Key value (password) is set as " AREA63*".*

!

interface Serial 1/1

ip ospf message-digest-key 2 md5 AREA65

!--- Message digest key with ID "2" and Key value (password) is set as " AREA65*".*

!

router ospf 100

area 0 authentication message-digest -->

!--- MD5 authentication is enabled for all interfaces in Area 0.

```
R6#show ip ospf interface serial 1/0
Serial1/0 is up, line protocol is up
  Internet Address 192.168.36.2/30, Area 0
  Process ID 100, Router ID 150.1.6.6, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.3.3
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Tabla X.XVII IP ospf interface serial 1/0 en R6

Autor: "Edgar Zurita"

```
R6#show ip ospf interface serial 1/1
Serial1/1 is up, line protocol is up
  Internet Address 192.168.56.2/30, Area 0
  Process ID 100, Router ID 150.1.6.6, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.5.5
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 2
```

Tabla X.XVIII IP ospf interface serial 1/1 en R6

Autor: "Edgar Zurita"

R3# debug ip ospf adj

```
R3#debug ip ospf adj
OSPF adjacency events debugging is on
R3#
*Mar  1 01:48:15.015: OSPF: Send with youngest Key 3
*Mar  1 01:48:25.015: OSPF: Send with youngest Key 3
*Mar  1 01:48:35.019: OSPF: Send with youngest Key 3
*Mar  1 01:48:45.023: OSPF: Send with youngest Key 3
*Mar  1 01:48:55.023: OSPF: Send with youngest Key 3
*Mar  1 01:49:05.027: OSPF: Send with youngest Key 3
*Mar  1 01:49:15.031: OSPF: Send with youngest Key 3
```

Tabla V.XIX Debug ip ospf adj en R3

Autor: "Edgar Zurita"

BGP

En realidad, la autenticación MD5 no está en la sesión BGP. La autenticación es el de la sesión TCP. Proporciona un método mediante el cual TCP es capaz de verificar con un mayor grado de certeza que los paquetes al parecer recibió por parte del interlocutor TCP en realidad se originó de los pares TCP. Esto evita que los paquetes que son falsificados en la sesión que se utilicen en forma de paquetes válidos en la sesión, para proporcionar otra capa de seguridad a la sesión de eBGP.

Configuración de un password para autentificar/validar la sesión y los mensajes del peer.

R1:

router bgp 1

neighbor 192.168.13.1 remote-as 101

neighbor 192.168.13.1 password cis

R3:

router bgp 101

!

address-family ipv4 vrf CustB

neighbor 192.168.13.2 remote-as 1

neighbor 192.168.13.2 password cis

exit-address-family

R2:

router bgp 2

neighbor 192.168.25.1 remote-as 101

neighbor 192.168.25.1 password cis

R5:

router bgp 101

!

address-family ipv4 vrf CustA

neighbor 192.168.25.2 remote-as 2

neighbor 192.168.25.2 password cis

exit-address-family

!

address-family ipv4 vrf CustB

neighbor 192.168.58.2 remote-as 8

neighbor 192.168.58.2 password cis

exit-address-family

R8:

router bgp 8

neighbor 192.168.58.1 remote-as 101

neighbor 192.168.58.1 password cis

R6:

router bgp 101

!

address-family ipv4 vrf CustA

neighbor 192.168.67.2 remote-as 7

neighbor 192.168.67.2 password cis

exit-address-family

R7:

router bgp 7

neighbor 192.168.67.1 remote-as 101

neighbor 192.168.67.1 password cis

```
R1#show ip bgp neighbors | include BGP
BGP neighbor is 192.168.13.1,  remote AS 101, external link
  BGP version 4, remote router ID 150.1.3.3
  BGP state = Established, up for 00:05:16
  BGP table version 4, neighbor version 4/0


R1#show ip bgp summary
BGP router identifier 150.1.1.1, local AS number 1
BGP table version is 4, main routing table version 4
3 network entries using 351 bytes of memory
3 path entries using 156 bytes of memory
2/1 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 755 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.13.1    4   101      11      12        4    0    0 00:08:15        0
```

Tabla V.XX IP bgp neighbors en R1

Autor: "Edgar Zurita"

ACLs

Listas de sentencias que se aplican a una interfaz del router.

Indican al router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar.

La aceptación y rechazo se pueden basar en dirección origen, dirección destino, protocolo de capa superior y número de puerto.

R3:

Interface fastEthernet 0/0

Ip Access-group 102 in

access-list 102 permit udp any any eq 179

access-list 102 permit ospf any any

access-list 102 permit tcp any any eq 646

access-list 102 permit udpany any eq 646

Interface serial 1/0

Ip Access-group 105 in

access-list 105 permit icmp any any

access-list 105 permit udp any any eq 179

```
*Mar  1 00:13:33.207: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:13:41.451: %LDP-5-NBRCHG: LDP Neighbor 150.1.4.4:0 (1) is DOWN (Disco
very Hello Hold Timer expired)
*Mar  1 00:14:01.155: %OSPF-5-ADJCHG: Process 100, Nbr 150.1.4.4 on FastEthernet
0/0 from FULL to DOWN, Neighbor Down: Dead timer expired


*Mar  1 00:25:02.959: %BGP-5-ADJCHANGE: neighbor 150.1.5.5 Down BGP Notification
 sent
*Mar  1 00:25:02.959: %BGP-3-NOTIFICATION: sent to neighbor 150.1.5.5 4/0 (hold
time expired) 0 bytes
```

Tabla V,XXI Protocolo bgp

Autor: "Edgar Zurita"

show ip interface

Muestra información de interfaz IP e indica si hay alguna ACL asociada a dicho interfaz.

show access-lists

Muestra el contenido de todas las ACLs definidas en el router.

show access-lists num_o_nombre_ACL

Muestra contenido de ACL específica indicada como parámetro.

```
R3#show access-lists
Extended IP access list 102
    10 permit ospf any any (406 matches)
    20 permit tcp any any eq bgp (483 matches)
    30 permit tcp any any eq 646 (495 matches)
    40 permit udp any any eq 646 (893 matches)
Extended IP access list 105
    10 permit udp any any eq 179
    20 permit icmp any any (20 matches)
    30 permit udp any any eq isakmp
    40 permit tcp any any eq bgp (12 matches)
```

Tabla V.XXII Access-lists

Autor: "Edgar Zurita"

IPsec

IPSec es una herramienta que los clientes pueden utilizar, para configurar IPSec basados en VPNs entre los dispositivos de sitio a sitio. Encapsula el tráfico con cabeceras de los paquetes nuevos, lo que ayuda a garantizar la entrega a destinos específicos. La redes privada porque el tráfico puede entrar en un túnel sólo en un extremo. Además, IPSec proporciona

confidencialidad de verdad (encriptación de la información)y puede llevar el tráfico cifrado.

R1:

```
policy-map FOO
class class-default
shape average 128000
!
crypto isakmp policy 1
        encr 3des
        authentication pre-share
        group 2
crypto isakmp key lanlocal address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile VTI
set transform-set TSET
!
!
interface Tunnel0
ip address 192.168.10.2 255.255.255.0
tunnel source 192.168.13.2
tunnel destination 192.168.58.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI
service-policy output FOO
```

R8:

```
policy-map FOO
class class-default
shape average 128000
!
crypto isakmp policy 1
```

```
        encr 3des
        authentication pre-share
        group 2
crypto isakmp key lanlocal address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10

!
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile VTI
set transform-set TSET
!
!
interface Tunnel0
        ip address 192.168.10.1 255.255.255.0
        tunnel source 192.168.58.2
        tunnel destination 192.168.13.2
        tunnel mode ipsec ipv4
        tunnel protection ipsec profile VTI
        service-policy output FOO
!
```

```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.10.2/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.13.2, destination 192.168.58.2
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "VTI")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3 packets input, 180 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Tabla V.XXIII Interface túnel 0

Autor: "Edgar Zurita"

```
R1#show crypto isakmp sa
dst             src             state          conn-id slot status
192.168.58.2    192.168.13.2    QM_IDLE              1    0 ACTIVE
```

Tabla V.XXIV Crypto isakmp sa

Autor: "Edgar Zurita"

```
R1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 192.168.58.2 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.168.58.2
      Desc: (none)
  IKE SA: local 192.168.13.2/500 remote 192.168.58.2/500 Active
         Capabilities:D connid:1 lifetime:23:54:52
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4607963/3293
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4607963/3293
```

Tabla V.XXV Crypto session detail

Autor: "Edgar Zurita"

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/30 is subnetted, 1 subnets
C       192.168.13.0 is directly connected, Serial1/0
     192.168.58.0/30 is subnetted, 1 subnets
B       192.168.58.0 [20/0] via 192.168.13.1, 01:09:12
C    192.168.10.0/24 is directly connected, Tunnel0
     172.31.0.0/24 is subnetted, 2 subnets
C       172.31.1.0 is directly connected, FastEthernet0/0
B       172.31.8.0 [20/0] via 192.168.13.1, 01:09:12
     150.1.0.0/32 is subnetted, 2 subnets
B       150.1.8.8 [20/0] via 192.168.13.1, 01:09:12
C       150.1.1.1 is directly connected, Loopback0
```

Tabla V.XXVI IP route en R1 con IPsec

Autor: "Edgar Zurita"

```
R1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.58.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.13.2, remote crypto endpt.: 192.168.58.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
     current outbound spi: 0x182478FC(405043452)

     inbound esp sas:
      spi: 0x1D343245(489960005)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607963/3062)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x182478FC(405043452)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607963/3046)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:
```

Tabla V.XXVII Crypto IPsec sa

Autor: "Edgar Zurita"

5.3. SOFTWARE UTILIZADO

5.3.1. GNS3

GNS3 es un simulador gráfico de redes que le permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en él. Hasta este momento

GNS3 soporta el IOS de routers, ATM/Frame Relay/switchs Ethernet y PIX firewalls.

Usted puede extender su red propia, conectándola a la topología virtual.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- Dynagen, un front-end basado en texto para Dynamips
- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes.

Acerca de Dynamips

Dynamips es un emulador de routers Cisco escrito por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200 , y ejecuta imágenes de IOS estándar.

Este tipo de emulador será útil para:

-Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real. Permitirá a la gente familiarizarse con dispositivos Cisco, siendo Cisco el líder mundial en tecnologías de redes.

-Probar y experimentar las funciones del Cisco IOS.

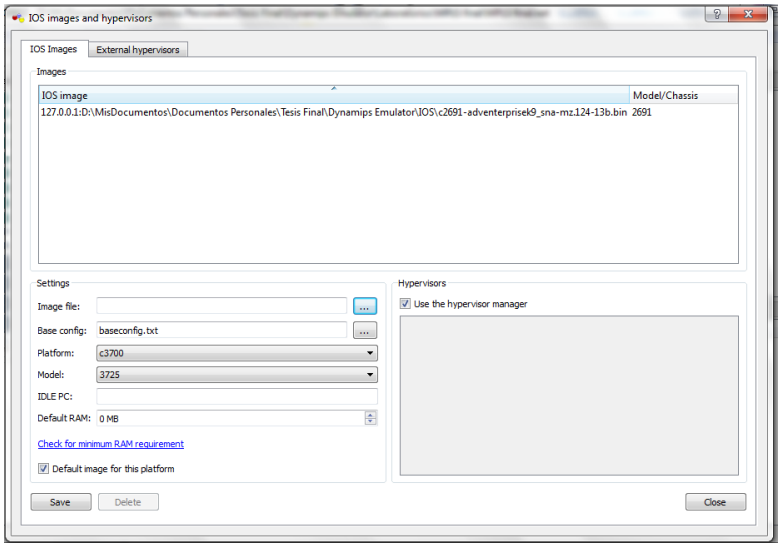
-Verificar configuraciones rápidamente que serán implementadas en routers reales.

-Por supuesto, este emulador no puede reemplazar a un router real, es simplemente una herramienta complementaria para los administradores de redes Cisco.

Así como Dynamips provee un switch virtual simple, no emula switches Catalyst (aunque si emula la NM-16ESW).

Acerca de Dynagen

Dynagen es un front end basado en texto para Dynamips escrito por Greg Anuzelli que provee una separada OOP API utilizada por GNS3 para interactuar con Dynamips. GNS3 también utiliza el formato .INI de configuración e integra la consola de administración de Dynagen que permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar y administrar los valores de idle-pc , realizar capturas, y mucho más.



FiguraV.46: Dynamips

Autor: "Edgar Zurita"

QEMU

QEMU es un emulador de procesadores basado en la traducción dinámica de binarios (conversión del código binario de la arquitectura fuente en código entendible por la arquitectura huésped). QEMU también tiene capacidades de virtualización dentro de un sistema operativo, ya sea GNU/Linux, Windows, o cualquiera de los sistemas operativos admitidos, (de hecho es la forma más común de uso). Esta máquina virtual puede ejecutarse en cualquier tipo de Microprocesador o arquitectura (x86, x86-64, PowerPC, MIPS, SPARC, etc.). Está licenciado en parte con la LGPL y la GPL de GNU.

El objetivo principal es emular un sistema operativo dentro de otro sin tener que reparticionar el disco duro, empleando para su ubicación cualquier directorio dentro de éste.

El programa no dispone de GUI, pero existe otro programa llamado QEMU manager que hace las veces de interfaz gráfica si se utiliza QEMU desde

Windows. También existe una versión para GNU/Linux llamado qemu-launcher. En Mac OS X puede utilizarse el programa Q que dispone de una interfaz gráfica para crear y administrar las máquinas virtuales.

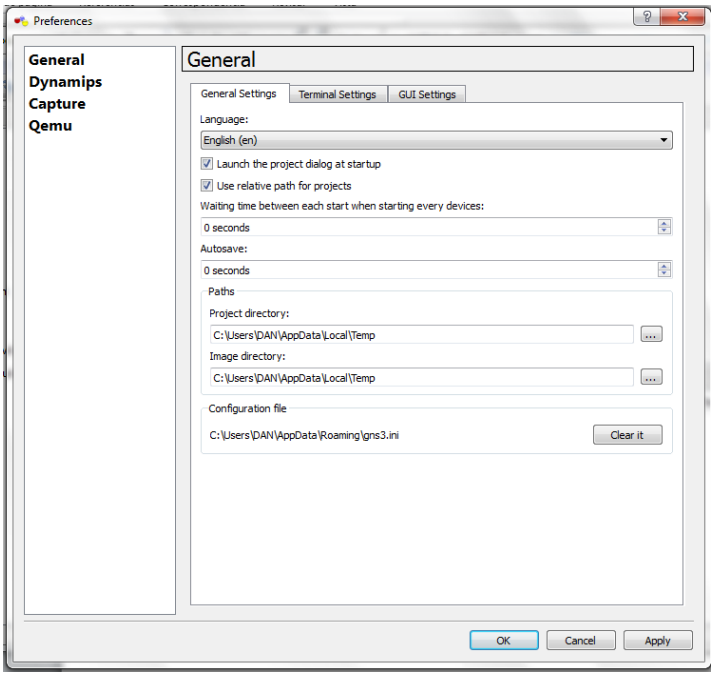


Figura V.47: QEMU

Autor: "Edgar Zurita"

Calculando los valores de Idle-PC

En las simulaciones el consumo de CPU de su sistema alcanza el 100% y permanece allí. Esto se debe a que Dynamips no detecta cuando el router virtual está en estado de idle o cuando está operando realmente.

El comando "idlepc" efectúa un análisis en la imagen que se está ejecutando para determinar cuáles son los posibles puntos en el código que representan un bucle de idle en el IOS. Una vez aplicado, Dynamips "duerme" ocasionalmente al router virtual cuando el bucle idle es ejecutado,

reduciendo significativamente el consumo de CPU del host sin reducir la capacidad del router virtual de realizar sus tareas.

Inicie el router y proceda a una sesión telnet. Si se le presenta la opción de autoconfig del IOS, responda "no".

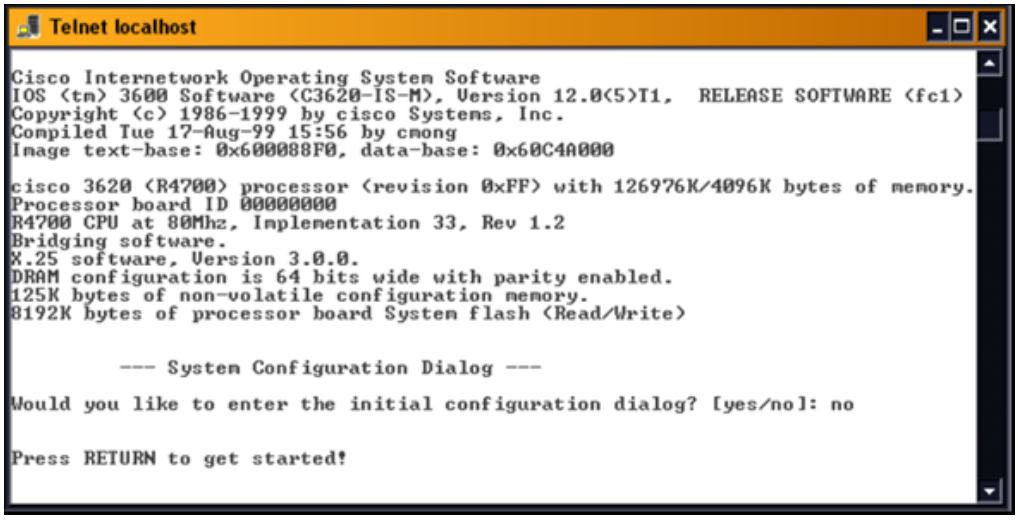


Figura V.48: Sesión Telnet

Autor: "Edgar Zurita"

Espere a que todas las interfaces estén activadas. Luego oprima enter para ver el prompt del IOS.

A continuación, vuelva a GNS3, oprima el botón derecho del mouse sobre el router y seleccione "Idle PC". Vera una pantalla en donde se recolecta una estadística, transcurridos unos 10 a 20 segundos vera una pantalla en donde se lista los valores potenciales de idlepc:

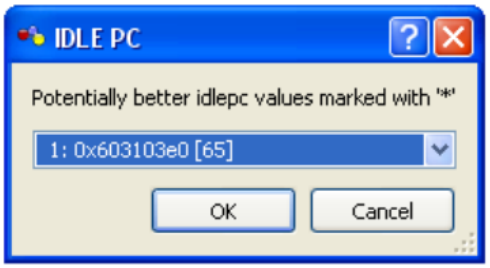


Figura V.49: IDLE PC

Autor: "Edgar Zurita"

Los valores que proveerán mejores resultados se verán marcados con un asterisco. Seleccione y oprima el botón OK. Notara que en su host (aquel en el que se ejecuta el proceso Dynamips) la utilización de CPU caerá drásticamente.

Ingrese exit en la consola de IOS, el consumo de CPU no debería incrementarse.

Si ocurre esto, ha encontrado un buen valor idlepc para un IOS en particular.

Si el uso de CPU no cae, deberá probar con un valor diferente (botón derecho sobre el router, no debe calcular el Idle PC nuevamente) y probar nuevamente estando conectado y también no conectado al router.

Los valores de Idle-PC son particulares a cada imagen IOS. Vararían según la versión de IOS, incluso para IOS de la misma versión pero con diferentes funciones. Por ello los valores de Idle-PC no son particulares para su PC, sistema operativo o versión de Dynamips.

También es posible que Dynamips no encuentre un valor de idlepc para una determinada imagen de IOS, o que el valor elegido no funcione correctamente. Si pasa esto, trate de repetir el proceso. Tal vez no haya tenido suerte con una imagen en particular (sin embargo esta situación es poco usual).

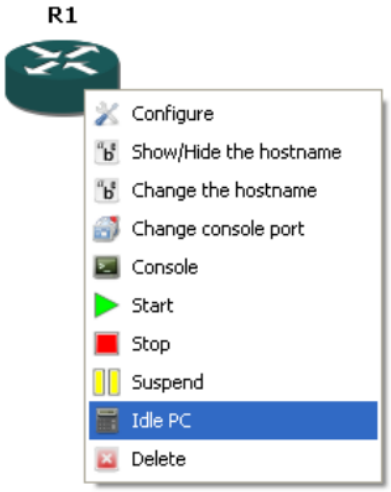


Figura V.50: Calculo de IDLE PC

Autor: "Edgar Zurita"

5.3.2. Programas para poder verificar el funcionamiento de la Red

5.3.2.1. Nmap

Nmap ('Network Mapper') es un programa de código abierto que sirve para efectuar rastreo de puertos, escrito originalmente por Gordon Lyon (más conocido por su alias *Fyodor Vaskovich*). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Características

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como *fingerprinting*).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Aplicaciones típicas

Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar entonces para auditar la

seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte:

Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Instalación en Linux

Siempre que esté basado en Debian o Ubuntu se instala con un simple comando:

sudo apt-get install nmap

Como usar Nmap

La forma más básica de usarlo es escribir en una consola algo como:

nmap 192.168.1.1

Es decir el comando nmap seguido de una ip o dominio. Este uso tan básico solo nos devuelve que puertos están abiertos tras un scan simple. Dependiendo de la seguridad de la ip que se escanee puede que nos bloquee el escaneo si lo hacemos de esa manera. Una forma más discreta de hacerlo que no deja registros en el sistema es así:

nmap –sS 192.168.1.1

Cabe resaltar que existen varios tipos de modificadores de scan lo más importante es lograr identificar la combinación más apropiada, los modificadores que se pueden utilizar para realizar el scan son los siguientes:

sT se intenta hacer un barrido de puertos por TCP la ventaja de esta técnica es que no requiere usuarios privilegiados, opuesto a sS

sU se intenta hacer un barrido de puertos por UDP, es útil cuando se intentan descubrir puertos de nivel superior que pueden estar detrás de un firewall, lenta pero permite hacer auditorias más exactas.

sA se usan mensajes de ACK para lograr que sistema responda y así determinar si el puerto está abierto algunos Firewall no filtran estos Mensajes y por ello puede ser efectivo en algunos casos.

sX puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red

sN puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red

sF puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red

sP este modificador ayuda a identificar que sistemas están arriba en la red (en funcionamiento) para luego poder hacer pruebas más específicas, similar a Ping.

sV intenta identificar los servicios por los puertos abiertos en el sistema esto permite evaluar cada servicio de forma individual para intentar ubicar vulnerabilidades en los mismos.

sO con esta opción se identifica que protocolos de nivel superior a capa tres (Red o Network) responden en el sistema, de esta manera es más fácil saber las características de la red o el sistema que se intenta evaluar.

Adicionalmente a las opciones de scan se pueden especificar opciones que permiten explotar más aun la herramienta, dentro de las opciones que más frecuentemente se usan están las de evitar el Ping o mostrar todos los resultados en pantalla al máximo detalle, veamos cuales son estas opciones:

b Para determinar si la víctima es vulnerable al "bounce attack"

n no hace conversiones DNS para hacer el -sP mas rapido

vv hacer la salida de la herramienta detallada en pantalla

fhabilita la fragmentación de esta forma es mucho más complejo para un firewall u otro tipo de sistema lograr hacer el rastreo.

oN redirige la salida a un archivo

oX redirige la salida a un archivo XML

--stylesheet con esta opción se usa una hoja de estilo que hace más fácil la lectura de la salida en XML

P0 indica que no se debe hacer ping a los sistemas objetivo antes de iniciar el análisis útil para evitar el bloque en algunos Firewall

p se usa para especificar puertos de análisis o rango de puertos.

T se usa para especificar la velocidad general del scan de esta forma se puede pasar inadvertido en algunos sistemas que detectan la velocidad de los paquetes entrantes.

Interfaces gráficas

Para esta herramienta existen un montón de interfaces gráficas, en linux la mayoría se instala con un simple sudo apt-get install así que solo se las voy a nombrar.

Nmapsi4: Interface completa basada en QT.

KNmap: Otra más para KDE basada en QT.

ZenMap: interfaz gráfica oficial para nmap, multiplataforma.

Umit: Otro más y este en español.

NmapFe y otras.

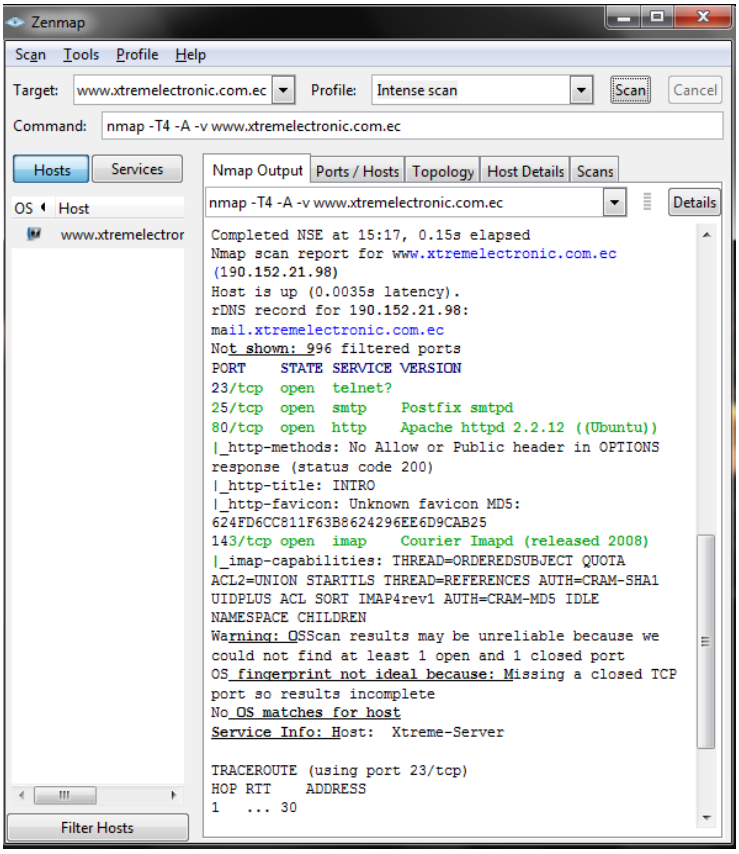


Figura V.51: Interface grafica Zenmap

Autor: "Edgar Zurita"

5.3.2.2. WireShark

ETHEREAL es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. En el argo IT se denominan analizadores de protocolos de red, analizadores de paquetes, *packet sniffer* o *sniffer*. Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

A partir del año 2006 Ethereal es conocido como WireShark y hoy en día está categorizado como uno de los TOP 10 como *sniffer* junto a Nessus y Snort ocupando el segundo lugar entre estos.

Algunas de las características de WireShark son las siguientes:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que WireShark no es un IDS (*Instrusion Detection System*) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Sin embargo, permite a los

profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

Interfaz de Usuario

A continuación se muestra y detalla la interfaz de usuario y como se aplican las principales funciones de WireShark (Capturar, Desplegar y Filtrar paquetes).

Existen dos maneras de iniciar la aplicación una es desde la línea de comando (*shell*) y otra desde el entorno gráfico. Cuando se inicia desde la línea de comando se tiene la posibilidad de especificar opciones adicionales que depende de las funciones que se quieran aprovechar.

La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.

  File, similar a otras aplicaciones GUI este contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.

  Edit, este menú contiene ítems aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.

  View, permite configurar el despliegue de la data capturada.

  Go, contiene ítems que permiten el desplazamiento entre los paquetes.

Capture, para iniciar y detener la captura de paquetes.

Analyze, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.

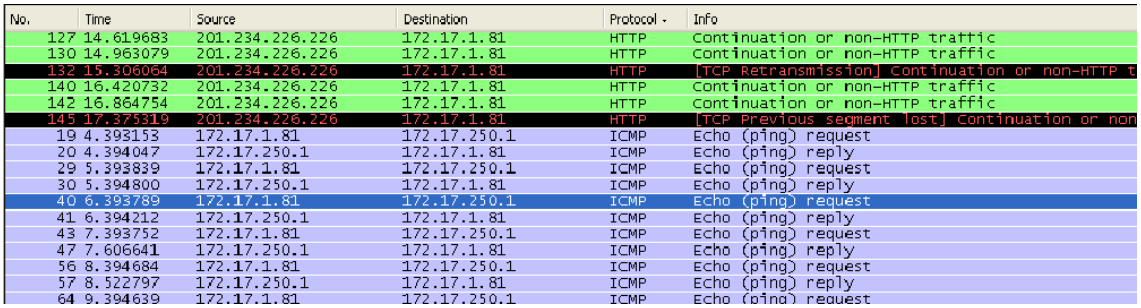
Statistics, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.

Help, menú de ayuda.

- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.

- Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.

- Panel de paquetes capturados, en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.



No.	Time	Source	Destination	Protocol	Info
127	14.619683	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
130	14.963079	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
132	15.306064	201.234.226.226	172.17.1.81	HTTP	[TCP Retransmission] Continuation or non-HTTP t
140	16.420732	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
142	16.864754	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
145	17.375319	201.234.226.226	172.17.1.81	HTTP	[TCP Previous segment lost] Continuation or non
19	4.393153	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
20	4.394047	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
29	5.393839	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
30	5.394800	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
40	6.393789	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
41	6.394212	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
43	7.393752	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
47	7.606641	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
56	8.394684	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
57	8.522797	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
64	9.394639	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request

Figura V.52: Panel de paquetes Capturados

Autor: "Edgar Zurita"

- Panel para detalles del paquete, aquí se despliega información detallada del paquete seleccionado en el panel de paquetes.

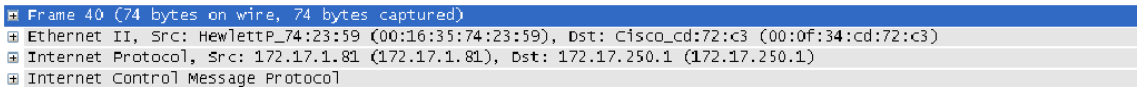


Figura V.53: Panel de detalles del paquete

Autor: "Edgar Zurita"

- Panel de paquetes capturados en bytes, despliega en bytes la información contenida en el campo seleccionado desde el panel de detalles del paquete seleccionado en el panel de paquetes.

- La barra de estado, muestra información acerca del estado actual del programa y de la data capturada.

La interfaz de usuario puede ser cambiada desde el menú principal en la opción de *Preferences* en el menú *Edit*, según sea las necesidades.

Panel de paquetes capturados

Cada línea corresponde a un paquete capturado al seleccionar una de estas, ciertos detalles son desplegados en el resto de los paneles (Detalles y bytes). Y las columnas muestran datos del paquete capturado, Wireshark dispone de una gran cantidad de detalles que pueden agregarse en estas columnas desde el menú *Edit->Preferences*, por defecto se tienen:

- No.: posición del paquete en la captura.

- *Time*: muestra el *Timestamp* del paquete. Su formato puede se modificado desde el menú *View->Time Display Format*.

- *Source*: dirección origen del paquete.

- *Destination*: dirección destino del paquete.
- *Protocol*: nombre del protocolo del paquete.
- Info: información adicional del contenido del paquete.

Panel para detalles de paquetes capturados

Contiene el protocolo y los campos correspondientes del paquete previamente seleccionado en el panel de paquetes capturados. Seleccionando una de estas líneas con el botón secundario del Mouse se tiene opciones para ser aplicadas según las necesidades.

Panel de paquetes capturados en Bytes

En este panel se despliega el contenido del paquete en formato hexadecimal.

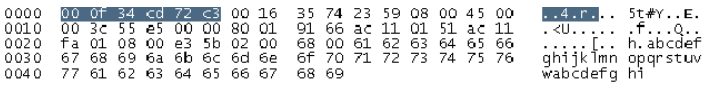


Figura V.54: Panel de paquetes capturados en Bytes

Autor: "Edgar Zurita"

De izquierda a derecha se muestra el *offset* del paquete seguidamente se muestra la data del paquete y finalmente se muestra la información en caracteres ASCII si aplica o "." (Sin comillas) en caso contrario.

Captura de Paquetes

Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

WireShark cuenta con cuatro maneras para iniciar la captura de los paquetes:

1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.

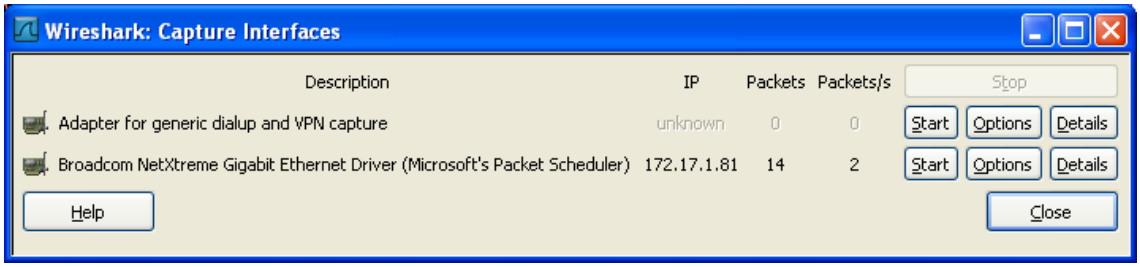


Figura V.55: Ventana Interfaces Locales

Autor: "Edgar Zurita"

Tres botones se visualizan por cada interfaz

- Start, para iniciar
- Options, para configurar

- Details, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.

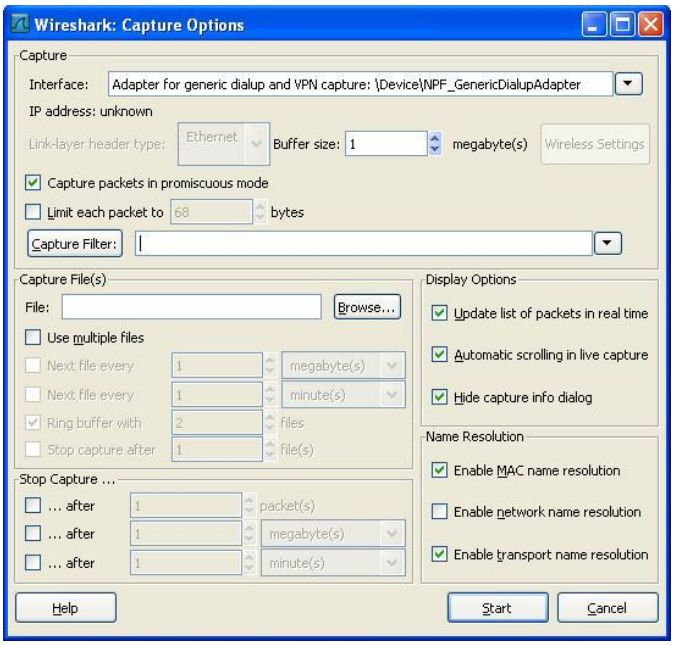


Figura V.56: Opciones de Configuración de la Interface

Autor: "Edgar Zurita"

3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
wireshark –i eth0 -k
```

Donde eth0 corresponde a la interfaz por la cual se desea iniciar la captura de paquetes.

5.4. Alcances y Limitaciones

Todas las configuraciones y pruebas fueron realizadas bajo el emulador GNS3 con el IOS cisco 2691, cabe mencionar que un enlace virtual es más lento y fácilmente congestionable que uno real. GNS3 trabaja conjuntamente con Dynamips y Dynagen, para realizar el "milagro" de la emulación; estos 3 componentes dotan a un PC tradicional de la capacidad de: conectarse vía Telnet a la consola de un router virtual, realizar capturas de los paquetes que pasan por sus enlaces virtuales, trabajar conjuntamente con varios emuladores para repartir su carga de procesamiento y lo más importante, permite la comunicación con equipos reales externos.

Las capacidades de procesamiento óptimas de emulador GNS3 dependen de la cantidad de routers que se desean emular, es decir, se requerirán más recursos de CPU y memoria RAM si se quieren emular topologías con muchos routers.

Obviamente GNS3 posee algunas deficiencias, como la incapacidad de emular ciertas aplicaciones o la falta de soporte a todas las plataformas CISCO disponible en el mercado, pero al ser una aplicación que está en

constante actualización y con gran aceptación en el público, es muy probable que estas carencias se solucionen en un futuro próximo.

5.5. Verificación de la hipótesis

Con el estudio de la tecnología MPLS se desarrolló una guía de seguridades para servicio de VPN comprobándose que la hipótesis es positiva.

La aplicación de las configuraciones que se detallan en dicha guía nos demuestra que existe ocultación del "core" ante los clientes y la separación entre las VPN proporcionada por esta tecnología es total. Únicamente los routers PE que dan acceso a la red MPLS son accesibles de manera directa desde los CE, ya que participan en el intercambio de rutas de la VPN, la solución es la autenticación y/o encriptación para los diferentes protocolos de enrutamiento y la utilización de ACL en toda la frontera, para filtrar las entradas indeseadas.

CONCLUSIONES

- Se redujo los riesgos de posibles vulnerabilidades en seguridad mediante el estudio de la tecnología MPLS (Multiprotocol Label Switching) para servicio de VPN por medio de la guía propuesta comprobándose que la hipótesis es afirmativa.
- A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen características comunes que las hacen menos eficientes frente a la solución MPLS. La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones, plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales, la gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.
- En MPLS la información de las VPNs circula separadamente, esta tarea se hace a nivel lógico gracias a las VRFs que mantienen separadas las direcciones de los diferentes clientes del PE. Esta tecnología ofrece la posibilidad de utilizar todo el rango de direcciones a sus clientes, se puede decir, que no puede un usuario de una VPN atacar al tráfico de otra VPN porque los tráficos se mantienen separados e inaccesibles.

- En MPLS, los elementos del interior del core no conocen ninguna información sobre las VPNs de los usuarios. Además, no se revela al exterior ninguna información sobre los elementos que componen el core. La única información que sí es conocida, es la dirección del PE conectado al CE del cliente. Igualmente, esta información no puede ser utilizada por un atacante para introducirse en el core.
- Hemos podido observar, que es muy difícil atacar MPLS desde el exterior. Evidentemente, existen algunos puntos en que esta tecnología tiene algunos problemas si no se utilizan contramedidas. La solución que comentamos era la utilización de ACL en toda la frontera, para filtrar las entradas indeseadas y la autenticación y/o encriptación para los diferentes protocolos de enrutamiento.
- La red MPLS es una red bastante segura ya que no se permite que los datos entren o salgan del LSP por lugares que no han sido establecidos por el administrador de la red, además, cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores más que por el módulo de envío MPLS, que intercambiará la etiqueta conforme a la tabla de envío del LSR, lo que impide en gran medida que usuarios malintencionados "husmeen" la información.
- MPLS impide los ataques de spoofing, si se consigue atacar una VPN, este ataque siempre permanecería en el interior de la VPN atacada, jamás se podría saltar a otra VPN. Por lo tanto, esta tecnología es resistente a este tipo de ataques.

- Los usuarios que no confíen en la seguridad del core pueden utilizar IPsec para sus conexiones, que ayuda a asegurar la confidencialidad de la información.

RECOMENDACIONES

- Para comprender profundamente una tecnología de nueva generación, es recomendable conocer y tener en claro las funciones de los elementos que son partícipes y que definen la topología de una red (MPLS VPN), teniendo en cuenta además la ubicación que deben tener los mismos.
- Para un cliente que desee entablar sus redes de voz y datos distantes geográficamente, se recomienda que un proveedor de servicios aplique redes privadas virtuales con tecnología MPLS como solución más viable tanto técnica como económicamente en la conexión punto a punto de las sucursales, logrando de esa manera que el cliente sienta que posee los enlaces físicos.
- Una empresa que necesita seguridad y gran cantidad de servicios en su red, (voz, datos y video) podría utilizar las dos tecnologías al mismo tiempo, MPLS para transportar diferentes tipos de tráfico con una VPN segura y con gran cantidad de servicios. Debido a la gran cantidad de topologías de red, y estructuras internas de cada empresa, la guía es solamente eso, una guía, no se debe tomar como un manual absoluto, por lo que se recomienda que se busque

documentación y ejemplos de configuración del fabricante del equipo a utilizar, como por ejemplo en este caso, cisco.

- Como último punto, cabe destacar que ninguna de las tecnologías basadas en VPN puede evitar un ataque desde el interior. Se recomienda la encriptación y autenticación del tráfico de control que ayuda a ello.

RESUMEN

El presente estudio pretende reducir los riesgos de posibles vulnerabilidades en la tecnología "Conmutación Multi-Protocolo mediante Etiquetas" (MPLS) para servicio de Redes Privadas Virtuales (VPN), por medio de una guía propuesta, debido a que la tecnología MPLS está siendo adoptada por la mayoría de Proveedores de Servicios de Internet (ISP) y las grandes compañías que adoptan este servicio necesitan estar seguras de que la información que transmiten, no corra peligro.

Mediante la utilización del método experimental se implementó un escenario de pruebas para identificar posibles vulnerabilidades de seguridad en la tecnología MPLS para servicio de VPN utilizando el software "Simulador de Red Gráfica" (GNS3) para la emulación de los routers.

Se deshabilito en todos los equipos frontera los servicios innecesarios y se estableció Listas de Control de Acceso (ACL) oportunas para evitar que un atacante pueda explotar alguna vulnerabilidad del equipamiento del núcleo "core" y hacerse con el control del mismo, se utilizó también autenticación, encriptación para los diferentes protocolos de enrutamiento. Los usuarios que no confíen en la seguridad del núcleo, pueden utilizar "Seguridad del

Protocolo Internet” (IPsec) para sus conexiones, que ayuda a asegurar la confidencialidad de la información.

El estudio de MPLS comprobó que la separación entre las VPN proporcionada por esta tecnología es total y la ocultación de los equipos del núcleo un hecho. Únicamente los routers del Borde del Proveedor (PE) que dan acceso a la red son accesibles de manera directa desde el Borde del Cliente (CE), ya que participan en el intercambio de rutas de la VPN, Los routers del Proveedor (P) no participan en el intercambio de dichas rutas. Es así que la guía propuesta puede ser usada para dar mayor seguridad al servicio.

Debido a la gran cantidad de topologías de red, y estructuras internas de cada empresa, la guía es solamente eso, una guía, no se debe tomar como un manual absoluto, por lo que se recomienda que se busque documentación y ejemplos de configuración del fabricante del equipo a utilizar.

SUMMARY

The present study tries to reduce the risks of possible vulnerabilities in the technology "Multiprotocol Label Switching" (MPLS) for a service of Virtual Private Network (VPN) by means of a proposed guide, because of the technology MPLS is being adopted by the majority of Internet Service Provider (ISP) and the big companies that adopt this service, need to be sure the information they transmit is not in danger.

By means of the use of the experimental method, a stage of test is implemented to identify possible vulnerabilities of safety in the technology MPLS for a service of VPN by using the software "Graphical Network Simulator" (GNS3) for the emulation of the routers.

Border disabled in all the teams the unnecessary services and Access Control List were established (ACL) opportune to avoid that an attacker can exploit some vulnerability of the team of the nucleus "core", authentication was used also, Encryption for the different protocols of routing. Users, who do not trust in the safety of the nucleus, can use "Internet Protocol Security" (IPsec) for their connections that help to assure information confidentiality.

The study of MPLS verified the separation between the VPN provided by this technology is entire and the concealment of the teams of the nucleus is a fact. Only the routers of Provider Edge (PE) that lead to the network are accessible in a direct way from the router of Customer Edge (CE), since they take part in the exchange of routers of the VPN. The routers of the Provider (P) do not take part in the exchange of the above mentioned routers. It is so the proposed guide can be used to give major safety to the service.

Due to the big quantity of topologies and internal structures of every company, the guide is only a guide and it is not necessary to take it as an absolute manual, therefore it is recommended to be looked papers and examples of the team manufacturer configuration.

GLOSARIO

ATM El Modo de Transferencia Asíncrona (Asynchronous Transfer Mode). Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

ACK Es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

ARP Address Resolution Protocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de enlace responsable de encontrar la dirección hardware (EthernetMAC) que corresponde a una determinada dirección IP.

AES Advanced Encryption Standard, también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado.

BGP Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

CERT Es una empresa de servicios especializados en las áreas de consultoría y educación para la conectividad de redes y telecomunicaciones.

CPU La unidad central de procesamiento, UCP o CPU (por el acrónimo en inglés de central processing unit), o simplemente el procesador o microprocesador, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

CNN Cable News Network (Cadena de Noticias por Cable), mejor conocido como CNN, es una cadena de televisión estadounidense fundada en 1980.

CIR Commited Information Rate. Mínimo de transmisión de datos que garantiza la telefonía a sus usuarios.

CPE El CPE (Equipo Local del Cliente) es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de

servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

CoS "Class of Service", Clase de Servicio. Puede ser clase de servicio de abonado, clase de servicio de línea interurbana o clase de servicio de facilidad privada y referirse a los accesos de origen o de terminación.

DWDM "Dense Wavelength Division Multiplexing", Multiplexación por División en Longitudes de Onda Densas. Es una técnica de transmisión de señales a través de fibra óptica.

DLCI Data Link Connection Identifier.Es el identificador de canal del circuito establecido en Frame Relay. Este identificador se aloja en la trama e indica el camino a seguir por los datos, es decir, el circuito virtual establecido.

DNS Domain Name System o sistema de nombres de dominio es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

DES Data Encryption Standard, es un algoritmo de cifrado, es decir, un método para cifrar información.

DoS Ataque de denegación de servicio, también llamado ataque DoS"Denial of Service", es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea

inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

FR Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.

HDLC "High-Level Data Link Control", control de enlace síncrono de datos, es un protocolo de comunicaciones de propósito general punto a punto y multipunto, que opera a nivel de enlace de datos.

IP Internet Protocol "Protocolo de Internet" o IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

ISO "International Oganization for Standardization", Organización Internacional para la normalización.

ISP Un proveedor de servicios de Internet"Internet Service Provider" es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de

diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

ICMP El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IETF Internet Engineering Task Force (IETF), en españolGrupo Especial sobre Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet.

IPsec IPsec, abreviatura de "Internet Protocol security", 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.

IPX/SPX Delinglés"Internetwork Packet Exchange/Sequenced Packet Exchange", Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare.

MPLS "Conmutación de etiquetas multiprotocolo", siglas de Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes.

MD2 Acrónimo inglés de "Message-Digest Algorithm 2", Algoritmo de Resumen del Mensaje 2, es una función de hashcriptográfica. El algoritmo está optimizado para computadoras de 8 bits.

MD5 En criptografía, MD5, abreviatura de "Message-Digest Algorithm 5", Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Multicast Se trata del envío de Información en una Red a múltiples destinos simultáneamente usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red solo una vez y creando copias cuando los enlaces en los destinos se dividen.

NSP "Network Service Provider". Proveedor de Servicio de Red. Es una compañía que provee servicios de backbone a un ISP (Internet Service Provider), la compañía que muchos usuarios del Web usan como acceso a la Internet.

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon, más conocido por su alias Fyodor Vaskovich. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

LAN Una red de área local, red local o LAN, del inglés "local area network", es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros

LDP "Label Distribution Protocol", Protocolo de distribución de Etiquetas). Es uno de los protocolos de enrutamiento implicito que se utiliza con frecuencia. LDP define el conjunto de procedimientos y mensajes a traves de los cuales los LSRs establecen LSPs en una red MPLS.

L2F El protocolo L2F "Layer 2 Forwarding", se creó en las primeras etapas del desarrollo de las red privada virtual. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas.

L2TP "Layer 2 Tunneling Protocol" fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolosPPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso

telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

OSI El modelo de interconexión de sistemas abiertos, también llamado OSI (en inglésopen system interconnection), es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

PVC Circuito virtual permanente (PVC), es un circuito virtual permanente establecido para uso repetido por parte de los mismos equipos de transmisión.

OSPF Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.

PPTP Point-To-Point Tunneling Protocol (PPTP), es un protocolo de comunicaciones, permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP.

PPP Point-to-point Protocol, es decir, Protocolo punto a punto, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

PDU Las unidades de datos de protocolo, también llamadas PDU (en inglés protocol data unit), se utilizan para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.

POP "Post Office Protocol" Protocolo de Oficina de Correos. Protocolo utilizado para recibir correo electrónico (emails).

PHP Hypertext Pre-processores un lenguaje de programacióninterpretado, diseñado originalmente para la creación de páginas web dinámicas.

QoS Calidad de Servicio"Quality of Service, en inglés" son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

RFC Serie de documentos empleado como medio de comunicación primaria para transmitir información acerca de Internet.

RIP Son las siglas de "Routing Information Protocol", Protocolo de información de enrutamiento. Es un protocolo de puerta de

enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

SYN Es un bit de control dentro del segmento TCP.

Smurf El ataque smurf, es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar (flood) un objetivo (sistema atacado).

SHA "Secure Hash Algorithm", Algoritmo de Hash Seguro, es un sistema de funciones hash criptográficas.

SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL Secure Sockets Layer -Protocolo de Capa de Conexión Segura- (SSL) y Transport Layer Security -Seguridad de la Capa de Transporte- (TLS), su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SLAs Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

TCP Transmission Control Protocol (Protocolo de Control de Transmisión), es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

TTL "Time To Live - Tiempo de Vida". Contador en el interior de los paquetesmulticast que determinan su propagación. Es un campo dentro del protocolo IP que especifica cuántos hops (saltos) puede dar un paquete antes de ser descartado o devuelto.

Unicast Es la comunicación establecida entre un solo emisor y un solo receptor en una Red.

VPI/VCI "Virtual Path Identifier/Virtual Channel Identifier", Identificador de Ruta Virtual/Identificador de Circuito Virtual. Se utiliza para identificar el próximo destino de una celda a medida que atraviesa una serie de switches ATM hasta llegar a su destino. Los switches ATM utilizan los campos VPI/VCI para identificar

el próximo VCL que una celda necesita para transitar hasta su destino final.

VPN Red Privada Virtual, retrata de una o mas WAN entrelazadas sobre una Red Publica compartida normalmente en Internet o en un núcleo estructural de Red IP desde un servicio proveedor de Redes (WSP) que simula el comportamiento de las dedicadas WAN enlazadas sobre líneas.

VoIP Voz sobre Protocolo de Internet, también llamado Voz sobre IP, (por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional.

WWW Web World Wide es un sistema de distribución de información basado en hipertexto o hipermedios enlazados y accesibles a través de Internet.

Wi-Fi (pronunciado en español /wɪfɪ/ y en inglés /waɪfaɪ/) es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec.

WAP Wireless Application Protocol o WAP (protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil.

3DES En criptografía el Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998.

ANEXOS

ANEXO 1

Guía Rápida de Configuración MPLS, BGP de un Router Cisco

Guía Rápida de Configuración MPLS, BGP de un Router Cisco

Este documento describe de forma resumida los principales comandos de configuración de un router Cisco para que pueda trabajar en un dominio MPLS. Cubre también los comandos necesarios para la realización de VPN sobre MPLS.

Configuración de una interfaz loopback

La interfaz de loopback nos servirá para el identificador del router. Una interfaz de loopback se crea de la siguiente manera:

```
cisco# configure terminal

cisco(config)# interface loopback<número de la interfaz>

cisco(config-if)# ip address <dirección IP><máscara>
```

El motivo de configurar una interfaz de loopback es que, como veremos más adelante en la configuración de OSPF y de BGP, asociaremos esta interfaz a los procesos OSPF y BGP, asegurándonos de que no vamos a perder las sesiones OSPF o BGP por un problema físico en el interfaz ya que las interfaces de loopback son interfaces lógicas.

Configuración de una subinterfaz

La creación y configuración de subinterfaces se realiza siguiendo los siguientes pasos:

```
cisco# configure terminal
```

cisco(config)# interface fastethernet<nº interfaz>.<nº subinterfaz>

cisco(config-subif)# encapsulation dot1Q <VLAN ID>

cisco(config-subif)# ip address <dir IP><máscara>

NOTA: Levantar la interfaz física (no shutdown).

Ejemplo:

cisco# configure terminal

cisco(config)# interface fastethernet0/0.100

cisco(config-subif)# encapsulation dot1Q 2

cisco(config-subif)# ip address 192.168.1.1 255.255.255.0

Configuración básica de ospf:

Vamos a configurar OSPF como protocolo de routing dinámico en el futuro backbone MPLS.

Ver el punto de Configuración básica de OSPF.

Recordar que OSPF es un protocolo de routing interno (IGP) del tipo estado de enlace.

Los equipos anuncian toda la información al arrancar el protocolo. Se enviarán entre sí paquetes link state cuando se detectan fallos en algún enlace. Entonces, todos los routers actualizan la base de datos topológica, se copian los link state e inundan a los vecinos.

Por tanto, sólo se van enviando las nuevas actualizaciones de rutas (y no la tabla completa).

Un comando de gran importancia para comprobar las adyacencias OSPF es:

show ip route

Permite ver la tabla de rutas del router donde se ejecuta el comando y si el router aprende las rutas por OSPF.

Verificación del estado de OSPF

Podremos comprobar el estado de OSPF por interfaz así como los vecinos OSPF que tendremos en un interfaz, mediante los comandos siguientes:

show ip ospf interface

show ip ospf neighbors

Configuración básica de bgp:

Antes de configurar MPLS en la red, debemos establecer un full-mesh de sesiones BGP en nuestro backbone y así dejar preparado el escenario de red para la configuración final de MPLS en los routers.

El uso de BGP en un dominio MPLS no es "del todo necesario", ya que se puede implementar una red con funcionalidad MPLS sobre OSPF directamente, el hecho de configurar BGP en un dominio MPLS es para dejarlo preparado por si se quieren crear servicios de redes privadas virtuales sobre MPLS (VPN-MPLS) que sí necesitan la configuración de un protocolo del tipo de BGP para poder ofrecer servicio.

La configuración de BGP requiere los siguientes pasos:

1. Configurar el proceso de routing BGP:

cisco# configure terminal

cisco(config)# router bgp <número de proceso BGP>

El número de proceso BGP que generalmente se pone es el 65000, para entorno de pruebas, ya que hay otras numeraciones que están reservadas, lo que realmente estamos configurando con el comando router bgp <numero de proceso BGP> es el sistema autónomo en el que queremos que se "hable" BGP.

2. Para cada pareja de routers que estén enfrentados hay que configurar lo siguiente:

En uno de los routers especificamos al router vecino y le indicamos que actualice el encaminamiento a través de la interfaz de loopback configurada anteriormente:

cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene

enfrentada> remote-as <número de proceso BGP >

cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene

enfrentada> update-source loopback <número de la interfaz>

NOTA: En el caso de que los routers no estén directamente conectados, la dirección IP que hay que indicar es la de la interfaz de loopback configurada en el otro router para que establezcan relaciones de vecindad.

En el otro router debemos especificar al router vecino con la interfaz de loopback con la que le hemos indicado que actualice el encaminamiento:

> cisco(config-router)# neighbor <dir IP de la interfaz de loopback del vecino> remote-as <número de proceso BGP >

Verificación del estado de BGP

Algunos comandos de interés relacionados con BGP para verificar su funcionamiento, son los siguientes:

1. show ip bgp neighbor

Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como la información relativa a esa relación.

2. show ip bgp summary

Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como el estado en el que se encuentran.

3. clear ip bgp *

Permite resetear las sesiones BGP establecidas.

Configuración básica de mpls

Una vez establecidos los protocolos de routing pasamos a establecer las funcionalidades MPLS en los routers. Para ello hay que arrancar el protocolo de distribución de etiquetas en las distintas interfaces por las que queremos "hablar MPLS".

La configuración de MPLS requiere los siguientes pasos:

1. Configurar el CEF (Cisco Express Forwarding) en todos los routers con funcionalidad "PE" y "P", CEF es el conjunto de funcionalidades que reúnen los equipos Cisco para poder trabajar en un entorno MPLS entre otras funciones.

Los comandos que hay que ejecutar para activar CEF en un router que soporte estas funcionalidades son:

```
cisco# configure terminal

cisco(config)# ip cef
```

Para comprobar si se ha activado CEF correctamente utilizaremos el siguiente comando:

```
show ip cef summary
```

En caso de que no se hubiese habilitado CEF no saldría nada a la salida de este comando.

2. Activación del protocolo de distribución de etiquetas LDP:

Hay que realizar la siguiente configuración en cada interfaz que vaya a hablar MPLS:

cisco(config)# interface <nombre de la interfaz>

cisco(config-if # mpls ip

cisco(config-if)# mpls label protocol ldp

Verificación del funcionamiento de MPLS en la red

Para realizar la verificación del funcionamiento de MPLS, algunos comandos de interés son los siguientes:

1. show mpls interfaces

Muestra las interfaces en las que está funcionando MPLS-LDP.

2. show mpls ldp parameters

Muestra los parámetros que está utilizando el protocolo en el equipo donde se ejecuta el comando.

3. show mpls ldp neighbor

Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando.

4. show mpls ldp binding

Muestra la tabla de etiquetas que está utilizando el router donde se ejecuta el comando.

5. show mpls forwarding-table

Muestra la tabla deforwarding del router donde se ejecuta el comando.

Configuración de VPNs sobre MPLS

La configuración que se detalla a continuación es para crear VPNs en las que el encaminamiento entre los equipos de cliente (CE) y los equipos del proveedor (PE) se realiza de forma dinámica mediante OSPF y la topología que se generará será totalmente mallada (Full-Mesh).

Hay una configuración distinta según estemos trabajando en un equipo de cliente (CE) o en un equipo de proveedor (PE).

Los routers con funcionalidad "CE" van a tener configurado el proceso 255 de OSPF en el área 0 en los enlaces que les unen al backbone MPLS, ya que es el proceso configurado en el backbone. Además, tendrán configurado otro proceso OSPF para las áreas distintas de la cero.

Configuración de equipos con funcionalidad PE

La configuración de VPNs sobre MPLS requiere los siguientes pasos en cada uno de los routers con funcionalidad "PE":

1. Configuración de la VRF asociada a la VPN que vamos a configurar en los routers con funcionalidad "PE":

Una VRF (VPN routing and forwarding) incluye las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN.

Los parámetros necesarios para crearla son:

Route Distinguisher (RD) que permite identificar unívocamente un prefijo de VPN-IPv4.

Route-Target (RT) que identifica los routers que deben recibir la ruta.

cisco# configure terminal

cisco (config)# ip vrf <nombre de la VRF>

cisco(config-vrf)# rd <valor del rd>

cisco(config-vrf)# route-target export <valor que tiene que exportar>

cisco(config-vrf)# route-target import <valor que tiene que importar>

El siguiente comando unifica en uno solo los dos últimos, para indicar que el router donde se ejecuta debe exportar e importar el mismos route-target:

cisco(config-vrf)# route-target both <valor que tiene que importary exportar >

NOTA: Los parámetros "rd" y "route-target" se pueden extraer del dibujo de la VPN en el enunciado de la práctica.

En una topología Hub & Spoke, el sitio que hace de "Hub" debe tener un conocimiento de enrutamiento completo de todos los sitios que pertenecen a la misma VPN. Todo el tráfico destinado a la VPN fluirá a través del sitio Hub. Con este tipo de topología, las sedes que hacen de Spoke

exportan sus rutas al Hub, por lo que el route-target debe cambiar con respecto a una topología Full-Mesh:

En el sitio que hace de Hub:

cisco(config-vrf)# route-target export <valor que tiene que exportar>

cisco(config-vrf)# route-target import <valor que tiene que importar>

En el sitio que hace de Spoke:

cisco(config-vrf)# route-target export <valor que importa el Hub >

cisco(config-vrf)# route-target import <valor que exportar el Hub>

2. Configuración del "forwarding" en las interfaces de los routers "PE" que están enfrentadas a los routers "CE":

cisco# configure terminal

cisco(config)# interface <nombre de la interfaz>

cisco(config-if)# ip vrf forwarding <nombre de la VRF>

3. Asignación de la dirección IP a la interfaz donde acabamos de configurar el "forwarding" dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz.

Después de ejecutar este último comando se mostrará un mensaje indicando que en la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla:

cisco(config-if)# ip address <dirección IP><máscara>

4. Configuración del encaminamiento dinámico en la VRF creada:

- Hay que arrancar un nuevo proceso OSPF dedicado al encaminamiento dentro de la VRF:

cisco# configure terminal

cisco(config)# router ospf <identificador del proceso> vrf <nombre VRF>

- Definir el área en la que se encuentran las interfaces pertenecientes a la VPN:

cisco(config-router)# network <red><wildcard> area 0

Por ejemplo:

cisco(config-router)# network 192.168.43.0 0.0.0.255 area 0

5. Configuración de iMBGP:

Para que los prefijos aprendidos puedan ser transmitidos a los otros equipos PE, hay que configurar iMBGP siguiendo los siguientes pasos:

- Comprobar que los vecinos iBGP siguen activos y operativos. Utilizar el comando show ip bgp summary.

- Nos metemos en la configuración de BGP del router:

cisco# configure terminal

cisco(config)# router bgp <número de proceso BGP que esté configurado>

- Entramos a configurar iMBGP para la VPN:

cisco(config-router)# address-family vpnv4

- Hay que activar los vecinos existentes con la nueva funcionalidad. Según se vayan ejecutando los comandos siguientes se irán reseteando las sesiones

BGP, este comportamiento es normal porque los vecinos renegocian sus "capabilities".

Configurar para cada vecino iBGP mostrado con el comando show ip bgp

summary lo siguiente:

cisco(config-router-af)# neighbor <dir IP del vecino iBGP> activate

cisco(config-router-af)# neighbor <dir IP del vecino iBGP> send-community both

6. Configuración del envío de los prefijos aprendidos al resto de los equipos con funcionalidad PE.

Una vez establecidas las sesiones iMBGP con el resto de equipos PE y verificada la conectividad local con los integrantes de la VPN, queda pendiente propagar los prefijos locales al resto de equipos PE para que éstos sepan encaminar los paquetes hacia dichos prefijos. Para ello, bastará con redistribuir OSPF en el iMBGP:

cisco# configure terminal

cisco(config)# router bgp <número de proceso BGP que esté configurado>

cisco(config-router)# address-family ipv4 vrf <nombre del VRF>

cisco(config-router-af)# redistribute ospf <identificador del proceso OSPF> vrf <nombre del VRF>

NOTA: El identificador del proceso OSPF se corresponde con el identificador del proceso OSPF que hemos utilizado para configurar el encaminamiento dinámico en la VRF en el paso 4.

7. Configuración del envío de los prefijos aprendidos a los equipos con funcionalidad CE:

cisco# configure terminal

cisco(config)# router ospf <identificador del proceso OSPF> vrf <nombre del VRF>

cisco(config-router)# redistribute bgp <número de proceso BGP que esté configurado> subnets metric 20

Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos podremos verificar que la VPN que hemos configurado está funcionando según lo esperado:

1. show ip route vrf <nombre VRF>

Con este comando podremos comprobar los prefijos que se han exportado y los que se han importado en la tabla de routing de la VRF y por ende los prefijos que formarán parte de la VPN.

2. traceroute vrf <nombre VRF><Dirección a la que queremos llegar>

El funcionamiento de este comando es exactamente el mismo que el de un traceroute normal, pero para comprobar el funcionamiento de la VPN y usando direcciones destino de la propia VPN, con origen un equipo que pertenezca a la misma VPN necesitamos añadir el parámetro vrf junto al nombre de la vrf que pertenece a nuestra VPN.

3. ping vrf <nombre VRF><Dirección a la que queremos llegar>

El funcionamiento es exactamente el mismo que el de un ping normal, la explicación del uso del parámetro vrf se aplica exactamente igual que en el comando anterior.

BIBLIOGRAFÍA

1. **AMENAZAS LÓGICAS**

   http://www.cert.org.Capítulo 6- Página 71

   2011/01/15

2. **ACL**

   http://equipe.nce.ufrj.br/naumann/Cisco/Bridge2-Esp/B2_ACLsamples_Sp.pdf

   2011/08/18

3. **AUTENTICACIÓN OSPF**

   http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml

   2011/07/12

4. **CONCEPTOS GENERALES**

   http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf

   2011/04/15

5. **IPSEC**

http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd8029d629_ps6635_Products_White_Paper.html

2011/09/20

6. **MULTIPROTOCOL LABEL SWITCHING**

http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

2011/04/04

7. **MPLS**

http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

2011/04/24

8. **MPLS VPN**

http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo3.pdf

2011/04/28

9. **MANUAL CONFIGURACIÓN**

http://hondo.diatel.upm.es/manuales/Cisco/Manual%20Corto%20Cisco%20MPLS-BGP-vnp.pdf

2011/05/01

10. **MD5 AUTHENTICATION BETWEEN BGP PEERS CONFIGURATION EXAMPLE**

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b52107.shtml

2011/07/25

11. **NMAP**

http://www.maestrosdelweb.com/editorial/nmap/

2011/08/16

12.LA SEGURIDAD EN NUESTRAS REDES

http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf

2011/02/13

13.LDP MD5

http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sb_md5.html

2011/07/16

14.SEGURIDADES

http://www.segu-info.com.ar/ataques/ataques.htm

2011/02/05

15.PROTOCOLO MÚLTIPLE POR CONMUTACIÓN DE ETIQUETAS

http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf

2011/04/25

16.TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS

http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

2011/01/30