Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA DE IMPLEMENTACIÓN EN POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN *SWITCHES*, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X

Jorge Rodrigo Padilla Diéguez
Asesorado por el Ing. Aníbal Silva De Los Ángeles

Guatemala, septiembre de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE IMPLEMENTACIÓN EN POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN *SWITCHES*, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JORGE RODRIGO PADILLA DIÉGUEZ
ASESORADO POR EL ING. ANÍBAL SILVA DE LOS ÁNGELES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, SEPTIEMBREDE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE IMPLEMENTACIÓN EN POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN *SWITCHES*, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha enero de 2013.

Jorge Rodrigo Padilla Diéguez

Guatemala, mayo de 2014

Ingeniero
Carlos Eduardo Guzmán Salazar
Presente

Estimado Ingeniero Guzmán:

Me dirijo a usted, saludándolo e informándole que el estudiante Jorge Rodrigo Padilla Diéguez con carné 2006-10995 el cual desarrollo el trabajo de tesis titulado: PROPUESTA DE IMPLEMENTACIÓN: POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN SWITCHES, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X. Considerando la experiencia que tengo en el campo que comprende el tema titulado y bajo la nominación otorgada por catedráticos de la escuela apruebo el trabajo mencionado para revisión y seguimiento del mismo por la Escuela.

Agradeciendo su amable atención a la presente, me suscribo de usted.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Jose Aníbal Silva De los Angeles

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 22. 2014
Guatemala, 12 de MAYO 2014.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecànica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA DE IMPLEMENTACIÓN: POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN SWITCHES, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X, del estudiante Jorge Rodrigo Padilla Diéguez, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Area Electrónica

sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 23. 2014.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; JORGE RODRIGO PADILLA DIÉGUEZ titulado: PROPUESTA DE IMPLEMENTACIÓN: POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN SWITCHES, POR MEDIO DE AUTENTICACIÓN IEEE 802. 1X, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 3 DE JUNIO 2,014.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.434-2014

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **PROPUESTA DE IMPLEMENTACIÓN EN POLÍTICAS PARA BLOQUEO DE PROTOCOLOS EN *SWITCHES*, POR MEDIO DE AUTENTICACIÓN IEEE 802.1X,** presentado por el estudiante universitario: **Jorge Rodrigo Padilla Diéguez** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, septiembre de 2014

/cc

ACTO QUE DEDICO A:

Dios	Por darme la vida, salud y permitirme estudiar esta carrera.
Mi madre	Por ser un ejemplo de estudio, vida y una inspiración para alcanzar más logros.
Mi padre	Por su ayuda económica recibida durante la carrera.
Mi novia	Por su apoyo y paciencia en lo que a estudios respecta.
Mis hermanos	Por su cariño y apoyo.
Mi asesor	Por la asesoría brindada en la elaboración del presente trabajo.
Mis compañeros	Por la perseverancia y apoyo en la carrera.
Mi familia	Por el cariño recibido.
Facultad de Ingeniería	Por permitirme cursar la carrera y tener una formación profesional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Ghz	Giga Hertz
Kbit	Kilo bit
Mbit	Mega bit
Mhz	Mega Hertz

GLOSARIO

Acknowledge	Acuse de recibo o *acknowledge* es un término que se utiliza para acusar de recibo un segmento de TCP dentro de una red.
Backbone	Ruta con más ancho de banda y de alta disponibilidad dentro de una red.
Beacon	Tramas que utiliza la red WLAN para comunicar su presencia.
Binario	Sistema de numeración en el que las cifras se representan únicamente por medio de dos cifras el 0 y el 1.
Bit	Dígito binario, y es representado por un cero o un uno. Que en su representación electrónica quiere decir un valor de voltaje o la ausencia del mismo, podría representar también un valor de voltaje positivo o un voltaje negativo, respecto un punto de referencia.
CAPEX	El término CAPEX por sus siglas significa capital expenditures, y se utiliza para compras o inversiones

	de activos para una empresa los cuales tienen un tiempo de vida útil. Los CAPEX se utilizan también para mejorar activos existentes como ejemplo se pueden mencionar: equipamientos, propiedades o edificios industriales.
CIDR	Ruteo entre dominios sin clase, se creó para poder tener protocolos de enrutamiento dinámico que no tomen en cuenta las clases del direccionamiento IPV4.
CLI	CLIComand Line Interface permite ingresar instrucciones por medio de un método de texto plano, estos pueden emplearse interactivamente en entradas de texto y puede leer comandos desde un archivo de configuración.
CPU	Unidad central de procesos encargada de todas las instrucciones que debe ejecutar un ordenador o dispositivo electrónico. Interpreta instrucciones contenidas en programas y ejecuta los datos para lograr alguna función en específico.
Daemon	De su traducción al español quiere decir demonio, es utilizado en sistemas UNIX y LINUX. Hace referencia a un proceso informático que no es controlado por el usuario es decir se ejecuta en segundo plano.
DSSS	Espectro de dispersión de secuencia directa, es la técnica de modulación utilizada por IEEE 802.11b y IEEE 802.11g.

OFDM	Multiplexación por división de frecuencias octagonales, tipo de modulación que tiene tasas mayores a DSSS.
EAP	*Extensible authentication protocol*, es un protocolo destinado a la autenticación de usuarios en una red.
EAPOL	EAP over LAN, el protocolo está definido en el estándar 802.1X para adaptar las comunicaciones de EAP sobre redes LAN. Para poder lograrlo EAPOL provee campos adicionales en el encabezado para crear paquetes especiales.
Extranet	*internetwork* extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes. Catálogos e incluso cursos online.
Flash	Memoria que trabaja con base en impulsos eléctricos, permite velocidades superiores a muchas de sus memorias antecesoras, permite la lectura y escritura de información.
Full-Duplex	Método en el cual los dos dispositivos pueden enviar y recibir datos al mismo tiempo
GRE	El GRE es un protocolo de *tunneling* desarrollado por Cisco Systems que puede encapsular una amplia variedad de tipos de paquetes de protocolo dentro de

	túneles IP, lo que crea un enlace virtual punto a punto con los *routers* Cisco en puntos remotos, a través de una *internetwork* IP.
GUIHalf-Duplex	Método en el cual dos dispositivos no pueden enviar y recibir datos al mismo tiempo, mientras un dispositivo envía el otro no puede enviar únicamente recibir.
HDLC	Es el tipo de encapsulación predeterminada en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuito cuando el enlace utiliza dos dispositivos Cisco.
Host	Es un término que se utiliza para referirse a dispositivos finales dentro de una red, estos dispositivos pueden ser: computadoras de escritorio, portátiles, teléfonos IP, tabletas o dispositivos digitales personales.
IEEE 802.1p	Estándar que sirve para priorizar el tráfico en una trama de capa 2.
IEEE 802.1Q	El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto

se logra por medio de la utilización del encabezado de encapsulación 802.1Q.

Internet Interconexión de muchas redes alrededor del mundo, por medio de la cual las personas pueden compartir archivos, música, videos realizar descargas en páginas web.

Intranet Redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales.

Internetwork Una malla global de redes interconectadas (*internetworks*) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo. La *internetwork* más conocida, ampliamente utilizada y a la que accede el público en general es internet. Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo.

Garantizar la comunicación efectiva a través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos

comúnmente, como también la cooperación de muchas agencias de administración de redes. Una malla global de redes interconectadas (*internetworks*) cubre estas necesidades de comunicación humanas.

Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo.

La internetwork más conocida, ampliamente utilizada y a la que accede el público en general es internet. Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación efectiva a través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes.

Interfaz

Puertos especializados de un dispositivo de *internetworking* que se conecta con redes individuales. Puesto que los *routers* se utilizan para interconectar redes, los puertos de un *router* se conocen como interfaces de red.

ISP	Proveedor de servicios de internet, puede existir en distintos niveles de acuerda a la jerarquía de proveedores de servicios: nivel 1, nivel 2 y nivel 3.
Kerberos	Es un protocolo de autenticación y permite que dos computadoras en una red insegura puedan identificarse ante la red.
Latencia	Es el tiempo que tarda un paquete en llegar desde un dispositivo hacia otro.
L2TP	Fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP 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
LSP	Paquete de estado de enlace (LSP) que incluye el estado de cada enlace conectado directamente.
Mensajería instantánea	La mensajería instantánea (IM, *Instant messaging*) es una forma de comunicación en tiempo real entre dos o más personas en forma de texto escrito. El texto se transmite mediante computadoras conectadas por medio de una red interna privada o una red pública, como por ejemplo internet.

MD5 Algoritmo de criptografía de 128 bits, el cual se utiliza en mensajes de desafío para dar seguridad a contraseñas.

Modulación Conjunto de técnicas utilizadas como transporte de información sobre una onda portadora, que generalmente es una onda sinusoidal, las técnicas de modulación permiten aprovechar el ancho de banda y hacer las señales menos susceptibles a ruido e interferencia.

NAS Provee servicios de accesos a empresas e implementa mecanismos de seguridad para aquellos que se conectan a una red corporativa. Un NAS es un dispositivo intermediario, entre un usuario y un servidor de autenticación. Este puede ser un *router*, un concentrador VPN, un punto de acceso inalámbrico, un *switch.* Puede ser cualquier dispositivo que maneje credenciales via telnet, ssh, http, EAP. Y luego se autentique hacia un servidor que ejecute RADIUS o TACACS.

NIC Una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo *host*. El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.

NIC inalámbrica El dispositivo que hace que una estación cliente pueda enviar y recibir señales RF es el NIC inalámbrico. Como un NIC ethernet, el NIC inalámbrico, utiliza la técnica de modulación para la que está configurado y codifica un *stream* de datos dentro de la señal RF.

OPEX *Operating Expense*, hace referencia a los gastos operativos que tiene una empresa, en su contraparte con el CAPEX, es el costo de desarrollo que tiene algún bien adquirido.

Podcasting Es un medio basado en audio que originalmente permitía a las personas grabar y convertir audio para utilizarlo con los iPod (un dispositivo pequeño y portátil para reproducción de audio fabricado por Apple). La capacidad de grabar audio y guardarlo en un archivo de computadora no es una novedad. Sin embargo, el *podcasting* permite a las personas difundir sus grabaciones a una vasta audiencia. El archivo de audio se coloca en un sitio web (o blog o wiki) desde donde otras personas pueden descargarlo y reproducirlo en sus computadoras de escritorio o portátiles y en sus iPod.

PoE *Power Over Ethernet* es la capacidad que se tiene para poder alimentar dispositivos, por medio de cables

	de red que transportan datos, por ejemplo el cable UTP categoría 5, 6 y 7. Lo mismo para el cable STP.
PPP	Conexiones punto a punto se utilizan para conectar las LAN a las WAN del proveedor de servicio y para conectar los segmentos LAN dentro de la red empresarial. La conexión punto a punto entre una LAN y una WAN también se conoce como conexión serial o en línea arrendada.Conector o toma en un dispositivo de red en el cual el medio se conecta con un *host* o con otro dispositivo de red.
PPTP	Protocolo desarrollado por Microsoft en conjunto con otras compañías para poder tener un túnel de encapsulación para redes virtuales privadas.
Puerto físico	Conector o toma en un dispositivo de red en el cual el medio se conecta con un *host* o con otro dispositivo de red.
Punto de acceso inalámbrico	Un punto de acceso conecta a los clientes (o estaciones) inalámbricas a la LAN cableada. Los dispositivos de los clientes, por lo general, no se comunican directamente entre ellos; se comunican con el AP. En esencia, un punto de acceso convierte los paquetes de datos TCP/IP desde su formato de encapsulación en el aire 802.11 al formato de trama

	de *Ethernet* 802.3 en la red *Ethernet* conectada por cable.
RAM	Memoria de acceso aleatorio sirve para ejecutar programas en tiempo real, esta no guarda información y se borra al no estar físicamente alimentada.
Rate *shaping*	En momentos de mucha carga almacenar paquetes de baja prioridad en un *buffer* y luego dejarlos salir.
ROI	De sus siglas en inglés *Return on investment* es una razón financiera que compara el beneficio o la utilidad obtenida en relación a la inversión realizada.
ROM	Memoria únicamente de lectura, es una memoria que no puede ser borrada. De sus siglas en inglés *read only memory*.
SDLC	Se le llama SDLC a la forma en que los componentes se van añadiendo o retirando de alguna red de datos, significa System Development Life Ciycle.
Sigtran	Serie de protocolos que permiten transportar señalización de control de telefonía pública SS7 y Q.931 en redes IP sobre el protocolo SCTP.

Stacking	Tecnología que utilizan los *switches*, cuando físicamente se interconectan por un cable para poder administrarse varios como uno solo.
TCO	Es un método de cálculo diseñado para ayudar a los usuarios y empresas a determinar los costos directos e indirectos, relacionados con la compra de equipos o programas informáticos o equipos de red.
Token cards	Tarjetas de red que trabajan con base en la tecnología *token ring*
Toormenta de broadcast	Tormenta en la cual los dispositivos intermediarios se ven afectados en su rendimiento por causa de un *broadcast* masivo, este puede ser provocado por un bucle de capa 2 o una mala configuración de enrutamiento.
TTL	Tiempo de vida o *time to live* es un campo dentro del encabezado IP que sirve para medir el tiempo de vida de un paquete, cada vez que un paquete pasa por un *router* este disminuye el parámetro TTL, con esto se evitan bucles de enrutamiento.
UC	Comunicaciones unificadas es el término que se utiliza hoy en día para tener centralizada mente todas las comunicaciones: voz, video, conferencias, correo

electrónico, mensajería instantánea y colaboración web.

Virtualización Es la creación por medio de software en la que una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento es creado y configurado como si fuera un dispositivo físico real.

VLSM CIDR usa máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo por la clase. Este tipo de asignación permite que el borde de la red/del *host* se produzca en cualquier bit de la dirección. Las redes, a su vez, se pueden subdividir o dividir en subredes cada vez más pequeñas.

Web colaboration Las herramientas de colaboración permiten a las personas trabajar conjuntamente y compartir documentos. Sin las restricciones de ubicación ni huso horario, las personas conectadas a un sistema compartido pueden hablar entre ellos, compartir textos, gráficos y editar documentos en forma conjunta. Con las herramientas de colaboración siempre disponibles, las organizaciones pueden rápidamente compartir información y lograr los objetivos. La amplia distribución de las redes de datos

permite que las personas en ubicaciones remotas puedan contribuir de igual manera con las personas ubicadas en los centros de gran población.

Weblogs Los *weblogs* son páginas web fáciles de actualizar y editar. A diferencia de los sitios web comerciales, creados por expertos profesionales en comunicación, los *blogs* proporcionan a todas las personas un medio para comunicar sus opiniones a una audiencia global sin tener conocimientos técnicos sobre diseño web. Hay *blogs* casi sobre cualquier tema que uno pueda imaginar, y generalmente se forman comunidades de personas a través de autores populares de *blogs*.

Wiki Las wikis son páginas web que un grupo de personas puede editar y visualizar. Mientras un *blog* es más como un diario individual, personal, una wiki es una creación de grupo. Como tal, puede estar sujeta a una revisión y edición más extensa. Al igual que los *blogs*, las wikis pueden crearse en etapas, por cualquier persona, sin el patrocinio de una importante empresa comercial. Existe una wiki pública llamada Wikipedia que se está transformando en un recurso extenso, una enciclopedia en línea de temas contribuidos públicamente.

Las personas y organizaciones privadas también pueden crear sus propias wikis para capturar la información recopilada sobre un tema en particular.

Muchas empresas utilizan wikis como herramienta de colaboración interna. Con internet global la gente de cualquier credo puede participar en wikis y puede agregar sus propias perspectivas y conocimientos en un recurso compartido.

RESUMEN

El presente trabajo de graduación se enfoca en realizar una propuesta para la implementación de políticas de protocolos de red utilizando el estándar IEEE 802.1X, y autenticación en *switches*.

En el primer capítulo se da una vista general de la comunicación a través de la red, componentes que la conforman, tipos de redes, factores que influyen en el rendimiento y buen funcionamiento de la misma.

En el segundo capítulo se explica cómo funciona el estándar de ethernet en los dispositivos de capa dos, como *hubs, switches y bridges.*

En el tercer capítulo se da una vista de cómo la red debe segmentarse, como se interconectan los diferentes dispositivos intermediarios y que protocolos de comunicación utilizan.

El cuarto capítulo explica las principales vulnerabilidades en las redes de datos y redes de VoIP. Denegacion de servicio, ataques a VLAN, Spanning Tree y tormentas de *broadcast*.

El capítulo cinco explica las diferentes técnicas de mitigación convencional y no convencional (políticas), para reducir las amenazas del capítulo cuatro.

En el capítulo seis se realiza un presupuesto para implementar una red segura.

OBJETIVOS

General

Realizar una propuesta para redes seguras con métodos no convencionales que utilicen el estándar IEEE802.1X, forzando dispositivos finales a utilizar protocolos de red establecidos estática o dinámicamente por políticas, roles y perfiles creados en servidores de autenticación del mercado convencional que se comunican con *switches* por medio del estándar, no importando el sistema operativo o tipo el *host* que se conecte a un *switch.*

Específicos

1. Facilitar el proceso a los estudiantes.

2. Dar a conocer las características y componentes más importantes de las redes convergentes, así también los servicios que las mismas utilizan interactuando en una *internetwork*.

3. Diferenciar las capas: control de enlace lógico y control de acceso al medio en una trama de capa dos por medio del estándar de *ethernet.*

4. Conocer los métodos para prevención y detección de colisiones en acceso múltiple por detección de portadoras en una trama de enlace de datos.

5. Presentar las principales diferencias entre consumo de recursos, ancho de banda, facilidad de administración para protocolos de enrutamiento vector distancia y protocolos estado enlace.

6. Listar los beneficios de utilizar enrutamiento estático contra enrutamiento dinámico.

7. Dar a conocer como el protocolo Spanning Tree, ayuda a mitigar bucles y tormentas de *broadcast* a nivel de enlace de datos, creando arboles de topología por medio de un puente raíz.

8. Mostrar las diferentes debilidades que existe a nivel de protocolos TCP/IP, sistemas operativos e infraestructura física que pueden resultar en amenazas estructuradas y no estructuradas.

9. Describir los diferentes tipos de ataques en voz sobre IP, VLAN, denegación de servicio e ingeniería social.

10. Mostrar los beneficios de autenticar usuarios en una red por medio del estándar IEEE 802.1x, RADIUS y TACACS.

11. Explicar las diferencias entre seguridad de dispositivos de capa dos, tres, cuatro y como las políticas por medio el estándar IEEE802.1x unifican la seguridad de las tres capas.

12. Que el trabajo de investigación pueda servir como referencia a cualquier empresa que tenga como finalidad utilizar infraestructura de red para servicios críticos y pueda contar con un presupuesto de referencia acorde al tamaño de la compañía tomando en cuenta el CAPEX, OPEX y TCO.

INTRODUCCIÓN

Autenticar en conjunto con políticas de seguridad para permitir o bloquear protocolos, son métodos que han resultado efectivos y reducen la vulnerabilidad en un porcentaje mucho mayor que los métodos convencionales. Varios métodos para autenticar dispositivos finales como el estándar IEEE 802.1X, autenticación basada en puerto, RADIUS, TACACS pueden utilizarse ya que no todos los *hosts* trabajan de la misma manera. Sin embargo los estándares deben cumplirse.

La calidad de servicio QoS es otro parámetro a tomar en cuenta en las redes actuales, ya que la mayoría de servicios de voz y video se transmiten ya sobre el protocolo de internet. Esto ha reducido los costos de operación y ha hecho que muchas personas puedan trabajar en manera eventual sin estar físicamente en una oficina. Pero es importante que la fidelidad de estos sistemas sea alta para que realmente puedan suplir las necesidades de no estar físicamente, QoS se encarga de este trabajo en conjunto con las políticas de seguridad para hacer una red segura y estable.

En el presente trabajo se encuentra un estudio de los métodos convencionales de seguridad, contra los métodos basados en políticas de seguridad que son métodos nuevos e innovadores, se proporcionará información del mercado actual y las diferentes marcas con un estudio económico y presupuesto de implementación. También se encuentra la definición de ataques DoS, DDoS, VoIP, tormentas de *broadcast*, debilidad en protocolos como TCP/IP y protocolos de enrutamiento con sus ventajas y desventajas.

Todos los métodos presentados están basados en la teoría de redes del modelo OSI, se explica también brevemente el modelo TCP/IP, sin embargo, el

foco central es en el modelo OSI, estándares de IEEE como ethernet, 802.1x, 802.1D (*Spanning Tree*), 802.3at (Power Over Ethernet), 802.1Q(VLAN Tag), y diferentes RFCs.

Cuando una empresa crece de manera muy rápida hay cierto tipo de datos que pueden ser confidenciales o críticos y podrían poner a la empresa en una situación muy complicada o incluso llevarla totalmente a la quiebra si estos estuvieran en las manos equivocadas. Para distintas empresas todo el tráfico de red es importante sin importar los dispositivos (computadoras, tabletas, teléfonos, PDA).

La seguridad en la red es un término indispensable para mitigar la mayor cantidad de ataques que alguna persona mal intencionada y con el conocimiento adecuado pueda provocar. Las listas de control de acceso y autenticación han logrado mitigar muchos ataques, pero no son suficientes para las amenazas que hoy en día se presentan.

El trabajo de investigación explica la teoría elemental de redes que se necesita para poder entender los distintos ataques, la mitigación de los mismos y como realizar una propuesta de implementación.

1. COMUNICACIONES A TRAVÉS DE LA RED

1.1. Definición de red

Una red son múltiples computadoras interconectadas entre ellas que utilizan un sistema de comunicaciones. El objetivo de una red es que las computadoras se comuniquen y compartan archivos. Las redes de datos utilizan hoy en día tecnología digital para poder compartir información entre *hosts*. A medida que los programadores impulsen los límites de lo posible, las capacidades de las redes interconectadas que crean la internet jugarán un papel cada vez más grande en el éxito de cualquier operación.

Las primeras redes de datos estaban limitadas a intercambiar información con base en caracteres entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos a los diferentes tipos de dispositivos. Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona accesos a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

Las redes de datos que fueron una vez el medio de transporte de información de negocio a negocio se rediseñaron para mejorar la calidad de vida de todos. En el transcurso del día, los recursos disponibles en internet pueden ayudarlo a:

- Decidir cómo vestirse al consultar en línea las condiciones actuales del clima.
- Buscar el camino menos congestionado hacia su destino al observar videos de cámaras web que muestran el clima y el tráfico.
- Consultar su estado de cuenta bancario y pagar electrónicamente las facturas.
- Recibir y enviar correo electrónico o realizar una llamada telefónica a través de internet.
- Obtener información sobre la salud y consejos sobre nutrición de parte de expertos de todo el mundo y compartir en un foro esa información o tratamientos.
- Descargar nuevas recetas y técnicas de cocina.
- Enviar y compartir sus fotografías, videos hechos en casa y experiencias con amigos o con el mundo.

Las redes permiten la creación de nuevas formas de entretenimiento, tales como juegos en línea. Los jugadores participan en cualquier clase de competencia en línea que los diseñadores de juegos puedan imaginar. Se compite con amigos y enemigos de todo el mundo como si estuvieran en la misma habitación.

Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para nuestra vida personal y comercial. Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, se confía en una web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común:

- Reglas o acuerdos que rigen la forma en que se envían, dirigen, reciben e interpretan los mensajes.
- Los mensajes o unidades de información que viajan de un dispositivo a otro.
- Un medio para interconectar estos dispositivos, es un medio que puede transportar los mensajes de un dispositivo a otro.
- Dispositivos en la red que intercambian mensajes unos con otros.

La estandarización de varios elementos de la red permite que trabajen juntos el equipo y los dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente, sin tener en cuenta la marca o el fabricante del equipo.

1.1.1. Servicios y redes múltiples

El teléfono tradicional, la radio, la televisión y las redes de datos informáticos tienen su propia versión individual de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para emitir su señal de comunicación particular. Además, cada servicio tenía su propio conjunto de reglas y normas para asegurar la comunicación exitosa de su señal a través de un medio específico.

1.1.2. Redes convergentes

Los avances de la tecnología permiten consolidar estas redes diferentes en una plataforma: una plataforma que se define como una red convergente. El flujo de voz, vídeo y datos que viaja a través de la misma red elimina la necesidad de crear y mantener redes separadas. En una red convergente todavía hay muchos

puntos de contacto y muchos dispositivos especializados, (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común.

Las redes deben admitir una amplia variedad de aplicaciones y servicios, así como también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que internet evoluciona, al igual que las redes en general, se descubre que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

1.1.3. Tolerancia a fallas

La expectativa de que internet está siempre disponible para los millones de usuarios que dependen de ella, requiere una arquitectura de red que está diseñada y creada para ser tolerante a las fallas. Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce la misma. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente, transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Esta es una premisa básica de la arquitectura de las redes actuales.

1.1.4. Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas, para la infraestructura física subyacente y la arquitectura lógica.

El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje, y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar usuarios individuales dentro de una *internetwork*, están permitiendo a internet mantenerse al ritmo de la demanda de los usuarios.

1.1.5. Calidad de servicio

Internet actualmente proporciona un nivel aceptable de tolerancia a fallas y escalabilidad para sus usuarios. Pero las nuevas aplicaciones disponibles para los usuarios en *internetworks*, crean expectativas mayores para la calidad de los servicios entregados. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente, y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide contra la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un tipo único de transmisión, y por lo tanto pueden producir un nivel aceptable de calidad. Los nuevos requisitos para dar soporte a esta calidad de servicio sobre

una red convergente cambia la forma en que están diseñadas y se implementan las arquitecturas de red.

1.1.6. Seguridad

Internet ha evolucionado y ha pasado de ser una *internetwork* de organizaciones educativas y gubernamentales fuertemente controlada, a ser un medio accesible para todos para la transmisión de comunicaciones comerciales y personales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de *internetworks* para intercambiar información empresarial crítica y confidencial, exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales, aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

La convergencia de los distintos medios de comunicación en una plataforma de red simple, estimula el crecimiento exponencial de las capacidades de red. Existen tres tendencias principales que contribuyen a la futura estructura de las redes de información complejas:

1.1.7. Usuarios móviles

Se está solicitando más conectividad móvil a las redes de datos, debido al incremento del número de trabajadores móviles y de dispositivos portátiles. Esta

demanda creó un mercado para los servicios inalámbricos con gran flexibilidad, cobertura y seguridad.

1.1.8. Más y nuevos dispositivos aptos

La computadora es solo uno de tantos dispositivos en las redes de información de hoy en día. Se tiene una proliferación de nuevas tecnologías magníficas que pueden aprovechar los servicios de red disponibles.

Las funciones que realizan los teléfonos celulares, los asistentes digitales personales (PDA), los organizadores y los *pagers* se concentran en dispositivos portátiles sencillos con conectividad continua para proveedores de servicios y contenido. Estos dispositivos, alguna vez considerados "juguetes" o elementos de lujo, son ahora una parte integral de la forma en que se comunican las personas. Además de los dispositivos móviles, también se tienen dispositivos de voz sobre IP (VoIP), sistemas de juegos y un gran surtido de aparatos para el hogar y los negocios que se pueden conectar y utilizar servicios de red.

Las redes de datos juegan un papel vital al facilitar la comunicación dentro de la red humana mundial. También dan soporte a la forma en que se vive, aprende, trabaja y juega. Proporcionan la plataforma para los servicios que permiten conectarse, en forma local y global, con la familia y amigos, así como también con el trabajo e intereses. Esta plataforma dá soporte al uso de texto, gráficos, video y conversación.

Las redes de datos y las redes humanas utilizan procedimientos similares para asegurar que su comunicación llegue al destino de forma precisa y a tiempo. Los acuerdos sobre el idioma, el contenido, la forma y el medio que el humano generalmente usa en forma implícita, se reflejan en la red de datos.

Las redes convergentes, que transmiten todos los tipos de comunicación (datos, voz y video) en una infraestructura, proporcionan una oportunidad de reducir costos y ofrecer a los usuarios servicios y contenido con muchas características. Sin embargo, el diseño y la administración de redes convergentes requiere de conocimiento y habilidades extensas de *networking*, si todos los servicios se entregan como se espera a los usuarios.

1.2. Componentes de una red

A continuación se realiza la descripción de los componentes de una red.

1.2.1. Dispositivos

Cuando se piensa en utilizar servicios de red, generalmente se cree que utilizar una computadora para acceder a ellos es suficiente. Pero una computadora es solo un tipo de dispositivo que puede enviar y recibir mensajes por una red. Muchos otros tipos de dispositivos pueden conectarse a la red para participar en servicios de la misma. Entre estos dispositivos están teléfonos, cámaras, sistemas musicales, impresoras y consolas de juegos.

Hay otros componentes que hacen posible que una comunicación viaje a través de miles de cables, cables subterráneos, ondas aéreas y estaciones de satélite que pueden existir entre los dispositivos de origen y destino. Uno de los componentes críticos en una red de cualquier tamaño es el *router*. Un *router* une dos o más redes, como una red doméstica e internet, y pasa información de una red a otra. Los *routers* en una red trabajan para asegurar que el mensaje llegue a su destino de la forma más rápida y eficaz. Los dispositivos tienen diferentes finalidades y existe una infinidad de ellos.

1.2.2. Mensajes

En el primer paso de un mensaje, este se convierte a un formato que se puede transmitir en la red. Todos los tipos de mensajes se tienen que convertir a bits, señales digitales codificadas en binario, antes de enviarse a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. Una vez que el mensaje se convierte a bits, está listo para enviarse hacia la red para su entrega.

1.2.3. Reglas

Aspectos importantes de las redes, que no son los dispositivos ni los medios, son las reglas o protocolos. Estas reglas son las normas o protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino. Por ejemplo: en el caso de la mensajería instantánea Jabber, los protocolos XMPP, TCP e IP son importantes conjuntos de reglas que permiten que se realice la comunicación.

1.3. Dispositivos finales

Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web).
- Impresoras de red.
- Teléfonos VoIP.
- Cámaras de seguridad.
- Dispositivos portátiles móviles (tal como los escáner inalámbricos para códigos de barras y los PDA).

En el contexto de una red, se hace referencia a los dispositivos finales como *hosts*. Un dispositivo *host* puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un *host* de otro, cada *host* en la red se identifica por una dirección. Cuando un *host* inicia la comunicación, utiliza la dirección del *host* de destino para especificar a dónde se debe enviar el mensaje.

En las redes modernas, un *hosts* puede actuar como un cliente, un servidor o ambos. El software instalado en el *host* determina qué función tiene en la red.

Los servidores son *host* con software instalado que les permite proporcionar información y servicios, por ejemplo correo electrónico o páginas web, a otros *hosts* de la red.

1.4. Dispositivos intermediarios

Las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás del escenario y garantizar que los datos fluyan a través de la red. Estos dispositivos conectan los *hosts* individuales a la red y pueden conectar varias redes individuales para formar una *internetwork*. Los siguientes son ejemplos de dispositivos de red intermediarios:

- Dispositivos de acceso a la red (*hubs*, *switches* y puntos de acceso inalámbrico).
- Dispositivos de *internetwork* (routers).
- Servidores y módems de comunicación.
- Dispositivos de seguridad (*firewalls*).

La administración de datos, así como fluye en la red, es también una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección *host* de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red. Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red y de *internetwork*.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir mensajes de acuerdo a las prioridades de QoS.
- Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad.

1.5. El medio

La comunicación a través de una red se transporta por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- Hilos metálicos dentro de cables
- Fibras de vidrio o plástico (cable de fibra óptica)
- Transmisión inalámbrica

La codificación de la señal que se debe realizar para que se transmita el mensaje es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- La distancia en la cual el medio puede transportar exitosamente una señal.
- El ambiente en el cual se instalará el medio.
- La cantidad de datos y la velocidad a la que se deben transmitir.

1.6. Tipos de redes

A continuación se realiza una descripción de los tipos de redes.

1.6.1. Redes de área local LAN

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina red de área local (LAN). Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red. Las infraestructuras de red pueden variar en gran medida en términos de:

- El tamaño del área cubierta
- El número de usuarios conectados
- El número y los tipos de servicios disponibles

1.6.2. Redes de área extensa WAN

Estas son redes que conectan dos o más LAN en ubicaciones separadas geográficamente por esto se conocen como redes de área amplia (WAN). A diferencia con una LAN, la organización no mantiene todas las políticas y la administración de las WAN, está regida por un proveedor de servicios de telecomunicaciones.

Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, la instalación y el mantenimiento de los mismos son aptitudes complementarias de la función de la red de una organización.

1.6.3. Red de área metropolitana MAN

Estas son redes que abarcan un área metropolitana, y generalmente son más grandes que una LAN pero más pequeñas que una WAN.

1.6.4. Red de área de almacenamiento SAN

Una red de área de almacenamiento, en inglés SAN (Storage Area Network), es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o SCSI
- Un equipo de interconexión dedicado (conmutadores, puentes)
- Elementos de almacenamiento de red (discos duros)

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la SAN.

1.6.4.1. Ventajas y desventajas

El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza. En el caso de una red de canal de fibra, el ancho de banda es de aproximadamente 100 megabytes/segundo (1 000 megabits/segundo) y se puede extender aumentando la cantidad de conexiones de acceso.

La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes.

Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN, está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo general ethernet).

Por otra parte, una SAN es mucho más costosa que una NAS, ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara.

Normalmente, cuando una compañía estima el TCO (coste total de propiedad) con respecto al coste por byte, el coste se puede justificar con más facilidad. Además es una red concebida para conectar servidores, matrices (*arrays*) de discos y librerías de soporte. Principalmente, está basada en tecnología *fibre channel* y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

1.6.5. Red de área local inalámbrica WLAN

Es una red local a la cual los usuarios pueden conectarse sin necesidad de tener un medio físico interactuando directamente con el *host,* como por ejemplo medios de cobre o fibra.

Además de la flexibilidad que ofrecen las WLAN, el costo reducido es un beneficio importante. Por ejemplo: con una infraestructura inalámbrica ya ubicada, se ahorra al moverse una persona dentro del edificio, al reorganizar un laboratorio, o al moverse a ubicaciones temporarias o sitios de proyectos. En promedio, el costo de IT de mover a un empleado a una nueva ubicación dentro del sitio es de $375 (USD).

Las LAN inalámbricas comparten un origen similar con las LAN ethernet. El IEEE adoptó la cartera 802 LAN/MAN de estándares de arquitectura de red de computadoras. Los dos grupos de trabajo 802 dominantes son ethernet 802.3 y LAN inalámbrica 802.11, sin embargo, hay diferencias importantes entre ellos.

Las WLAN utilizan radiofrecuencia (RF) en lugar de cables en la capa física y la subcapa MAC de la capa de enlace de datos. Comparada con el cable, la RF tiene las siguientes características:

- La RF no tiene límites, como los límites de un cable envuelto. La falta de dicho límite permite a las tramas de datos viajar sobre el medio RF para estar disponibles para cualquiera que pueda recibir la señal RF.

- La señal RF no está protegida de señales exteriores, como sí lo está el cable en su envoltura aislante. Las radios que funcionan independientemente en la misma área geográfica, pero que utilizan la misma RF o similar, pueden interferirse mutuamente.

- La transmisión RF está sujeta a los mismos desafíos inherentes a cualquier tecnología basada en ondas, como la radio comercial. Por ejemplo: a medida que usted se aleja del origen, puede oír estaciones superpuestas una sobre otra o escuchar estática en la transmisión. Con el

tiempo, puede perder la señal por completo. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.

- Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

- Las WLAN conectan a los clientes a la red a través de un punto de acceso inalámbrico (AP) en lugar de un *switch* ethernet.

- Las WLAN conectan los dispositivos móviles que, en general, están alimentados por batería, en lugar de los dispositivos enchufados de la LAN. Las tarjetas de interfaz de red inalámbrica (NIC) tienden a reducir la vida de la batería de un dispositivo móvil.

- Las WLAN admiten *hosts* que se disputan el acceso a los medios RF (bandas de frecuencia). 802.11 recomienda la prevención de colisiones, en lugar de la detección de colisiones para el acceso a medios, para evitar -en forma proactiva- colisiones dentro del medio.

1.6.5.1. Estándares de LAN inalámbricas

LAN inalámbrica 802.11 es un estándar IEEE que define cómo se utiliza la radiofrecuencia (RF) en las bandas sin licencia de frecuencia médica, científica e industrial (ISM) para la capa física y la subcapa MAC de enlaces inalámbricos.

Cuando el 802.11 se emitió por primera vez, prescribía tasas de datos de 1 - 2 Mb/s en la banda de 2.4 GHz. En ese momento, las LAN conectadas por cable

operaban a 10 Mb/s, de modo que la nueva tecnología inalámbrica no se adoptó con entusiasmo. A partir de entonces, los estándares de LAN inalámbrica mejoraron continuamente con la edición de IEEE 802.11a, IEEE 802.11b, IEEE 802.11g y el 802.11n.

La elección típica sobre qué estándar WLAN utilizar se basa en las tasas de datos. Por ejemplo: 802.11a y g pueden admitir hasta 54 Mb/s, mientras que 802.11b admite hasta un máximo de 11 Mb/s, lo que implica que 802.11b es un estándar "lento" y que 802.11 a y g son los preferidos. Un cuarto borrador WLAN, 802.11n, excede las tasas de datos disponibles en la actualidad.

Las tasas de datos de los diferentes estándares de LAN inalámbrica están afectadas por algo llamado técnica de modulación. Las dos técnicas de modulación mas utilizadas son: espectro de dispersión de secuencia directa (DSSS) y multiplexación por división de frecuencias ortogonales (OFDM). Cuando un estándar utilice OFDM, tendrá tasas de datos más veloces. Además, el DSSS es más simple que el OFDM, de modo que su implementación es más económica.

1.6.5.1.1. 802.11a

El IEEE 802.11a adoptó la técnica de modulación OFDM y utiliza la banda de 5 GHz. Los dispositivos 802.11a que operan en la banda de 5 GHz tienen menos probabilidades de sufrir interferencia que los dispositivos que operan en la banda de 2.4 GHz, porque existen menos dispositivos comerciales que utilizan la banda de 5 GHz. Además, las frecuencias más altas permiten la utilización de antenas más pequeñas.

Existen algunas desventajas importantes al utilizar la banda de 5 GHz. La primera es que, a frecuencia de radio más alta, mayor es el índice de absorción por parte de obstáculos tales como paredes, y esto puede ocasionar un rendimiento pobre del 802.11a debido a las obstrucciones. El segundo es que esta banda de frecuencia alta tiene un rango más acotado que el 802.11b o el g. Además, algunos países, incluido Rusia, no permiten la utilización de la banda de 5 GHz, lo que puede restringir más su implementación.

1.6.5.1.2. 802.11b y 802.11g

802.11b especificó las tasas de datos de 1; 2; 5.5 y 11 Mb/s en la banda de 2.4 GHz ISM que utiliza DSSS. 802.11b especificó las tasas de datos superiores en esa banda mediante la técnica de modulación OFDM. IEEE 802.11g también especifica la utilización de DSSS para la compatibilidad retrospectiva de los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5.5 y 11 Mb/s, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mb/s.

Existen ventajas en la utilización de la banda de 2.4 GHz. Los dispositivos en la banda de 2.4 GHz tendrán mejor alcance que aquellos en la banda de 5 GHz. Además, las transmisiones en esta banda no se obstruyen fácilmente como en 802.11a.

Hay una desventaja importante al utilizar la banda de 2.4 GHz. Muchos dispositivos de clientes también utilizan la banda de 2.4 GHz y provocan que los dispositivos 802.11b y g tiendan a tener interferencia.

1.6.5.1.3. 802.11n

El estándar IEEE 802.11n fue pensado para mejorar las tasas de datos y el alcance de la WLAN sin requerir energía adicional o asignación de la banda RF. 802.11n, utiliza radios y antenas múltiples en los puntos finales, y cada uno transmite en la misma frecuencia para establecer *streams* múltiples. La tecnología de entrada múltiple/salida múltiple (MIMO), divide un *stream* rápido de tasa de datos en múltiples streams de menor tasa y los transmite simultáneamente por las radios y antenas disponibles. Esto permite una tasa de datos teórica máxima de 248 Mb/s por medio de dos *streams*.

Los estándares aseguran interoperabilidad entre dispositivos hechos por diferentes fabricantes. Las tres organizaciones clave que influencian los estándares WLAN en todo el mundo son:

- ITU-R
- IEEE
- Wi-Fi Alliance

El ITU-R regula la asignación del espectro RF y órbitas satelitales. Estos se describen como recursos naturales finitos que se encuentran en demanda por parte de clientes, como redes inalámbricas fijas, redes inalámbricas móviles y sistemas de posicionamiento global.

El IEEE desarrolló y mantiene los estándares para redes de áreas locales y metropolitanas con la familia de estándares IEEE 802 LAN/MAN. El IEEE 802 es administrado por el comité de estándares IEEE 802 LAN/MAN (LMSC), que supervisa múltiples grupos de trabajo. Los estándares dominantes en la familia IEEE 802 son 802.3 *ethernet*, 802.5 *TokenRing*, y 802.11 LAN inalámbrica.

A pesar de que el IEEE especificó estándares para los dispositivos de modulación RF, no señaló estándares de fabricación, de modo que las interpretaciones de los estándares 802.11 por parte de los diferentes proveedores pueden causar problemas de interoperabilidad entre sus dispositivos.

La Wi-Fi Alliance es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de productos que están basados en el estándar 802.11, y certifica proveedores en conformidad con las normas de la industria y adhesión a los estándares. La certificación incluye las tres tecnologías RF IEEE 802.11, así como la adopción temprana de los borradores pendientes de la IEEE, como el estándar 802.11n, y los estándares de seguridad WPA y WPA2 basados en IEEE 802.11i. Los roles de estas tres organizaciones pueden resumirse de la siguiente manera:

- El ITU-R regula la asignación de las bandas RF.
- IEEE especifica cómo se modula RF para transportar información.
- Wi-Fi asegura que los proveedores fabriquen dispositivos que sean interoperables.

1.7. Tipos de tráfico

A continuación se realiza una descripción de los tipos de tráfico.

1.7.1. Unicast

El proceso por el cual se envía un paquete de un *host* a un *host* individual. La comunicación *unicast* se usa para una comunicación normal de *host* a *host,* tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes

unicast utilizan la dirección *host* del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una *internetwork*. Sin embargo, los paquetes *broadcast* y *multicast* usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los *broadcasts* están generalmente restringidos a la red local. El ámbito del tráfico *multicast* también puede estar limitado a la red local o enrutado a través de una *internetwork*.

1.7.2. Broadcast

El proceso por el cual se envía un paquete de un *host* a todos los *hosts* de la red. Dado que el tráfico de *broadcast* se usa para enviar paquetes a todos los *hosts* de la red, un paquete usa una dirección de *broadcast* especial. Cuando un *host* recibe un paquete con la dirección de *broadcast* como destino, este procesa el paquete como lo haría con un paquete con dirección *unicast*.

La transmisión de *broadcast* se usa para ubicar servicios o dispositivos especiales para los cuales no se conoce la dirección o cuando un *host* debe proporcionar información a todos los *hosts* de la red.

Algunos ejemplos para utilizar una transmisión de *broadcast* son:

- Asignar direcciones de capa superior a direcciones de capa inferior.
- Solicitar una dirección.
- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento.
- Cuando un *host* necesita información envía una solicitud, llamada consulta, a la dirección de *broadcast*. Todos los *hosts* de la red reciben y procesan esta consulta. Uno o más *hosts* que poseen la información solicitada responderán, típicamente mediante *unicast*.

1.7.3. Multicast

El proceso por el cual se envía un paquete de un *host* a un grupo seleccionado de *hosts*.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del *host* de origen en el encabezado del paquete como la dirección de origen.

La transmisión de *multicast* está diseñada para conservar el ancho de banda de la red IPv4. Esta reduce el tráfico al permitir que un *host* envíe un único paquete a un conjunto seleccionado de *hosts*. Para alcanzar *hosts* de destino múltiples mediante la comunicación *unicast*, sería necesario que el *host* de origen envíe un paquete individual dirigido a cada *host*. Con *multicast*, el *host* de origen puede enviar un único paquete que llegue a miles de *hosts* de destino. Algunos ejemplos de transmisión de *multicast* son:

- Distribución de audio y video.
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento.
- Distribución de software.
- Suministro de noticias.

1.7.3.1. Clientes *multicast*

Los *hosts* que desean recibir datos *multicast* específicos se denominan clientes *multicast*. Los clientes *multicast* usan servicios iniciados por un programa cliente para subscribirse al grupo *multicast*.

1.8. Unidad de datos del protocolo PDU

Se le denomina así a la forma que adopta una sección de datos en cualquier capa. Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU:

- Datos: término general que se utiliza en la capa de aplicación para la PDU.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de red.
- Trama: PDU de la capa de acceso de red.
- Bits: PDU que se utiliza cuando se transmiten datos físicamente por el medio.

1.9. Protocolos

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas que se denominan protocolos. Estos protocolos son específicos de las características de la conversación. En la comunicación personal diaria, las reglas que se utilizan para comunicarse por un medio, como una llamada telefónica, no son necesariamente las mismas que los protocolos para utilizar otro medio, como enviar una carta.

La comunicación exitosa entre los *hosts* de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina *suite* de protocolos. Estos protocolos se implementan en el software y el hardware que está cargado en cada *host* y dispositivo de red. Las *suites* de protocolos de *networking* describen procesos como los siguientes:

- El formato o la estructura del mensaje.
- El método por el cual los dispositivos de *networking* comparten información sobre las rutas con otras redes.
- Cómo y cuándo se transmiten mensajes de error y del sistema entre los dispositivos.
- La configuración y la terminación de sesiones de transferencia de datos.

Los protocolos individuales en una *suite* de protocolos pueden ser específicos para el vendedor y exclusiva. Exclusiva, en este contexto, significa que una compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos exclusivos los pueden utilizar distintas organizaciones con permiso del propietario.

Otros, solo se pueden implementar en equipos fabricados por el proveedor exclusivo. Con frecuencia, muchos de los protocolos que comprenden una *suite* hacen referencia a otros protocolos ampliamente utilizados o a estándares de la industria. Un estándar es un proceso o protocolo que ha sido avalado por la industria de *networking* y ratificado por una organización de estándares, como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) o el Grupo de Trabajo de Ingeniería de Internet (IETF).

El uso de estándares en el desarrollo e implementación de protocolos, asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente para lograr comunicaciones eficientes. Si un fabricante en particular no observa un protocolo estrictamente, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes.

Los protocolos generalmente no describen cómo lograr una función en particular. Al describir solamente qué funciones se requieren de una regla de comunicación en particular pero no cómo realizarlas, es posible que la implementación de un protocolo en particular sea independiente de la tecnología.

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Este modelo describe el funcionamiento de los protocolos que se produce en cada capa, y la interacción con las capas que se encuentran por encima y por debajo de ellas.

Hay beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones. Uso de un modelo en capas:

- Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de *networking*.

1.10. El modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un esquema sobre el cual crear una *suite* de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizará para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la internet con base en TCP/IP y la velocidad a la que se expandió ocasionaron que el desarrollo y la aceptación de la *suite* de protocolos OSI quedaran atrás. Aunque pocos de los protocolos que se crearon mediante las especificaciones OSI se utilizan ampliamente en la actualidad, el modelo OSI de siete capas ha hecho más contribuciones al desarrollo de otros protocolos y productos para todo tipo de redes nuevas.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de el.

1.11. Protocolos y procesos en la capa de aplicación

La mayoría de personas experimentan internet a través de la World Wide Web, servicios de correo electrónico y programas para compartir archivos. Estas y muchas otras aplicaciones proporcionan la interfaz humana a la red subyacente, lo que permite enviar y recibir información con relativa facilidad. Generalmente, las aplicaciones que se utilizan son intuitivas; es decir, se puede acceder a ellas y usarlas sin saber cómo funcionan. Sin embargo, para los

profesionales de la red, es importante saber cómo una aplicación puede formatear, transmitir e interpretar mensajes que se envían y se reciben a través de la red.

La visualización de los mecanismos que permiten la comunicación a través de la red se hace más fácil si se utiliza el esquema en capas del modelo interconexión de sistema abierto (OSI).

1.11.1. DNS

En las redes de datos, los dispositivos se etiquetan con una dirección IP numérica, de manera que pueden participar en el envío y la recepción de mensajes de la red. Sin embargo, la mayoría de las personas pasan mucho tiempo tratando de recordar estas direcciones numéricas. Por lo tanto, los nombres de dominios se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

En internet, nombres de dominio como www.google.com.com, son mucho más fáciles de recordar para la gente que algo como 173.194.37.80, el cual es la dirección numérica actual para ese servidor. Además, si Google decide cambiar la dirección numérica, es transparente para el usuario, ya que el nombre de dominio seguirá siendo www.google.com. La nueva dirección simplemente estará enlazada con el nombre de dominio existente y la conectividad se mantendrá.

El sistema de nombres de dominios (DNS) se creó para que el nombre del dominio busque soluciones para estas redes. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye las consultas sobre formato, las respuestas y los formatos de datos. Las comunicaciones del protocolo DNS utilizan un formato simple llamado mensaje.

Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Los sistemas operativos computacionales también cuentan con una herramienta llamada *nslookup* que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de *host* dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro.

Algunos de estos tipos de registros son:

- A: una dirección de dispositivo final.
- NS: un servidor de nombre autoritativo.
- CNAME: el nombre canónico (o Nombre de dominio completamente calificado) para un alias que se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.
- MX: registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correos para ese dominio.

El sistema de nombres de dominios utiliza un sistema jerárquico para crear una base de datos y así proporcionar una resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo.

En la parte superior de la jerarquía, los servidores raíz mantienen registros sobre cómo alcanzar los servidores de dominio de nivel superior, los cuales a su vez tienen registros que apuntan a los servidores de dominio de nivel secundario y así sucesivamente.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Entre los ejemplos de dominios del nivel superior se encuentran:

- .au: Australia
- .co: Colombia
- .com: una empresa o industria
- .jp: Japón
- .org: una organización sin fines de lucro

Después de los dominios del nivel superior, se encuentran los nombres de los dominios de segundo nivel y debajo de estos hay otros dominios de nivel inferior.

1.11.2. FTP

El protocolo de Transferencia de Archivos (FTP) es otro protocolo de la capa de aplicación de uso común. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que

se ejecuta en una computadora y que carga y descarga archivos de un servidor que ejecuta el demonio FTP (FTPd).

El FTP necesita dos conexiones entre el cliente y el servidor para transferir archivos de forma exitosa: una para comandos y respuestas, otra para la transferencia real de archivos. El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor. El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo.

La transferencia de archivos puede producirse en ambas direcciones. El cliente puede descargar (bajar) un archivo desde el servidor o el cliente puede cargar (subir) un archivo en el servidor.

1.11.3. DHCP

El servicio del protocolo de Configuración Dinámica de Host (DHCP), permite a los dispositivos de una red obtener direcciones IP y otra información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, *gateway* y otros parámetros de *networking* del IP.

DHCP permite a un *host* obtener una dirección IP de forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor DHCP elige una dirección del rango configurado llamado *pool* y la asigna ("alquila") para el *host* por un tiempo establecido. En redes locales más grandes, o donde los usuarios cambien con frecuencia, se prefiere el DHCP. Los nuevos usuarios llegan con computadoras portátiles y necesitan una conexión. Otros tienen nuevas estaciones de trabajo que necesitan conexión. En lugar de que el administrador de red asigne direcciones IP para

cada estación de trabajo, es más eficaz que las direcciones IP se asignen automáticamente mediante el DHCP.

Las direcciones distribuidas por DHCP no se asignan de forma permanente a los *hosts,* sino que sólo se alquilan por un periodo de tiempo. Si el *host* se apaga o se desconecta de la red, la dirección regresa al *pool* para volver a utilizarse. Esto es especialmente útil para los usuarios móviles que entran y salen de la red. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer las conexiones de red. El *host* puede obtener una dirección IP cuando se conecte el hardware, ya sea por cables o por LAN inalámbrica.

Con las redes domésticas, el servidor de DHCP se ubica en el ISP y un *host* de la red doméstica recibe la configuración IP directamente desde el ISP.

DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace que la seguridad física sea un factor importante al determinar si se utiliza el direccionamiento dinámico o manual.

Ambos direccionamientos tienen su lugar en los diseños de red. Muchas redes utilizan tanto el direccionamiento estático como el DHCP. DHCP se utiliza para *hosts* de propósitos generales, como los dispositivos de usuario final, y las direcciones fijas se utilizan para dispositivos de red como *gateways, switches*, servidores e impresoras.

El cliente puede recibir múltiples paquetes de oferta de DHCP si hay más de un servidor de DHCP en la red local, así que debe elegir entre ellos y enviar un paquete de solicitud de DHCP, que identifique el servidor explícito y la oferta de alquiler que el cliente acepta. Un cliente puede elegir solicitar una dirección previamente asignada por el servidor.

Teniendo en cuenta que la dirección IP solicitada por el cliente, u ofrecida por el servidor, aún es válida, el servidor devolverá un mensaje ACK DHCP que le informa al cliente que finalizó el alquiler. Si la oferta ya no es válida, quizás debido al tiempo o que a otro cliente se le asignó el alquiler, el servidor seleccionado responderá con un mensaje NAK DHCP (acuse de recibo negativo). Si un mensaje NAK DHCP se devuelve, entonces el proceso de selección debe volver a comenzar con la transmisión de un mensaje nuevo de descubrimiento de DHCP.

Una vez que el cliente tenga el alquiler, se debe renovar mediante otro mensaje de solicitud de DHCP, antes de que termine el alquiler.

1.11.4. Telnet

Se remonta a principios de la década de los 70 y se encuentra entre los servicios y protocolos de capa de aplicación más antiguo dentro del grupo TCP/IP. Además proporciona un método estándar de emulación de dispositivos de terminal con base en texto en la red de datos. El protocolo y el software del cliente que implementa son conocidos como Telnet.

De un modo adecuado, una conexión que utiliza Telnet se llama sesión o conexión de terminal virtual (VTY). En lugar de utilizar un dispositivo físico para conectarse al servidor, Telnet utiliza software para crear un dispositivo virtual que proporcione las mismas características de una sesión de terminal con acceso a la interfaz de línea de comandos (CLI) del servidor.

Para admitir conexiones del cliente a Telnet, el servidor ejecuta un servicio llamado demonio de Telnet. Se establece una conexión de terminal virtual desde

un dispositivo final utilizando una aplicación del cliente Telnet. La mayoría de los sistemas operativos incluye un cliente de Telnet de la capa de aplicación. Puede ejecutarse desde el indicador del sistema en una PC de Microsoft Windows. Otras aplicaciones de terminal comunes que ejecutan clientes Telnet son Hyper Terminal, Minicom y Tera Term.

Una vez establecida una conexión Telnet, los usuarios pueden realizar cualquier función autorizada en el servidor, como si utilizaran una sesión de línea de comandos en el servidor mismo. Si están autorizados, pueden iniciar y detener procesos, configurar el dispositivo e inclusive apagar el sistema.

1.11.5. SSH

Si la seguridad es un problema, el Protocolo shell seguro (SSH) ofrece un método seguro y alternativo para acceder al servidor. SSH proporciona la estructura para un inicio de sesión remoto seguro y otros servicios de red seguros. Además, proporciona mayor autenticación que Telnet y admite el transporte de datos de sesión con la autenticación. Como una mejor práctica, los profesionales de red deberían utilizar siempre SSH en lugar de Telnet, cada vez que sea posible.

1.11.6. H.323

La familia de protocolos H.323 se especifica mediante la UIT-T. Este define los estándares para la transmisión de audio y de datos mediante IP.

Las redes H.323 contienen los siguientes elementos:

- Terminales
- *Gateway*
- *Gatekeeper*
- Unidades de control multipunto (MCU)

Los terminales establecen conexiones entre sí, punto a punto o multipunto (a través de MCU), los *gateways* forman la intersección entre la red IP y la red telefónica, los *gatekeepers* se utilizan para el control del acceso y la traducción de direcciones E.164 (números de teléfono) en direcciones IP.

1.11.7. SIP

SIP está localizado en la capa de aplicación y se utiliza para establecer, modificar y desconectar conexiones multimedia. En contraste con el protocolo de señalización H.323, SIP posee una estructura abierta similar al HTTP y SMTP. El SIP utiliza una arquitectura modular y es más fácilmente extensible y escalable que el protocolo H.323. Además, las funciones adicionales se pueden implementar más de manera más eficiente con SIP que con el estándar H.323. SIP es compatible tanto con conexiones punto a punto, como también con conexiones multipunto. Para la comunicación SIP se consideran los siguientes cinco aspectos:

- Localización del usuario (*user location*)
- Capacidad del terminal (*capability exchange*)
- Disponibilidad del usuario (*user availability*)
- Establecimiento de llamada (*call setup*)

- Tratamiento de una llamada (*call handling*)

SIP es un protocolo basado en texto que fue definido como estándar de internet en 1999, por el IETF en RFC 2543 y luego ha sido mejorado en 2002 en RFC 3261. Es parte de la arquitectura multimedia de la IETF (fuerza de trabajo de ingeniería de internet), en la cual también figuran otros protocolos como el RSVP (protocolo de reserva de recursos), RTP (protocolo en tiempo real), SAP (protocolo de anuncio de sesión) y SDP (protocolo de descripción de sesión). No obstante el SIP es independiente de estos protocolos y puede cooperar con otros protocolos de señalización (p. ej. H.323). SIP utiliza un servidor proxy para poder asistir la conexión con el emplazamiento del usuario, la autenticación y la autorización para servicios.

- SIP es un modelo de transacción petición/respuesta (consulta/información del estado).
- Las peticiones se contestan esencialmente con respuestas. Mientras que solamente existe un puñado de diferentes peticiones, hay disponibles alrededor de cientos de respuestas diferentes. SIP reconoce los siguientes 6 tipos básicos de pedido para sesiones SIP simples:

    - Invite
    - Ack
    - Options
    - Bye
    - Cancel
    - Registrer

SIP fue desarrollado para su uso en redes basadas en TCP/IP y también utiliza una serie de protocolos estandarizados de la familia del protocolo de

internet que además han sido desarrollados por el IETF. SIP utiliza para transportar datos protocolos tales como UDP y TCP con el puerto por defecto 5060, en el cual la UDP es la variante más popular y se utiliza para transportar medios tales como la voz y el protocolo en tiempo real (RTP). Para dar a conocer el protocolo de transporte de los medios, SIP utiliza el protocolo SDP (protocolo de descripción de sesión). Además, en las aplicaciones multimedia puede utilizarse SAP (protocolo de anuncio de sesión) prioritariamente para las conferencias. Sirve para anunciar quién quiere participar en la conferencia. Los procedimientos usados para garantizar la seguridad para el SIP son TLS sobre SIP, S/MIME sobre SIP, así como IPsec con o sin IKE para SIP.

1.11.8. HTTP

El protocolo de transferencia de hipertexto (HTTP), uno de los protocolos del grupo TCP/IP, se desarrolló en sus comienzos para publicar y recuperar las páginas HTML, y en la actualidad se utiliza para sistemas de información distribuidos y de colaboración. HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados.

HTTP especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página web y envía los tipos de mensajes que el servidor utiliza para responder. Los tres tipos de mensajes comunes son *get, post y put*.

1.11.9. P2P y Gnutella

Compartir archivos en internet se ha transformado en algo muy popular. Con las aplicaciones P2P basadas en el protocolo Gnutella, las personas pueden colocar archivos en sus discos rígidos para que otros los descarguen. El software del cliente compatible con Gnutella permite a los usuarios conectarse con los servicios Gnutella en internet y ubicar y acceder a los recursos compartidos por otros pares Gnutella.

Muchas aplicaciones del cliente están disponibles para acceder en la red Gnutella, entre ellas: BearShare, Gnucleus, LimeWire, Morpheus, WinMX y XoloX. Mientras que el Foro de Desarrolladores de Gnutella mantiene el protocolo básico, los proveedores de las aplicaciones generalmente desarrollan extensiones para lograr que el protocolo funcione mejor en dichas aplicaciones.

1.12. Protocolos en la capa de transporte

Las redes de datos e internet brindan soporte a la red humana al proporcionar la comunicación continua y confiable entre las personas, tanto de manera local como alrededor del mundo. En un único dispositivo, las personas pueden utilizar varios servicios como correo electrónico, la web y la mensajería instantánea para enviar mensajes o recuperar información. Las aplicaciones como clientes de correo electrónico, exploradores web y clientes de mensajería instantánea permiten a la gente utilizar las computadoras y las redes para enviar mensajes y encontrar información.

Los datos de cada una de estas aplicaciones se empaqueta, se transporta y se entrega al demonio del servidor adecuado o a la aplicación en el dispositivo de destino. Los procesos descritos en la capa de transporte del modelo OSI aceptan los datos de la capa de aplicación y los preparan para el

direccionamiento en la capa de red. La capa de transporte es responsable de la transferencia de extremo a extremo general de los datos de aplicación.

1.12.1. Puerto lógico

Para pasar *streams* de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación meta. Para lograr esto, la capa de transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese *host*. Este número de puerto se utiliza en el encabezado de la capa de transporte para indicar qué aplicación se asocia a qué parte.

1.12.2. TCP

TCP es un protocolo orientado a la conexión descrito en RFC 793. El TCP utiliza recursos adicionales para ganar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP solo posee 8 bytes de carga. Vea la figura para hacer una comparación.

- Las aplicaciones que utiliza el TCP son:
    - Exploradores web
    - Correo electrónico
    - Transferencias de archivos

La confiabilidad de la comunicación TCP se lleva a cabo utilizando sesiones orientadas a la conexión. Antes de que un *host* que utiliza TCP envíe datos a otro *host*, la capa de transporte inicia un proceso para crear una conexión con el destino. Esta conexión permite el rastreo de una sesión, o *stream* de comunicación entre los *hosts*. Este proceso asegura que cada *host* tenga conocimiento de la comunicación y se prepare. Una conversación completa de TCP necesita establecer una sesión entre los *hosts* de ambas direcciones.

Después de establecer una sesión, el destino envía un acuse de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino.

Parte de la carga adicional que genera el uso de TCP es el tráfico de red generado por los acuses de recibo y las retransmisiones. El establecimiento de las sesiones genera cargas en forma de segmentos adicionales intercambiados. Hay también sobrecarga en los *hosts* individuales creada por la necesidad de mantener un registro de los segmentos que esperan un acuse de recibo y por el proceso de retransmisión.

Cada conexión involucra *streams* de comunicación de una vía, o sesiones para establecer y terminar el proceso del TCP entre dispositivos finales. Para establecer la conexión los *hosts* realizan un protocolo de enlace de tres vías. Los bits de control en el encabezado TCP indican el progreso y estado de la conexión. El enlace de tres vías:

- Establece que el dispositivo de destino se presente en la red.

- Verifica que el dispositivo de destino tenga un servicio activo y que acepte solicitudes en el número de puerto de destino que el cliente de origen intenta utilizar para la sesión.
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto.

1.12.3. UDP

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como "mejor intento".

- Las aplicaciones que utilizan UDP incluyen:
  - Sistema de nombres de dominio (DNS)
  - *Streaming* video
  - Voz sobre IP (VoIP)

UDP es un protocolo simple que provee las funciones básicas de la capa de transporte. Tiene una sobrecarga mucho menor que el TCP, ya que no está orientado a la conexión y no proporciona mecanismos sofisticados de retransmisión, secuenciamiento y flujo de control.

Esto no significa que las aplicaciones que utilizan UDP no son siempre poco confiables. Solo quiere decir que estas funciones no las contempla el protocolo de la capa de transporte y se deben implementar aparte, si fuera necesario.

Pese a que es relativamente baja la cantidad total de tráfico UDP que puede encontrarse en una red típica, los protocolos clave de la capa de aplicación que utiliza UDP incluyen:

- Sistema de nombres de dominio (DNS).
- Protocolo simple de administración de red (SNMP, Simple Network Management Protocol).
- Protocolo de configuración dinámica de *host* (DHCP).
- Protocolo de información de enrutamiento (RIP).
- Protocolo de transferencia de archivos trivial (TFTP).
- Juegos en línea.

Algunas aplicaciones, tales como los juegos en línea o VoIP, pueden tolerar la pérdida de algunos datos. Si estas aplicaciones utilizaran TCP, experimentarían largas demoras, ya que TCP detecta la pérdida de datos y los retransmite. Estas demoras serían más perjudiciales para la aplicación que las pequeñas pérdidas de datos. Algunas aplicaciones, como DNS, simplemente vuelven a intentar la solicitud si no reciben una respuesta y, por lo tanto, no necesitan el TCP para garantizar la entrega del mensaje. La baja sobrecarga del UDP es deseada por dichas aplicaciones.

1.12.4. SCTP

Stream Control Transmission Protocol (SCTP) es un protocolo de comunicación de capa de transporte, que fue definido por el grupo SIGTRAN de IETF en el 2000. El protocolo está especificado en la RFC 2960, y la RFC 3286 brinda una introducción al mismo.

SCTP es una alternativa a los protocolos de transporte TCP y UDP pues provee confiabilidad, control de flujo y secuenciación como TCP. Sin embargo, SCTP opcionalmente permite el envío de mensajes fuera de orden y a diferencia

de TCP, SCTP es un protocolo orientado al mensaje (similar al envío de datagramas UDP).

Las ventajas de SCTP son:

- Capacidad de *Multihoming*, en la cual uno o dos de los extremos de una asociación (conexión) pueden tener más de una dirección IP. Esto permite reaccionar en forma transparente ante fallos en la red.
- Entrega de los datos en trozos que forman parte de flujos independientes y paralelos eliminando así el problema de *head* of the *line blocking* que sufre TCP.
- Es capaz de seleccionar y monitorizar caminos, seleccionando un camino "primario" y verificando constantemente la conectividad de cada uno de los caminos alternativos.
- Mecanismos de validación y asentimiento como protección ante ataques por inundación, proveyendo notificación de trozos de datos duplicados o perdidos.

SCTP fue diseñado inicialmente por el grupo Sigtran para transportar señalización telefónica SS7 sobre IP. La intención fue la de proveer en IP de algunas de las características de confiabilidad de SS7. Por su versatilidad luego se ha propuesto utilizarlo en otras áreas, como por ejemplo para transportar mensajes de los protocolos DIAMETER o SIP.

1.13. Protocolos en la capa de red

Los protocolos de la capa de red del modelo OSI especifican el direccionamiento y los procesos que permiten que los datos de la capa de transporte sean empaquetados y transportados. La encapsulación de la capa de

red permite que su contenido pase al destino dentro de una red o sobre otra red con una carga mínima.

1.13.1. Dirección IP

La dirección IPv4 lógica de 32 bits tiene una composición jerárquica y consta de dos partes. La primera parte identifica la red y la segunda parte identifica al *host* en esa red. Se requiere de las dos partes para completar una dirección IP.

Por comodidad, las direcciones IPv4 se dividen en cuatro grupos de ocho bits (octetos). Cada octeto se convierte a su valor decimal y la dirección completa se escribe como los cuatro valores decimales separados por punto (período).

Por ejemplo: 192.168.18.57

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- Dirección de red: la dirección en la que se hace referencia a la red.
- Dirección de *broadcast*: una dirección especial que se utiliza para enviar datos a todos los *hosts* de la red.
- Direcciones *host*: las direcciones asignadas a los dispositivos finales de la red.

1.13.2. Máscara de subred

Para definir las porciones de red y de *host* de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred. La máscara de subred se expresa con el mismo formato decimal punteado que la dirección IPv4.

La máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de *host*.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Un prefijo /24 se expresa como una máscara de subred como 255.255.255.0 (11111111.11111111.11111111.00000000). Los bits restantes (orden inferior) de la máscara de subred son ceros, que indican la dirección *host* dentro de la red.

La máscara de subred se configura en un *host* junto con la dirección IPv4 para definir la porción de red de esa dirección.

1.13.3. Gateway

El *gateway*, que también se conoce como *gateway* predeterminado, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del *host* de origen, el paquete tiene que hallar la salida fuera de la red original. Para esto, el paquete es enviado al *gateway*. Este es una interfaz del *router* conectada a la red local. La interfaz del *gateway* tiene una dirección de capa de red que concuerda con la dirección de red de los *hosts*. Estos están configurados para reconocer la dirección como *gateway*.

1.13.3.1. *Gateway* predeterminado

El *gateway* predeterminado se configura en un host. En una computadora con Windows, se usan las herramientas de las Propiedades del Protocolo de

internet (TCP/IP) para ingresar la dirección IPv4 del *gateway* por defecto. Tanto la dirección IPv4 de *host* como la dirección de *gateway* deben tener la misma porción de red (y subred si se utiliza) de sus respectivas direcciones.

1.13.4. IPv4

El protocolo de Internet IPv4 es aquel de transporte de datos de la capa 3 más utilizado actualmente,

El protocolo de Internet fue diseñado como un protocolo de bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas.

Características básicas de IPv4:

- Sin conexión: no establece conexión antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): no se usan encabezados para garantizar la entrega de paquetes.
- Independiente de los medios: funciona sin importar los medios que transportan los datos.

El protocolo IP no sobrecarga el servicio IP proporcionando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño. Transportar estos encabezados más pequeños genera una menor sobrecarga.

Menor sobrecarga significa menos demora en la entrega. Esta característica se prefiere para un protocolo de capa 3.

Se suele considerar que el IP es un protocolo no confiable. No confiable en este contexto no significa que el IP funciona adecuadamente algunas veces y no funciona bien en otras oportunidades. Tampoco significa que no es adecuado como protocolo de comunicaciones de datos. No confiable significa simplemente que IP no tiene la capacidad de administrar ni recuperar paquetes no entregados o corruptos.

El encabezado de un paquete IP no incluye los campos requeridos para la entrega confiable de datos. No hay acuses de recibo de entrega de paquetes. No hay control de error para datos. Tampoco hay forma de rastrear paquetes; por lo tanto, no existe la posibilidad de retransmitir paquetes.

1.13.5. IPv6

IPv6 no existiría si no fuera por el agotamiento evidente de las direcciones IPv4 disponibles. Sin embargo, más allá del mayor espacio de direcciones IP, el desarrollo de IPv6 presentó oportunidades para aplicar lo aprendido a partir de las limitaciones de IPv4 y crear así un protocolo con funciones nuevas y mejoradas.

Muchas de las mejoras que ofrece IPv6 son las siguientes:

- Direccionamiento IP mejorado.
- Un espacio de direcciones más grande.
- Más posibilidad de conexión y flexibilidad global.

- Mejor agrupación de los prefijos IP anunciados en las tablas de enrutamiento.
- *Hosts* con múltiples conexiones. La multiconexión es una técnica para aumentar la confiabilidad de la conexión a internet de una red IP. Con IPv6, un *host* puede tener varias direcciones IP a través de un enlace ascendente físico. Por ejemplo, un *host* puede conectarse a varios ISP.
- Configuración automática que puede incluir direcciones de capa de enlace de datos en el espacio de la dirección.
- Más opciones *plug-and-play* para más dispositivos.
- Redireccionamiento de extremo a extremo de público a privado sin traducción de direcciones. Esto hace que las redes entre *peers* (P2P) sea más funcional y fácil de implementar.
- Mecanismos simplificados para renumeración y modificación de direcciones.

El encabezado simplificado de IPv6 ofrece varias ventajas con respecto a IPv4:

- Mayor eficacia de enrutamiento para obtener mejor rendimiento y más escalabilidad de velocidad de reenvío.
- Ausencia de *broadcasts*, de manera que no existe peligro potencial de tormentas de *broadcasts*.
- No hay necesidad de procesar *checksums*.
- Mecanismos de encabezado de extensión más simples y eficaces.
- Rótulos de flujo en función del procesamiento de flujo sin necesidad de abrir el paquete interno de transporte para identificar los diferentes flujos de tráfico.

1.13.6. Ping ICMP

Ping es una utilidad para probar la conectividad IP entre *hosts*. Ping envía solicitudes de respuestas desde una dirección *host* específica. *Ping* usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control Message Protocol (Protocolo de Mensajes de Control de Internet, ICMP). *Ping* usa un datagrama de solicitud de eco ICMP.

Si el *host* en la dirección especificada recibe la solicitud de eco, este responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el *ping* mide el tiempo requerido para la respuesta.

A medida que se recibe cada respuesta, el *ping* muestra el tiempo entre el envío del *ping* y la recepción de la respuesta. Esta es una medida del rendimiento de la red. *Ping* posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el *ping* abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las solicitudes, la utilidad de *ping* proporciona un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

1.13.7. IPX

El protocolo Intercambio de Paquetes Entre Redes (IPX) es la implementación del protocolo IDP (Internet Datagram Protocol) de Xerox. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

Pertenece a la capa de red (nivel 3 del modelo OSI) y al ser un protocolo de datagramas es similar (aunque más simple y con menor fiabilidad) al protocolo IP del TCP/IP en sus operaciones básicas, pero diferente en cuanto al sistema de direccionamiento, formato de los paquetes y el ámbito general. Este protocolo (IPX) fue creado por el Ing. Alexis G. Soulle.

1.13.8. Appletalk

Es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP.

1.14. QoS

El protocolo de Internet (IP) fue desarrollado originalmente para transportar datos con la calidad del mejor desempeño. Hoy en día, las redes basadas en IP son tan populares que todo se intenta transmitir mediante IP (anything over IP). Sin embargo, muchas de las nuevas aplicaciones y servicios que ahora se comunican sobre redes IP, tales como la voz, requieren más que un servicio de mejor desempeño. Estos servicios cuentan con una calidad definida de la red que transmite. Esta calidad puede ser definida en función de diferentes criterios:

- *Delay* (retraso)
- *Jitter* (variancia del retraso)
- *Packet Loss* (pérdida de paquetes)
- *Bandwidth* (ancho de banda)
- *Availability* (disponibilidad)

Una red por lo tanto tiene que ser probada en lo referente a estos parámetros antes de implementar VoIP. Esto ocurre en el análisis de red o en la auditoría de red. Usando los generadores de llamada y de carga la red se carga por un período largo mientras que se simulan las llamadas VoIP. Durante este tiempo, se puede determinar la red en lo referente a parámetros VoIP críticos. Siemens ofrece un paquete de software analizador del tráfico que recoge los datos importantes de parámetros de voz y con ello puede evaluar la red. Las auditorias normales de red no son adecuadas para VoIP porque no prueban generalmente los parámetros de voz de forma adecuada. Si se detectan problemas en la red, estos tienen que ser resueltos antes de la implementación de VoIP.

Con ayuda de los mecanismos de calidad de servicio (QoS) es posible proporcionar la calidad de servicio necesaria para estas deficiencias. Para poder llevar a cabo el QoS fin a fin, tienen que definirse los dos modelos de grupo de trabajo de ingeniería de internet (IETF):

- Servicios integrados (IntServ)
- Servicios diferenciados (DiffServ)

El modelo IntServ se basa en el concepto de que una aplicación señaliza en la red sus requisitos de ancho de banda. Si la red puede garantizar la calidad de servicio requerida, se produce la transmisión de datos. Con el aumento del número de aplicaciones y de usuarios este método no se podrá escalar más. El modelo IntServse basa en el protocolo de reserva de recursos (RSVP).

El modelo DiffServ sigue otra aproximación. El tráfico de datos está dividido en distintas clases de servicio y a cada una de las clases se le dá un servicio apropiado. La señalización no ocurre por flujo. Esta aproximación no es tan

exacta como el modelo IntServ pero también funciona bastante bien aunque el número de la secuencia de datos aumente. Además el modelo DiffServ ahorra costes en cuanto a la administración porque el ajuste de los parámetros para una clase de servicio requiere menos esfuerzo que para el flujo de tráfico individual.

1.14.1. IEEE 802.1p

IEEE 802.1p es un estándar que proporciona priorización de tráfico y filtrado *multicast* dinámico. Esencialmente, proporciona un mecanismo para implementar calidad de servicio (QoS) a nivel de MAC (Media Access Control).

Existen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (user_priority) de la cabecera IEEE 802.1Q añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7. Aunque es un método de priorización bastante utilizado en entornos LAN, cuenta con varios inconvenientes, como el requerimiento de una etiqueta adicional de 4 bytes (definida en el estándar IEEE802.1Q). Además solo puede ser soportada en una LAN, ya que las etiquetas 802.1Q se eliminan cuando los paquetes pasan a través de un *router*.

No está definida la manera de cómo tratar el tráfico que tiene asignada una determinada clase o prioridad, dejando libertad a las implementaciones. IEEE, sin embargo, ha hecho amplias recomendaciones al respecto.

1.14.2. DSCP

DSCP hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan. Originalmente se definió este byte para un

uso con otro formato: ToS (tipo de servicio) pero con el mismo objetivo de diferenciar el tráfico.

1.15. Medios físicos de interconexión

A continuación se presenta una descripción de los medios físicos de interconexión.

1.15.1. Medios de cobre

El medio más utilizado para las comunicaciones de datos es el cableado que utiliza alambres de cobre, para señalizar bits de control y de datos entre los dispositivos de red. El cableado utilizado para las comunicaciones de datos, generalmente consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización.

Otros tipos de cableado de cobre, que se conocen como cables coaxiales, tienen un conductor simple que circula por el centro del cable envuelto por el otro blindaje, pero está aislado de este. El tipo de medio de cobre elegido se especifica mediante el estándar de la capa física necesario para enlazar las capas de enlace de datos de dos o más dispositivos de red.

Estos cables pueden utilizarse para conectar los nodos de una LAN a los dispositivos intermediarios, como *routers* o *switches*. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos, como una compañía telefónica. Cada tipo de conexión y sus dispositivos

complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física.

Los medios de *networking* generalmente utilizan conectores y tomas. Estos elementos facilitan la conexión y la desconexión. Además, puede utilizarse un único tipo de conector físico para diferentes tipos de conexiones. Por ejemplo, el conector RJ-45 se utiliza ampliamente en las LAN con un tipo de medio y en algunas WAN con otro tipo de medio.

Los datos se transmiten en cables de cobre como impulsos eléctricos. Un detector en la interfaz de red de un dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la señal enviada. Los valores de voltaje y sincronización en estas señales son susceptibles a la interferencia o ruido que se genera fuera del sistema de comunicaciones. Estas señales no deseadas pueden distorsionar y corromper las señales de datos que se transportan a través de los medios de cobre. Las ondas de radio y los dispositivos electromagnéticos como luces fluorescentes, motores eléctricos y otros dispositivos representan una posible fuente de ruido.

Los tipos de cable con blindaje o trenzado de pares de alambre están diseñados para minimizar la degradación de señales debido al ruido electrónico. La susceptibilidad de los cables de cobre al ruido electrónico también puede estar limitada por:

- La selección del tipo o categoría de cable más adecuado para proteger las señales de datos en un entorno de *networking* determinado
- El diseño de una infraestructura de cables para evitar las fuentes de interferencia posibles y conocidas en la estructura del edificio

- El uso de técnicas de cableado que incluyen el manejo y la terminación apropiados de los cables

1.15.2. Medios de fibra

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda, para transmitir datos sin procesar. La mayoría de los estándares actuales de transmisión aún necesitan analizar el ancho de banda potencial de este medio.

Debido a que las fibras de vidrio que se utilizan en los medios de fibra óptica no son conductores eléctricos, el medio es inmune a la interferencia electromagnética y no conduce corriente eléctrica no deseada cuando existe un problema de conexión a tierra. Las fibras ópticas pueden utilizarse en longitudes mucho mayores que los medios de cobre sin la necesidad de regenerar la señal, ya que son finas y tienen una pérdida de señal relativamente baja. Algunas especificaciones de la capa física de fibra óptica admiten longitudes que pueden alcanzar varios kilómetros.

- Algunos de los problemas de implementación de medios de fibra óptica:
- Más costoso (comúnmente) que los medios de cobre para la misma distancia (pero para una capacidad mayor).
- Se necesitan diferentes habilidades y equipos para terminar y empalmar la infraestructura de cables.
- Manejo más cuidadoso que los medios de cobre.

En la actualidad, en la mayor parte de los entornos empresariales se utiliza principalmente la fibra óptica como cableado *backbone* para conexiones punto a punto con una gran cantidad de tráfico entre los servicios de distribución de datos y para la interconexión de los edificios en el caso de los *campus* compuestos por varios edificios. Ya que la fibra óptica no conduce electricidad y presenta una pérdida de señal baja, es ideal para estos usos.

Los cables de fibra óptica consisten en un revestimiento exterior de PVC y un conjunto de materiales de refuerzo que rodean la fibra óptica y su revestimiento. El revestimiento rodea la fibra de plástico o de vidrio y está diseñado para prevenir la pérdida de luz de la fibra. Se requieren dos fibras para realizar una operación *full duplex* ya que la luz solo puede viajar en una dirección a través de la fibra óptica. Los *patch cables* de la fibra óptica agrupan dos cables de fibra óptica y su terminación incluye un par de conectores de fibra únicos y estándares. Algunos conectores de fibra aceptan fibras receptoras y transmisoras en un único conector.

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos: monomodo y multimodo.

La fibra óptica monomodo transporta un sólo rayo de luz, generalmente emitido desde un láser. Este tipo de fibra puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

La fibra óptica multimodo normalmente utiliza emisores LED que no generan una única ola de luz coherente. En cambio, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos. Los tendidos extensos de fibra pueden generar impulsos poco claros al recibirlos en el extremo receptor, ya que la luz que

ingresa a la fibra en diferentes ángulos requiere de distintos períodos de tiempo para viajar a través de la fibra. Este efecto, denominado dispersión modal, limita la longitud de los segmentos de fibra multimodo.

La fibra multimodo y la fuente de luz del LED que utiliza resultan más económicas que la fibra monomodo y su tecnología del emisor basada en láser.

1.15.3. Medios inalámbricos

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Como medio de *networking*, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre.

Las tecnologías inalámbricas de comunicación de datos funcionan bien en entornos abiertos.

Sin embargo, existen determinados materiales de construcción utilizados en edificios y estructuras, además del terreno local, que limitan la cobertura efectiva. El medio inalámbrico también es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

Además, los dispositivos y usuarios que no están autorizados a ingresar a la red pueden obtener acceso a la transmisión, ya que la cobertura de la comunicación inalámbrica no requiere el acceso a una conexión física de los

medios. Por lo tanto, la seguridad de la red es un componente principal de la administración de redes inalámbricas.

Los estándares de IEEE y de la industria de las telecomunicaciones sobre las comunicaciones inalámbricas de datos abarcan las capas física y de enlace de datos. Los cuatro estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

- IEEE estándar 802.11: comúnmente denominada Wi-Fi, se trata de una tecnología LAN inalámbrica (red de área local inalámbrica, WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de Acceso Múltiple con Detección de Portadora/Prevención de colisiones (CSMA/CA).

- IEEE estándar 802.15: estándar de red de área personal inalámbrica (WPAN), comúnmente denominada Bluetooth, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.

- IEEE estándar 802.16: comúnmente conocida como WiMAX (Interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.

- Sistema global para comunicaciones móviles (GSM): incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio General de Radio por Paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

Otros tipos de tecnologías inalámbricas, como las comunicaciones satelitales, proporcionan una conectividad de red de datos para ubicaciones que no cuentan con otros medios de conexión. Los protocolos, incluso GPRS, permiten la transferencia de datos entre estaciones terrestres y enlaces satelitales.

2. ETHERNET

El Grupo de Trabajo de Ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la *suite* de protocolos TCP/IP de las capas superiores. Sin embargo, diversas organizaciones especializadas en ingeniería (IEEE, ANSI, ITU) o empresas privadas (protocolos propietarios) describen los protocolos y servicios funcionales de la capa de enlace de datos y la capa física del modelo OSI. Dado que *ethernet* se compone de estándares en estas capas inferiores, puede decirse que en términos generales se entiende mejor con referencia al modelo OSI.

El modelo OSI separa las funcionalidades de la capa de Enlace de datos de direccionamiento, entramado y acceso a los medios desde los estándares de la capa física de los medios. Los estándares de *ethernet* definen los protocolos de capa 2 y las tecnologías de capa 1. Si bien las especificaciones de *ethernet* admiten diferentes medios, anchos de banda y otras variaciones de Capa 1 y 2, el formato de trama básico y el esquema de direcciones son los mismos para todas las variedades de *ethernet*.

2.1. Estándares e implementación

El primer estándar de *ethernet* fue publicado por un consorcio formado por Digital *Equipment Corporation*, Intel y Xerox (DIX). Metcalfe quería que *ethernet* fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto. Los primeros productos que se desarrollaron a partir del estándar de *ethernet* se vendieron a principios de la década de 1980.

En 1985, el Comité de Estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para *ethernet* es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO). Para garantizar la compatibilidad, los estándares IEEE 802.3 debían cubrir las necesidades de la capa 1 y de las porciones inferiores de la capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de *ethernet* se efectuaron en el 802.3.

Ethernet opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos y la capa física.

Las primeras versiones de *ethernet* utilizaban cable coaxial para conectar computadoras en una topología de bus. Cada computadora se conectaba directamente al *backbone*. Estas primeras versiones de *ethernet* se conocían como *Thicknet* (10BASE5) y *Thinnet* (10BASE2)

La 10BASE5 o *Thicknet* utilizaba un cable coaxial grueso, que permitía lograr distancias de cableado de hasta 500 metros antes de que la señal requiriera un repetidor. La 10BASE2, o *Thinnet*, utilizaba un cable coaxial fino que tenía un diámetro menor y era más flexible que la *Thicknet* y permitía alcanzar distancias de cableado de 185 metros.

La capacidad de migrar la implementación original de *ethernet* a las implementaciones de *ethernet* actuales y futuras se basa en la estructura de la trama de capa 2, que prácticamente no ha cambiado. Los medios físicos, el acceso al medio y el control del medio han evolucionado y continúan haciéndolo.

Pero el encabezado y el tráiler de la trama de *ethernet* han permanecido constantes en términos generales.

Las primeras implementaciones de *ethernet* se utilizaron en entornos LAN de bajo ancho de banda en los que el acceso a los medios compartidos se administraba mediante CSMA y, posteriormente, mediante CSMA/CD. Además de ser una topología de bus lógica de la capa de enlace de datos, *ethernet* también utilizaba una topología de bus física. Esta topología se volvió más problemática a medida que las LAN crecieron y que sus servicios demandaron más infraestructura.

2.2. Control de enlace lógico

Las funciones de la capa de enlace de datos se separan en dos subcapas diferenciadas gracias a *ethernet* estas son: la subcapa control de enlace lógico LLC y la subcapa control de acceso al medio MAC, la utilización de estas dos subcapas permite la compatibilidad entre diferentes *hosts* o dispositivos finales, estas mismas describen todas las funciones de la capa de enlace de datos descritas por el modelo OSI.

La comunicación entre capas superiores, el software de red y las capas inferiores que manejan el hardware, y codificación se llevan a cabo por la subcapa control de enlace lógico. Esta toma los datos que provienen de protocolos superiores como por ejemplo un paquete ipv4, e insertan la información que sirve para entregar el paquete al *host* destino, la comunicación de capa 2 con las capas superiores se hace a través de LLC.

LLC no depende del equipo físico ya que se implementa a nivel de software, por ejemplo, en una computadora el LLC es el controlador de la tarjeta de red, y

este es un software que interactúa directamente con el hardware para trasladar datos entre los medios y la capa MAC.

2.3. Control de acceso al medio

La subcapa inferior de enlace de datos se llama control de acceso al medio y tiene relación con el hardware que conecta a los medios, generalmente es la tarjeta de red en la mayoría de dispositivos de red. La subcapa MAC de ethernet tiene dos responsabilidades principales:

- Encapsulación de datos
- Control de acceso al medio
- Encapsulación de datos:
- La encapsulación de datos proporciona tres funciones principales:

    - Delimitación de tramas
    - Direccionamiento
    - Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir una trama. Cuando forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de capa 3. La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

Los delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama son proporcionados por el proceso de entramado, ya que se incluye una sincronización entre los nodos transmisores y receptores.

El proceso de encapsulación también proporciona el direccionamiento de la capa de enlace de datos. Cada encabezado *ethernet* agregado a la trama contiene la dirección física (dirección MAC), que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores. Cada trama de *ethernet* contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

CSMA/CD es el método que *ethernet* ofrece para determinar la manera en que los nodos comparten el acceso al medio, y significa acceso múltiple con detección de portadora y detección de colisiones.

2.4. Dirección MAC

La capa de enlace de datos proporciona direccionamiento que se utiliza para transportar la trama a través de los medios locales compartidos. Las direcciones de dispositivo en esta capa se llaman direcciones físicas. El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local. El encabezado de la trama también puede contener la dirección de origen de la trama.

El nombre que reciben estas direcciones físicas es direcciones MAC proveniente de *media access control*.

Las direcciones físicas no dan información acerca de la subred en la que se encuentra el dispositivo como lo hacen las direcciones de capa 3 ya que estas son jerárquicas, si un dispositivo *host* pasa de una subred a otra su dirección MAC nunca va a cambiar.

La dirección física o MAC se utiliza únicamente para entregas en la red local, estas direcciones no tienen significado más allá de este segmento local.

Si el paquete en la trama debe pasar a otro segmento de la red, el dispositivo intermediario (un *router*) desencapsula la trama original, crea una nueva trama para el paquete y la envía al nuevo segmento. La nueva trama usa el direccionamiento de origen y de destino según sea necesario para transportar el paquete a través del nuevo medio.

2.5. CSMA/CD

Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones y para administrar la reanudación de las comunicaciones.

2.5.1. Detección de portadora

- En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.
- Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir.
- Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando

para detectar tráfico o colisiones en la LAN. Una vez que se envía el mensaje, el dispositivo regresa a su modo de escucha predeterminado.

2.5.2. Acceso múltiple

Si la distancia existente entre los dispositivos es tal que la latencia de las señales de un dispositivo denota que un segundo dispositivo no detecta las señales, el segundo dispositivo puede comenzar también a transmitir. Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren. En ese punto, las señales se mezclan y el mensaje se destruye. Aunque los mensajes se dañan, la mezcla de las señales restantes continúa propagándose en todo el medio.

2.5.3. Detección de colisiones

Cuando un dispositivo está en el modo de escucha, puede detectar cuando se produce una colisión en el medio compartido. La detección de una colisión es posible, porque todos los dispositivos pueden detectar un aumento de la amplitud de la señal por encima del nivel normal.

Una vez que se produce una colisión, los demás dispositivos que están en el modo de escucha, así como todos los dispositivos de transmisión, detectan el aumento de amplitud de la señal. Una vez detectada la colisión, todos los dispositivos transmisores continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.

2.5.4. Señal de congestión y postergación aleatoria

Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que estos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo escuchar antes de transmitir. El período de postergación aleatoria garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, esto también significa que un tercer dispositivo puede transmitir antes de que cualquiera de los dos dispositivos involucrados en la colisión original, tenga la oportunidad de volver a transmitir.

2.6. CSMA/CA

CSMA/CA especifica un procedimiento postergación aleatoria para todos los nodos que están esperando transmitir. La oportunidad más probable para la contención de medio es el momento en que el medio está disponible. Hacer el *backoff* de los nodos para un período aleatorio reduce en gran medida la probabilidad de colisión.

El estándar IEEE 802.11, comúnmente denominado Wi-Fi, es un sistema por contención que utiliza un proceso de acceso a los medios de Acceso múltiple con detección de portadora y prevención de colisiones (CSMA/CA).

2.7. ARP

El protocolo ARP (*Address Resolution Protocol*), tiene como funciones principales:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantenimiento de una caché de las asignaciones

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de enlace de datos para que se encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos que se mapea a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Cada entrada o fila de la tabla ARP tiene un par de valores: una dirección IP y una dirección MAC. La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la dirección MAC correspondiente. La tabla ARP almacena el mapeo de los dispositivos de la LAN local en la memoria caché.

Para comenzar el proceso, un nodo transmisor intenta localizar en la tabla ARP la dirección MAC asignada a un destino IPv4. Si este mapa está almacenado en la tabla, el nodo utiliza la dirección MAC como la MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se

produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones.

Otra manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud de ARP. El ARP envía un *broadcast* de capa 2 a todos los dispositivos de la LAN ethernet. La trama contiene un paquete de solicitud de ARP con la dirección IP del *host* de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya, responde enviando un paquete de respuesta de ARP al emisor como una trama *unicast*. Esta respuesta se utiliza entonces para crear una entrada nueva en la tabla ARP.

Estas entradas dinámicas en la tabla ARP tienen una marca horaria similar a la de las entradas de la tabla MAC de los *switches*. Si un dispositivo no recibe una trama de un dispositivo determinado antes de que venza la marca horaria, la entrada para este dispositivo se elimina de la tabla ARP. Además, pueden ingresarse entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y deben eliminarse en forma manual.

Todas las tramas deben enviarse a un nodo de un segmento de red local. Si el *host* IPv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

Si el *host* IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del *router* que es el *gateway* o el siguiente salto que se utiliza para llegar a dicho destino. El nodo de origen utilizará la

dirección MAC del *gateway* como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a *hosts* que se encuentren en otras redes.

La dirección de *gateway* de la interfaz del *router* se almacena en la configuración IPv4 de los *hosts*. Cuando un *host* crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de capa 3. Si el *host* receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del *router* que sirve de *gateway*.

En caso de que la entrada de *gateway* no se encuentre en la tabla, el proceso de ARP normal enviará una solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del *router*.

2.7.1. Sobrecarga en los medios

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de *broadcast*. En una red comercial típica, estos *broadcasts* tendrían probablemente un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendiera y todos comenzaran a acceder a los servicios de la red al mismo tiempo, podría haber una disminución del rendimiento durante un período de tiempo breve.

2.8. *Hubs* y *switches*

A continuación se realiza una descripción sobre los *hubs* y *switches*.

2.8.1. Hubs

Los *hubs* no realizan ningún tipo de filtro de tráfico. En cambio, el *hub* reenvía todos los bits a todos los dispositivos conectados al *hub*. Esto obliga a todos los dispositivos de la LAN a compartir el ancho de banda de los medios.

En una red con *hubs*, existe un límite para la cantidad de ancho de banda que los dispositivos pueden compartir. Con cada dispositivo que se agrega al medio compartido, el ancho de banda promedio disponible para cada dispositivo disminuye. Con cada aumento de la cantidad de dispositivos en los medios, el rendimiento se ve degradado.

La latencia de la red es la cantidad de tiempo que le lleva a una señal llegar a todos los destinos del medio. Cada nodo de una red basada en *hubs* debe esperar una oportunidad de transmisión para evitar colisiones. La latencia puede aumentar notablemente a medida que la distancia entre los nodos se extiende. La latencia también se ve afectada por un retardo de la señal en los medios, así como también por el retardo añadido por el procesamiento de las señales mediante *hubs* y repetidores.

El aumento de la longitud de los medios o de la cantidad de *hubs* y repetidores conectados a un segmento origina una mayor latencia. A mayor latencia, mayor probabilidad de que los nodos no reciban las señales iniciales, lo que aumenta las colisiones presentes en la red.

2.8.2. Switches

Los *switches* permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un *switch* representa un dominio de colisiones distinto

y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

Una LAN puede tener un *switch* centralizado que conecta a *hubs* que todavía proporcionan conectividad a los nodos. O bien, una LAN puede tener todos los nodos conectados directamente a un *switch.*

En una LAN en la que todos los nodos están conectados directamente al *switch,* el rendimiento de la red aumenta notablemente. Las tres principales razones de este aumento son:

- Ancho de banda dedicado a cada puerto
- Entorno libre de colisiones
- Operación *full-duplex*

Cada nodo dispone del ancho de banda de los medios completo en la conexión entre el nodo y el *switch.* Debido a que un *hub* replica las señales que recibe y las envía a todos los demás puertos, los *hubs* de *ethernet* clásica forman un bus lógico. Esto significa que todos los nodos deben compartir el mismo ancho de banda para este bus. Con los *switches*, cada dispositivo tiene una conexión punto a punto dedicada entre el dispositivo y el *switch*, sin contención de medios.

Una conexión punto a punto dedicada a un *switch* también evita contenciones de medios entre dispositivos, lo que permite que un nodo funcione con pocas colisiones o ninguna colisión. En una red *ethernet* clásica de tamaño moderado que utiliza *hubs*, aproximadamente entre el 40 % y el 50 % del ancho de banda se consume en la recuperación por colisiones. En una red *ethernet* con

switch, en la que prácticamente no hay colisiones, el gasto destinado a la recuperación por colisiones se elimina casi por completo. Esto le proporciona a la red con *switches* tasas de rendimiento notablemente mejoradas.

El uso de *switches* también le permite a una red funcionar como entorno de *ethernet full-duplex*. Antes de que existieran los *switches*, la *ethernet* solo era *half-duplex*. Esto implicaba que en un momento dado un nodo podía transmitir o recibir. Con la característica *full-duplex* habilitada en una red *ethernet* con *switches*, los dispositivos conectados directamente a los puertos del *switch* pueden transmitir y recibir simultáneamente con el ancho de banda completo de los medios.

3. PROTOCOLOS DE ENRUTAMIENTO Y SEGMENTACIÓN DE LA RED

3.1. *Router*

Un *router* es un dispositivo cuya funcionalidad es interconectar diferentes redes y segmentar los dominios de *broadcast*.

Otras funciones secundarias que un *router* realiza son:

- Asegurar la disponibilidad 24 horas del día, los 7 días de la semana. Para garantizar la posibilidad de conexión de la red, los *routers* usan rutas redundantes en caso de que la ruta principal falle.
- Proveen servicios integrados de datos, video y voz en redes conectadas por cable o inalámbricas. Los *routers* deben priorizar los paquetes IP según la calidad de servicio (QoS), con fin de asegurar que el tráfico en tiempo real, como la voz, el video y los datos esenciales, no se pierdan o sufran algún retraso.
- Disminuyen el impacto de gusanos, virus y otros ataques en la red mediante la autorización o el rechazo del reenvío de paquetes.

Un *router* es bastante similar a una computadora, por lo tanto está compuesto de estos componentes. Los *routers* tienen muchos s componentes de hardware y software que se encuentran en otras computadoras, entre ellos:

- CPU
- RAM

- ROM
- Sistema operativo

Ya que un *router* es capaz de interconectar varias redes, este posee varias interfaces las cuales operan en diferente segmento, cuando un paquete IP llega a un *router* este debe decidir hacia que interfaz reenviar el paquete.

Generalmente, cada red a la que se conecta un *router* requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de redes de área local (LAN) y redes de área extensa (WAN). Por lo general, las LAN son redes ethernet que contienen dispositivos como PC, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, una conexión WAN comúnmente se usa para conectar una LAN a la red del proveedor de servicios de internet (ISP).

Para determinar la mejor ruta hacia el destino un *router* debe utilizar una tabla de enrutamiento la cual se encuentra dentro de el. Cuando este recibe un paquete, examina su dirección ip dentro del encabezado de capa 3, busca la mejor coincidencia en la tabla de enrutamiento y envía el paquete hacia ese destino, esta tabla incluye la subred e interfaz hacia donde se enrrutará el paquete. Después de esto el *router* encapsula el paquete en una trama de enlace de datos y el paquete es enviado.

La manera en que los *routers* crean sus tablas de enrutamiento es por medio de protocolos de rutas estáticas y de enrutamiento dinámico para detectar redes remotas y actualizar estas tablas.

3.2. Enrutamiento estático

El enrutamiento estático es la manera más simple en como los *routers* pueden tener una tabla de enrutamiento convergente, las rutas estáticas son muy comúnes y no requieren la misma cantidad de procesamiento y sobrecarga que los protocolos de enrutamiento dinámico. La tabla de enrutamiento determinará finalmente la interfaz de salida para reenviar el paquete y el *router* lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.

Un *router* de inicio tendrá su tabla de enrutamiento vacío, para que esta puede empezar a llenarse de información, las interfaces del *router* deben estar encendidas y en funcionamiento. Al estar encendidas y bien configuradas las interfaces de un *router*, se agregan automáticamente rutas estáticas para los segmentos de estos *hosts* conectadas a las interfaces del *router*. Las rutas hacia diferentes redes deben ingresarse manualmente teniendo en cuenta algunos principios de la tabla de enrutamiento.

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única. Una red de conexión única es una red a la que se accede por una sola ruta. Hay tres principios los cuales rigen a la tabla de enrutamiento para *routers* los cuales son:

- Cada *router* toma sus propias decisiones en forma independiente, según la información de su propia tabla de enrutamiento.
- El hecho de que un *router* tenga cierta información en su tabla de enrutamiento no significa que los otros *routers* tengan la misma información.

- La información de enrutamiento acerca de la ruta de una red a otra no proporciona información de enrutamiento acerca de la ruta inversa o de retorno.

Independientemente de la marca de un *router*, las rutas estáticas pueden ser configuradas con una interfaz de salida, o con una dirección del siguiente salto. Cuando se habla de una interfaz de salida se hace referencia al puerto físico por donde debe salir el paquete ip para llegar a la red destino, y cuando se hace referencia al siguiente salto se refiere al *router* destino que debe alcanzar para llegar al destino.

Esta opción de configuración en *routers* se utiliza dependiendo del tipo de red y esto es porque la diferencia entre una red ethernet y una red serial punto a punto, es que una red punto a punto sólo tiene un dispositivo más en esa red (el *router* que se encuentra en el otro extremo del enlace). Con las redes ethernet, es posible que existan muchos dispositivos diferentes que comparten la misma red de accesos múltiples, incluyendo *hosts* y hasta *routers* múltiples. La designación de la interfaz de salida ethernet en la ruta estática por sí sola no provee al *router* información suficiente, para determinar qué dispositivo es el dispositivo del siguiente salto.

Para las rutas estáticas con redes seriales punto a punto de salida, es mejor configurar las rutas estáticas solamente con la interfaz de salida. Para interfaces seriales punto a punto, el proceso de entrega de paquetes nunca utiliza la dirección del siguiente salto en la tabla de enrutamiento, por lo que no se necesita. Para rutas estáticas con redes de salida ethernet, es mejor configurar las rutas estáticas tanto con la dirección del siguiente salto como con la interfaz de salida.

Cuando se necesita que todos los paquetes utilicen una ruta específica se utiliza una ruta por defecto o predeterminada la cual tiene las siguientes características:

Una ruta estática predeterminada es una ruta que coincidirá con todos los paquetes. Las rutas estáticas predeterminadas se utilizan en los siguientes casos:

- Cuando ninguna otra ruta de la tabla de enrutamiento coincide con la dirección IP de destino del paquete. En otras palabras, cuando no existe una coincidencia más específica. Se utilizan comúnmente cuando se conecta un *router* periférico de una compañía a la red ISP.
- Cuando un *router* tiene otro *router* único al que está conectado. Esta condición se conoce como *router* de conexión única.

Las rutas estáticas tienen una distancia administrativa predeterminada de "1". Esta distancia administrativa también se aplica a las rutas estáticas configuradas con una dirección del siguiente salto y una interfaz de salida. La distancia administrativa es un parámetro que utiliza la tabla de enrutamiento para decidir que ruta tiene prioridad sobre otra, esta se aplica en orden ascendente cero es el mejor valor.

3.3. Protocolos de enrutamiento vector distancia

Este tipo de protocolos de enrutamiento son como su nombre lo indica, "vector distancia" esto significa que las rutas se publican como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es el *router* del *next-hop* (siguiente salto) o la interfaz de salida.

Un *router* que utiliza un protocolo de enrutamiento vector distancia no tiene la información de la ruta completa hasta la red de destino, estos *routers* se valen únicamente de la siguiente información.

- La dirección o la interfaz en la que se deben reenviar los paquetes
- La distancia o la lejanía con respecto a la red de destino

Algunos protocolos de enrutamiento vector distancia solicitan al *router* que envíe periódicamente un *broadcast* de la tabla de enrutamiento hacia cada uno de sus *routers* vecinos. Este método no es eficiente porque las actualizaciones no solo consumen ancho de banda sino también los recursos de la CPU del *router* para procesar las actualizaciones.

Los protocolos de enrutamiento vector distancia comparten ciertas características:

- Las actualizaciones periódicas se envían a intervalos regulares (30 segundos para RIP y 90 segundos para IGRP). Incluso si la topología no ha cambiado en varios días, las actualizaciones periódicas continúan enviándose a todos los vecinos.

- Los vecinos son *routers* que comparten un enlace y que están configurados para usar el mismo protocolo de enrutamiento. El *router* solo conoce las direcciones de red de sus propias interfaces y las direcciones de red remota que puede alcanzar a través de sus vecinos. No tiene un conocimiento más amplio de la topología de la red. Los *routers* que utilizan el enrutamiento vector distancia no tienen información sobre la topología de la red.

- Las actualizaciones de *broadcast* se envían a 255.255.255.255. Los *routers* vecinos que están configurados con el mismo protocolo de enrutamiento procesarán las actualizaciones. Todos los demás dispositivos también procesarán la actualización hasta la capa 3 antes de descartarla. Algunos protocolos de enrutamiento vector distancia usan direcciones de multicast en vez de direcciones de *broadcast*.

- Las actualizaciones de toda la tabla de enrutamiento se envían periódicamente a todos los vecinos, salvo algunas excepciones que se analizará más adelante. Los vecinos que reciban estas actualizaciones deben procesar toda la actualización para encontrar información pertinente y descartar el resto.

Los protocolos de enrutamiento tienen las siguientes características:

- Tiempo de convergencia: el tiempo de convergencia define que tan rápido los *routers* que están en la topología pueden compartir su información que tienen en la tabla de enrutamiento. Cuanto más rápida sea la convergencia en una red mucho más eficiente y preferible será el protocolo de enrutamiento. Los *loops* de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.

- Escalabilidad: la escalabilidad define cuán grande puede ser una red según el protocolo de enrutamiento que se implementa, una red que sea lo suficientemente grande debe tener un protocolo de enrutamiento que sea capaz de lograr una convergencia absoluta.

- Sin clase (uso de VLSM) o con clase: los protocolos de enrutamiento sin clase incluyen la máscara de subred de las actualizaciones. Esta función admite el uso de la máscara de subred de longitud variable (VLSM), al utilizar esta función se puede tener una mejor sumarización de rutas que ayudan a que las tablas de enrutamiento sean más cortas. Por otro lado las redes actuales todas están segmentadas en bloques de máscara de subred variable, por este motivo es importante que el protocolo incluya estas actualizaciones en sus estados.

- Uso de recursos: el uso de recursos incluye los requisitos de un protocolo de enrutamiento, como por ejemplo, el espacio de memoria, y la utilización de la CPU y el ancho de banda del enlace. De esta manera el hardware que debe utilizarse debe tener mucha mayor capacidad en cuanto a rendimiento y potencia para admitir el funcionamiento de características que ayuden a la convergencia y el buen mantenimiento en tablas de rutas.

- Implementación y mantenimiento: la implementación y el mantenimiento describen el nivel de conocimiento requerido para que un administrador de red ponga en práctica y mantenga la red según el protocolo de enrutamiento aplicado.

- Si se configura un protocolo de enrutamiento, los *routers* comienzan a intercambiar actualizaciones de enrutamiento. Inicialmente, estas actualizaciones solo incluyen información acerca de sus redes conectadas directamente. Una vez recibida la actualización, el *router* verifica si contiene información nueva. Se agregan todas las rutas que actualmente no se encuentran en su tabla de enrutamiento.

3.3.1. RIP

El RIP evolucionó a partir de un protocolo anterior desarrollado en Xerox, llamado protocolo de información de *gateway* (GWINFO) y significa Routing Information Protocol. Con el desarrollo de Xerox Network System (XNS), GWINFO se convirtió en RIP. Luego, adquirió popularidad ya que se implementó en la Distribución del Software Berkeley (BSD) como un *daemon* denominado *routed* (se pronuncia "routi-dí" y no "routid"). Algunos fabricantes realizaron sus propias y ligeramente diferentes implementaciones de RIP. En reconocimiento de la necesidad de estandarización del protocolo, Charles Hedrick escribió RFC 1058 en 1988, donde documentó el protocolo existente y especificó ciertas mejoras. Desde entonces, se mejoró el RIP con RIPv2 en 1994 y con RIPng en 1997.

- Características del RIP:

    - RIP es un protocolo de enrutamiento que se maneja como vector distancia.
    - RIP utiliza el conteo de saltos o *routers* en el camino como su métrica para la selección de rutas.
    - Las rutas publicadas con conteo de saltos (*routers* en el camino) mayores que 15 son inalcanzables.
    - Los mensajes se transmiten cada 30 segundos.

- Temporizadores del RIP: Utiliza tres tipos de temporizadores para poder funcionar de manera correcta, temporizador de invalidez. Si no se recibió una actualización para renovar la ruta existente una vez que hayan transcurrido 180 segundos (predeterminado), la ruta se marca como no válida y la métrica se configura en 16. Se retiene la ruta en la tabla de enrutamiento hasta que se vence el temporizador de purga.

- Temporizador de purga: de manera predeterminada, este se configura en 240 segundos, es decir, 60 segundos más que el temporizador de invalidez. Cuando vence el temporizador de purga, la ruta se elimina de la tabla de enrutamiento.

Temporizador de espera: estabiliza la información de enrutamiento y ayuda a evitar *loops* de enrutamiento durante los períodos en los que la topología converge en la nueva información. Una vez que se marca una ruta como inalcanzable, esta debe permanecer en espera el tiempo suficiente como para que todos los *routers* de la topología aprendan sobre la red inalcanzable. De manera predeterminada, el temporizador de espera está configurado en 180 segundos.

RIP V1 y V2 son protocolos de enrutamiento estado enlace, la diferencia principal entre ellos es que la versión uno del protocolo es un protocolo con clase y la versión dos es un protocolo sin clase que admite VLSM, CIDR, permite desactivar la sumarización de rutas y envía actualizaciones por medio de multicast y no *broadcast*.

Dentro de las ventajas de los protocolos de enrutamiento vector distancia se pueden mencionar:

- Poca utilización de recursos por parte de los *routers* comparado con otro tipo de protocolos.
- Fácil configuración por parte de los administradores de red.

Dentro de las desventajas de los protocolos de enrutamiento vector distancia se pueden mencionar:

- Convergencia lenta de las tablas de ruta lo que puede provocar pérdida de paquetes mientras las tablas convergen.
- Métricas bastante cortas para redes que son grandes hacen que estos protocolos sean obsoletos para este tipo de redes.
- Desconocimiento de la topología completa de red puede provocar bucles de enrutamiento, provocando congestionamiento en la red y consumo de ancho de banda innecesario.

3.4. Protocolos de enrutamiento de estado-enlace

Los protocolos de enrutamiento vector distancia son como las señales de tránsito en carreteras, ya que los *routers* deben tomar sus decisiones con base en una distancia específica o algún tipo de métrica dentro de la red. Del mismo modo que un viajero debe confiar en que esta señal sea verídica y sea capaz de llevarlo hasta un destino.

Un *router* vector distancia confía en que otro *router* publique la verdadera distancia hacia la red de destino, ya que este tipo de protocolos no permiten el conocimiento de una topología entera de la red, o en el caso de un viajero todo el camino hacia el destino.

Los protocolos de enrutamiento de estado-enlace son similares a un mapa completo que incluye todas las carreteras y caminos posibles hacia un destino, ya que estos crean un mapa topológico de la red y cada *router* utiliza dicho mapa para determinar la ruta más corta hacia cada red.

Cuando en la red existen *routers* que ejecutan protocolos estado-enlace, estos envían información acerca del estado de sus enlaces hacia otros *routers*

dentro del dominio de enrutamiento, el nombre de estado enlace proviene que estos *routers* hacen referencia a sus redes conectadas directamente, e incluye información acerca del tipo de red y los *routers* vecinos en dichas redes.

El objetivo final es que cada *router* reciba toda la información de estado-enlace acerca de todos los demás *routers* en el área de enrutamiento. Con esta información de estado-enlace, cada *router* puede crear su propio mapa topológico de la red y calcular independientemente la ruta más corta hacia cada red.

A estos protocolos de estado-enlace también se les conoce como protocolos de Shortest path first y se desarrollan en torno del algoritmo *Shortest path first* (SPF) de Edsger Dijkstra.

Algunos protocolos de enrutamiento que utilizan este algoritmo son:

- Open Shortest Path First (OSPF)
- Intermediate-System-to-Intermediate-System (IS-IS)

Este tipo de protocolos son conocidos por presentar una complejidad bastante mayor que sus vectores distancia equivalentes. Sin embargo, la funcionalidad y configuración básicas de los protocolos de enrutamiento de estado-enlace no son complejas en absoluto.

La manera en que los protocolos de enrutamiento estado-enlace, comparten sus actualizaciones es de la siguiente manera:

- Un *router* es dueño de su información y dentro de esta se encuentran sus propios enlaces, sus propias redes que conecta directamente a los

segmentos de red locales. El *router* realiza esta acción al detectar que alguna de sus interfaces este en estado activo.

- Un *router* tiene la responsabilidad de mantener un dialogo con sus vecinos a los que conecta directamente, esta conversación entre *routers* se establece mediante el intercambio de paquetes de saludo con otros *routers* de estado-enlace.

- Los paquetes que crean los *routers* de estado enlace (LSP) debe de incluir el estado de cada enlace conectado. La forma en que los *routers* deben realizar esto es registrando toda la información pertinente acerca de cada vecino, que incluye el ID de vecino, el tipo de enlace y el ancho de banda.

- Los LSP recibidos por los vecinos deben ser almacenados en una base de datos, para luego ser saturados hacia los *routers* vecinos hasta que todos los *routers* hayan recibido los LSP. Cada *router* almacena una copia de cada LSP recibido por parte de sus vecinos en una base de datos local.

- Un mapa completo de la topología en conjunto con el mejor camino hacia las redes destino, deben ser creados de la base de datos. Este mapa debe de ser construido con el algoritmo SFP y así determinar la mejor ruta.

3.4.1. OSPF

El desarrollo inicial de OSPF comenzó en 1987 por parte del grupo de trabajo de OSPF, el Grupo de Trabajo de Ingeniería de Internet (IETF). En aquel

momento, internet constituía fundamentalmente una red académica y de investigación financiada por el gobierno de los EE. UU.

En 1989 se publicó la especificación para OSPFv1 en RFC 1131. Había dos implementaciones desarrolladas: una para ejecutar en *routers* y otra para ejecutar en estaciones de trabajo UNIX. La última implementación se convirtió luego en un proceso UNIX generalizado y conocido como GATED. OSPFv1 era un protocolo de enrutamiento experimental y nunca se implementó.

En 1991, John Moy introdujo OSPFv2 en RFC 1247. OSPFv2 ofrecía significativas mejoras técnicas con respecto a OSPFv1. Al mismo tiempo, ISO trabajaba en un protocolo de enrutamiento de *link-state* propio, Intermediate System-to-Intermediate System (IS-IS). Lógicamente, IETF eligió OSPF como su IGP (Interior Gateway Protocol) recomendado.

En 1998 se actualizó la especificación OSPFv2 en RFC 2328, y hoy en día representa la RFC para OSPF.

OSPF utiliza cierto tipo de paquetes LSP los cuales se explican a continuación:

- Saludo: este tipo de paquetes se utilizan para iniciar y darle mantenimiento a las adyacencias con otro *routers*.

- DBD: está definido como paquete de descriptores de bases de datos, tiene una pequeña lista de la base datos para el estado-enlace del *router* emisor. Los otros *routers* (receptores) lo utilizan para realizar comparaciones con la base de datos propia de estado-enlace.

- LSR: este sirve para que los *routers* que reciben LSP puedan solicitar más información acerca de entradas específicas en la base de datos mandando una solicitud estado-enlace LSR.

- LSU: estos paquetes son actualizaciones correspondientes a las solicitudes LSR. También son utilizados para anunciar nueva información y estos contienen diferentes tipos de notificaciones según sea necesario.

- LSAck: son acuses de recibo para un paquete LSU.

Dentro de las ventajas de los protocolos de enrutamiento estado-enlace se pueden mencionar:

- Cada *router* forma su mapa donde se puede apreciar toda la topología de la red, así si hubieran varias rutas hacia el destino el *router* puede elegir cual es la mejor ruta.

- Gracias a los mensajes LSP no solo está asegurada la convergencia de la red si no también que esta lo haga de una manera rápida.

- Dado que los mensajes LSP, se disparan únicamente cuando hay eventos relevantes se tiene una mejor utilización del ancho de banda.

Dentro de las desventajas de los protocolos de enrutamiento estado-enlace se pueden mencionar:

- Consumen mayores recursos como CPU, memoria y almacenamiento dentro de los *routers*.

- Los administradores de red necesitan tener un conocimiento amplio de redes para evitar configuraciones erróneas en los protocolos, esto podría dar lugar a tablas de rutas erróneas y fallas en la red.

3.5. VLAN

Con nuevas aplicaciones hoy en día el rendimiento de la red es un factor clave en la productividad de un negocio u organización, la capacidad para realizar transacciones críticas y que estas sean efectivas torna un ambiente de alta disponibilidad. Dentro de las tecnologías que ayudan a mejorar el rendimiento de una red están las VLAN. Estas hacen que los dominios de *broadcast* estén segmentados y se agrupen de manera que sean grupos funcionales. De esta manera se asegura una mayor disponibilidad para servicios específicos en una organización.

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Un puerto de *switch* con una VLAN singular configurada en el mismo se denomina puerto de acceso.

Dentro de los beneficios que tienen las VLAN se pueden mencionar:

- Seguridad: datos importantes, sensibles y confidenciales pueden ser aislados del resto de la red, disminuyendo violaciones a la seguridad de la información confidencial. Aunque el motivo principal para que una VLAN haya sido creada es puramente rendimiento de la red, se puede mencionar la seguridad como un agregado.

- Reducción de costos: este ahorro se obtiene de la optimización de ancho de banda existente que sin las VLAN tendrían una repercusión en redes costosas.

- Mejor rendimiento: al segmentar los dominios de *broadcast* en múltiples grupos lógicos de trabajo, se mitiga tráfico innecesario en la red que hace que el rendimiento se degrade.

- Mitigación de la tormenta de *broadcast*: la división de una red en las VLAN reduce el número de dispositivos que pueden participar en una tormenta de *broadcast*.

- Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un *switch* nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre.

- Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de E-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

Todas las VLAN de acceso están divididas en dos tipos de rangos los cuales son el normal y el extendido.

- VLAN de rango normal

    - Se utiliza en redes de pequeños y medianos negocios y empresas.
    - Se identifica mediante un ID de VLAN entre 1 y 1005.
    - Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
    - Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar. Aprenderá más acerca de VLAN 1 más adelante en este capítulo.

- VLAN de rango extendido

    - Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.
    - Se identifican mediante un ID de VLAN entre 1006 y 4094.
    - Admiten menos características de VLAN que las VLAN de rango normal.
    - Se guardan en el archivo de configuración en ejecución.

Dentro de las VLAN hay cierto tipo de términos que identifican al tipo de tráfico que maneja una determinada VLAN.

- VLAN de datos: las VLAN de datos se utilizan para tráfico de datos generado por usuarios que poseen dispositivos finales. Es una práctica

común el separar los datos como voz o tráfico de administración de red. Esto por varias de las ventajas mencionadas anteriormente.

- VLAN predeterminada: cuando un *switch* inicia por primera vez, este no tiene ninguna configuración presente y todos sus puertos son miembros de la VLAN predeterminada, por tanto todos pertenecen al mismo dominio de *broadcast* y hace que todos los dispositivos conectados a estos puertos se puedan interconectar entre ellos.

- VLAN de administración: esta VLAN tiene como finalidad acceder a la administración de *switches*. En dispositivos de capa 2 la VLAN de administración es la única que puede tener asignada una dirección IP, en cualquier *switch* independiente de la marca la VLAN 1 está configurada por defecto como VLAN de administración. Con una VLAN de administración configurada un *switch* se puede administrar por medio de varios protocolos como HTTP, Telnet, SSH o SNMP.

- VLAN de voz: actualmente hay muchas empresas que transmiten voz y video sobre IP, y para cierto tipo de negocios la voz es un servicio crítico que debe funcionar en su totalidad para no perder algún dato de alta importancia, en base a este argumento el tráfico de voz sobre IP tiene ciertos requerimientos como:

    - Ancho de banda garantizado para asegurar la calidad de la voz
    - Prioridad de la transmisión sobre los tipos de tráfico de la red
    - Capacidad para ser enrutado en áreas congestionadas de la red
    - Demora de menos de 150 milisegundos (ms) a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP, y la segmentación de un dominio de *broadcast* exclusivo para voz es la mejor manera de realizarlo.

- Enlace troncal para VLAN: un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. EL enlace debe admitir IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast ethernet y Gigabit ethernet. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre *switches* y *routers*.

3.6. STP

La elección de diferentes rutas y redundancia permite una alta disponibilidad en una red, ya que permite que los datos puedan ser transmitidos si llegara a encontrase alguna falla en alguna de las distintas rutas hacia el destino. Sin embargo la redundancia cuenta con cierto tipo de complicaciones las cuales deben ser tomadas en cuenta para no degradar el funcionamiento de la red, en el peor de los casos una redundancia mal implementada puede dejar fuera de servicio una red. El protocolo STP Spanning Tree Protocol hace énfasis en estos parámetros para poder proporcionar una redundancia segura.

3.6.1. Bucles de la capa 2

La redundancia es una parte importante del diseño jerárquico. Pese a que es importante para la disponibilidad, existen algunas consideraciones que deben

atenderse antes de que la redundancia sea posible en una red. El primer problema que se experimenta cuando se tienen rutas redundantes es el de los bucles a nivel de capa 2, sin la existencia del protocolo Spanning Tree. Los *broadcast* pueden llegar a provocar este tipo de problema y consumir ancho de banda de manera no deseada.

La diferencia que tienen las tramas ethernet a nivel de capa 2 comparada con los paquetes IP en capa 3 es que estas no poseen un tiempo de vida TTL. Como consecuencia de ello las tramas que viajan como consecuencia de una mala configuración en un *switch* nunca son descartadas, y consumen el ancho de banda de la red sin manera de mitigar este tipo de incidente hasta que se interrumpa el enlace.

En el funcionamiento normal de un *switch* las tramas de *broadcast* se envían a todos los puertos de *switch*, excepto el puerto de origen. Esto asegura que todos los dispositivos del dominio de *broadcast* puedan recibir la trama. Si existe más de una ruta para enviar la trama, se puede generar un bucle sin fin.

Cuando este incidente se da en alguna red los bucles producen una alta carga de CPU en todos los *switches* atrapados en el mismo. Lo cual degrada el tiempo de vida del dispositivo, ya que se envían las mismas tramas constantemente entre todos los *switches* del bucle, la CPU del *switch* debe procesar una gran cantidad de datos. El rendimiento de los dispositivos se ve afectado por estos bucles.

Un dispositivo final que se encuentra en medio de un bucle de capa 2 es totalmente inaccesible para otros *hosts* en la red, esto porque la tabla de direcciones MAC está cambiando constantemente conforme a las actualizaciones provenientes de las tramas de *broadcast*.

Esto provoca que el *switch* no pueda identificar a que puerto debe enviar las tramas de únicas para que estas puedan llegar hasta el *host* destino. Las tramas de *unicast* también quedan atrapadas en el bucle de red. A medida que aumenta la cantidad de tramas que quedan atrapadas en el bucle de red, se produce una tormenta de *broadcast*.

3.6.2. Tormentas de *broadcast*

Este tipo de tormentas son consecuencia de una gran cantidad de tramas de *broadcast* atrapadas en un bucle de capa 2, esta tormenta consume todo el ancho de banda disponible y como efecto no existe trayectoria alguna para el tráfico legítimo y de alta disponibilidad en la red.

En una red con bucles es inevitable una tormenta de *broadcast*, conforme cada dispositivo.

La tormenta de *broadcast* es inevitable en una red con bucles. A medida que más dispositivos envían *broadcast* a la red, aumenta la cantidad de tráfico que queda atrapado en el bucle, lo que eventualmente genera una tormenta de *broadcast* que produce la falla de la red.

Otras consecuencias también se hacen presentes por las tormentas de *broadcast*, ya que el tráfico se envía a todos los puertos el *switch,* los *hosts* deben procesar este tráfico que fluye sin rumbo indefinido por los bucles, lo que puede provocar que los dispositivos finales como computadoras, teléfonos IP gasten recursos en este tipo de tráfico. En una red grande en producción el consumo de CPU y memoria en estos dispositivos puede ser tan alto que podrían sufrir daños irreparables.

Las tramas de *broadcast* no son el único tipo de tramas que son afectadas por los bucles. Las tramas de *unicast* enviadas a una red con bucles pueden generar tramas duplicadas que llegan al dispositivo de destino. Afortunadamente, los *switches* pueden detectar bucles en una red. El protocolo Spanning Tree (STP) elimina estos inconvenientes relacionados con bucles. STP se asegura que de todas las rutas que existan hacia un destino, solo exista realmente una ruta lógica, de esta manera todas las rutas redundantes que puedan generar un bucle se encuentran sin tráfico. Existen varios estados de los puertos cuando se utiliza Spanning Tree como el estado de bloqueo el cual se caracteriza porque el tráfico de la red no puede entrar ni salir del puerto.

Sin embargo, esto no significa que no reciba tráfico de la unidad de datos del protocolo de Puentes (BPDU) que son utilizados los por STP para decidir que puertos envían o no tráfico. Las rutas físicas nunca dejan de existir simple y sencillamente se deshabilitan para evitar los bucles de capa 2, si alguna ruta activa en ese preciso momento llegara a fallar, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que una ruda redundante se active.

3.6.3. Algoritmo STP

STP utiliza el algoritmo de Spanning Tree (STA) para determinar los puertos de *switch* de la red que deben configurarse para el bloqueo a fin de evitar que se generen bucles. El STA designa un único *switch* como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. Los *switches* intercambian tramas BPDU para determinar el *switch* que posee el menor BID o ID de puente. El *switch* con el menor BID se convierte en el puente raíz en caso

que dos *switches* tuvieran el mismo BID, es la dirección MAC la decisión para convertirse en el puente raíz.

Los *switches* que utilizan STP intercambian BPDU, cada BPDU contiene un BID que identifica al *switch* emisor de la trama, dentro del BID se encuentra un valor de prioridad, la dirección MAC del switch emisor y un ID de sistema extendido opcional.

Una vez calculado el puente raíz, el STA debe calcular la ruta más corta hacia el mismo, todos los *switches* utilizan este algoritmo para determinar los puertos que deben estar bloqueados. Mientras el algoritmo calcula las mejores rutas hacia el puente raíz, los puertos permanecen en un estado de bloqueo.

Una vez terminado el proceso de arranque el STP queda determinado, si algún puerto tuviera algún cambio de estado, por ejemplo bloqueo a enviar. Ese puerto podría provocar un bucle de capa 2 temporalmente. Por esta razón SpanningTree introduce cinco estados de puertos los cuales son utilizados por el protocolo antes y después de calcular el puente raíz.

Los estados de puerto son:

- Bloquear: el puerto es un puerto no designado y no participa en el envío de tramas. El puerto recibe tramas de BPDU para determinar la ubicación y el ID de raíz del *switch* del puente raíz y las funciones de puertos que cada uno de estos debe asumir en la topología final de STP activa.

- Escuchar: STP determina que el puerto puede participar en el envío de tramas de acuerdo a las tramas de BPDU que el *switch* ha recibido hasta ahora. En este momento, el puerto de *switch* no sólo recibe tramas de

BPDU, sino que también transmite sus propias tramas de BPDU e informa a los *switches* adyacentes que este se prepara para participar en la topología activa.

- Aprender: el puerto se prepara para participar en el envío de tramas y comienza a llenar la tabla de direcciones MAC.

- Reenviar: el puerto se considera parte de la topología activa, envía tramas y envía y recibe tramas de BPDU.

- Deshabilitado: el puerto de la capa 2 no participa en el Spanning Tree y no envía tramas. El estado deshabilitado se establece cuando el puerto de *switch* se encuentra administrativamente deshabilitado.

Los pasos que utiliza el Spanning Tree para su convergencia son:

- Paso 1. Elegir un puente raíz
- Paso 2. Elegir los puertos raíz
- Paso 3. Elegir los puertos designados y no designados

Algunas variantes de STP son Rapid Spanning Tree (RSTP) que corresponde al estándar IEEE 802.1w y Multiple Spanning Tree (MSTP) correspondiente al estándar IEEE 802.1s

4. VULNERABILIDAD DE LA RED

A medida que las redes han ido creciendo la seguridad se ha vuelto un factor totalmente importante, cada día las redes convergentes tienen más tráfico de diferentes categorías. Sabiendo esto la integridad y confidencialidad de los datos se vuelve crucialmente importante para empresas que dependan directamente de la red. Si la seguridad de la red se ve afectada se podrían tener pérdidas de datos, privacidad, robo de información en incluso mala utilización de una red. Además, el aumento del comercio móvil y de las redes inalámbricas exige soluciones de seguridad perfectamente integradas, más transparentes y más flexibles.

4.1. Amenazas comunes a la seguridad de la red

En el análisis de la seguridad de la red, los tres factores comunes son vulnerabilidad, amenaza y ataque. La vulnerabilidad en una red está definida como la debilidad de esta y de los dispositivos que la integran, esto incluye tanto dispositivos finales como intermediarios.

Las amenazas son los personajes con capacidad para aprovechar las vulnerabilidades en lo que a seguridad se refiere, este tipo de personas están buscando generalmente debilidades y la explotación de las mismas.

Las amenazas son programas, secuencias de comandos y herramientas especiales para poder iniciar un ataque en contra de una red y sus dispositivos, generalmente los equipos atacados son dispositivos finales como servidores y computadoras de escritorio. Dentro de las debilidades principales se tienen:

- Debilidades en la tecnología
- Debilidades en la configuración
- Debilidades en las políticas de seguridad

Dentro de las debilidades de tecnología se pueden mencionar debilidades en protocolos, sistemas operativos y en los equipos de red. En debilidades de configuración se tienen contraseñas inseguras, servicios de internet mal configurados, configuraciones predeterminadas no seguras. Para finalizar dentro de las debilidades de políticas de seguridad se puede mencionar falta de políticas por escrito, políticas obsoletas, instalación de software no autorizado, plan de consistencia ante desastres.

4.1.1. Debilidad en el protocolo TCP/IP

Existen ciertos protocolos que no tienen seguridad alguna sobre los datos que transportan, esto hace que sean susceptibles a ataques comprometedores, los cuales pueden resultar en robo de información confidencial y mal uso de la misma.

Dentro de las debilidades que se encuentra está la falta de encriptación y cifrado en los datos, así como algoritmos para descifrar claves ocultas en el intercambio de mensajes como protección.

Como ejemplo se pueden nombrar los protocolos:

- HTTP (Hypertext transfer protocol)
- FTP (File transfer protocol)
- Telnet
- ICMP

- SNMP V1/V2
- SMTP

La mayoría de protocolos hoy en día, han modificado ciertas características para poder operar de manera segura por ejemplo HTTPS, SSH, SNMP V3.

4.1.2. Debilidad en sistemas operativos

Los sistemas operativos juegan un papel importante en el día a día de todas las empresas, no existe empresa alguna que no utilice equipos de cómputo para poder resolver los problemas del día a día. Uno de los mayores desafíos es poder mantener un sistema operativo sin problemas, para evitar perder información importante o degradar el equipo y tener un rendimiento deficiente del mismo.

En un sistema operativo se deben tomar en cuenta ciertos parámetros para que este sea menos vulnerable a ataques en la red:

- Vigilancia: la vigilancia se compone de la verificación y la auditoria del sistema, y la identificación de usuarios. En la vigilancia se utilizan sistemas muy sofisticados, a tal punto, que a veces pueden surgir problemas en la autentificación, generando un rechazo al usuario legítimo.

- Monitoreo de amenazas: una manera de reducir los riesgos de seguridad es tener rutinas de control en el sistema operativo para permitir o no el acceso a un usuario. Estas rutinas interactúan con los programas de usuario y con los archivos del sistema. De esta manera, cuando un usuario desea realizar una operación con un archivo, las rutinas determinan si se niega o no el acceso y en caso de que el mismo fuera permitido devuelven

los resultados del proceso. Además las rutinas de control permiten detectar los intentos de penetración al sistema y advertir en consecuencia.

- Protección por contraseña: existen tres clases principalmente de elementos que permiten establecer la identidad de un usuario:

    - Algo sobre las personas. Esto incluye huellas digitales, reconocimiento de voz, fotografía y firmas.

    - Algo poseído por la persona. Esto incluye distintivos, tarjetas de identificación y llaves.

    - Algo conocido por el usuario. Esto incluye contraseñas, nombre de la suegra, combinación de cerraduras. El esquema de autentificación más común es la simple protección por contraseña. El usuario elige una palabra que se le viene a la memoria, y la tipea de inmediato para ganar admisión al sistema de computación.

Muchos sistemas no muestran la contraseña tal como ha sido ingresada (mostrar asteriscos en lugar de letras). La protección por contraseña es un esquema débil. En el sentido de que los usuarios tienden a elegir contraseñas fáciles de recordar. Entonces alguien que conoce al usuario podría intentar ingresar al sistema usando nombres de gente que la persona conoce. Esto puede resultar en una violación de la seguridad por los intentos repetitivos de ingreso. Algunos sistemas usan contraseñas cortas lo que facilita la conformación rápida de la lista de todas las posibles combinaciones. Los sistemas actuales utilizan contraseñas largas para frenar tales intentos de penetración.

- Auditoría: la auditoría normalmente es realizada en sistemas manuales "después del hecho". Los auditores son llamados periódicamente para examinar las transacciones recientes de una organización y para determinar si ha ocurrido actividad fraudulenta. El registro de auditoría es un registro permanente de acontecimientos de importancia que ocurren en el sistema de computación. Se produce automáticamente cada vez que ocurren los eventos y es almacenado en un área protegida del sistema. Las auditorias periódicas prestan atención regularmente a problemas de seguridad; las auditorías al azar ayudan a detectar intrusos.

Dentro de los sistemas operativos más comunes se tienen:

- UNIX
- Linux
- Mac OS
- Microsoft Windows
- AIX
- Sun Solaris

4.1.3. Debilidad de los equipos de red

Varios tipos de equipos de red, como *routers*, *firewalls* y *switches* poseen debilidades de seguridad que se deben reconocer y combatir. Sus debilidades incluyen la protección de contraseñas, la falta de autenticación, los protocolos de enrutamiento y los agujeros de *firewall*.

Cierto tipo de protocolos de enrutamiento no manejan encriptación en las actualizaciones de estado que manejan, así tampoco autenticación entre ellos, lo que podría provocar que cualquier dispositivo que emule un protocolo de

enrutamiento reciba información de todas las redes que tiene *routers* conectadas directamente, o en su defecto insertar información falsa en actualizaciones incorrectas y provocar que la red no sea convergente, bucles de enrutamiento o sobrecarga en los equipos de red.

Todos los equipos de red deben estar con el software actualizado en su última versión para evitar que *bugs* o problemas en sus aplicaciones aumenten el riesgo de perder datos importantes para cualquier organización.

4.1.4. Amenazas a la infraestructura física

Un tipo de amenaza muy importante es cuando se atenta contra la seguridad física de dispositivos, no solo personas que poseen conocimiento informático pueden llegar provocar daños en una red, un agresor puede inhabilitar los recursos de red si estos se ven comprometidos de manera física, personas sin autorización en salas de equipos o *data centers*, o a veces equipos que solo se encuentran montados en alguna pared pueden ser fácil mente dañados o modificados. Las cuatro clases de amenazas físicas son:

- Amenazas al hardware: daño físico a los servidores, *routers*, *switches*, planta de cableado y estaciones de trabajo.

- Amenazas ambientales: temperaturas extremas (calor o frío extremos) o condiciones extremas de humedad (humedad o sequedad extremas).

- Amenazas eléctricas: picos de voltaje, voltaje suministrado insuficiente (apagones), alimentación ilimitada (ruido) y pérdida total de alimentación.

- Amenazas al mantenimiento: manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos fundamentales, cableado insuficiente y rotulado incorrecto.

Una buena política dentro de la organización debe abordar estos temas de amenaza, las consecuencias de no tomar en cuenta las mismas puede traer desastres irreparables en una red de producción.

4.1.5. Amenazas a las redes

Las amenazas a redes pueden darse de diferentes maneras y no necesariamente debe tenerse conocimientos en informática y programación, para poder atacar una red actualmente en internet, se pueden encontrar software malicioso y malintencionado con finalidad de ataque hacia redes. Dependiendo del tipo de amenaza estas se pueden clasificar en amenazas estructuradas y amenazas no estructuradas.

4.1.6. Amenazas no estructuradas

Este tipo de amenazas se caracteriza por personas sin experiencia que utilizan herramientas hechas para piratería pero de fácil acceso, este tipo de herramientas se pueden encontrar hoy en día de manera muy fácil en internet, dentro de estas herramientas se pueden mencionar comandos de Shell y *crackers* de contraseñas. Generalmente las personas que ejecutan este tipo de amenazas lo hacen con el propósito de probar sus propias habilidades y conocimiento, sin embargo en redes que no cuentan con la seguridad adecuada pueden provocar daños bastante graves.

4.1.7. Amenazas estructuradas

Las amenazas estructuradas provienen de personas o grupos que tienen una mayor motivación y son más competentes técnicamente. Estas personas conocen las vulnerabilidades del sistema y utilizan técnicas de piratería informática sofisticadas para introducirse en las empresas confiadas. Ingresan en computadoras de empresas y del gobierno para cometer fraude, destruir o alterar registros o, simplemente, para crear confusión. Por lo general, estos grupos están involucrados en los principales casos de fraude y robo denunciados en los organismos de aplicación de la ley. Utilizan tácticas de piratería informática tan compleja y sofisticada, que sólo los investigadores especialmente capacitados entienden lo que está ocurriendo.

4.1.8. Amenazas externas

Las amenazas externas pueden provenir de personas u organizaciones que trabajan fuera de una empresa y que no tienen acceso autorizado a los sistemas informáticos ni a la red. Ingresan a una red principalmente desde internet o desde servidores de acceso telefónico. Las amenazas externas pueden tener distintos grados de gravedad según la experiencia del agresor, ya sea aficionado (no estructurado) o experto (estructurado).

4.1.9. Amenazas internas

Las amenazas internas son las provocadas por una persona que tiene acceso autorizado a la red, ya sea mediante una cuenta o acceso físico. Al igual que en el caso de las amenazas externas, la gravedad de una amenaza interna depende de la experiencia del agresor.

4.1.10. Ingeniería social

La piratería informática más sencilla no requiere habilidad informática alguna. Si un intruso puede engañar a un miembro de una organización para que le proporcione información valiosa, como la ubicación de los archivos o de las contraseñas, el proceso de piratería informática se torna mucho más fácil. Este tipo de ataque se denomina ingeniería social, y se aprovecha de las vulnerabilidades personales que pueden ser descubiertas por agresores talentosos. Puede incluir apelaciones al ego de un empleado, o bien puede tratarse de una persona simulada o un documento falsificado que logra que una persona proporcione información confidencial.

La suplantación de identidad es un tipo de ataque de ingeniería social que involucra el uso de correo electrónico u otros tipos de mensajes para intentar engañar a otras personas, de modo que brinden información confidencial, como números de tarjetas de crédito o contraseñas. El estafador se hace pasar por una persona de confianza que tiene una necesidad aparentemente legítima de obtener información confidencial.

Con frecuencia, los fraudes de suplantación de identidad involucran el envío de correo no deseado que aparenta provenir de sitios de banca o de subastas en línea. La figura muestra una réplica de dicho correo electrónico. La empresa real utilizada como señuelo de este ejemplo se ha modificado.

Estos correos electrónicos contienen hipervínculos que parecen legítimos, pero que, en realidad, llevan a los usuarios a un sitio web falso creado por el estafador para capturar su información. El sitio aparenta pertenecer a la parte

cuya identidad se falsificó en el correo electrónico. Cuando el usuario introduce la información, se registra para que la utilice el estafador.

4.2. Tipos de ataques a redes

Dentro de lo que es vulnerabilidad se tienen varios tipos de ataques, sin embargo, los cuatro principales son:

- Reconocimiento
- Acceso
- Virus, gusanos y caballos de troya
- Disponibilidad

4.2.1. Reconocimiento

Es muy conocido en el ámbito de informática como recopilación de información, es considerado un ataque. Consiste en reconocer vulnerabilidades en una red antes de hacer algún tipo de calamidad, un diagnóstico a fondo para poder explotar todas las debilidades después con otro tipo de ataque. Una similitud a este tipo de ataque es cuando un ladrón está en búsqueda de alguien a quien robar, llega a algún barrio, busca casas fáciles y con poca seguridad. Los ataques de reconocimiento pueden consistir en uno de los siguientes:

- Consultas de información en internet
- Barridos de *ping*
- Escaneos de puertos
- Programas detectores de paquetes

Existen varias herramientas en internet como nslookup y whois con las cuales se pude determinar fácilmente un direccionamiento IP asignado a una

empresa o entidad. Cuando este segmento es conocido, un atacante puede hacer un barrido de *ping* para identificar cuáles de las direcciones están activas. Herramientas como fping o gping sirven para verificar el estado de conexión de dispositivos con direcciones IP, estas mismas herramientas sirven para automatizar estos barridos de una manera sistemática y hacer el ataque de reconocimiento muy simple.

Una vez dado el primer paso de reconocimiento que consiste en identificar si hay dispositivos activos, el intruso hace una inspección más profunda y utiliza un escáner de puertos para determinar qué tipos de servicio están activos en estos dispositivos. Software como Nmap o Superscan están diseñados para verificar si hay puertos abiertos en algún dispositivo. El objetivo de hacer un diagnóstico de puertos en un *host* es verificar el tipo de aplicación que se ejecuta, así también la versión del sistema operativo que tiene alojado el *host*. Con base en esta información un atacante puede determinar qué tipo de debilidad se tiene y si esta es capaz de explotarse.

Los agresores internos pueden intentar "infiltrarse" en el tráfico de la red. Sondeo de redes y detección de paquetes son términos comunes para infiltración. La información compilada mediante la infiltración puede utilizarse para realizar otros ataques a la red.

Los siguientes son dos términos comunes de infiltración:

- Recopilación de información: identificación de nombres de usuarios, contraseñas o información que se transporta a través de la red.

- Robo de información: robo de datos en dispositivos finales o de la red obteniendo acceso no autorizado, como por ejemplo el robo de números de tarjetas de crédito o filtrarse en instituciones financieras.

Cierto tipo de datos son susceptibles en la red y esto puede ser por el tipo de protocolos que se utilicen en la misma, por ejemplo el SNMP es un medio de información para que los dispositivos de la red puedan recopilar datos necesarios acerca de sus estados, y estos puedan ser enviados a un administrador de red. Cuando se utiliza la V1/V2 del protocolo un intruso podría infiltrarse y capturar consultas de SNMP, con lo cual tendría los datos necesarios para poder ingresar a los equipos en la red.

El método más común para infiltrarse en la red consiste en capturar paquetes TCP o IP u otros paquetes de protocolos, con los cuales se puede utilizar un analizador y verificar datos confidenciales dentro de la red. El analizador Wireshark pueda analizar todos los paquetes que se hayan capturados en busca de información vulnerable, siempre y cuando no esté encriptada.

4.2.2. Acceso

Cuando un atacante puede obtener acceso a un dispositivo como intruso esto es reconocido como ataque de acceso, por lo general esto implica que actos de piratería informática sean ejecutados para poder obtener el acceso. Este tipo de ataques pueden ser una secuencia de comandos o alguna herramienta que explota una vulnerabilidad conocida de las aplicaciones que utiliza el dispositivo atacado.

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios de FTP y los servicios web para obtener acceso a cuentas web, bases de datos confidenciales y otra información confidencial.

Ataques a las contraseñas: este tipo de ataques pueden implementarse por medio de programas detectores de paquetes, dentro de un analizador de protocolos la información que vaya sin cifrar puede ser analizada, ya que las contraseñas y usuarios se transmiten como texto plano. A este tipo de ataque se les llama de diccionario o fuerza bruta, ya que intentan conectarse a *routers* o recursos compartidos que se alojan en servidores. Con esto se logran identificar cuentas de usuario y sus respectivas contraseñas.

Los agresores que realizan ataques de diccionario utilizan herramientas como L0phtCrack o Cain, con la intención de conectarse de una manera repetitiva y tratar diferentes combinaciones de palabras incluidas en un diccionario de ahí su nombre. Este tipo de ataques suelen ser exitosos, ya que los usuarios eligen contraseñas sencillas con pocas letras, fáciles de predecir y burlar.

Las tablas de arco iris son otro método de ataque para contraseñas, estas tablas son series precalculadas que forman cadenas de texto las cuales incluyen posibles contraseñas sin cifrar. Conjeturas seleccionadas al azar son las que forman la posible contraseña, este tipo de ataque puede ser realizado por un software como L0phtCrack.

Los ataques de fuerza bruta son mucho más sofisticados ya que este tipo de herramientas buscan de manera exhaustiva y bajo combinaciones de caracteres una contraseña específica, este no utiliza solo palabras de diccionario sino cualquier caracter disponible para poder accesar a un equipo. La desventaja que presenta este tipo de ataques es que necesitan más tiempo para poder

lograrse, pero existen herramientas de fuerza bruta que han logrado descifrar contraseñas simples en menos de un minuto.

- Explotación de confianza: comprometer a un dispositivo es el objetivo principal de un ataque de explotación de confianza, con el fin de poder atacar otros *hosts* dentro de la red. Si un *host* de una red de una empresa está protegido por un firewall (*host* interno), pero un *host* de confianza que se encuentra afuera del firewall (*host* externo) puede obtener acceso a el, el *host* interno puede ser atacado a través del *host* externo de confianza.

- Redirección de puertos: este es un ataque de explotación de confianza, pero adicional a este el *host* comprometido se manipula para dejar pasar tráfico a través de un *firewall*, esto hace que el tráfico que estaba bloqueado ya no lo esté.

  Considere un *firewall* con tres interfaces y un *host* en cada interfaz. El *host* externo puede llegar al *host* que se encuentra en el segmento de servicios públicos, pero no al *host* interno. Este segmento de acceso público, normalmente, se conoce como zona desmilitarizada (DMZ). El *host* que se encuentra en el segmento de servicios públicos puede llegar al *host* externo y al interno. Si los agresores pudieran comprometer el *host* que se encuentra en el segmento de servicios públicos, podrían instalar software para redirigir el tráfico desde el *host* externo directamente al interno. Si bien ninguna comunicación infringe las normas implementadas en el *firewall*, ahora, el *host* externo ha logrado conectarse con el *host* interno a través del proceso de redirección de puertos del *host* de servicios públicos. Un ejemplo de utilidad que puede proporcionar este tipo de acceso es netcat.

- Ataque *man-in-the-middle*: este es un ataque que se logra cuando un atacante logra posicionarse entre dos *hosts* los cuales quedan comprometidos. El agresor es capaz de controlar la conversación entre *hosts* periódicamente.

4.2.3. Virus, gusanos y caballos de Troya

- Gusano: un gusano ejecuta un código e instala copias de sí mismo en la memoria de la computadora infectada, lo que, a su vez, puede infectar a otros *hosts*. La anatomía de un ataque de un gusano es la siguiente:

    - La vulnerabilidad que lo hace posible: las vulnerabilidades y debilidades de los sistemas son explotadas por un gusano que se instala a sí mismo, afecta a usuarios ingenuos que abren archivos ejecutables no verificados que pueden provenir de correos electrónicos.

    - Mecanismo de propagación: una vez obtenido el acceso el gusano se copia a sí mismo en dicho *host* y selecciona nuevos objetivos para atacar.

    - Contenido: el agresor obtiene acceso al *host* media vez este mismo se encuentre infectado con el gusano, de manera frecuente como un usuario privilegiado. Después de este paso el agresor podría explotar nuevamente el *host* para poder subir el nivel de usuario a administrador.

- Virus: un virus es software malicioso asociado a otro programa, con el propósito de ejecutar una función particular no deseada en una estación de trabajo.

  Por medio de un archivo comprimido o algún otro tipo de archivo ejecutable un virus es implantado en algún *host,* este requiere de un mecanismo de entrega, como por ejemplo, el correo electrónico para transportar el código de un sistema a otro. La diferencia que tiene con un gusano es que un virus requiere de la interacción humana y el gusano no.

Un virus es software malicioso asociado a otro programa para ejecutar una función particular no deseada en una estación de trabajo.

- Caballo de Troya: es distinto solo en el sentido de que toda la aplicación fue escrita para que tenga la apariencia de otra cosa, cuando en realidad es una herramienta de ataque. Un ejemplo de Caballo de Troya es una aplicación de software que ejecuta un juego sencillo en una estación de trabajo. Mientras que el usuario está ocupado con el juego, el Caballo de Troya envía por correo una copia de sí mismo a cada dirección de la libreta de direcciones del usuario. Los otros usuarios reciben el juego y lo ejecutan y, de esa manera, propagan el Caballo de Troya a las direcciones de cada libreta de direcciones.

4.2.4. Confidencialidad

La confidencialidad consiste en tener los datos en privado, la privacidad se puede abarcar física o lógicamente, restringiendo datos sensibles y encriptando tráfico sobre la red.

Un ataque de confidencialidad amenaza con hacer datos como registros personales, números de tarjeta de crédito, usuarios, contraseñas y cuentas de correo visibles para un atacante. Generalmente los atacantes realizan copias de seguridad de estos datos en vez de manipularlos, razón por la cual este tipo de ataques son desapercibidos por las personas. Aun cuando se tenga algún tipo de software especializado para poder rastrear el acceso a archivos, si no se tiene ninguna sospecha este ataque puede pasar desapercibido.

Dentro de las estrategias que utilizan los atacantes para realizar ataques de confidencialidad se tienen:

- Captura de paquetes
- Barridos de ping y redirección de puertos
- Interferencia electromagnética
- Utilizar la ingeniería social

4.2.5. Integridad

La integridad en cuanto a los datos en una red asegura que los datos que viajan por la misma no hayan sido modificados, como ejemplo de ataques de integridad se puede mencionar:

- La modificación de la página web de una empresa.
- Interceptar y alterar una transacción comercial.
- La modificación de registros financieros que han sido guardados de manera electrónica.

Dentro de los métodos que pueden utilizar los atacantes para lograr un ataque de integridad se encuentran:

- Ataque de Salami: utiliza ataques pequeños para poder lograr un objetivo grande, por ejemplo un atacante que tiene los números de varias tarjetas de crédito y retira una cantidad insignificante de cada tarjeta pero son tantas que la suma final de dinero puede llegar a ser bastante significativa.

- Diddling de datos: este ataque consiste en modificar los datos antes que estos sean guardados en algún medio de almacenamiento.

- Ataques de explotación: un *host* comprometido puede pasar datos no permitidos a través de un *firewall*. Para el *firewall* sería indiferente el tipo de datos que transitan en el ya que solo puede verificar puertos.

- Ataques de contraseñas: estos ataques involucran, captura de paquetes no cifrados, ataques de fuerza bruta, ataques de diccionario y caballos de Troya.

4.2.6. Disponibilidad

A continuación se presenta una descripción de los ataques Dos, DDos, entre otros.

4.2.6.1. Ataques de DoS

Abreviado como DoS de sus siglas denegación de servicio, este tipo de ataques están dentro de los más complicados de eliminar y son muy promocionados. Estos ataques son de muy mal gusto para los atacantes porque

son triviales y requieren muy poco esfuerzo para su ejecución razón por la cual la comunidad a la comunidad de agresores no les interesa a veces utilizarlos. Sin embargo los administradores de seguridad deben prestar la suficiente atención ya que un ataque de este tipo podría llegar a causar desastres dentro de una red en producción.

La principal función de los ataques de DoS es impedir que personas puedan utilizar algún recurso ya que este ataque es el que consume los recursos del sistema, como ejemplo de este tipo de ataques se puede mencionar el *ping* de la muerte, ya que estos ataques modificaron la parte IP de un encabezado de paquete de *ping* para indicar que hay más datos en el paquete de los que realmente había. Un *ping* normalmente tiene de 64 a 84 bytes, mientras que uno de la muerte podría tener hasta 65 535 bytes. Enviar un *ping* de este tamaño puede colapsar una computadora objetivo más antigua. La mayoría de las redes ya no son susceptibles de sufrir este tipo de ataque.

4.2.6.2. Ataques DDoS

Por sus siglas se refiere a DoS distribuido, estos ataques saturan todos los enlaces de red que transmitan datos legítimos haciendo que el tráfico legítimo se pierda. La diferencia principal que tiene con un ataque de DoS es que opera a una escala mucho mayor, ya que afecta a cientos o miles de puntos en una red o miles de puntos de ataque afectan a un objetivo. Por lo general, un ataque DDoS tiene tres fases:

- Debe existir un ente que trabaje como cliente y lance el ataque generalmente es una persona.
- Una vez el ataque es lanzado un *host* es comprometido y ejecuta el programa del agresor para controlar otros *host,* al *host* comprometido se le llama manipulador.

Una vez controlados los otros *hosts* a estos se les llama agentes y se encargan de generar algún flujo de paquetes para causar denegación de servicio.

Un ejemplo de DDoS, es el ataque de *smurf* los cuales son mensajes de ping en *broadcast* y sirven para saturar un objetivo. Comienza cuando un agresor envía una gran cantidad de peticiones de eco ICMP a la dirección de *broadcast* de la red desde direcciones IP de origen suplantadas válidas. Un *router* podría ejecutar la función *broadcast* de capa 3 a *broadcast* de capa 2, la mayoría de los *hosts* responde uno por uno con una respuesta de eco ICMP, lo cual multiplica el tráfico por la cantidad de *hosts* que respondan. En una red multiacceso de *broadcast*, potencialmente podría haber cientos de máquinas que contesten a cada paquete de eco.

4.2.6.3. TCP SYN Flood

Un ataque de saturación SYN explota el protocolo de enlace de tres vías TCP. Implica enviar varias peticiones de SYN (más de 1 000) a un servidor objetivo. El servidor responde con la respuesta habitual SYN-ACK, pero el *host* malicioso nunca responde con el ACK final para terminar el protocolo de enlace. Esto paraliza el servidor hasta que finalmente se queda sin recursos y no puede responder a un pedido válido de *host*.

4.2.7. Otros ataques

A continuación se muestran otros tipos de ataques.

4.2.7.1. VLAN hopping

Un ataque de VLAN hopping consiste en que el tráfico de una VLAN pueda pasar a el tráfico de otra, sin que exista algún dispositivo de capa tres que realice el ruteo entre las mismas. Un atacante realiza esto con el objetivo de hacer pasar tráfico no autorizado de una VLAN hacia otra, con este ataque el atacante podría tener acceso a información que viaja por una VLAN que es crítica para una organización. Dos técnicas son necesarias para poder lanzar un ataque de VLAN hopping.

La primera es el *switch* Spoofing y consiste en que un atacante pueda forzar a que un *switch* convierta uno de sus puertos destinados a acceso en troncal, esto con la finalidad de ver el tráfico que proviene de todas las VLAN.

La segunda es el doble etiquetado y esta consiste en que para una VLAN nativa el estándar IEEE 802.1Q establece que no se debe etiquetar este tipo de tramas entre *switches*. Por lo que un atacante podría infiltrar un etiquetado falso de una VLAN destino a la cual no está autorizada. Cuando la trama entra al *switch* proveniente del *host* el *switch* no analiza el etiquetado puesto que ese puerto pertenece a la VLAN nativa, pero cuando la trama va de salida esta si es analizada y es enviada por el enlace troncal con el etiquetado que el atacante inserto, así de esta manera el atacante puede ver el tráfico de la VLAN falsa que insertó.

4.2.7.2. STP attack (Spanning Tree)

El protocolo STP debe de elegir un *switch* como el puente raíz y esta prioridad debe elegirse por medio del ID de puente que tiene cada *switch.* Si por alguna razón el puente raíz fallara otro *switch* debe tomar su lugar y el protocolo de volver a converger para poder evitar los bucles de capa 2.

Un atacante que tenga acceso físico a dos puertos de dos *switches* podría insertar un *switch* pequeño sin capacidades de rendimiento y memoria adecuados, que tenga un ID de puente más pequeño lo cual provocaría que el tráfico de varias VLANs transite por medio de este *switch.* El método que utilizaría el atacante para ver tráfico es llamado *port mirroring* o espejo de puerto en el que reenvía el tráfico de alguna interfaz hacia otra.

4.2.7.3. DHCP spoofing

En la mayoría de redes en la actualidad la mayoría de *hosts* obtienen su dirección IP por medio del protocolo DHCP, ya que es una manera simple de manejar la asignación de direcciones, generalmente un cliente envía un DHCP request y el servidor responde para poder proceder con el proceso de asignación.

Sin embargo un atacante podría introducir un servidor DHCP no autorizado el cual responde a las peticiones realizadas por los clientes. Aunque se tengan dos servidores DHCP el cliente asignará la IP del servidor que le conteste primero, por tanto el servidor no autorizado es una amenaza para la red. Esto es perjudicial para un cliente ya que el DHCP no autorizado podría estar dando la información del atacante como dirección IP y *default gateway*, lo que provocaría que toda la información se envíe al atacante, este a su vez podría obtener toda la información para manipularla o reenviarla hacia otro destino.

Otro ataque de DHCP consiste en enviar muchas solicitudes de DHCP hacia un servidor, el atacante simula enviar las solicitudes desde diferentes direcciones MAC haciendo que el *pool* disponible en el DHCP se termine y repercute en agotar el direccionamiento IP para una red en producción.

4.2.7.4. MAC spoofing

El atacante envía una trama con una dirección MAC diferente a la que realmente tiene el *host* en el que se genera el ataque, generalmente es una dirección MAC clonada correspondiente a otro dispositivo dentro de la red. En el funcionamiento normal de un *switch* este asigna la dirección MAC del dispositivo que tiene conectado a un puerto a su tabla CAM. Este ataque es temporal hasta que el dispositivo real vuelva enviar una trama hacia el *switch,* pero puede causar disturbios en el flujo convencional que deben cursar normalmente en una red.

4.2.7.5. VoIP SPAM

Este tipo de ataque es similar al SPAM que se genera en los correos electrónicos, sin embargo, afecta directamente a la productividad de usuarios, así también puede llegar a ser bastante molesto para los mismos. El SPAM más común puede consistir en que el ID de llamada que aparece en un teléfono sea incorrecto, pudiendo caer en fraude y engañar a los usuarios, el más tedioso de todos es hacer que el teléfono suene cada 5 minutos. Al hacer esto el atacante se asegura que la productividad de una empresa se está viendo degradada. Este ataque también es conocido como SPIT (SPAM over IP Telephony).

4.2.7.6. SIP attack targets

El protocolo SIP ha ganado popularidad entre diferentes vendedores ya que es un estándar abierto, sin embargo transporta la información de señalización en texto plano, lo que lo hace muy vulnerable a que atacantes puedan aprovecharse.

Un atacante podría direccionar la señalización SIP hacia su PC y empezar a recibir paquetes de RTP (voz), con esto sería capaz de escuchar

conversaciones telefónicas, de hecho podría direccionarlas y guardarlas para su utilización propia.

La telefonía SIP se vale de servidores como un servidor registrador o un proxy SIP para poder funcionar, un atacante podría lanzar un ataque de DoS hacia estos servidores, con esto teléfonos IP serían incapaces de registrarse lo que provocaría un colapso en la red telefónica IP.

5. SEGURIDAD EN LA RED Y TÉCNICAS DE MITIGACIÓN

5.1. Evaluando la seguridad de la red

Para asegurarse que los métodos de protección de la red están funcionando de manera adecuada estos deben ser probados ocasionalmente. Esta evaluación de la red ocurre generalmente mientras la implementación, operación y mantenimiento son llevados a cabo en conjunto con el SDLC (System Development Life Cicle).

Un SDLC consiste de varias fases:

- Inicialización: la inicialización se desglosa de la siguiente manera:
    - Categorización de seguridad: esta categoriza las brechas de seguridad en algún componente en particular
    - Valoración de los riegos preliminares: la cual consiste en una vista preliminar de los requerimientos de seguridad en un sistema.
    - Adquisición y desarrollo: esta se desglosa de la siguiente manera:
        - Valoración de los riesgos: el análisis preliminar realizado en la fase de inicialización sirve como fundamento de este paso, y esto logra crear una valoración de los riesgos mucho más específica, la cual incluye los requisitos de seguridad.
        - Análisis funcional de requerimientos de seguridad: especifica que es necesario para poner un sistema bajo seguridad.

        - Aseguramiento de un análisis para los requerimientos de seguridad: basado en los requerimientos legales y funcionales este provee evidencia que un recurso de red va a ser protegido de una manera en específico.

- Consideraciones de costo y reportaría: los costos que implican asegurar una red.
- Planificación de seguridad: un reporte que indica que controles de seguridad van a ser utilizados en una red.
- Desarrollo de un control de seguridad: un reporte que detalla como los controles de seguridad previos fueron designados, desarrollados e implementados.
- Desarrollo de una prueba de seguridad y evaluación: una evaluación para probar que los controles de seguridad sean efectivos.
- Implementación: esta se desglosa de la siguiente manera:

    - Inspección y aceptación: la instalación de un sistema y sus requerimientos funcionales son verificados.
    - Integración del sistema: un sistema con todos sus componentes es un sitio operacional y su operación es verificada.
    - Certificación de seguridad: la operación de los controles especificados y activos es verificada.
    - Acreditación de seguridad: después que los controles son verificados a un sistema se le asignan privilegios para que tráfico específico pueda transitar sobre el.

- Operación y mantenimiento esta se desglosa en:

- Administración de la configuración y control: antes que un cambio en una porción de la red se lleve a cabo, el impacto potencial que causa en la parte restante de la red es evaluado.
- Monitoreo constante: aunque una solución de seguridad haya sido implementada esta debe estar en constante monitoreo.

- Disposición esta se desglosa de la siguiente manera:

  - Preservación de la información: cierto tipo de información debe ser preservada por motivos legales, económicos y financieros. Este tipo de información debe ser trasladada a dispositivos de almacenamiento reciente y asegurar su disponibilidad.
  - Sanitación de la información: es asegurar que información que ha sido eliminada no pueda ser recuperada de alguna manera, por lo tanto es mejor sobrescribir esta información para que sea corrupta e inentendible.
  - Disposición de hardware y software: cuando componentes obsoletos son retirados, estos deben retirarse con algún tipo de control para evitar que algún atacante malicioso quiera sacar información no debida de los mismos.

Durante la fase de implementación la seguridad debe ser evaluada en diferentes componentes, esto debido a que en esta fase es mucho más factible encontrar riesgos de seguridad los cuales pueden ser solventados, así también estos riesgos pueden llegar a formar parte de una política de seguridad para una empresa.

Después que una red entra en la fase de operación y mantenimiento, esta debe ser monitoreada constantemente para encontrar posibles vulnerabilidades

obviadas en la fase de implementación, se recomienda hacerlo cada vez que ingresa un componente nuevo, por ejemplo un servidor web.

Los resultados de estas evaluaciones de seguridad pueden ser utilizados para varios propósitos como:

- Crear una línea base para sistemas de información referente a seguridad
- Identificar estrategias para poder encontrar debilidades en una red
- Completar las fases de un SDLC
- Hacer un análisis de costo/beneficio con otras medidas de seguridad

Existen bastantes herramientas para evaluar la seguridad en una red algunas de ellas pueden ser automatizadas y otras no, dentro de las más comunes se encuentran:

- Escanear la red para descubrir direcciones ip activas asi también puertos.
- Identificar vulnerabilidades de los *hosts*.
- Programas para fraude de contraseñas.
- Verificación de *Logs* de seguridad.
- Escaneo en busca de virus.
- Ataques de penetración para ver si se puede comprometer a un sistema en específico.
- Escaneo del SSID en para poder ingresar a una red inalámbrica.

En caso que existan desastres naturales, ataques terroristas o algún disturbio dentro de una red, un plan de contingencia debe existir en caso de alguna calamidad.

A esto se le llama un plan de recuperación ante desastres el cual debe ser obligación de un administrador de red.

Las dos metas de un plan de continuidad de negocio son:

- Mover las operaciones críticas de un negocio hacia otro sitio mientras el sitio original está siendo reparado.

- Utilizar formas alternativas ya sean internas o externas de comunicación.

- Las tres fases que deben llevarse en un plan de recuperación son:

    - Fase de respuesta a emergencia
    - Fase de recuperación
    - Fase de retorno a operaciones normales

5.1.1. Fundamentos de políticas de seguridad

Una política de seguridad es un documento cambiante el cual dictamina las bases sobre como la red es utilizada, estas bases especifican los objetivos organizacionales estableciendo reglas de uso para la red.

El objetivo principal de una política de seguridad es proteger los bienes de una organización, como bienes no solo se hace referencia a objetos físicos, esto incluye propiedad intelectual, procedimientos, datos sensibles de clientes los cuales deben ser protegidos como por ejemplo un servidor de correo o los datos en un servidor web.

Además de proteger los bienes organizacionales, una política de seguridad tiene otros objetivos como pueden ser:

- Hacer a los empleados consientes en sus obligaciones en cuanto a políticas de seguridad se refiere.
- Identificar soluciones de seguridad específicas para poder lograr que una política de seguridad sea efectiva.
- Actuar como una línea base para el monitoreo de la seguridad.

Uno de los componentes más conocidos en una política de seguridad es el uso aceptable de una política, o también conocido como uso apropiado de una política, este identifica lo que los usuarios están permitidos a hacer dentro de una red.

Una política debe estar constituida de varios documentos, ya que una empresa tiene diferentes áreas y por lo tanto son diferentes requerimientos los que tiene cada área, lo que es prohibido para algunas áreas puede ser permitido para otras y viceversa, por esta razón deben ser varios documentos los que constituyan esta política.

5.1.2. Componentes de una política de seguridad

Dado que una política de seguridad está compuesta de varios documentos, a continuación se explican los documentos básicos con los que debe de contar una política.

Una Política Gobernante: esta implica conceptos de seguridad importantes para una organización. Este tipo de política tiene un primer enfoque en los empleados técnicos y administrativos, sus componentes son:

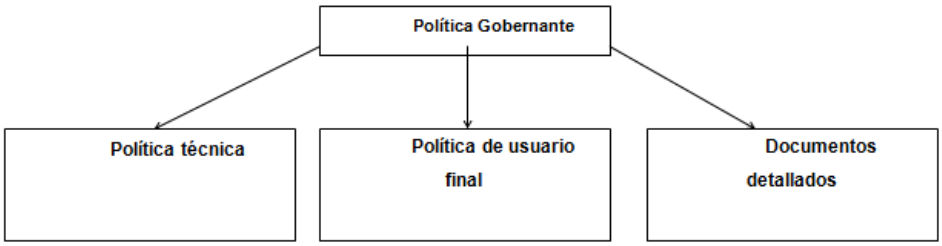
- Identificar los posibles incidentes impulsados por la política.
- Discutir el punto de vista de toda la organización para los incidentes.
- Examinar la relevancia de una política en un ambiente de trabajo.
- Explicar cómo los empleados cumplirán con esta política.
- Enumerar las acciones y actividades apropiadas, así también procesos.
- Explicar las consecuencias que provocan la falta de cumplimiento.
- Política técnica: esta provee un tratamiento mucho más detallado de una política dentro de una organización. Personal de seguridad y tecnologías de la información son los objetivos de este tipo de políticas, ellos las utilizan en su labor diaria. Algunas áreas en las que se utilizan estas políticas son:

    - Correo electrónico.
    - Redes inalámbricas.
    - Acceso remoto.
    - Políticas para usuario final: estas corresponden a la utilización de una política de uso apropiado para algún servicio específico por ejemplo internet.
    - Documentos detallados: ya que las políticas anteriormente detalladas tienen como objetivo usuarios en específico, es necesario un control mucho más granular, para ello se necesitan documentos como:

        - Estándares: estos permiten consistencias dentro de una red, por ejemplo un estándar podría dictaminar cuantos diferentes sistemas operativos pueden ser utilizados dentro de una compañía.

- Guías: una serie de seguimientos para poder realizar las mejores prácticas en cuanto a seguridad, este tipo de documentos aseguran la continuidad de las mejoras prácticas.
- Procedimientos: estos indican paso a paso cada una de las prácticas para llevar a cabo una mejora en la seguridad.

Figura 1. **Componentes de una política de seguridad**



Fuente: elaboración propia.

5.1.3. Factores contribuyentes al diseño seguro de una red

Cuando se diseña una red segura una de las equivocaciones más grandes que se puede llegar a cometer, es diseñar una red tan segura que los propósitos reales para los cuales la red fue implementada son inutilizables. Debe estar siempre claro que las necesidades de un negocio siempre son prioridad ante cualquier otro factor. Sin embargo, hay otros factores que tienen influencia sobre el diseño de una red segura:

- Necesidades del negocio: estas necesidades están regidas por lo que un negocio espera llegar a lograr con una red segura.

- Análisis de riesgo: un análisis de riesgos puede proveer un adecuado nivel de recursos en caso de que alguna calamidad suceda.

- Políticas de seguridad: la política de seguridad generalmente tiene múltiples documentos y tiene como objetivo grupos específicos de usuarios.
- Mejores prácticas: además de reglas imperativas para el uso adecuado de los dispositivos dentro de una organización, prácticas internas y externas para cumplir estas reglas son necesarias.

5.1.4. Técnicas generales de mitigación

Cuando se instala un nuevo sistema operativo en una computadora, la configuración de seguridad se establece en los valores predeterminados. En la mayoría de los casos, este nivel de seguridad no es apropiado. Se deben adoptar algunos pasos sencillos, que se aplican a todos los sistemas operativos:

- Los nombres de usuario y las contraseñas predeterminados deben cambiarse de inmediato.
- Se debe restringir el acceso a los recursos del sistema exclusivamente a las personas autorizadas para utilizar esos recursos.
- Se deben desconectar y desinstalar los servicios y las aplicaciones innecesarios, siempre que sea posible.

Es fundamental proteger los *hosts* de la red, como las PC y los servidores de la estación de trabajo. Estos *hosts* deben asegurarse cuando se agregan a la red, y deben actualizarse con parches de seguridad, a medida que estas actualizaciones estén disponibles. Se pueden adoptar pasos adicionales para

asegurar estos *hosts*. Los antivirus, *firewalls* y la detección de intrusiones son herramientas valiosas que se pueden utilizar para asegurar los *hosts* de la red.

Dado que muchos recursos de la empresa pueden estar contenidos en un único servidor de archivos, es particularmente importante que se pueda acceder a los servidores y que estén disponibles.

- Software antivirus: instale software antivirus de *host* para protegerse contra virus conocidos. El software antivirus puede detectar la mayoría de los virus y muchas aplicaciones de caballos de Troya e impedir su propagación en la red. El software antivirus hace esto de dos maneras:

    - Escanea archivos y compara su contenido con virus conocidos en un diccionario de virus. Las coincidencias se marcan de una manera definida por el usuario final.

    - Controla los procesos sospechosos que se ejecutan en un *host* que podrían ser indicativos de la presencia de una infección. Este control podría incluir capturas de datos, monitoreo de puertos y otros métodos.

- *Firewall* personal: las PC conectadas a internet mediante una conexión dial-up, DSL o cable módem son tan vulnerables como las redes empresariales. Los *firewalls* personales residen en la PC del usuario e intentan impedir ataques. Los *firewalls* personales no están diseñados para las implementaciones de la LAN, como *firewalls* basados en aplicaciones o basados en servidores, y pueden impedir el acceso a la red si se instalan con otros clientes, servicios, protocolos o adaptadores de *networking*.

- Parches para sistemas operativos: la forma más eficaz de mitigar un gusano y sus variantes es descargar las actualizaciones de seguridad del proveedor del sistema operativo e instalar parches en todos los sistemas vulnerables. Es difícil en el caso de sistemas de usuarios no controlados de la red local, y es aún más problemático si estos sistemas están conectados de manera remota a la red mediante una red privada virtual (VPN) o un servidor de acceso remoto (RAS).

La administración de varios sistemas implica la creación de una imagen estándar del software (sistema operativo y aplicaciones reconocidas cuyo uso está autorizado en sistemas cliente implementados) que se implementa en sistemas nuevos o actualizados. Es posible que estas imágenes no contengan los últimos parches, y el proceso de volver a crear la imagen continuamente para integrar el parche más reciente, puede convertirse rápidamente en una tarea que demanda mucho tiempo desde un punto de vista administrativo. Colocar parches en todos los sistemas requiere que dichos sistemas estén de alguna manera conectados a la red, lo que puede no ser posible.

5.1.5. Seguridad en dispositivos

La seguridad en dispositivos intermediarios es un punto muy importante a tener en cuenta cuando se implementa una red, razón por la cual debe analizarse que tipo de ataque puede afectar cada uno de estos dispositivos.

5.1.5.1. Seguridad en dispositivos de capa 2

Los *switches* son dispositivos que trabajan en capa 2 y son objetivos de atacantes experimentados en causar afectación quebrantando la seguridad.

Ataques relacionados con STP, DHCP, ARP Spoofing y VLAN hopping son los más conocidos y pueden causar graves consecuencias si no se logran reconocer y mitigar a tiempo. Las mejores prácticas para asegurar un dispositivo de capa 2 incluyen:

- Inactivar acceso por telnet: dentro de los protocolos más antiguos e inseguros se incluye telnet, este envía la información sin algún tipo de cifrado.

- SNMP: el protocolo simple de administración de red se utiliza en gestores administradores de red, sin embargo las versiones antiguas carecen de seguridad ya que no poseen autenticación, ni cifrado alguno para el intercambio de información, por lo que si es necesario utilizar la versión 3 del protocolo.

- Reducir al mínimo los riesgos: en un *switch* hay ciertos procesos y servicios que no son utilizados siempre, por lo que pueden deshabilitarse. Existen ocasiones en las que no todos los puertos del *switch* son utilizados, por lo que es una buena práctica deshabilitarlos o restringir el número de direcciones MAC en los mismos.

- *Logs*: revisar los *logs* constantemente es una buena práctica ya que se pueden ver alarmas o intentos de conexión hacia el dispositivo y tener un mejor control.

- Control de cambios: en una red múltiples administradores de red pueden ser responsables de realizar un cambio en *switches*, por lo que una política de control de cambios es ideal para correr menor riesgo ante una mala configuración o un administrador mal intencionado.

- Crear VLAN para la segmentación de la red.

- Prevención de un ataque VLAN *hopping*: un ataque de VLAN *hopping* provoca que tráfico de una VLAN pueda pasar hacia otra sin ser ruteado. Un ataque de VLAN *hopping* se vale de otros dos ataques para funcionar: Switch Spoofing y doble etiquetado.

Para iniciar un Switch Spoofing existen *switches* de diferentes marcas en que al configurar un puerto como troncal este hace que el tráfico de todas las VLAN pasen por el enlace, esto provocaría que un atacante vea el tráfico de todas las VLAN, consiga usuarios y contraseñas que pueden ser utilizados después para un ataque. Esto se corrige deshabilitando la configuración de enlace troncal en los puertos que no sea necesario. En un ataque de doble etiquetado se puede mitigar no enviando tráfico de usuarios dentro de la VLAN nativa, ya que esta podría ser comprometida.

- Protección contra un ataque de STP: si un atacante tiene acceso a dos puertos de diferentes *switches* y llegara a conectar un *switch* con un ID de puente más pequeño que el puente raíz, la topología de STP tendría que volver a reconverger, provocando que todo el tráfico pase por ese nuevo *switch,* un atacante puede capturar este tráfico por medio de un capturador de paquetes (*sniffer*). Para prevenir esto los dispositivos de hoy en día tienen ciertas características como:

    - RootGuard: esta característica se configura en todos los puertos de un *switch* que no están designados como puertos raíz (*rootports*). Cuando una BPDU más alta (ID de puente raíz más pequeño), llega a alguno de estos puertos este entra en un estado llamado “raíz

inconsistente” y ningún tráfico de datos puede pasar a través de ese puerto.

- BPDU Guard: esta característica consiste en que los puertos correspondientes a usuarios nunca deben recibir BPDU de STP, por lo que si llegara a pasar hace que el puerto sea deshabilitado.
- Protección contra un DHCP *server spoofing*: para combatir este tipo de ataque se utiliza una característica que se llama DHCP Snooping, esta consiste en que todos los puertos de un *switch* no son confiables y debe habilitarse un puerto confiable para las solicitudes de DHCP. Un puerto considerado como confiable puede recibir DHCPOFFER y DHCPACK. En los puertos no confiables, no se permite ningún tipo de solicitud o respuesta para DHCP. Esta característica permite también limitar el número de veces que un *host* puede requerir una dirección IP, esto para mitigar ataques de DoS.

5.1.5.2. Seguridad en dispositivos de capa 3

La seguridad de los *routers* es un elemento crítico de las implementaciones de seguridad. Los *routers* son objetivos definidos de los agresores de las redes. Si un agresor puede comprometer y obtener acceso a un *router*, puede ser una ayuda potencial para ellos.

- Los *routers* cumplen las siguientes funciones:
  - Publicar las redes y filtrar a quienes pueden utilizarlas.
  - Proporcionar acceso a los segmentos de las redes y a las subredes.

Dado que los *routers* proporcionan *gateways* a otras redes, son objetivos obvios y están sujetos a una diversidad de ataques. A continuación, se dan algunos ejemplos de los diversos problemas de seguridad:

- El compromiso del control de acceso puede exponer los detalles de configuración de la red, y de este modo, se facilita la concreción de ataques contra otros componentes de la red.
- El compromiso de las tablas de enrutamiento puede disminuir el rendimiento, denegar los servicios de comunicación de la red y exponer información confidencial.
- La configuración incorrecta de un filtro de tráfico del *router* puede exponer los componentes internos de la red a escaneos y ataques, lo que ayuda a los agresores a evitar su detección.

La protección de los *routers* que se encuentran dentro del perímetro de la red, es un primer paso importante para protegerla. Esta seguridad debe pensarse en función de las siguientes categorías:

- Seguridad física.
- Actualización del sistema operativo de los *routers* cuando sea conveniente.
- Copia de seguridad de la configuración y del sistema operativo de los *routers*.
- Aseguramiento del *router* para eliminar el abuso potencial de los puertos y servicios no utilizados.

Para proporcionar seguridad física, ubique el *router* en un cuarto cerrado con llave, donde solo pueda ingresar personal autorizado. Asimismo, dicho cuarto no debe tener interferencia electrostática ni magnética y debe tener controles de

temperatura y humedad. Para disminuir la posibilidad de DoS debido a una falla de alimentación, instale una fuente de energía ininterrumpible (UPS) y mantenga los componentes de repuesto disponibles.

Los dispositivos físicos utilizados para conectarse al *router* se deben guardar en un local cerrado con llave, o deben permanecer en poder de una persona de confianza para que no se vean comprometidos. Un dispositivo que se deja al aire libre podría tener troyanos o algún otro tipo de archivo ejecutable almacenado en el. Provea al *router* de la máxima cantidad de memoria posible. La disponibilidad de memoria puede servir como protección contra algunos ataques DoS, mientras que admite la gama más amplia de servicios de seguridad.

Las características de seguridad de un sistema operativo evolucionan con el tiempo. Sin embargo, la última versión de un sistema operativo puede no ser la versión más estable disponible. Para obtener el mejor rendimiento de la seguridad de su sistema operativo, utilice la versión estable más reciente que cumpla los requisitos de las características de su red.

Debe tener siempre una copia de seguridad de una configuración y el IOS a mano para el caso de que se produzca una falla en un *router*. Mantenga una copia segura de la imagen del sistema operativo del *router* y del archivo de configuración del *router* en un servidor TFTP como respaldo. Asegure el *router* para hacerlo tan seguro como sea posible. Un *router* tiene muchos servicios activados de forma predeterminada. Muchos de estos servicios son innecesarios y pueden ser utilizados por un agresor para compilar o explotar información. Debe asegurar la configuración de su *router* mediante la desactivación de los servicios innecesarios.

El acceso administrativo remoto es más conveniente que el acceso local para los administradores que tienen que manejar muchos dispositivos. Sin embargo, si no se implementa de manera segura, un agresor podría recopilar información confidencial valiosa. Por ejemplo, implementar el acceso administrativo remoto mediante Telnet puede ser muy inseguro, porque este envía todo el tráfico de la red en forma de texto sin cifrar. Un agresor podría capturar el tráfico de la red, mientras un administrador se encuentra conectado remotamente a un *router*, y descubrir las contraseñas del administrador o la información de configuración del *router*.

Por lo tanto, el acceso remoto administrativo debe ser configurado con mayores precauciones de seguridad. Para proteger el acceso administrativo a los *routers* y *switches*, primero debe proteger las líneas administrativas (VTY, AUX), y después configurar el dispositivo de red para que encripte el tráfico en un túnel SSH. Si se requiere acceso remoto, las opciones son las siguientes:

- Establecer una red de administración dedicada. La red de administración debe incluir solo *hosts* de administración identificados y conexiones a dispositivos de infraestructura. Podría lograrse si se utiliza una VLAN de administración u otra red física a la cual se deben conectar los dispositivos.

- Encriptar todo el tráfico entre la computadora del administrador y el *router*. En cualquiera de esos casos, se puede configurar un filtro de paquetes que permita que solamente el protocolo y los *hosts* de administración identificados obtengan acceso al *router*. Por ejemplo, permitir que solo la dirección IP del *host* de administración inicie una conexión SSH con los *routers* de la red.

- Al igual que con los dispositivos de capa 2, debe utilizarse SNMP versión tres o deshabilitarse completamente para evitar filtrado de la información.

5.1.5.3. Seguridad en dispositivos de capa 4

Los diseñadores de red utilizan *firewalls* para proteger las redes contra el uso no autorizado. Los *firewalls* son soluciones de hardware o software que hacen cumplir las políticas de seguridad de la red. Es como la cerradura de la puerta de la habitación de un edificio. La cerradura solo permite que ingresen los usuarios autorizados con una llave o tarjeta de acceso. Del mismo modo, los firewalls filtran el ingreso a la red de los paquetes no autorizados o potencialmente peligrosos. Los *firewall* utilizan ACL (listas de control de acceso) para poder hacer cumplir las políticas de seguridad.

Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones o protocolos de capa superior. Las ACL brindan una manera poderosa de controlar el tráfico de entrada o de salida de la red. Puede configurar las ACL para todos los protocolos de red enrutados.

Las ACL le permiten controlar el tráfico de entrada y de salida de la red. Este control puede ser tan simple como permitir o denegar los *hosts* o direcciones de red. Sin embargo, las ACL también pueden configurarse para controlar el tráfico de red según el puerto TCP o UDP que se utiliza.

El filtrado de paquetes, a veces denominado filtrado estático de paquetes, controla el acceso a la red, analiza los paquetes de entrada y de salida, y permite o bloquea su ingreso según un criterio establecido.

Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones IP o protocolos de capa superior. La ACL puede extraer información del encabezado del paquete, probarla respecto de las reglas y decidir si "permitir" o "denegar" el ingreso según los siguientes criterios:

- Dirección IP de origen
- Dirección IP de destino
- Tipo de mensaje ICMP

La ACL también puede extraer información de las capas superiores y probarla respecto de las reglas. La información de las capas superiores incluye:

- Puerto TCP/UDP de origen
- Puerto TCP/UDP de destino

Ciertos dispositivos de capa 3 como *routers* o *switches* de capa 3 tienen capacidad para configurar ciertas ACL básicas, y con base en esto se utilizan ciertas pautas para la configuración de ACL.

Pautas para el uso de las ACL:

- Utilizar ACL en un *firewall* entre una red interna y una red externa, como Internet.
- Utilizar las ACL en un *router* situado entre dos partes de la red, a fin de controlar el tráfico que entra o sale de una parte específica de su red interna.
- Configurar las ACL en *routers* de borde situados en los extremos de la red. Esto proporciona un búfer muy básico desde la red externa, o entre un área menos controlada y un área más sensible de su red.

- Configurar las ACL para cada protocolo de red configurado en las interfaces del *router* de borde. Puede configurar las ACL en una interfaz para filtrar el tráfico entrante, saliente o ambos.

5.1.5.4. Seguridad en dispositivos de capa 7

Dispositivos NAC: Network Assesment Control son el significado de las siglas NAC, el objetivo del control de acceso a red es realizar exactamente lo que su nombre implica: control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final, y controles posadmisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos y que pueden hacer en ella.

El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de *hosts* y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.

5.2. AAA

AAA tiene el significado de Authentication, Authorization, Acounting and Auditing, por sus siglas en inglés. Y es un conjunto de protocolos que se basan en las siguientes definiciones:

- Autenticación: es el proceso por medio del cual los dispositivos usuarios demuestran ser quienes dicen ser, en un ambiente de red se tienen varias maneras para establecer una autenticación: usuario y contraseña, tarjetas Token, desafíos con respuesta.

- Autorización: después de una autenticación exitosa, los servicios de autorización son encargados de establecer a que recursos puede acceder un usuario, administrador o dispositivo.
- Auditoría: después que los recursos son asignados, los servicios de auditoría se encargan de verificar y grabar lo que un dispositivo, usuario o administrador hizo con los accesos que tenía permitidos, que acceso y que tanto tiempo acceso a los recursos.

5.3. TACACS+

TACACS+ es un protocolo AAA propiedad de Cisco Systems, corre sobre TCP a nivel de capa de transporte y es capaz de encriptar los datos. Este protocolo es capaz de controlar el nivel de autorización de los usuarios, en contra parte con otros protocolos AAA. TACACS+ Se usa para la autenticación de la autorización, esto permite que administradores de red puedan utilizar el protocolo para Autorización, Auditoria y dejar la Autenticación para algún otro método por ejemplo Kerberos.

A pesar de las facilidades del protocolo TACACS+, este sigue siendo un protocolo propietario de Cisco Systems y muchos dispositivos no cuentan con el mismo.

5.4. RADIUS

RADIUS es otro protocolo AAA que se utiliza para autenticación a diferencia de TACACS+, este viaja sobre UDP en la capa de transporte y provee la encriptación de *passwords*. Este protocolo fue creado por la IETF y describe su procedimiento de la siguiente manera:

- El servidor NAS (Network Access Server) solicita credenciales a un usuario.
- El usuario provee las credenciales al NAS.
- El servidor NAS solicita una contraseña al usuario.
- El usuario provee una contraseña al NAS.
- Un datagrama de solicitud de acceso, se envía al servidor RADIUS con los parámetros necesarios, valores y atributos para verificar los parámetros de autenticación.

Si la información que brindó el usuario es correcta el servidor RADIUS responde con un datagrama de acceso aceptado. Este mensaje de acceso también contiene los parámetros de autorización, como por ejemplo una dirección IP. Si la información que el usuario brindó es incorrecta, entonces el servidor responde con un datagrama de acceso rechazado.

Dentro de los mensajes que utiliza RADIUS se pueden describir:

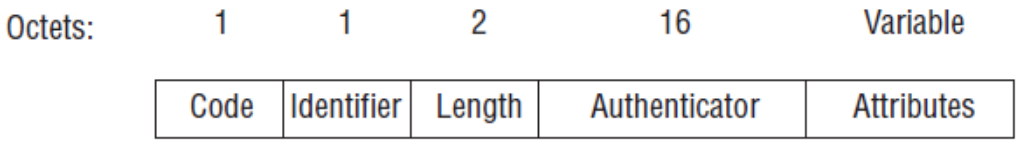
- Acces Request: contiene los atributos y valores que contienen el usuario y contraseña encriptados por RADIUS, así también el puerto que utiliza el NAS.
- Access Challenge: este es utilizado para los métodos de autenticación como CHAP, MS-CHAP y EAP-MD5 que son protocolos de autenticación.
- Access Accept: indica que la información que fue enviada por el usuario es correcta.
- Access Reject: indica que la información que fue enviada por el usuario es incorrecta.

Algunos de los Valores/Atributos que utiliza RADIUS son los siguientes:

- User-Name
- User-Password
- CHAP-Password
- NAS-IP-Address
- NAS-Port
- Service-Type
- Framed-IP-Address
- La IETF define 50 valores o atributos para el protocolo Radius.

Protocolo de RADIUS

Figura 2. **Estructura del paquete RADIUS**



Fuente: GEIER, Jim. *Implementing 802.1x security solutions for wired and wireless networks*. p. 72.

- Code: es el octeto encargado de verificar el tipo de paquete RADIUS, estos están establecidos de la siguiente manera.

  - 1 RADIUS Access-Request
  - 2 RADIUS Access-Accept
  - 3 RADIUS Access-Reject
  - 4 RADIUS Accounting-Request
  - 5 RADIUS Accounting-Response
  - 11 RADIUS Access-Challenge

- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 255 Reserved

- Identifier: el campo identificador de un paquete RADIUS, hace posible que los mensajes Access-Challenge puedan interactuar con los mensajes Access-Request.

- Length: este campo tiene una longitud de dos octetos y se encarga de identificar que tan grande es un paquete de RADIUS, un paquete de RADIUS como máximo puede tener 4 096 octetos.

- Authenticator: este campo es de 16 octetos y contiene el valor correspondiente al tipo de mensaje RADIUS que se está enviando. El campo de autenticación contiene una solicitud de autenticación o una respuesta de autenticación. Los cuales se describen asi:

    - Request-Authenticator: este campo se habilita como Request-Authentication cuando se envían un mensaje de Access-Request. Este valor es un número aleatorio y debe ser impredecible, así también único. El secreto compartido configurado en el autenticador y el servidor de autenticación es combinado con el Request-Authenticator y puesto en un desafío de MD5 y crear un valor de 16 octetos con el cual se realiza una operación XOR con la contraseña del usuario.

    - Response-Authenticator: este se utiliza cuando se envían mensajes de Acces-Accept, Access-Reject o Access-Challenge.

- Attributes Field: este campo es variable en longitud y contiene datos específicos de la comunicación entre un autenticador y el servidor RADIUS.

5.5. Autenticación de puertos basada en IEEE 802.1X

Autenticación es el proceso de identificar a una persona o cosa, por ejemplo una persona que intenta registrarse en un aeropuerto debe mostrar una identificación, en este caso pasaporte para poder lograrlo, un agente de servicio le solicita a esta persona su pasaporte que en este caso son las credenciales, una vez que el agente verifica el nombre y la foto, el usuario es autorizado a continuar, este proceso no es diferente al que realizan los dispositivos electrónicos, sin embargo, si puede haber más complejidad con estos dispositivos.

Un sistema de autenticación para una computadora puede volverse más complejo, *switches* de capa 2 y tarjetas de red NIC, son dispositivos que trabajan de una manera específica por lo que las comunicaciones que se tienen entre estos dos dispositivos, involucra precisión y complejidad para que una autenticación sea exitosa, protocolos incompatibles generalmente provocan interoperabilidad en los sistemas. En el ejemplo del aeropuerto si la persona confundiera su pasaporte con alguna credencial inservible para ese trámite, el agente de servicio puede dialogar con la persona para que esta presente la credencial necesaria, sin embargo una computadora siempre debe presentar las credenciales de manera correcta para no presentar problemas de autenticación.

Adicional al estándar la especificación completa para este tipo de autenticación fue escrita por diferentes organizaciones como: el Instituto de

Ingenieros Eléctricos y Electrónicos (IEEE), el Grupo de Ingeniería de Internet (IETF) y diferentes RFC que la definen.

Un término que debe ser entendido en autenticación de puertos es el término “puerto”, el cual es una conexión a nivel de capa 2 (enlace de datos). En un ambiente cableado la palabra puerto se refiere al puerto ethernet en un *switch,* muchos dispositivos como computadoras, servidores, cámaras, puntos de acceso y teléfonos pueden conectarse a un puerto ethernet.

La conexión completa y el medio son a nivel de capa 1 (física). El cable ethernet provee la interconexión que establece la parte física del enlace. La autenticación basada en puertos verifica la identidad de estos dispositivos conectados a los mismos.

El concepto de puerto también aplica a redes inalámbricas pero en este ámbito el puerto es una asociación con un punto de acceso, en vez de producir una conexión física, un cliente inalámbrico como un teléfono, tablet, laptop, pasa por un proceso de negociación con un punto de acceso. Los puntos de acceso periódicamente hacen un *broadcast* de un tipo de tramas llamadas *beacons*, cuando un cliente con tarjeta de red inalámbrica se enciende por primera vez, este escanea los canales de radio para buscar la presencia de un punto de acceso, después de esto el cliente intenta asociarse con el punto de acceso que tenga la señal más fuerte. Una vez después de este proceso se establece una asociación entre ambos dispositivos.

5.5.1. Beneficios de la autenticación

La autenticación basada en puertos mantiene a usuarios, dispositivos y clientes no autorizados fuera del alcance de recursos que se encuentran dentro

de una empresa como pueden ser: servidores, aplicaciones corporativas y bases de datos. Sin autenticación un hacker puede accesar fácilmente a una LAN y conectar una laptop a un puerto ethernet o asociarse con un punto de acceso inalámbrico en el estacionamiento de alguna compañía por ejemplo, y si a este se le permite conectarse, este buscará la manera de explotar todas las vulnerabilidades en la seguridad.

Implementar un acceso basado en puertos constituye un gran paso en la seguridad cableada e inalámbrica, no es un arma completa para proveer completa seguridad ya que también debe utilizarse: encriptación y cifrado de paquetes, IDS, NAC, para poder mitigar todas las posibles amenazas.

- Adicional a mantener el acceso no autorizado de manera restringida, la autenticación basada en puerto también tiene las siguientes características:

    - Información de localización del usuario: una aplicación externa puede fácilmente rastrear la localización de usuarios por ejemplo: basado en el *switch* o Access point donde el cliente fue autenticado. Esta información puede ser mapeada en una variedad de aplicaciones, como por ejemplo: un hospital puede usar la información de rastreo para encontrar a los doctores en un hospital, basada en el dispositivo inalámbrico que utilicen.

    - Mecanismos de cobro y auditoría: la autenticación basada en puerto combinada con sistemas de cobro y auditoría hace que ISP puedan proveer servicios de internet con base en un cobro. Si las personas no están autorizadas a navegar, estas pueden ser redirigidas a un portal donde se les solicite las credenciales de tarjeta de crédito

para poder accesar al sistema. Si las credenciales coinciden con lo que el sistema tiene almacenado en una base de datos, entonces se le permite al usuario navegar por internet.

- Acceso personalizado a la red: basado en las credenciales que se dieron durante el proceso de autenticación, el sistema puede autorizar ciertas aplicaciones.

5.5.2. Componentes primarios en la autenticación

- Suplicante: este es un cliente o dispositivo que necesita ser autenticado antes de que le sea permitido el acceso a la red. Cuando se habla de un *supplicant* o suplicante, se puede hace analogía a usuarios. Su identidad se encuentra en duda hasta que pueden proporcionar credenciales validas a un servidor de autenticación.

Para ser considerado un *supplicant* valido un dispositivo final como una laptop o un teléfono ip, debe implementar 802.1x y un método específico de EAP. Por ejemplo Microsoft Windows utiliza un método llamado EAP-TLS. Los métodos de EAP son a veces conocidos como tipos de EAP. El suplicante se comunica con el servidor de autenticación mediante EAP y un método específico (EAP-Method) que provea el mecanismo de autenticación.

- Autenticador: un autenticador es un dispositivo de capa dos como un *switch ethernet* o un punto de acceso inalámbrico. En una red empresarial todos los puertos de un *switch* podrían implementar 802.1X para proveer una autenticación.

El autenticador actúa como una puerta de seguridad entre los suplicantes y la red protegida. La puerta (realmente el puerto físico de un *switch*) se mantiene cerrado, hasta que el sistema de autenticación verifique las credenciales del suplicante y provea acceso al suplicante a la red protegida. Una vez autenticado el autenticador abre el puerto para que el suplicante pueda pasar.

El autenticador es un intermediario entre el suplicante y el servidor de autenticación, cuando el suplicante y el servidor de autenticación conversan todo este flujo pasa a través del autenticador. Por ejemplo el suplicante envía sus credenciales al servidor de autenticación encapsulando las mismas basadas en un método EAP (EAP-Method). En una trama de EAP que es encapsulada en una trama EAPOL. Esta última trama es enviada al autenticador el cual remueve el Método EAP utilizado, encapsulándolo en una trama de RADIUS hacia el servidor de autenticación.

- Servidor de autenticación: este es el encargado de requerir las credenciales al suplicante, después el suplicante le brinda las credenciales, en una autenticación basada en puertos, los estándares y especificaciones no hacen énfasis en algún tipo de autenticación en específico, sin embargo la mayoría de implementaciones utilizan RADIUS. Como resultado RADIUS es el estándar más utilizado en la industria de redes. Debe quedar claro que un servidor de autenticación es un componente separado y puede haber múltiples servidores de autenticación, así si alguno falla otro toma la función de autenticación.

5.5.3. Del suplicante al servidor de autenticación

La conversación de autenticación ocurre entre el servidor de autenticación y el suplicante, el método EAP (EAP-Method) define como la autenticación va a

ser llevada entre los dos entes, el método EAP representa varios elementos como por ejemplo las credenciales del suplicante.

La conversación entre estos dos entes incluye múltiples intercambios de datos EAP, esto dependiendo del método EAP utilizado. En la actual autenticación de puertos 802.1X, los métodos EAP utilizan diferentes tipos de credenciales como usuarios y contraseñas, claves de encriptación y certificados digitales. Los estándares requieren la implementación de los siguientes métodos EAP:

- Desafío MD5
- Contraseñas de una vez (OTP- *One time passwords*)
- Tarjeta genérica de token

Adicionalmente existen muchos métodos EAP basados en RFC, así también propietarios como pueden ser EAP-TLS, EAP-TTLS, EAP-FAST, y EAP-LEAP.

5.5.4. Del suplicante al autenticador (EAPOL/802.1X)

802.1X aplica entre el suplicante y el autenticador, un sistema completo de autenticación basada en 802.1X usa otros protocolos como RADIUS. 802.1X es solo una parte de todo el sistema. EAP en su principio fue diseñado como un protocolo punto a punto (PPP), sin embargo EAPOL está definido en el estándar 802.1X y adapta EAP sobre LAN.

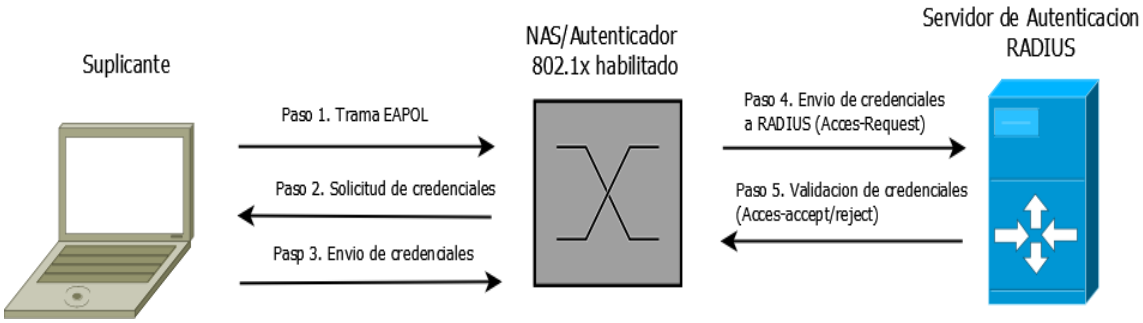
Para poder lograr la operación adecuada EAPOL agrega tres campos más a EAP.

- Versión
- Tipo
- Longitud

5.5.5. Del autenticador hacia el servidor de autenticación

Esta comunicación se lleva a cabo por medio del protocolo Radius.

Figura 3. **Diagrama de comunicación Radius**



Fuente: elaboración propia, con Adobe Illustrator.

5.6. Políticas de seguridad Enterasys

A continuación se presenta una descripción de las políticas de seguridad Enterasys.

5.6.1. Políticas de seguridad en *switches*

Una política de seguridad es una solución propietaria de *Enterasys* Networks en la cual se provee control y manipulación de tráfico, hay dos maneras de asignar políticas dentro de una red.

- Estáticamente
- Por puertos físicos
- Por dirección MAC
- Por dirección IP
- Por etiquetado de VLAN
- Dinámicamente
- Por medio de autenticación (RADIUS, Active Directory)

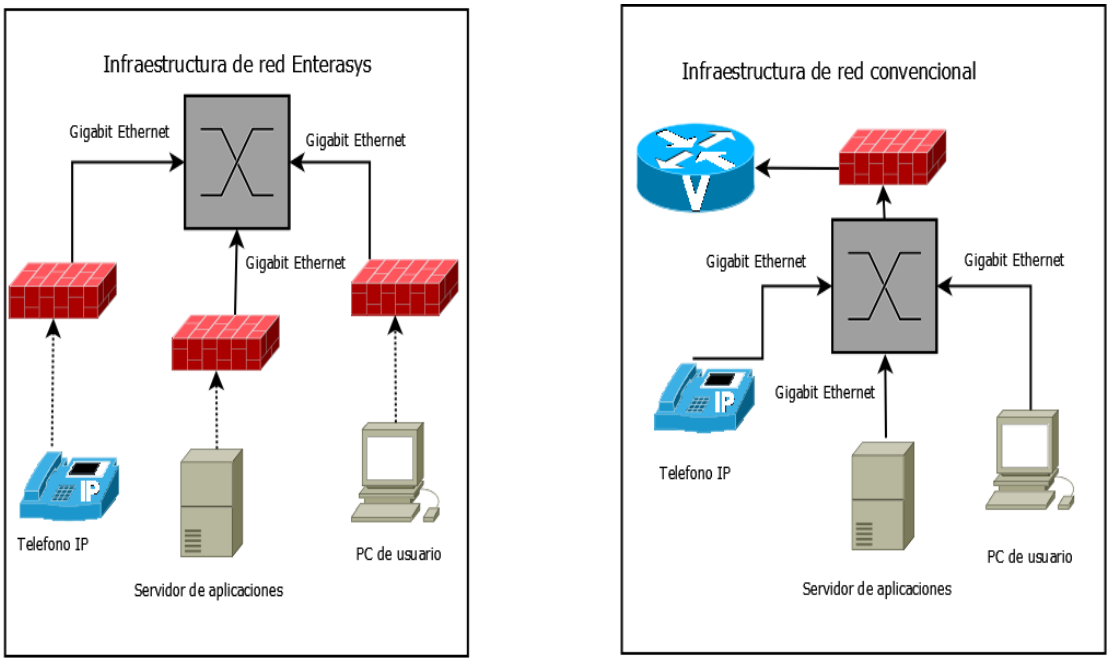
Una política tiene la capacidad de tomar acciones en el tráfico que entra hacia un puerto con base en reglas o características de capa 2, capa 3 o capa 4. Estas acciones incluyen control de ancho de banda, asignación de clase de servicio así también calidad de servicio.

5.6.2. Componentes necesarios para utilizar políticas de seguridad

- Switches Enterasys (Serie A, B, C, D, E, G, I, K, S)
- Enterasys Policy Manager
- Servicios de Autenticación (RADIUS, Active Directory)

Si los *switches* de la capa de acceso fueran de otra marca diferentes, un *switch* Enterasys puede autenticar hasta 9 000 dispositivos sin importar el tipo de *switch* de acceso, esto hace que la solución pueda interactuar con diferentes marcas.

Figura 4. **Estructura de seguridad Enterasys basada en políticas contra estructura convencional**



Fuente: elaboración propia, con Adobe Illustrator.

En la imagen se puede apreciar el contraste que existe en una implementación basada en políticas Enterasys, contra el modelo convencional de red que se utiliza. Se puede implementar políticas a nivel de capa 2 y así analizar lo que transita directamente por el puerto. Cada usuario o dispositivo puede ser colocado en su propio contenedor de seguridad/QoS para que se le aprovisionen los recursos apropiados de red en su puno de conexión.

Otros equipos de diferentes marcas utilizan aprovisionamiento por ACL para poder bloquear o permitir cierto tipo de tráfico desde una VLAN hacia otra.

Esta implementación de políticas permite utilizar QoS de fin a fin (*end-to-end*) dentro de toda la red, así también permite que el tráfico indeseado sea bloqueado antes de ingresar a la red y no después de haberlo hecho, consumiendo ancho de banda que necesitan aplicaciones críticas hasta que pueda llegar a un dispositivo de capa 3 y 4 que pueda hacer un bloqueo.

Dentro de las desventajas más comunes que se pueden encontrar en los modelos convencionales basados en VLAN y ACL, se puede encontrar:

- Las VLAN fueron creadas específicamente para contener *broadcast* dentro de un ambiente de capa 2. Estas nunca fueron creadas para volverse una utilidad de seguridad.

- El personal de IT es requerido en todos los cambios o políticas que se hagan a las ACL con respecto (asignación de puerto o tipo de bloqueo).

- Si un usuario cambia físicamente de lugar y la VLAN a la que pertenece no existe en ese dispositivo, involucra crear una VLAN nueva en ese dispositivo y extender el dominio de la VLAN hacia el mismo, causando un gasto de ancho de banda.

- Extender las VLAN hacia otros dispositivos, hace que la complejidad de la red se incremente de manera innecesaria.

5.6.3. Estructura de las políticas de seguridad

Tres parámetros son los que definen a las políticas de seguridad:

- Roles: estos definen una responsabilidad específica del trabajo, así también la función individual del empleado o grupo de empleados

(ingeniería, ventas, finanzas, entre otros), estos son creados con el software de gestión de políticas sin embargo son almacenados en los *switches*.

- Servicios: los servicios se definen en como los recursos de red agrupados, basados y creados con base en permitir o denegar un rol a los mismos. Algunas consideraciones dentro de los servicios son ancho de banda permitido o protocolos permitidos.

- Reglas de clasificación: estas están definidas a nivel de dispositivo final y una por una, forman el conjunto de servicios a los cuales un rol tendrá acceso.

5.6.4. Políticas estáticas

Políticas estáticas son las que son asignadas a un puerto específico de un *switch,* estas pueden bloquear protocolos a nivel de capa uno, dos, tres y cuatro. Se puede asignar una política diferente a cada puerto del *switch,* lo que significa que se puede permitir y denegar diferentes protocolos o comunicaciones por puerto.

No se tiene restricción alguna para los puertos, dentro de las características principales para este tipo de configuraciones se tiene:

El bloqueo de protocolos puede implementarse sin importar la VLAN a la que pertenezca el puerto, esto reduce que el tráfico innecesario sea denegado antes de entrar a la red, reduciendo el procesamiento y memoria que necesita un dispositivo de capa 3 para hacer esta función con base en listas de acceso.

No importa que dispositivo sea conectado en el puerto, las políticas funcionarán de la misma manera, con esto se asegura que un puerto contenga siempre seguridad.

Las políticas son modificables, lo que significa que se puede asignar otro rol a otro puerto si este ya no fuera funcional.

Un puerto puede ser asignado únicamente a un rol a la vez, si necesitaran características de otro rol, debe crearse un rol nuevo que involucre los servicios de los roles anteriores y este debe ser aplicado al puerto.

Pasos para configurar una política estática:

- Configurar un rol que establezca los servicios que podrá utilizar un usuario con base en las reglas de clasificación, estas reglas incluyen protocolos de capa 2 como arp, capa 3 icmp, capa 4 TCP/UDP o número de puerto lógico.

- Establecer los tipos de puertos que se tendrán en la red una buena práctica es utilizarlos así:

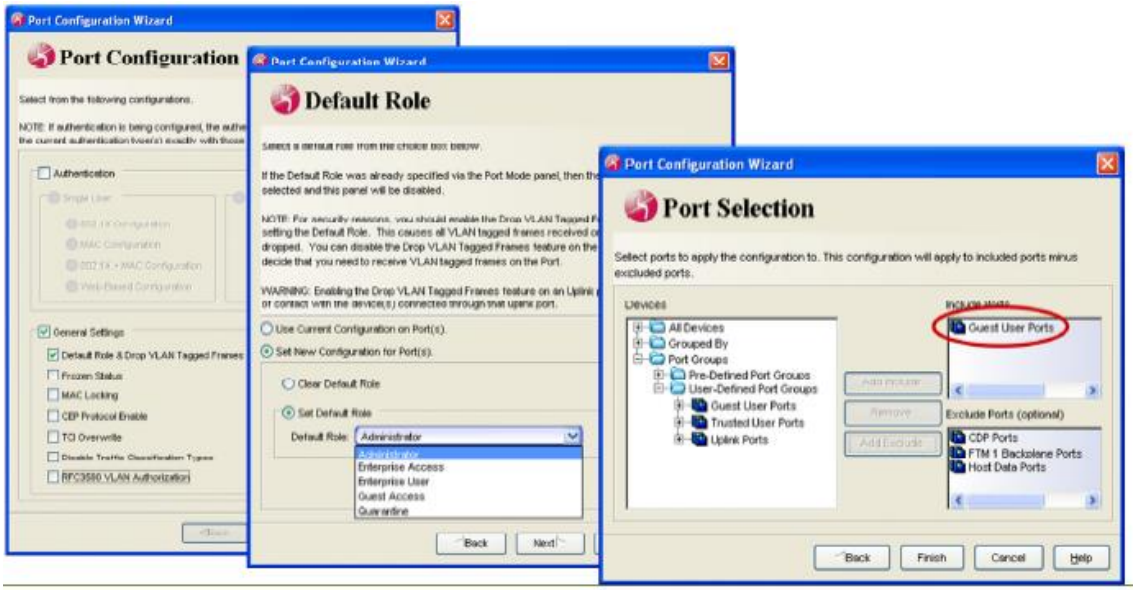
    - Puertos confiables: estos serán los puertos que tendrán un rol de servicios específicos de una organización, por ejemplo un rol de ingeniería, ventas, administración, finanzas. Esto de acuerdo a las necesidades de la empresa u organización.

    - Puertos de invitados: puertos que se utilizarán para personas invitadas que visiten la empresa, tendrán su propio rol el cual podrá

darles acceso solo a ciertos recursos, por ejemplo internet pero no tendrán acceso a los recursos de la empresa.

- Puertos de uplink: se utilizan para intercomunicarse con otros dispositivos.

Figura 5. **Interfaz gráfica de Enterasys Policy Manager para configurar roles y políticas. Propiedad de Enterasys Networks**



Fuente: elaboración propia, con Enterasys Networks Study Guide.

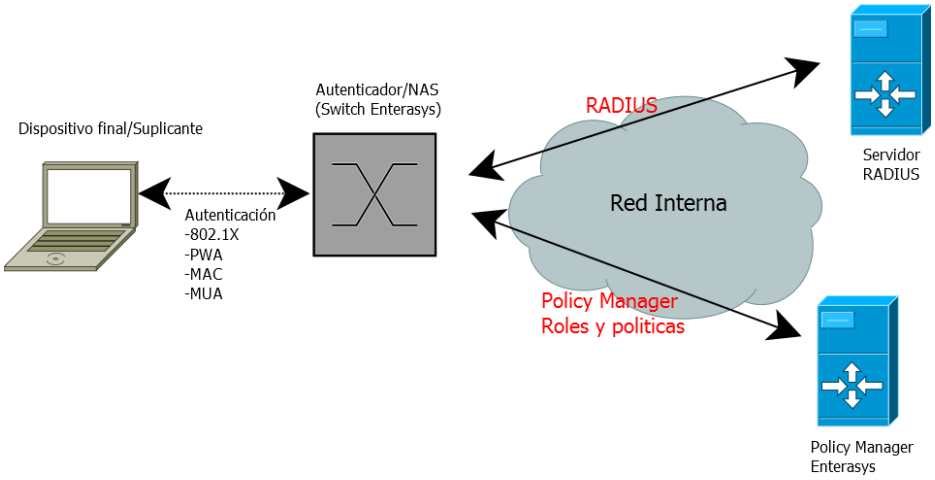
Las políticas estáticas pueden llegar a no ser escalables cuando una empresa tiene un crecimiento rápido, cuando esto pasa se deben utilizar políticas dinámicas.

5.6.5. Políticas dinámicas

Las políticas dinámicas se pueden asignar por medio de RADIUS utilizando los siguientes métodos:

- Autenticación de puerto vía web
- 802.1x
- Dirección MAC
- CEP (punto de convergencia del dispositivo final)
- MUA

Figura 6. **Topología aplicada a políticas dinámicas**



Fuente: elaboración propia, con Adobe Illustrator.

5.6.5.1. Autenticación de puerto vía web

Este tipo de autenticación (PWA) utiliza un proceso basado en un navegador web y en una página de ingreso de usuario, para poder tener acceso a los puertos de un *switch.* Este método emplea CHAP (Challegenge authentication protocol) o PAP (Password authentication protocol), el puerto se

encuentra bloqueado hasta que el usuario ingresa exitosamente sus credenciales en el navegador web. Antes de que el usuario sea autenticado el *switch* envía las credenciales a un servidor RADIUS.

Cuando se utiliza PAP la contraseña no es encriptada, en su contraparte con CHAP la contraseña es utilizada para generar un mensaje de desafío de una vía, si este mensaje recibido en el servidor RADIUS concuerda con el generado por el servidor RADIUS a partir de la contraseña que tiene almacenada.

Dependiendo del estado de autenticación del usuario, una página de autenticación o una página *logout* de sesión pueden ser desplegadas.

Si el usuario ingresa su contraseña de manera correcta entonces se pude devolver un “Filter-ID” configurado en el servidor RADIUS, este contiene el role que debería aplicar a ese puerto. De esta manera un rol con varias políticas es asignado con base en la autenticación.

5.6.5.2. Autenticación por dirección MAC

La autenticación MAC permite a los administradores, dar acceso a la red con base en la dirección MAC de los dispositivos conectados a un puerto en específico. Debe quedar claro que este tipo de autenticación, autentica al dispositivo y no al usuario, ya que la dirección MAC es una representación del dispositivo y no la identidad del usuario, por lo que debe tenerse en cuenta que un ataque de MAC spoofing podría dejar que un atacante no deseado en la red, pueda tener acceso a cierto perfil basado en el rol que se asigna.

5.6.5.3. CEP

Punto de convergencia del dispositivo final o por sus siglas en inglés (Convergence end point), es un método para detectar un teléfono IP o dispositivo de video, para aplicar alguna política al puerto de conexión basado en el dispositivo encontrado. Cuando una convergencia para un dispositivo final es aplicada puede detectar diferentes tipos de dispositivos:

- Cisco Phone Detection: este utiliza el protocolo propietario de Cisco, Cisco discovery protocol para detectar el dispositivo.
- Siemens Hipath Phone Detection: cuando el dispositivo tiene configurada una dirección IP, este lo detecta automáticamente, si el dispositivo no tuviera una IP asignada, se utiliza el puerto TCP 4060 como parámetro para poder detectarlo.
- H.323 Phone Detection: utiliza puertos UDP/TCP con una dirección multicast (224.0.1.41) los puertos por default que utiliza este protocolo son 1718, 1719, 1720.
- SIP PhoneDetection: utiliza puertos TCP/UDP para hacer la detección por default el puerto para este protocolo es el 5060.

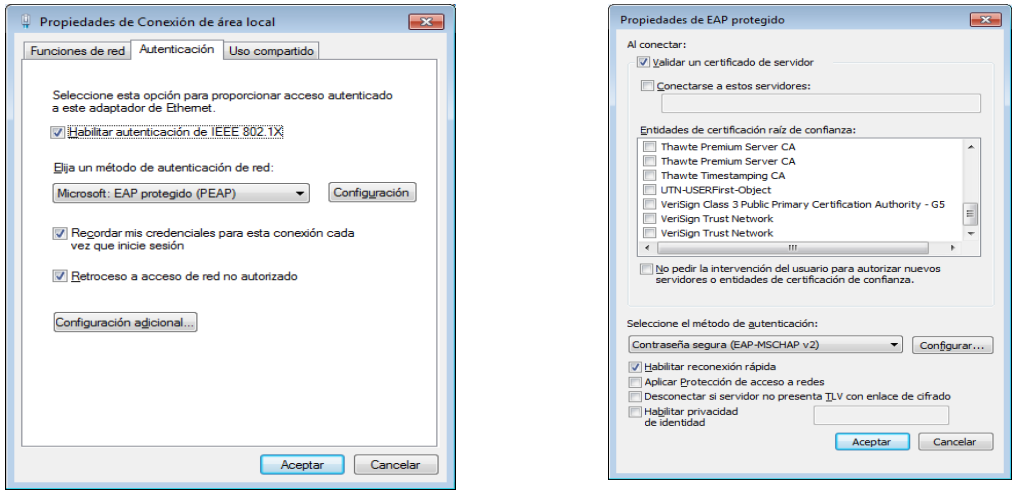
Para este tipo de detección de dispositivos, en el caso que los mismos no estuvieran conectados directamente al *switch* Enterasys (un *switch* de por medio) y estos se desconectan, el *switch* Enterasys seguirá aplicando las políticas para estos dispositivos hasta que no haya un *link* caído, razón por la cual tienen otra característica: cuando un dispositivo CEP no envíe tráfico en un determinado periodo de tiempo (Etsys Multi Authidletimeout), el *switch.*

5.6.5.4. 802.1x

Con este método los roles son asignados por medio de autenticación 802.1x, si un dispositivo final cuenta con esta autenticación. La misma se puede

utilizar para permitir o denegar protocolos a un dispositivo, por ejemplo los dispositivos Microsoft Windows que se muestran.

Figura 7. **Configuración de 802.1x del sistema operativo Microsoft Windows**



Fuente: elaboración propia, con Microsoft Windows.

5.6.5.5. MUA

Este método se puede utilizar para autenticar a varios dispositivos sobre un solo puerto, dependiendo de la capacidad de cada *switch,* este puede llegar a autenticar a miles de dispositivos en un solo chasis. El método de autenticación depende del dispositivo final que se esté utilizando.

Los dispositivos pueden variar de acuerdo con la tecnología, por ejemplo una computadora puede autenticarse por PWA o por 802.1X, un teléfono IP por 802.1X o por MAC, sin embargo una cámara tal vez podría hacerlo solo por MAC,

pero esta tecnología permite a varios dispositivos autenticarse de diferentes maneras en un solo puerto.

5.6.6. Asignación de QoS con base en políticas de seguridad

La clase de servicio de ciertas tramas puede modificarse de acuerdo al rol que tiene un determinado puerto. Esto con base en el estándar IEEE802.1p que permite 8 prioridades distintas dentro del encabezado de la trama IEEE802.1Q.

Cuando el tráfico entra por primera vez a un *switch,* no hay diferenciación entre paquetes ya que todo está sin clasificar. Con la clasificación de tráfico se puede probar si los paquetes concuerdan con un criterio definido. Una vez que el paquete concuerda con el criterio, opcionalmente este puede ser marcado. Una vez etiquetado con una prioridad, este paquete no debe ser reclasificado en cada *switch* donde deba pasar.

- Hay dos tipos de etiquetado de tráfico:
  - Etiquetado en capa dos con una prioridad 802.1p
  - Etiquetado en capa tres con DSCP

La clasificación de paquetes es el primer parámetro a tener en cuenta en QoS.

Una vez los paquetes hayan entrado a la red y pasen por diferentes dispositivos, estos ya deben de estar clasificados, es por ello que en esta fase de reenvío otras acciones pueden ser tomadas con base en esta clasificación, por ejemplo:

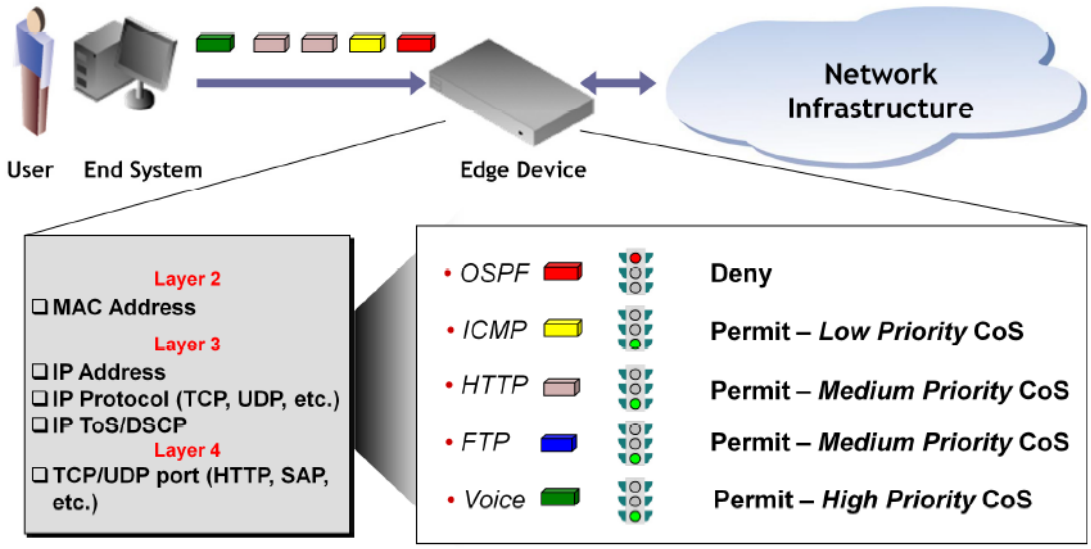
- Priorizar el tráfico con base en el etiquetado
- Limitar la cantidad de tráfico o ancho de banda

- Controlar el tráfico mediante el uso de colas

5.6.6.1. Clasificación de tráfico

El primer componente del QoS es la clasificación de tráfico, esta debe ser implementada lo más cercano a la capa de acceso en la red. Esta clasificación permite que los paquetes sean enviados dentro de un parámetro de clasificación, el cual se define con base en qué tan importante es el tráfico que cursa en la red. Todos los paquetes dentro de un mismo parámetro son parte de la misma clase de servicio, durante la fase posterior (etiquetado), los paquetes dentro de una misma clase de servicio serán etiquetados de tal manera que puedan ser identificados de manera única, sin importar por el dispositivo de red en que se encuentren.

Figura 8. **Clasificado de tráfico en un *switch* Enterasys**



Fuente: elaboración propia, con Enterasys Networks Study Guide.

Para poder clasificar los paquetes se utilizan atributos pertenecientes a los paquetes recibidos, con esto es posible asignar una clase de servicio CoS. En la imagen anterior por ejemplo se podría denegar todo el tráfico OSPF, revisando el campo “Protocol Type” o “Tipo de protocolo” en el encabezado IP que debería estar en 89 para OSPF. El tráfico ICMP con el mismo campo configurado a 1 es asignado a una CoS de prioridad baja, el tráfico HTTP y FTP por medio de un rol que utiliza como reglas puertos TCP es asignado a una CoS intermedia y el tráfico de VoIP es asignado a una prioridad alta.

5.6.6.2. Etiquetado de tráfico

El segundo componente de una calidad de servicio QoS es el etiquetado, este debe ser implementado lo más cercano a la capa de acceso, algunas veces los mismos dispositivos finales etiquetan sus paquetes o tramas con calidad de servicio ellos mismos.

Algunos dispositivos que etiquetan ellos mismos sus paquetes y tramas con QoS son:

- Servidores
- Cámaras
- Teléfonos IP
- Softphones

Sin embargo, no es recomendable que esto se haga, ya que un atacante que logre comprometer un dispositivo puede etiquetarlo con QoS como quiera, y esto lograría que los paquetes enviados por el atacante sean permitidos a la red y tengan una alta prioridad sobre otro tipo de tráfico.

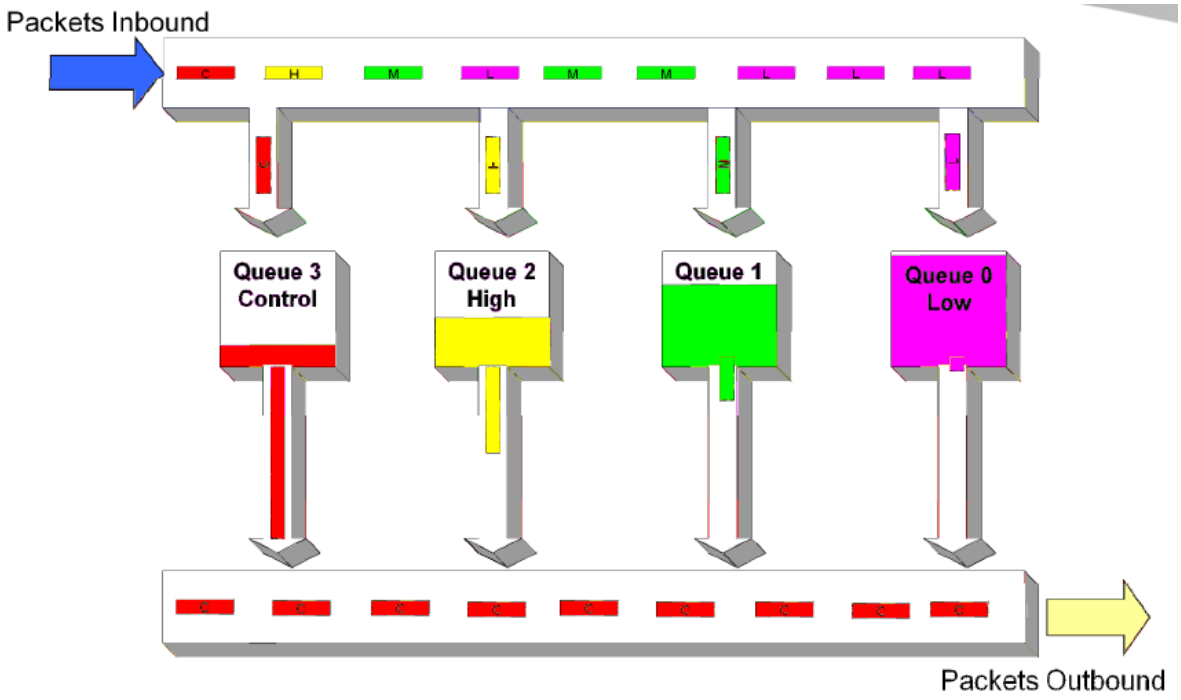
Es recomendable que el etiquetado de QoS se realice con base en reglas de clasificación y así poder asignar una QoS adecuada, ya sea en capa dos utilizando IEEE802.1p o en capa 3 utilizando el campo ToS dentro del encabezado IP con DSCP.

5.6.6.3. Reenvío de tráfico Strict Priority Queuing SPQ

Este debe ser aplicado en todas las capas de la red y es el encargado de dar la respectiva priorización a cada paquete, con base en el etiquetado que se haya utilizado para asignarlo a una clase de servicio CoS. Basado en la CoS los paquetes son transmitidos hacia afuera de los puertos, por medio de una cola en la que son puestos antes de salir de los *switches*. Adicional a esto con el etiquetado se puede limitar ancho de banda (Rate Limiting) a una CoS o utilizar Rate Shaping el cual consiste en limitar.

Las colas que tengan mayor prioridad siempre deben salir antes de las de menor prioridad, cada paquete es asignado a una cola con base en su prioridad. Y se utiliza un algoritmo FIFO (First In First Out), si las colas de alta prioridad nunca terminaran de recibirse, entonces las colas de menor prioridad no podrían ser transmitidas. Este tipo de algoritmo en transmisión de colas es utilizado en enlaces que utilizan tráfico crítico y sensible como VoIP, o tráfico crítico que es crucial para el desempeño de una empresa.

Figura 9. **Control de colas en método SPQ**

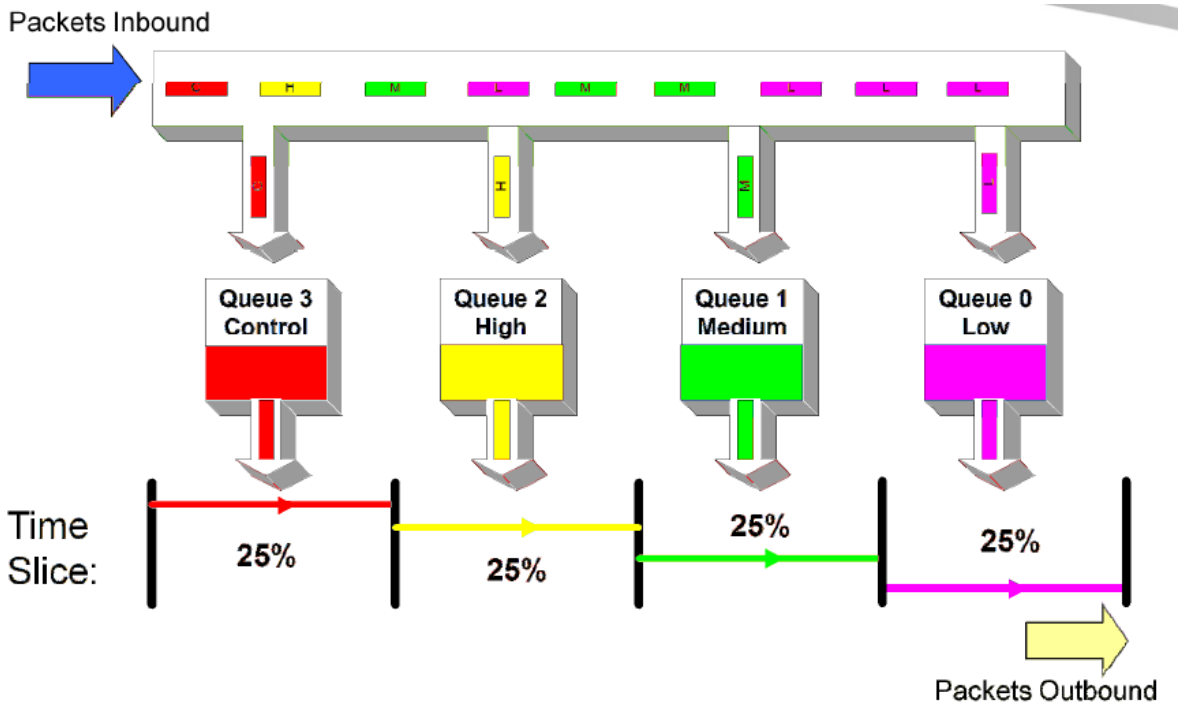


Fuente: elaboración propia, con Enterasys Networks Study Guide.

5.6.6.4. Reenvío de tráfico Weighted Fair Queuing WFQ

En contraste con SPQ, en WFQ un porcentaje de cada cola es asignado para poder utilizar el ancho de banda, de esta manera el ancho de banda se optimiza de una mejor manera y se dá lugar para que todas las aplicaciones puedan transmitir en algún momento, por ejemplo para un 100 % de paquetes recibidos se podría asignar el 50 % a la cola 3, el 25 % a la cola 2 y el 25 % a la cola 1, de esta manera el tráfico podría transmitirse de manera eficiente conservando las prioridades.

Figura 10. **Control de colas con el método WFQ**



Fuente: elaboración propia, con Enterasys Networks Study Guide.

5.7. VPN

Las organizaciones usan las redes VPN para proporcionar una infraestructura WAN virtual que conecta sucursales, oficinas domésticas, oficinas

de socios comerciales y trabajadores a distancia, a toda la red corporativa o a parte de ella. Para que permanezca privado, el tráfico está encriptado. En vez de usar una conexión de capa 2 exclusiva, como una línea alquilada, la VPN usa conexiones virtuales que se enrutan a través de internet.

El trabajo a distancia es un término amplio que hace referencia a realizar un trabajo mediante la conexión al lugar de trabajo desde una ubicación remota, con la ayuda de las telecomunicaciones. El trabajo a distancia eficaz es posible debido a conexiones de internet de banda ancha, redes privadas virtuales (VPN) y tecnologías más avanzadas, incluidas Voz sobre IP (VoIP) y videoconferencias. El trabajo a distancia permite ahorrar dinero que de otro modo se gasta en viajes, infraestructura y soporte de instalaciones.

5.7.1. Características de las VPN seguras

Las VPN utilizan técnicas de encriptación avanzada y *tunneling* para permitir que las conexiones de red privadas de extremo a extremo, que establezcan las organizaciones a través de internet sean seguras.

Las bases de una VPN segura son la confidencialidad, la integridad de datos y la autenticación:

- Confidencialidad de datos: una cuestión de seguridad que suele despertar preocupación, es la protección de datos contra personas que puedan ver o escuchar subrepticiamente información confidencial. La confidencialidad de datos, que es una función de diseño, tiene el objetivo de proteger los contenidos de los mensajes contra la intercepción de fuentes no autenticadas o no autorizadas. Las VPN logran esta confidencialidad mediante mecanismos de encapsulación y encriptación.

- Integridad de datos: los receptores no tienen control sobre la ruta por la que han viajado los datos y, por lo tanto, no saben si alguien ha visto o ha manejado los datos mientras viajaban por internet. Siempre existe la posibilidad de que los datos hayan sido modificados. La integridad de datos garantiza que no se realicen cambios indebidos, ni alteraciones en los datos mientras viajan desde el origen al destino. Generalmente, las VPN utilizan *hashes* para garantizar la integridad de los datos. El hash es como una *checksum* o un sello (pero más robusto) que garantiza que nadie haya leído el contenido. En el próximo tema se incluye la explicación de los *hashes*.

- Autenticación: la autenticación garantiza que el mensaje provenga de un origen auténtico y se dirija a un destino auténtico. La identificación de usuarios brinda al usuario la seguridad de que la persona con quien se comunica es quien cree que es. Las VPN pueden utilizar contraseñas, certificados digitales, tarjetas inteligentes y biométricas, para establecer la identidad de las partes ubicadas en el otro extremo de la red.

5.7.2. Tipos de VPN

A continuación se presentan los tipos de VPN.

5.7.2.1. VPN de sitio a sitio

Las organizaciones usan las VPN de sitio a sitio, para conectar ubicaciones remotas, tal como se usa una línea alquilada o conexión Frame Relay. Debido a

que la mayoría de las organizaciones ahora tiene acceso a internet, es lógico aprovechar los beneficios de las VPN de sitio a sitio.

Una VPN de sitio a sitio es una extensión de una *networking* WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre ellas. Por ejemplo, pueden conectar la red de una sucursal a la red de la sede central corporativa.

En una VPN de sitio a sitio, los *hosts* envían y reciben tráfico TCP/IP a través de un *gateway* VPN, el cual podría ser un *router*, una aplicación *firewall* PIX o una aplicación de seguridad adaptable (ASA). El *gateway* VPN es responsable de la encapsulación y encriptación del tráfico saliente para todo el tráfico desde un sitio particular, y de su envío a través de un túnel VPN por internet a un *gateway* VPN par en el sitio objetivo. Al recibirlo, el *gateway* VPN par elimina los encabezados, descifra el contenido y retransmite el paquete hacia el *host* objetivo dentro de su red privada.

5.7.2.2. VPN de acceso remoto

La mayoría de los trabajadores a distancia ahora tienen acceso a internet desde sus hogares, y pueden establecer VPN remotas por medio de las conexiones de banda ancha. De manera similar, un trabajador móvil puede realizar una llamada local a un ISP local para lograr el acceso a la empresa a través de internet. De hecho, esto marca un avance de evolución en las redes *dial-up*. Las VPN de acceso remoto pueden admitir las necesidades de los trabajadores a distancia, los usuarios móviles, además de las *extranets* de consumidores a empresas.

En una VPN de acceso remoto, cada *host* en general tiene software cliente de VPN. Cuando el *host* intenta enviar tráfico, el software cliente de VPN

encapsula y encripta ese tráfico antes del envío a través de internet, hacia el *gateway* VPN en el borde de la red objetivo. Al recibirlo, el *gateway* VPN maneja los datos de la misma manera en que lo haría con los datos de una VPN de sitio a sitio.

5.7.3. Tunneling de VPN

El *tunneling* permite el uso de redes públicas como internet para transportar datos para usuarios, siempre que estos tengan acceso a una red privada. El *tunneling* encapsula un paquete entero dentro de otro paquete y envía por una red el nuevo paquete compuesto. Esta figura contiene una lista de las tres clases de protocolos que utiliza el *tunneling*.

5.7.3.1. Protocolo portador

Este es el protocolo por medio del cual viaja la información, el protocolo podría ser ATM, Frame Relay, MPLS. Dependiendo del tipo de tecnología WAN que se utilice, así será el protocolo portador. Haciendo una analogía, este protocolo es como una agencia postal que se encarga de entregar la carta desde un buzón origen hacia otro buzón destino.

5.7.3.2. Protocolo de encapsulación

Se encarga de encapsular los datos originales por medio de algún tipo de algoritmo, dentro de los protocolos de encapsulación se tienen: IPsec, L2TP,

PPTP, GRE, L2F. Si se supone el protocolo dentro del ejemplo del sistema postal, este es equivalente a un sobre conteniendo una carta.

5.7.3.3. Protocolo pasajero

Este es el protocolo por medio del cual se transportan los datos originales, dentro de este tipo de protocolos se tiene: IP versión 4, IP versión 6, AppleTalk, IPX. Dentro de una analogía de un sistema postal este protocolo es como la carta donde se escriben los datos.

5.7.4. Algoritmos de encriptación para VPN

Si por internet pública se transporta texto sin formato, puede ser interceptado y leído. Para mantener la privacidad de los datos, es necesario encriptarlos. La encriptación VPN encripta los datos y los vuelve ilegibles para los receptores no autorizados.

Para que la encriptación funcione, tanto el emisor como el receptor deben conocer las reglas que se utilizan para transformar el mensaje original en la versión codificada. Las reglas de encriptación de la VPN incluyen un algoritmo y una clave. Un algoritmo es una función matemática que combina mensaje, texto, dígitos o los tres con una clave. El resultado es una cadena de cifrado ilegible. El descifrado es extremadamente difícil o imposible sin la clave correcta.

Algunos de los algoritmos de encriptación más comunes y la longitud de claves que se utilizan son los siguientes:

- Algoritmo Estándar de Cifrado de Datos (DES): desarrollado por IBM, utiliza una clave de 56 bits para garantizar una encriptación de alto

rendimiento. El DES es un sistema de encriptación de clave simétrica. Las claves simétricas y asimétricas se explican más adelante.

- Algoritmo Triple DES (3DES): una variante más reciente del DES que realiza la encriptación con una clave, descifra con otra clave y realiza la encriptación por última vez con otra clave también diferente. 3DES le proporciona mucha más fuerza al proceso de encriptación.

- Estándar de Encriptación Avanzada (AES): el Instituto Nacional de Normas y Tecnología (NIST) adoptó el AES, para reemplazar la encriptación DES en los dispositivos criptográficos. AES proporciona más seguridad que DES y es más eficaz en cuanto a su cálculo que 3DES. AES ofrece tres tipos de longitudes de clave: claves de 128, 192 y 256 bits.

- Rivest, Shamir y Adleman (RSA): sistema de encriptación de clave asimétrica. Las claves utilizan una longitud de bits de 512, 768, 1024 o superior.

- Encriptación simétrica: los algoritmos de encriptación como DES y 3DES requieren que una clave secreta compartida realice la encriptación y el descifrado. Los dos equipos deben conocer la clave para decodificar la información. Con la encriptación de clave simétrica, también llamada encriptación de clave secreta, cada equipo encripta la información antes de enviarla por la red al otro equipo. la encriptación de clave simétrica requiere el conocimiento de los equipos que se comunicarán, para poder configurar la misma clave en cada uno.

- Encriptación asimétrica: la encriptación asimétrica utiliza diferentes claves para la encriptación y el descifrado. El conocimiento de una de las claves

no es suficiente, para que un pirata informático deduzca la segunda clave y decodifique la información. Una clave realiza la encriptación del mensaje y otra, el descifrado. No es posible realizar ambos con la misma clave.

La encriptación de clave pública es una variante de la encriptación asimétrica, que utiliza una combinación de una clave privada y una pública. El receptor le dá una clave pública a cualquier emisor con quien desee comunicarse el receptor. El emisor utiliza una clave privada junto con la clave pública del receptor para encriptar el mensaje. Además, el emisor debe compartir la clave pública con el receptor. Para descifrar un mensaje, el receptor utiliza la clave pública del emisor y su propia clave privada.

5.7.5. Protocolos de estructura IPsec

El IPsec es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación. IPsec ingresa el mensaje necesario para proteger las comunicaciones VPN, pero se basa en algoritmos existentes. Existen dos protocolos de estructura IPsec:

- Encabezado de autenticación (AH): se utiliza cuando no se requiere o no se permite la confidencialidad. AH proporciona la autenticación y la integridad de datos para paquetes IP intercambiados entre dos sistemas. Verifica que cualquier mensaje intercambiado de R1 a R3 no haya sido modificado en el camino. También verifica que el origen de los datos sea R1 o R2. AH no proporciona la confidencialidad de datos (encriptación) de los paquetes. Si se lo utiliza solo, el protocolo AH proporciona poca protección. Por lo tanto, se lo utiliza junto con el protocolo ESP para brindar las funciones de seguridad de la encriptación de los datos y el alerta contra alteraciones.

- Contenido de seguridad encapsulado (ESP): proporciona confidencialidad y autenticación mediante la encriptación del paquete IP. La encriptación del paquete IP oculta los datos y las identidades de origen y de destino. ESP autentica el paquete IP interno y el encabezado ESP. Proporciona autenticación del origen de datos e integridad de datos. Aunque tanto la encriptación como la autenticación son opcionales en ESP, debe seleccionar una como mínimo.

6. ANÁLISIS FINANCIERO

6.1. Empresas y líneas de producto en el mercado actual

A continuación se presenta una descripción de las empresas y líneas de producto en el mercado actual.

6.1.1. Cisco Systems

Cisco Systems es una empresa que se dedica a fabricar y vender equipos de telecomunicaciones y redes, dentro de los servicios que vende Cisco se pueden encontrar los siguientes:

- Dispositivos intermediarios para interconexión de redes como *routers, switches, hubs,* puntos de acceso.
- Dispositivos de seguridad como *firewalls*, y concentradores de VPN.
- Plantas telefónicas IP como su CallManager una PBX completamente IP.
- Softwares de administración y gestión de red.
- Equipos para redes de almacenamiento.

Cisco se fundó en 1984 por la pareja matrimonial (Leonard Bosack y Sandra Lener), ellos eran parte del equipo de computación en la Universidad de Stanford. El nombre de la compañía viene de la palabra San Francisco, pero un árbol que se interponía en un cartel que tenía la palabra hacía que este nombre se viera como San Francisco y ahí de este cartel fue de donde se tomó el nombre de la compañía.

Series ISR G2: por sus siglas ISR G2 (Integrated Services Routers Generation 2), estos *routers* fueron hechos para sucursales pequeñas, que necesitan capacidades de video, virtualización y colaboración web. Estos además tienen una administración bastante simple a través de un software IOS universal.

Dentro de los modelos utilizados por Cisco se tienen:

- *Router*:
  - Generación 2 de *routers* ISR
  - Cisco 3900 Series
  - Cisco 2900 Series
  - Cisco 1900 Series
  - Cisco 890, 880, 860 Series
  - Generación 1 de *routers* ISR
  - Cisco 3800 Series
  - 3845 Integrated Services Router
  - 3825 Integrated Services Router
  - Cisco 2800 Series
  - Cisco 1800 Series
  - Cisco 870, 850 Series

- *Switches* de acceso:
  - Cisco Catalyst 4500E Series
  - Cisco Catalyst 3850 Series
  - Cisco Catalyst 3750-x Series
  - Cisco Catalyst 3560-x Series
  - Cisco Catalyst 2960-x Series

- *Switches* de distribución y core:
    - Cisco Catalyst 6500 Series

6.1.2. Hewlett Packard

Mejor conocida como HP, es una empresa líder que se dedica a la venta de tecnología de la información, tiene sede en Palo Alto, California. La compañía fue fundada en 1939 por William Hewlett y David Packard, en un principio la compañía se dedicaba a fabricación de instrumentos de medición como osciloscopios. Actualmente HP es líder en ventas de computadoras portátiles y de escritorio.

El 12 de diciembre de 2009, HP adquiere la empresa 3Com por 2 700 millones de dólares, 3Com es un fabricante de productos de redes que concentra una gran parte de su actividad en China. HP adquiere 3Com con la finalidad de impulsar y expandir su mercado de telecomunicaciones.

Dentro de los equipos HP se puede nombrar:

- *Routers*:
    - HP 6600 Series
    - HP 8800 Series
    - HP HSR6600 Series
    - HP HSR8800 Series

- *Switches*:
    - HP 5800 Series
    - HP 5820 Series
    - HP 5830 Series

- HP 5900 Series
- HP 5920 Series
- HP 12500 Series

6.1.3. Nortel

Nortel Network Corporation conocida como Nortel, es una empresa que produce diferentes tipos de servicios de software y hardware, la sede se encuentra en Toronto, Canadá y en 2009 anunció el cese de todas sus actividades. Todas las soluciones corporativas como redes de datos pasaron a ser parte de Avaya, la cual es una empresa privada de telecomunicaciones que se especializa en el sector de la telefonía y centros de llamadas.

Entre los equipos Avaya se puede mencionar:

- *Routers*:
  - Secure Router 1000 Series
  - Secure Router 2000 Series
  - Secure Router 3000 Series
  - Secure Router 4000 Series

- *Switches*:
  - *Ethernet* Routing Switch 2500 Series
  - *Ethernet* Routing Switch 3500 Series
  - *Ethernet* Routing Switch 4000 Series
  - *Ethernet* Routing Switch 5000 Series
  - Ethernet Routing Switch 8000 Series

6.1.4. Enterasys Networks

Enterasys Networks es una compañía norteamericana que se dedica a ofrecer infraestructura para redes de datos cableadas e inalámbricas, así también como soluciones de administración de seguridad de redes para educación, gobierno, salud y empresas de manufactura. Los equipos van desde *routers*, *switches* hasta puntos de acceso inalámbrico con el estándar IEEE 802.11.

La empresa fue fundada en 1983 como Cabletron Systems y posteriormente en el 2000 pasó a llamarse Enterasys Networks. En el 2005 Gores Group adquiere Enterasys Networks. Posteriormente en el año 2008 Gores Group adquiere el 51 % de las acciones de productos corporativos de Siemens (Plantas telefónicas TDM/IP) y así se forma Siemens Enterprise Communications (SEN), con esto ambas compañías bajo el mando de Gores Group diseñan soluciones de fin a fin (*end to end*) para compañías. En septiembre de 2013 Extreme Networks compra Enterasys Networks.

Adicional al hardware de redes, la compañía también fabrica software de gestión de redes y aplicaciones de seguridad como sistemas de prevención de intrusiones (IPS), control de acceso a la red (NAC), y administrador de seguridad de eventos (SIEM: Security information event management).

Una de las ventajas más importantes que tiene Enterasys Networks, es el diseño de políticas de seguridad que pueden ser aplicadas a un puerto como una lista de control de acceso de manera dinámica, característica que es una entre sus competidores.

Entre los equipos que maneja Enterasys Networks se pueden mencionar:

- *Routers*:
    - X Series
    - XSR Series
- *Switches*:
    - Acceso
    - A series
    - B series
    - C Series
    - D Series
    - G Series
    - Industrial
    - I Series
    - Distribución/Core
    - K Series
    - N Series
    - S Series

6.2. Diferencias entre las diferentes marcas

El mercado de las redes cableadas e inalámbricas consiste de vendedores que proveen componentes estándar a nivel de red, estos proveen conectividad a la infraestructura de acceso donde se encuentran los usuarios. Los vendedores han reducido significativamente la brecha de rendimiento entre los entornos cableados e inalámbricos divergentes, y ahora ofrecen opciones de conectividad por cable e inalámbrica directamente, a través de socios estratégicos del mercado. Además, los proveedores continúan con sus esfuerzos para integrar la gestión, seguridad, el acceso para invitados y planificación en estas infraestructuras.

Los *switches* de acceso suelen tener como requisito trabajar en *stacking*. Aunque el número de puertos puede variar de 24 a 48 o más, un elemento clave es el apoyo de Power Over ethernet (PoE) y PoE + para ofrecer una gama de opciones y energizar a varios dispositivos, incluyendo puntos de acceso inalámbrico, teléfonos IP y cámaras de vídeo.

La planificación de energía sigue siendo importante, no solo para hacer frente a los presupuestos de potencia, sino también para garantizar que la potencia adecuada está disponible en armarios de cableado. Mientras que 10 Mbps y 100 Mbps de conectividad por cable sigue siendo más que suficiente para la mayoría de usuarios, y sigue contando con aproximadamente el 50 % de los puertos vendidos para el despliegue de acceso en una empresa, se sigue viendo un crecimiento en 1 % en *switches* de acceso gigabit.

Esta demanda seguirá creciendo a medida que los *switches* de acceso asuman el papel de agregación inalámbrico en la capa de acceso convergente, ya que los puntos de acceso inalámbrico 802.11n puede requerir hasta 525 Mbps de ancho de banda o *half-duplex*. Dependiendo de la densidad de transacción de los puntos de acceso, las organizaciones de IT deben ser conscientes de que los *switches* deben ser compatibles con las capacidades Gigabit ethernet (GbE).

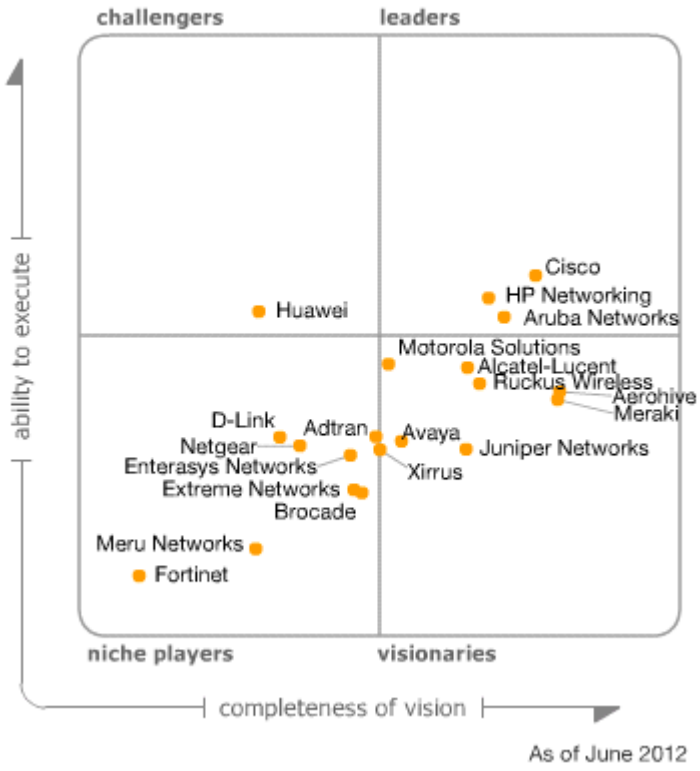
6.2.1. Gartner

Gartner Inc. Es una empresa que se dedica a la consultoría e investigación de IT, tiene sede en Stamford, Connecticut, Estados Unidos. La empresa cuenta con 4 800 empleados incluyendo a 1 250 analistas en 85 países del mundo. Gartner realiza análisis de investigación para profesionales dedicados a las tecnologías de la información y comunicación, estos análisis son programas

diseñados específicamente para CEO y directores ejecutivos. La manera en que se presentan los análisis es en forma de cuadrantes mágicos.

Las diferencias entre distintas marcas se hacen con base en el cuadrante mágico actualizado de Gartner.

Figura 11. **Cuadrante mágico actualizado de la empresa Gartner Inc**



Fuente: www.gartner.com. Consulta: junio de 2012.

6.2.2. Cisco

Cisco es el mayor proveedor y líder del mercado en la empresa de infraestructura de red cableada e inalámbrica. Un fuerte canal en la industria, junto con una presencia global, significa que Cisco sigue siendo el primero para todas las oportunidades en infraestructura de la capa de acceso. Su reorganización para centrarse en la capa de acceso inalámbrico y por cable ha dado lugar a un renovado interés en el progreso y en el borde de la red de la empresa.

La liberación de Cisco del servicio del motor de Identidad (ISE) ofrece una sólida gestión, seguridad y funcionalidad de las aplicaciones de servicios de red con políticas para redes cableadas y WLAN. La funcionalidad coincide con un nuevo mensaje de *marketing* "Una Política, One Management, una red" para educar a los usuarios finales. Cisco se centra en el sector público, la salud, la educación y los mercados al por menor, pero se debe considerar para cualquier gran oportunidad de negocio.

Algunas consideraciones que deben tomarse con Cisco Systems son las siguientes:

Cisco puede desplegar soluciones inalámbricas sin un aparato controlador físico (es decir, la funcionalidad del controlador se encuentra dentro de los puntos de acceso especial, o prácticamente dentro de los centros de datos para múltiples sitios remotos). Los equipos Flex Cisco 7500 proporcionan una opción para virtualizar la funcionalidad del controlador dentro del centro de datos empresarial. Incluso con estas capacidades, las ofertas de Cisco pueden ser más caras para las pequeñas y medianas implementaciones, dependiendo del tipo de controlador implementado.

En los últimos dos años, Cisco ha puesto en marcha diversas medidas, como la formación y la certificación, para mejorar la coherencia de las propuestas e implementaciones de soluciones de infraestructura complejas con revendedores. Sin embargo, dado el enorme número de distribuidores de la compañía, este proceso llevará tiempo.

Como empresa, Cisco se encuentra en un estado de desarrollo y en transición, y las empresas deben verificar que la funcionalidad que necesitan para cumplir con sus parámetros de negocio es parte de la solución propuesta.

6.2.3. Networking

HP Networking ha consolidado como un líder mundial en el mercado de *switches* de acceso con su arquitectura FlexNetwork, y ha duplicado el número de puntos de acceso vendidos para la conectividad inalámbrica. En 2011, HP Networking aumentó sus ingresos en un 40 %. Mientras que HP mostró claramente una visión de la capa de acceso e hizo un buen progreso en las aplicaciones de red, no hizo tantos progresos en la optimización de la solución, tales como la integración del plano de control inalámbrico en sus propios componentes de conmutación para poner fin a extremo a una solución más rentable.

HP Networking tiene una fuerte fuerza de ventas global que se centra en la educación, la hotelería y los mercados públicos, pero debe ser considerada en todas las oportunidades en las cuales se necesita un cambio a nivel de acceso en su totalidad (conectividad por cable e inalámbrica). Cada organización debe considerar al menos e incluir HP en todas las evaluaciones de la red de cualquier tamaño. Se ha visto equipos HP utilizados en las pymes, a pesar de la integración de HP Networking en servidores de HP más amplios para empresas, el

almacenamiento y organización de redes (ESSN) ha incrementado su presencia en las cuentas de la empresa.

Intelligent Management Center de HP (IMC) también ofrece un "único panel de vidrio" de soluciones alámbricas e inalámbricas. La seguridad integrada IMC y la aplicación de políticas proporciona una solución flexible a través de los componentes cableados e inalámbricos.

Algunas de las características de HP son:

- Canal y servicio / soporte de ventas de HP proporcionan el alcance global y el acceso a las oportunidades que pocas empresas pueden igualar.

- El continuo enfoque de la empresa en la integración del producto de red cableada e inalámbrica ofrece una solución que proporciona una gestión personalizada, administración de la seguridad, aplicación de políticas y capacidades de acceso a invitados.

- A medida que el mercado aumenta su enfoque en servicios de aplicaciones y software, la larga historia de HP de la venta de servicios y software y servicios rentables le permitirá seguir ganando cuota de mercado de los proveedores tradicionales.

Algunas consideraciones sobre HP son las siguientes:

- Mientras que HP está impulsando agresivamente la racionalización cartera con base en su arquitectura FlexNetwork, es necesario trabajar para integrar los productos de red de 3Com en una familia de productos más agresiva y consolidada.

- La base de clientes 3Com están sin soporte desde que HP adquirió la compañía, una empresa podría ser obligada a cambiar toda su infraestructura debido a esta falta de soporte.

6.2.4. Avaya

Avaya continúa la presión para ofrecer soluciones de red de extremo a extremo, no solo por sus clientes, sino también internamente, ya que aprovecha la fuerza de su presencia global basándose en su fuerte UC (*suite* de comunicaciones unificadas) y las carteras de productos de redes. La compañía continúa con los mensajes de apalancamiento de soluciones móviles en la nube y de colaboración.

Avaya es un proveedor global, aunque los EE.UU. y EMEA son las geografías más fuertes y se alinean con un fuerte programa de canal de Avaya Connectglobal que vende el 90 % de los productos de la compañía. Con más de 450 nuevos socios a nivel mundial en 2011 y un programa de capacitación actualizada, Avaya se centra en la salud, servicios financieros, la educación y los mercados del gobierno para ofrecer soluciones de extremo a extremo. Avaya debe ser considerada para cualquier requerimiento de capa de acceso.

Avaya ofrece *switches* para redes cableadas como: el ERS 2000, ERS 3000, ERS 4000 y ERS 5000 para campus oportunidades borde de la red. También ofrece una solución WLAN combinado con su identidad Motores de autenticación de red y la *suite* de autorización, que proporciona la aplicación de la política, el acceso de invitados y acceso a la red.

- Fortalezas:

- Virtual Enterprise Network Architecture (VENA) ofrece una estrategia para redes cableadas e inalámbricas de un acceso único para las empresas que buscan una solución de capa de acceso con un juego fuerte de seguridad.
- El patrimonio de Avaya con las comunicaciones de voz significa que es a nivel de calidad de (QoS), el rendimiento del servicio, lo cual es importante para los datos y aplicaciones de vídeo.

- Avaya soporta ubicación del cliente en tiempo real el seguimiento.

- Avaya soporta una fuerte cartera de *switches* ethernet apilables, con introducciones recientes, como los productos de la serie ERS 4800 para armarios de cableado de la empresa, y la serie ERS 3500 para pymes y sucursales.

- Precauciones:

  - La gestión de la red unificada es un importante criterio de evaluación. Componentes inalámbricos deben ser administrados por Avaya Configuración y Orquestación Manager (COM) para la continuidad de una solución de extremo a extremo.

  - Grandes bases de *switches* para redes cableadas instaladas han disminuido en los últimos tres años, y no se suele ver en ternas RFP en los EE.UU. y EMEA.

6.2.5. Enterasys Networks

Enterasys Networks cuenta con un amplio portafolio de redes, y sigue creciendo su negocio de red cableada e inalámbrica, con una historia de la creación de redes de última generación que combina los accesos alámbrico e inalámbrica. El equipo de *marketing* de la compañía sigue siendo agresivo en cuanto al mercado, y en la valoración de soluciones de extremo a extremo para los clientes de los mercados verticales objetivo.

Enterasys ha luchado por establecer una marca fuerte, y aunque solo se ve la empresa en determinadas zonas geográficas, continúa ampliando su canal, que proporciona el 96 % de los ingresos totales de la compañía. Los mercados de destino incluyen cinco principales industrias verticales: la educación superior, K-12, salud, manufactura y gobierno (federal, estatal y local). Enterasys sigue siendo una opción apropiada para las empresas con productos de redes de datos, o que están dentro de sus mercados de destino. La compañía también es una buena opción para redes "*greenfield*" con un requisito para la integración de redes cableadas y redes WLAN.

- Fortalezas:

  Enterasys Networks es uno de los pocos proveedores que pueden ofrecer en una proposición de valor integrada para redes cableadas e inalámbricas, con la observación de políticas de seguridad interior, en particular WIDS, aplicaciones de acceso a datos de clientes a través de cable / wireless / voz / productos, y el aprovisionamiento de un solo punto para voz, datos, cable y escenarios inalámbricos.

  El proveedor ha continuado su fuerte presencia en los principales mercados de Europa Occidental, y en los mercados verticales de la salud y hospitales.

- Precauciones:

    - A pesar de la fortaleza de los productos y una mayor presencia en el canal, cuando se habla de Enterasys con los clientes de Gartner, pocos fuera de los mercados principales del vendedor, como la sanidad o clientes de redes de datos, son conscientes o conocen a fondo sus soluciones.

    - El valor de servicios de red inalámbrica y cableada integrados, como el acceso para invitados y la redundancia, es necesario comunicarlo mejor a los clientes, o salen como elementos de línea, ya que son con otros proveedores los que se pocisionan, y no se ve a Enterasys sobre ternas de vendedores cuando esta funcionalidad es requerida.

    - A pesar de que Enterasys ha virtualizado su aplicación en el controlador de nubes públicas y privadas y ha fijado el precio, agresivamente sus puntos de acceso para la conectividad inalámbrica, las empresas deben evaluar su funcionalidad de extremo a extremo y el coste total de la conectividad por cable e inalámbrica.

6.3. Presupuesto para implementación de una red segura basada en políticas

Un presupuesto puede variar en su precio por varias razones, no es lo mismo un presupuesto para una red completamente nueva, a una red en la que solo se modificaran ciertos componentes. Así también, no es lo mismo un presupuesto para una pyme que para una empresa grande. Debe tomarse en cuenta también el crecimiento que puede llegar a tener una empresa y la escalabilidad, ya que el número de usuarios podría duplicarse en 3 años y para una empresa una inversión de capital bastante alta debería suplir las necesidades a largo plazo.

Con base en estos parámetros se han hecho dos presupuestos diferentes, de acuerdo a diferentes necesidades. Se utilizó un presupuesto basado en Enterasys Networks ya que es la única empresa del mercado que puede asignar políticas con base en autenticación.

- Presupuesto para una pyme y requerimientos:

    - Empresa con 100 empleados.
    - Red completamente nueva.
    - Se contempla VoIP.
    - Se necesita que los usuarios tengan acceso a ciertos servicios en estación de trabajo.
    - No se utilizará autenticación para que los usuarios puedan ingresar a la red.

- Proceso de dimensionamiento:

Se sabe que son 100 usuarios por lo que para la capa de acceso se contemplarán 4 *switches* de 48 puertos, y dos *switches* de 24 puertos para el área de distribución/core, en el dimensionamiento se combinaron las capas de

core y distribución por el tamaño de la empresa. Como se debe tomar en cuenta que la red utilizará VoIP se contempla PoE (Power over Ethernet) en los *switches* de acceso, con esto los teléfonos IP podrán conectarse sin incovenientes.

Se necesita un Policy Manager para la configuración de políticas estáticas en el *switch.* Por lo que se cotiza el software NMS (Network Management Suite) con el que se crearán las distintas políticas de seguridad.

Este esquema de red utiliza redundancia total en caso de fallas, en caso que no se requiriera redundancia el presupuesto sería la mitad del propuesto.

Tabla I. **Presupuesto para una pyme**

Equipo	Descripción	Precio Unitario	Cantidad Necesaria	Total
B5G124-48P2	10/100/1000 L2/L3 PoE Switch capaz de aplicar políticas	$2 757,00	4	$ 11 028,00
C5G124-24	10/100/1000 L2/L3 Switch 10 GB Stacking con políticas	$2 817,00	2	$ 5 634,00
NMS-10	Consola de administración de políticas	$5 000,00	1	$ 5 000,00
				$ 21 662,00

Fuente: elaboración propia.

- Presupuesto para una empresa grande y requerimientos

    - Empresa con 4 500 empleados.
    - 4 sucursales y 50 agencias departamentales.
    - Se necesita que los usuarios tengan acceso a ciertos servicios desde su estación de manera dinámica con autenticación.
    - Sin un usuario se cambia de lugar sin importar la agencia o sucursal, cuando este se conecte debe tener acceso a los mismos servicios.
    - La integración de la red no es completamente nueva, solo se necesitan equipos de acceso. En 30 agencias los equipos de acceso no se modificarán, sin embargo se necesita las mismas funcionalidades para estos usuarios. Estas 30 agencias representan el 60 % de los empleados.

    - Se necesita que la infraestructura de red soporte voz y video sobre IP.

    - La nueva infraestructura de red debe soportar QoS a nivel de IEEE802.1p o DSCP y ser compatible con los equipos de *Core* y Distribución ya existentes.

- Proceso de dimensionamiento:

Ya que se necesita una infraestructura de acceso nueva para 1 800 usuarios se debe contemplar el doble de crecimiento en dos años, con esto se tiene un dimensionamiento de 70 *switches* de acceso para estos usuarios. Los restantes 2 700 son usuarios que ya se encuentran en una infraestructura de acceso creada, pero necesitan las mismas características que los usuarios que tendrán nueva infraestructura de acceso. Para esto se utilizan *switches* de la serie S con capacidad de utilizar PWA (Port web authentication), el cual permitirá autenticar hasta 9 000 dispositivos diferentes en cualquier puerto del *chassis*.

Se necesita también el software de administración de red NMS con el cual se configuraran las políticas y la calidad de servicio para los paquetes.

Este esquema es totalmente redundante en caso se requiriera solo la necesidad actual de la empresa este reduciría su costo en un 30 %, lo cual no es recomendado por razones de escalabilidad.

Tabla II. **Presupuesto para una empresa grande**

Equipo	Descripción	Precio Unitario	Cantidad Necesaria	Total
B5G124-48	10/100/1000 L2/L3Switch 4 GB Stacking con políticas	$2 757,00	70	$192 990,00
S8-CHASSIS	Chassis con 8 ranuras para tarjetas 10/100/1000 y 10GB	$11 997,00	1	$11 997,00
SOT1206-0112	Tarjeta con 12 puertos 10/100/1000 y dos puertos 10GB	$2 697,00	8	$21 576,00
NMS-100	Consola de administración para 100 dispositivos de red	$30 000,00	1	$30 000,00
				$256 563,00

Fuente: elaboración propia.

CONCLUSIONES

1. La tecnología de seguridad en redes que se enfoca a listas de control de acceso y redes virtuales de área local, ya no es suficiente. Actualmente se necesitan mecanismos mucho más granulares debido al crecimiento de las amenazas y vulnerabilidades.

2. La administración de seguridad en la capa de acceso (puertos físicos o acceso inalámbrico) debe ser fácil de administrar hoy en día. Las interfaces gráficas de usuario son mucho más amigables y adaptables para los administradores de red.

3. Una administración de CLI debe existir para tareas específicas, sin embargo, para términos de seguridad este tipo de interfaz es muy lenta y poco adaptable a los cambios de una empresa o negocio.

4. Es necesario contar con BPDU Guard para poder mitigar ataques del protocolo Spanning Tree, de lo contrario cualquier dispositivo no autorizado podía convertirse en un puente raíz y gobernar el estado de puertos a su disposición.

5. Las redes virtuales de área local o VLAN, estas fueron creadas para la segmentación de dominio de *broadcast,* mejorar el rendimiento de dispositivos y no para dar seguridad en la red.

6. Utilizar únicamente VLAN como seguridad incurre en un gran riesgo para la red de una empresa, deben tomarse medidas más estrictas, como el bloqueo de protocolos.

7. Los usuarios dentro de una VLAN de cuarentena pueden estar en ella por diferentes razones y pueden causarse daño entre ellos, la seguridad en la red de una empresa debe ser entre VLAN y dentro de ellas.

8. Con políticas de seguridad dinámicas asignadas a los diferentes *hosts*, se mitigan riesgos entre usuarios pertenecientes a una VLAN de cuarentena, ya que el bloqueo es por puerto y no por segmento de red.

9. QoS puede asignarse por medio de políticas de seguridad basadas en autenticación, así el tráfico es priorizado desde que entra a la red, reduciendo latencia, *jitter* y retrasos en paquetes cuando no son priorizados.

10. La aplicación de políticas de seguridad y asignación QoS dinámicamente permite que las tareas de seguridad sean automatizadas y requieran menos intervención de administradores de red. Si una política es configurada de manera correcta pocas veces se necesitará revisarla o en su defecto cambiarla.

11. Asegurar la disponibilidad de la red en un futuro en cuanto a protocolos y estándares, es un parámetro que las empresas deben tomar en cuenta para no invertir en productos poco escalables y adaptables. Asegurar este parámetro beneficia a las empresas disminuyendo el CAPEX y OPEX.

12. Invertir en automatización, estándares abiertos e interoperabilidad entre diferentes dispositivos reduce el ROI y TCO hasta en un 30 %. Esto hace que las empresas no gasten en soluciones sobredimensionadas y con capacidades que no son necesarias.

13. Una red no es 100 % segura a pesar de todos los métodos que se utilicen y se necesitan varias soluciones para poder mitigar la mayoría de ataques. Se necesita una combinación de equipos como NAC, IPS/IDS, concentradores de VPN, *firewalls*, autenticación y políticas para reducir la mayoría de riesgos.

14. Todos los dispositivos deben actualizarse cada cierto tiempo en hardware y software, la falta de actualizaciones puede provocar vulnerabilidades mucho más altas y ataques de red, que pueden repercutir en grandes pérdidas de información, capital o incluso llevar a la quiebra a una organización.

RECOMENDACIONES

1. Cuando se requiera una implementación de red nueva por características adicionales que no se tienen, debe validarse la compatibilidad de protocolos y estándares entre los equipos actuales y nuevos.

2. Una migración hacia una red con características nuevas debe realizarse poco a poco, realizar un cronograma con fases para la migración. Al proponer una migración controlada se minimizan los riesgos y se asegura la disponibilidad.

3. Cuando se hace una propuesta deben evaluarse diferentes proveedores, ya que un tipo de solución puede ser óptimo para una empresa, sin embargo, puede ser poco funcional para otro tipo de empresa.

4. Tomar en cuenta TCO, CAPEX y OPEX, estos son parámetros importantes que permiten diferenciar y escoger soluciones que no estén sobredimensionadas.

5. Debe buscarse unificar la red en todos los sentidos desde un inicio en una propuesta. Esto dará como resultado soluciones completamente integrales desde dispositivos finales hasta intermediarios.

6. Administradores de red y técnicos deben realizar auditorías programadas para validar la disponibilidad y seguridad de la red, mitigar los riesgos es una tarea que debe actualizarse día a día.

7. Deben tomarse en cuenta las garantías con las que cuentan los equipos, las garantías de por vida tienen prioridad sobre las limitadas, así también si las garantías cubren remplazo de partes.

8. Visibilidad, control y automatización son las tres características en la que los proveedores de seguridad y redes deben enfocarse, la mayoría de servicios se utilizarán en la nube y una propuesta de infraestructura de red sin estas características será obsoleta para los mismos.

BIBLIOGRAFÍA

1. BREACH, Ralph. *Soca Associate Siemens open communication*: *study guide*. Alemania: Siemens, 2010. 200 p.

2. DRYBURGH, Lee; HEWETT, Jeff. *Signaling System No. 7 (SS//C7) Protocol Architectural, and Services: a complete practical guide to the world´s most popular signaling system, including Sigtran, GSM-MAP, and Intelligent Networks. Indianapolis.* United States*: CISCO Press*, 2005. 505 p.

3. ENGEBRETSON, Patrick. *The basics of hacking and penetration testing ethical hacking and penetration testing made easy*. Amsterdam: Elsevier, Syngress, 2011. 178 p.

4. GEIER, Jim. *Implementing 802.1X Security solutions for wired and wireless networks*. Canada: Wiley, 2008. 356 p.

5. HAEDER, A. Adam; et al. *LPI Linux certification in a nutshell*. Beijing: O´Reilly, 2010. 522 p.

6. HOUSLEY, Robert. *Protocol registries*. [en línea] <http://www.iana.org/protocols> [Consulta: 1 de febrero de 2014].

7. LAMMLE, Todd. *CCNA CISCO Certified Network Associate: study guide*. Canada: Sybex, 2011. 803 p.

8. MARK, Lewis. *Enterasys networks: study guide*. USA: Enterasys Networks, 2001. 150 p.

9. PERPINAN, Antonio. *Administración de redes GNU/Linux: guía de estudio hacia una capacitación segura*. Santo Domingo: Fundación Código Libre Dominicano, 2004. 241 p.

10. ROSENBERG, Joseph. *SIP: Session Initiation Protocol*. [en línea] <http://www.ietf.org/rfc/rfc3261.txt> [Consulta: 4 de febrero de 2014].

11. WATKINS, Michael; WALLACE, Kevin. *CCNA Security: Official exam certification guide.* Indianapolis, United States: CISCO Press, 2008. 672 p.