Capítulo 3

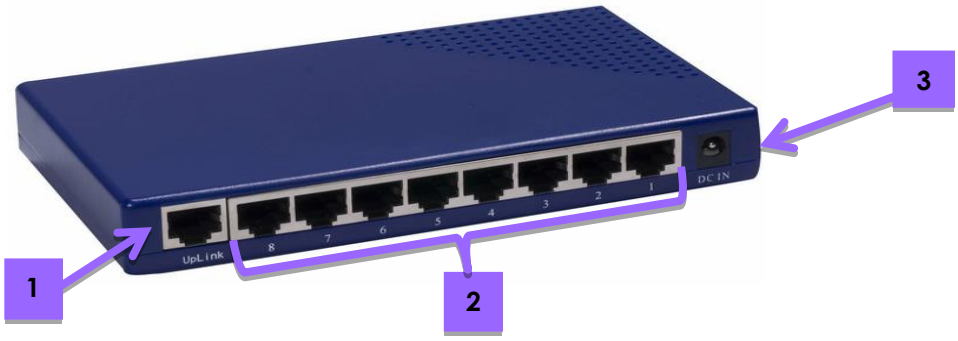
Retos y Habilidades

3.1 Estructura física de los dispositivos que interconectan las redes

Los dispositivos que conforman una red local tienen una función específica, por lo que se requiere identificar cada uno de ellos y conocerlos con detalle tanto en su estructura lógica y física. En los siguientes temas se explicará de forma gráfica la estructura general que tiene cada uno de los dispositivos, así como la función que realiza cada uno de los módulos que lo componen.

Hub

Un Hub es un dispositivo que funciona en la capa física del modelo OSI, Este dispositivo es considerado un amplificador de señales o repetidor, el cual reenvía la información que llega a uno de los puertos y la retransmite a cada uno de los dispositivos que se encuentra conectado a él. El ancho de banda total disponible en el Hub se reparte en función de las estaciones conectadas. En la Figura 3.1 se muestra la estructura física del Hub.



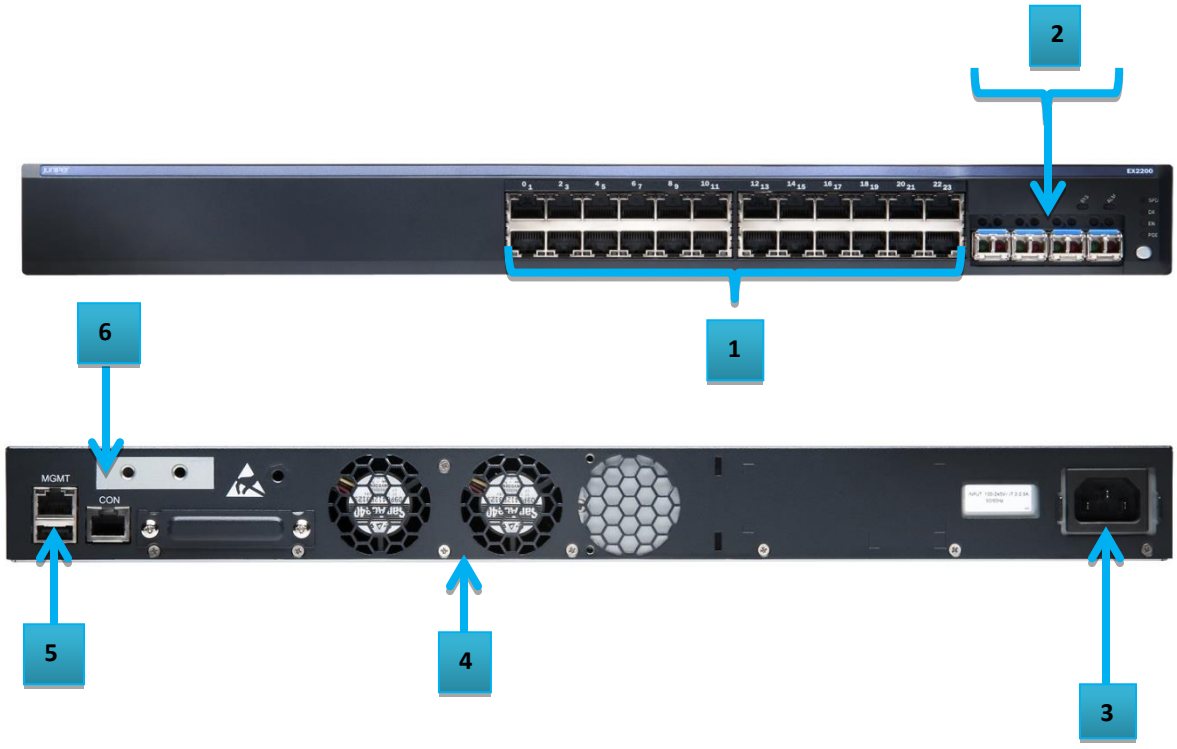
Número	Componente	Descripción
1	Puerto UpLink	Es el puerto que permite interconectar Hubs entre sí mediante un cable Ethernet
2	Puerto Ethernet	Son los puertos en donde se conectan los dispositivos finales a los que se retrasmitirán los datos. Todos los puertos tienen la capacidad de enviar y recibir la información.
3	Conector AC	Es el utilizado por el cable eléctrico que sirve para alimentar con corriente el dispositivo.

Figura 3.1 - Componentes físicos del Hub

Cabe mencionar que este tipo de dispositivos no son administrables, debido a sus características de funcionamiento como se vio en el capítulo anterior, motivo por el cual se ha vuelto obsoleto.

Switch

Al principio este dispositivo fue diseñado para trabajar en la capa 2 del modelo OSI para mitigar los problemas que el Hub ocasionaba con su uso. En la actualidad existen tres tipos de Switch los cuales operan en las capas 2, 3 y 4 del modelo OSI (capítulo 2). Aunque su funcionamiento lógico es distinto su estructura física es la misma. En la Figura 3.2 se muestran las partes que componen un Switch.



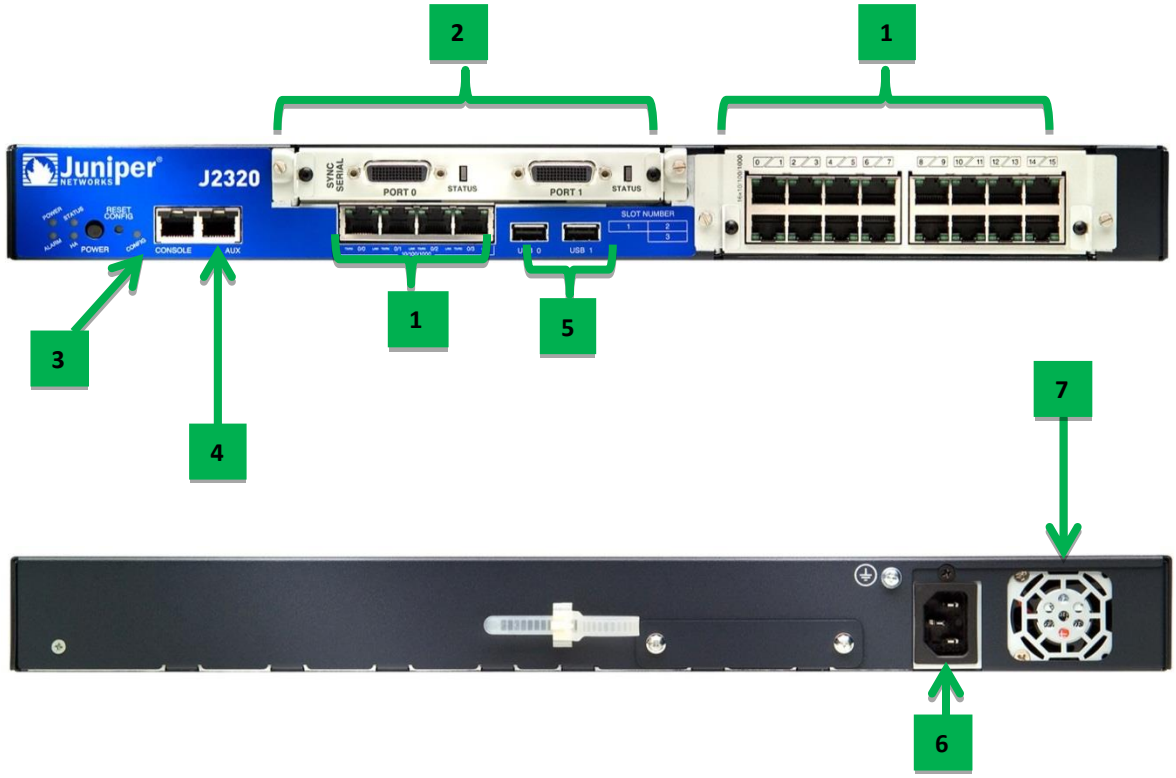
Número	Componente	Descripción
1	Puerto Ethernet	Son los puertos en donde irán conectados aquellos dispositivos que conforman la red local.
2	Puerto de Fibra Óptica	Son los puertos utilizados para brindar mayor velocidad de transferencia.
3	Conector AC	Es el utilizado por el cable eléctrico que sirve para alimentar con corriente el dispositivo.
4	Ventiladores	Son los encargados de regular la temperatura del dispositivo.
5	Puerto de administración	Es el puerto utilizado para llevar a cabo la administración y configuración del equipo que está incorporado a la red.
6	Puerto consola	Es el que proporciona ingresar y administrar al equipo sin la necesidad de estar dentro de la red, esto permite una conexión directa con el equipo.

Figura 3.2 - Componentes físicos del Switch

Existen dos tipos de Switch: los administrados y no administrados, los no administrados son utilizados en redes pequeñas como una casa, un café Internet, entre otras, ya que no es necesario configuraciones previas para su funcionamiento. Los Switches administrados son utilizados en grandes organizaciones ya que el tipo de configuración que se puede realizar en estos permite que la red trabaje de una mejor forma, una de las principales configuración que se llevan a cabo en estos dispositivos es la creación de VLANs.

Router

Es un dispositivo que trabaja en la capa 3 del modelo OSI, su función principal es el enrutamiento de paquetes a través de redes locales o redes que se encuentran en zonas geográficas distintas como se estudió en el capítulo 2. Existen distintos modelos de Routers esto es dependiendo del fabricante, sin embargo, todos tiene en común los componentes que se muestra en la Figura 3.3.



Número	Componente	Descripción
1	Puerto Ethernet	Son los puertos en donde irán conectados aquellos dispositivos que conforman la red local.
2	Puerto Serial	Son los puertos utilizados para conectar las redes WAN
3	Puerto consola	Es el que proporciona ingresar y administrar al equipo sin la necesidad de estar dentro de la red, esto permite una conexión directa con el equipo.
4	Puerto AUX	Este puerto puede actuar como un puerto de respaldo al puerto consola aunque originalmente está diseñado para conectarse al dispositivo utilizando una conexión dial-up.
5	Puerto USB	Su función es proveer de carga eléctrica a dispositivos con este tipo de entrada.
6	Conector AC	Es el utilizado por el cable eléctrico que sirve para alimentar con corriente el dispositivo.
7	Ventiladores	Son los encargados de regular la temperatura del dispositivo.

Figura 3.3 - Componentes físicos del Router

Access Point

Este dispositivo opera en la capa 2 del modelo OSI, su funcionamiento consiste en extender la red local cableada a lugares donde la red Ethernet no puede llegar, este dispositivo trabaja mediante sistemas de radio frecuencia y se encarga de recibir y transmitir la información generada por dispositivos inalámbricos hacia su destino final. Los principales componentes de este equipo son 4: Las antenas, el puerto Ethernet, el Puerto consola o de administración y el cable de alimentación, los cuales se muestran en la Figura 3.4.

Número	Componente	Descripción
1	Antenas	Están diseñadas para emitir o recibir las ondas electromagnéticas hacía el espacio libre.
2	Conector AC	Es el utilizado por el cable eléctrico que sirve para alimentar con corriente el dispositivo.
3	Puerto Ethernet	Son los puertos en donde irán conectados aquellos dispositivos que conforman la red local.
4	Puerto consola	Es el que proporciona ingresar y administrar al equipo sin la necesidad de estar dentro de la red, esto permite una conexión directa con el equipo.

Figura 3.4 - Componentes físicos del Access Point

3.2 Tipos de servidores

Un servidor es una computadora que cumple con características especiales de Hardware y Software distintas a una computadora de escritorio, por lo regular éste tiene gran cantidad de almacenamiento en disco duro, memoria RAM de gran capacidad, procesadores sumamente rápidos y un sistema operativo especial para este tipo de equipos.

En una organización por lo regular existen distintos tipos de servidores, cada uno dedicado a una tarea en específico, a continuación se detallan algunos de los servidores más utilizados:

- **Servidor Web**

Se encarga de alojar sitios Web y aplicaciones, las cuales son consultadas por el cliente utilizando un navegador que se comunica con el servidor utilizando los protocolos HTTP Y HTTPS. Éste se ejecuta continuamente en el servidor, manteniéndose a la espera de peticiones por parte de un cliente, cuando éste recibe una petición responde enviando una página Web la cual está escrita en lenguaje HTML. Además de transferir código HTML, el servidor puede entregar aplicaciones Web, éstas son fragmentos de código que se ejecuta cuando se realizan ciertas peticiones o respuestas HTTP.

- **Servidor de Impresión**

Es un concentrador, que conecta una o varias impresoras a la red, para que cualquier dispositivo que tenga la posibilidad de imprimir, ingrese a este y realice la impresión sin depender de otra computadora. Existen distintos software que además de servidor, ayudar a la administración de la impresión, ya sea proporcionando permisos a cierto grupo de usuarios, hasta la administración de los servicios de impresión.

Los servidores de impresión por lo general no poseen una gran cantidad de memoria, en vez de almacenar los trabajos de impresión en la memoria, este simplemente almacena la información del equipo que desea imprimir, así como el protocolo involucrado en la cola de impresión. Cuando la impresora deseada se encuentra disponible, el servidor permite la transmisión de los datos al puerto de la impresora correspondiente. Los servidores de impresión pueden entonces simplemente encolar e imprimir cada impresión en el orden que lo requerimientos son recibidos, sin importar el protocolo o el tamaño de la impresión.

- **Servidor FTP**

Un servidor FTP es un programa que se ejecuta en un equipo, el cual permite el intercambio de archivos entre diferentes servidores y computadoras. La aplicación más común de este tipo de servidores, es el almacenamiento de cualquier tipo de archivo. Una desventaja de utilizar este tipo de servicio es que la información trasmitida, así como las contraseñas utilizadas para autenticarse, viajan de manera no cifrada y cualquier

persona que intercepte la comunicación entre cliente y servidor podrá tener acceso a la información transmitida. Para solventar este problema, se utiliza un protocolo seguro como SFTP (Secure File Transfer Protocol), el cual tiene la capacidad cifrar la información transmitida.

Cuando un navegador no cumple con los requerimientos para ejecutar el protocolo FTP, es necesario utilizar un programa cliente, este es un programa que se instala en la máquina del usuario y permite conectarse al servidor para transferir o descargar archivos. Para utilizar el cliente es necesario saber el nombre del archivo además la ruta completa donde se encuentra. Algunos clientes de FTP básicos vienen integrados en los S.O tales como Windows, Linux y Unix, sin embargo existen una serie de clientes con opciones añadidas y con interfaz gráfica que ayudan al usuario a la transferencia de archivos de manera fácil y amigable, sin la necesidad de interactuar con la línea de comandos.

- **Servidor de correo**

Es un software que está diseñado para el envío y recepción de correos electrónicos, está basado en protocolos como POP, POP3, IMAP Y SMTP. Cuando un correo electrónico es enviado, éste es enrutado a través de varios servidores hasta llegar al servidor de correo del destinatario, estos servidores son llamados MTA (Mail Transport Agent). En Internet los MTA se comunican entre sí utilizando el protocolo SMTP (Simple Mail Transfer Protocol), debido a esto se les conoce como servidores SMTP o servidores de correo saliente.

Una vez que el MTA del destinatario haya recibido el correo, éste lo entrega a un servidor MDA (Mail Delivery Agent), el cual tiene la función de almacenar el correo electrónico hasta que el usuario lo acepte. Existen dos protocolos utilizados para recuperar un correo de un MDA:

- **POP3** (Post Office Protocol), el cual permite a los usuarios descargar su correo electrónico mientras tiene conexión y revisarlo posteriormente incluso si no están conectados a Internet.

- **IMAP** (Internet Message Access Protocol), Permite ver únicamente los encabezados del mensaje antes de decidir si abrirlo o eliminarlo, el servidor retiene el correo hasta que se solicite su eliminación. Una de las características de este protocolo es que el usuario puede consultar su correo desde diferentes dispositivos ya que éstos se encuentran alojados en el servidor, además permite operaciones avanzadas como creación de carpetas y buzones en el servidor

Por esta razón, los servidores de correo entrante se llaman servidores POP o servidores IMAP, según el protocolo utilizado.

Para evitar que cualquiera lea los correos electrónicos de otros usuarios, el MDA está protegido por un nombre de usuario llamado registro y una contraseña. La recuperación del correo se logra a través de un programa de software llamado MUA (Mail User Agent), el cual puede ser de dos tipos.

- **Cliente de correo electrónico**: es un agente que se instala en el sistema del usuario y es utilizado para descargar el correo desde el MUA, algunos ejemplos de este son: : Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail o Lotus Notes

- **Correo electrónico**: Es aquel que utiliza una interfaz Web para interactuar con el servidor de correo MUA, algunos ejemplos de éste son: Gmail, Yahoo, Hotmail, y demás.

A continuación se muestra en la Figura 3.5 el proceso por el cual se envía un mensaje a través de los distintos servidores.

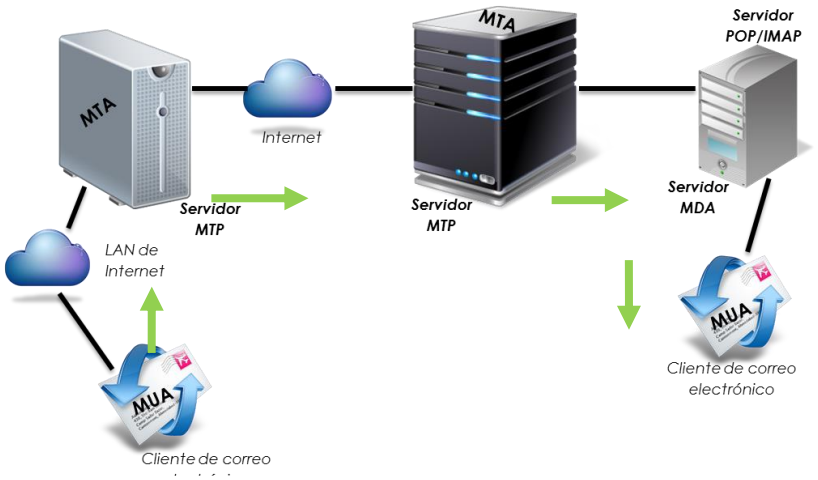


Figura 3.5 - Servidores de correo

- **Servidor de Bases de Datos**

Un servidor de bases de datos se encarga de gestionar el repositorio de datos de toda una organización manejando grandes e importantes volúmenes de datos de una manera segura, funcionando con base en la arquitectura cliente/servidor, esto es, todas las estaciones de trabajo obtienen la información de las bases de datos realizando peticiones de información al servidor a través de la red ofreciendo soluciones de forma fiable, rentable y de alto rendimiento.

Actualmente existen dos modos principales para el servicio de bases de datos:

- El primero consiste en utilizar una base de datos principal en donde se almacenan todos los datos nuevos o modificados, es conocido también como Sistema de Gestión de Bases de Datos (SGBD), cuyo objetivo es garantizar que se realicen todas las modificaciones introducidas en las bases de datos.

- El otro modo consiste en registrar las modificaciones que se hacen localmente en cada una de las bases de datos (se refieren a las copias de la base principal). Es

entonces, el sistema de gestión local el que se encarga de mantener la coherencia del conjunto de copias.

- **Servidor Proxy**

Es una aplicación que interviene entre el tráfico que se produce dentro de una red interna e Internet. Este tipo de servidor se utiliza para registrar el histórico de Internet, bloquear el acceso a una serie de sitios Web no permitidos por la empresa y además sirven para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo que brinda salida a Internet. Una de las principales ventajas de utilizar un servidor Proxy es la capacidad de ocultar la red interna de las redes exteriores, esto se hace debido a que todos los paquetes que pasan por el Proxy, aparecen en el exterior con la dirección IP de éste.

Existen también los servidores Proxy inverso que son colocados en la DMZ de la red corporativa a fin de interceptar las peticiones provenientes de una red externa dirigidas hacia un servidor interno, las analiza para asegurarse que tengan los permisos necesarios y de ser así les permite el paso. En la Figura 3.6 se muestra un escenario genérico de un servidor Proxy y Proxy Inverso.

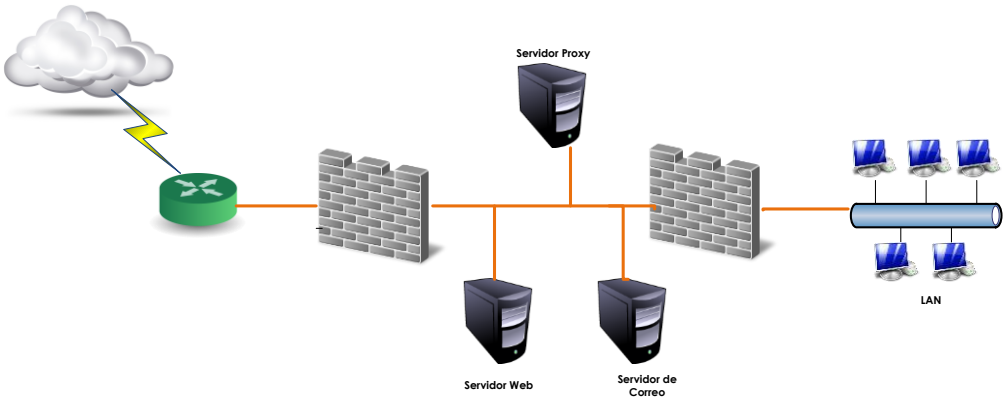


Figura 3.6 - Servidor Proxy

- **Servidor de aplicaciones**

Un servidor de este tipo es un Software que proporciona aplicaciones a los dispositivos clientes por Internet, además se utiliza el protocolo HTTP para la comunicación, este tipo de servidores se distinguen de los servidores Web por el uso extensivo del contenido dinámico y frecuente integración con base de datos. Un servidor de aplicaciones maneja la mayoría de las transacciones relacionadas con la lógica y el acceso a los datos de las aplicaciones, la ventaja principal de este servidor es la facilidad para desarrollar aplicaciones, ya que éstas no necesitan ser programadas y en cambio, son formadas a partir de módulos provistos por el mismo servidor. Un ejemplo de este tipo de servidores es donde residen aplicaciones como: la web 2.0

3.3 Redes LAN Virtuales (VLAN)

Una VLAN es una red de área local que agrupa un conjunto de dispositivos de manera lógica dentro de una red LAN, además de crear un dominio de Broadcast y otro de Multicast. Las redes virtuales son redes que agrupan usuarios y recursos de la red independientemente de su conexión física. El concepto principal de VLAN es permitir que usuarios específicos o grupos de usuarios se comuniquen como si estuvieran ubicados en el mismo segmento de red aun cuando estén localizados en segmentos distintos o ubicaciones geográficas diferentes.

La tecnología de VLAN es implementada en los dispositivos Switch, en estos equipos es donde se lleva a cabo el control inteligente de la información, por lo que es capaz de aislar el tráfico y distribuirlo de la mejor manera con el fin de aprovechar los recursos al máximo. Los principales beneficios que se obtienen al utilizar VLAN en la red son:

- **Seguridad:** Se separan los datos sensibles del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

- **Reducción de costos:** Las VLAN reducen los costos administrativos relacionados a los problemas asociados con las nuevas implementaciones en la infraestructura de red, adiciones y/o cambios de usuarios.

- **Mejor rendimiento:** La división de las redes planas de capa 2 en múltiples grupos lógicos de trabajo reduce el tráfico innecesario en la red y potencia el rendimiento.

- **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 en el 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.

- **Administración más simple:** 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.

Rangos de ID que son utilizadas para las VLAN

Cuando se crea una VLAN, ésta es identificada con un ID, el cual se clasifica de dos formas:

- **ID de rango normal:** Es utilizado en redes pequeñas y de tamaño medio, a éste se le asigna un ID que va de entre el 1-1005, cabe señalar que los ID que abarcan entre 1002 y 1005 son reservadas para VLAN Token Ring y FDDI.

- **ID de rango extendido:** Es empleada para incrementar el tamaño de la infraestructura teniendo una capacidad de usuarios lo suficientemente grande para necesitar un rango de ID extendido. Este rango comprende del 1006-4094, este tipo de ID tiene menos características que las VLAN de rango normal.

Tipos de VLAN

Las VLAN se clasifican de dos maneras ya sea por el tipo de tráfico que envían o por la función que desempeña, a continuación se mencionan las más utilizadas:

- **VLAN de datos:** Este tipo está configurada para el envío solamente de tráfico de datos.

- **VLAN predeterminada:** Todos los puertos de un Switch por default son miembros de la VLAN predeterminada, inmediatamente después del arranque de éste.

- **VLAN nativa:** A la conexión que se hace entre un Switch y un Router se le conoce como enlace troncal, cuando se lleva a cabo este tipo de conexión se le asignada una VLAN nativa, la cual tiene con función compartir de forma transparente el mismo medio físico sin interferir entre ellas las VLANs.

- **VLAN de administración:** Es una VLAN que se configura para acceder a la interfaz de administración de un Switch. Por defecto, es la VLAN 1 la dedicada a tareas de administración, salvo que se defina otra VLAN. La VLAN de administración requiere una dirección IP y una máscara de subred del mismo segmento que tiene configurado el equipo. En esta VLAN se lleva a cabo la configuración de otras VLAN.

Generación de VLAN

Actualmente existen distintas formas para efectuar la implementación de VLAN según el criterio de comunicación y el nivel en el que se lleva a cabo, a continuación se enlistan los tipos de VLAN.

- **VLAN basados en puertos:** Consiste en configurar en cada puerto del Switch la VLAN a la que va a pertenecer el dispositivo conectado a dicho puerto.

- **VLAN basadas en dirección MAC:** Se realiza la asociación de la dirección MAC de un dispositivo con la VLAN a la cual va a pertenecer el dispositivo. Este tipo de configuración ofrece mayor ventaja a diferencia que la VLAN por puerto.

- **VLAN por protocolo:** En esta configuración se crea una VLAN para cada protocolo de enrutamiento, la ventaja que se obtiene al implementar este tipo de VLAN, radica en que dependiendo del protocolo que emplee cada usuario, éste se conectará automáticamente a la VLAN correspondiente.

- **VLAN Binding:** En ella se establecen un cierto número de parámetros como dirección MAC, puerto y protocolo que deben ser cumplidos en su totalidad para que un dispositivo sea asignado a una VLAN, de lo contrario no se lleva a cabo la conexión o se envía a otra VLAN.

Implementaciones VLAN

Existen dos formas de llevar a cabo la configuración de una VLAN en un Switch, la forma estática y la dinámica, a continuación se examinan cada uno de los métodos.

- **VLAN Estática**

Se habla de VLAN estática cuando a cada puerto del Switch le es asignada una VLAN fija, este tipo de configuración se mantiene hasta que un administrador de red realiza los cambios necesarios para que el puerto cambie a otra VLAN. El implementar este tipo de VLAN tiene sus ventajas ya que es segura, fácil de configurar y ofrece un control óptimo.

- **VLAN Dinámica**

Este tipo de VLAN se caracteriza por que los puertos del Switch pueden determinar automáticamente sus funciones, basándose en la dirección MAC, el direccionamiento lógico o el tipo de protocolo de los paquetes de datos. Al momento que un dispositivo se conecta a un puerto de un Switch éste comprueba si la dirección MAC existe en una base de datos de administración de VLANs y configura dinámicamente el puerto con la configuración de la VLAN correspondiente. Una de las principales ventajas de usar este tipo de implementación es que si un usuario decide cambiar de lugar de trabajo dentro de la organización a éste se le configura automáticamente la VLAN asignada.

Enlaces troncales

Un enlace troncal proporciona una forma eficaz para distribuir la información entre VLANs, este tipo de conexión es utilizada para disminuir el número de conexiones físicas entre Switch permitiendo que el tráfico viaje a través de un mismo canal de forma independiente, esto es, un enlace troncal es un enlace punto a punto que admite varias VLAN donde agrupa múltiples enlaces virtuales en un enlace físico. Esto permite que el tráfico de varias VLAN viaje a través de un solo cable entre los Switches.

Existen dos mecanismos para enlaces troncales estándar, que son:

- Etiquetado de tramas y,
- Filtrado de tramas.

Ambas técnicas examinan la trama cuando se recibe o reenvía por el Switch, con base en el conjunto de reglas que defina el administrador, dichas tareas determinan donde va a ser enviada, filtrada o difundida la trama.

- **Filtrado de tramas**

Examina la información de cada trama, en cada Switch se desarrolla una tabla de filtrado; esto proporciona un alto nivel de control administrativo, ya que se pueden examinar muchos atributos de cada trama. En función de la tecnología que ofrece el Switch, es posible agrupar a los usuarios con base en las direcciones MAC o el tipo de protocolo de capa de red. En donde el Switch compara las tramas que filtra con las entradas de la tabla, y toma la acción oportuna con base en las entradas.

La primera forma de implementar una VLAN fue mediante el mecanismo basado en filtros donde agrupaban a los usuarios en base a una tabla del filtrado. Este modelo no escalaba bien, ya que se tenía que relacionar cada trama con un arreglo a una tabla de filtrado.

- **Etiquetado de tramas**

El etiquetado de trama asigna un ID de VLAN a cada trama. Los ID de VLAN son asignados a cada VLAN cuando se lleva a cabo la configuración del Switch. Esta técnica fue la elegida por la IEEE debido a la gran escalabilidad que ofrece. El etiquetado de trama ha ganado una gran aceptación como mecanismo normal de Trunking (enlace troncal); en comparación con el filtrado de trama, proporciona una solución más escalable al despliegue VLAN que es implementado en todo el campus. La IEEE 802.1Q establece que el etiquetado de trama coloca un identificador único en la cabecera de cada trama cuando es reenviada por el Backbone de red.

El etiquetado de trama VLAN es una solución que ha sido desarrollada para las comunicaciones conmutadas. Este mecanismo coloca un identificador único en la cabecera de cada trama cuando es reenviada por el enlace central (Backbone) de red. Este identificador es entendido y examinado por cada Switch, con antelación a las difusiones a otros Switches, Routers o dispositivos finales. Cuando la trama sale del enlace central, el Switch elimina el identificador antes de que se transmita la trama a la estación final de destino. La identificación de trama de capa 2 requiere algo de procesamiento o estructura administrativa.

3.4 Firewall

Los Firewall son dispositivos que generalmente son utilizados para evitar el acceso no autorizado de usuarios de redes externas hacia redes internas, todo el tráfico de comunicación que pasa a través de este equipo es filtrado tanto de entrada como de salida permitiendo o denegando la transferencia de información en función de una serie de criterios denominados reglas o políticas. Estos sistemas generalmente se encuentran ubicados entre la red interna e Internet, para garantizar la transferencia de la información de una manera segura, asimismo son empleados para crear diferentes zonas de seguridad con el objetivo de mejorar la seguridad en la red.

Estos dispositivos son clasificados en dos grupos:

Por su implementación	Por la capa del modelo OSI
•Firewall Hardware •Firewall Software	•Router con filtrado de paquetes •Firewall Stateful •Nueva Generación

Por su implementación

- **Firewall por Software:** este tipo de Firewall es instalado en dispositivos finales tales como laptops, computadoras de escritorio o servidores. Su objetivo es analizar el tráfico entrante o saliente de un equipo, basándose en protocolos, puertos, aplicaciones y demás. Existen distintos programas en el mercado que cumplen estas funciones además de estar integrados con alguna solución de antivirus.

- **Firewall por Hardware:** Son dispositivos dedicados que son utilizados para la seguridad perimetral, con este tipo de Firewall se protegen todos los equipos conectados a la red, un firewall basado en hardware es más fácil de gestionar y configurar que los firewall basados en Software, en ellos se permite crear VPNs, publicación de servicios, filtrado de contenido Web, análisis de paquetes, y demás.

Por la capa del modelo OSI en la que trabajan

- **Router con filtrado de paquetes** Este tipo de Firewall es utilizado en Routers que tiene integrado un módulo de filtrado basados en reglas. Este equipo es el encargado de filtrar los paquetes de datos acorde a los siguientes criterios: el protocolo utilizado, la dirección IP origen y destino, y el puerto TCP/UPD de origen y destino.

Cuando se utiliza un firewall de filtrado de paquetes, éste analiza los paquete de la siguiente manera: Cuando una aplicación crea una nueva sesión TCP con un host remoto, se establece un puerto en el host origen con el objetivo de recibir en el los paquetes provenientes del sistema remoto. De acuerdo a las especificaciones del protocolo TCP los host pueden iniciar comunicación entre los puerto 1023 - 16384, y el sistema remoto establecerá un puerto de comunicación menor al 1024. En resumen este tipo de firewall permitir el tráfico entrante en todos los puertos superiores, para permitir que los datos de retorno lleguen en los puertos inferiores al 1024. Este tipo de conexiones permiten que se abra una brecha en la seguridad ya que cualquier aplicación con la capacidad de descubrir los puertos abiertos, puede iniciar algún tipo de ataque.

Estos dispositivos tienen la ventaja de ser económicos, tener un alto nivel de desempeño y su configuración es transparente para los usuarios conectados a la red. Sin embargo, presentan desventajas como:

- Es incapaz de proteger las capas superiores del modelo OSI.
- La configuración para aplicaciones o reglas para la Web 2.0 es complicada de implementar solamente con filtros de protocolos y puertos debido a su dinamismo.
- No esconde la topología de red interna por lo que expone la red privada a la red exterior.
- Sus capacidades de auditoría, resolución de problemas y monitoreo son limitadas.
- No son capaces de soportar políticas de seguridad complejas como autenticación de usuarios y control de accesos programados en un horario en particular.

- **Firewall con inspección de estado** Este firewall es considerado como de segunda generación, y su funcionamiento es similar al de un firewall de filtrado de paquetes, solo que éste construye una tabla que contiene todas la sesiones TCP abiertas así como los puertos utilizados para recibir los datos, de esta forma no se permite el trafico entrante de ningún paquete que no corresponda con ninguna sesión o puerto. Cabe señalar que el paquete no será enviado a su destino hasta que la conexión haya sido exitosa y verificada, una vez que la conexión ha finalizado la información de la conexión contenida en la tabla es eliminada.

  La principal ventaja de implementar este tipo de firewall es que ofrece una gran velocidad en el filtrado, debido a que solo opera a nivel de la capa de sesión y por lo tanto no tiene que inspeccionar todo el paquete de datos, brindando así una mejora en el ancho de banda del firewall. Sus principales debilidades, residen en la imposibilidad de verificar protocolos de niveles superiores además de estar imposibilitado para implementar algunos servicios como el filtrado de URL.

- **Firewall de Nueva Generación (NGFW)** La evolución de las aplicaciones que existen hoy en día en la Web 2.0 ha complicado el mantener segura la red, ya que los firewall tradicionales utilizados no son capaces de resguardar y mantener un nivel adecuado de seguridad.

  Hoy en día existen un sinfín de aplicaciones y páginas Web que utilizan sofisticadas técnicas para evitar los controles de seguridad implementados en la red, estas aplicaciones utilizan diversos mecanismos como: puertos dinámicos, puertos aleatorios, transmisión de información a través de un túnel y demás.

  La solución que se utiliza actualmente para hacer frente a esta situación y cumplir con las expectativas de seguridad que una empresa necesita al manejar aplicaciones de la Web 2.0 son los llamados Firewall de Nueva Generación o Firewall 2.0 los cuales adoptan métodos efectivos ante los nuevos requerimientos de seguridad.

  Un Firewall de Nueva Generación posee las siguientes características:

  - Identifica aplicaciones independientemente de protocolo.
  - la codificación o la táctica evasiva y uso de la identidad como base para las políticas de seguridad.
  - Identifica usuarios y no direcciones IP, mediante los directorios activos de la empresa para brindar la visibilidad, creación de políticas, generación de informes e investigación forense sin importar donde se encuentre el usuario.
  - Realiza el bloqueo y detección de amenazas en tiempo real provenientes de cualquier punto de la red.
  - Simplifica la gestión de políticas mediante herramientas gráficas que hacen más sencilla la administración.
  - Garantiza que todos los usuarios conectados a la red incluidos los usuarios remotos mantengan una seguridad constante.
  - Combina Hardware y Software creados específicamente para tener un óptimo desempeño de la herramienta.

El mayor exponente y pionero en esta tecnología es el Firewall de Palo Alto Networks el cual innovó la seguridad al permitir la clasificación del tráfico basándose en la identificación exacta de la aplicación y no solo del puerto y protocolo como hasta ahora se ha manejado en los Firewall de primera y segunda generación.

3.5 Tendencias de las tecnologías de redes y seguridad

El papel de las tecnologías de la información cambia rápidamente y actualmente se va involucrando en las actividades que día con día llevan a cabo las personas. En 1984 existían solo 1,000 dispositivos conectados a Internet, en cambio se estima que para el 2015 serán 15,000 millones sometido a los sistemas de TI de todo el mundo a exigencias sin precedentes.

Debido a la incesante evolución y desarrollo en el campo de las tecnologías de la información por parte las redes de datos, aplicaciones y tecnologías que son utilizadas por los usuarios, ha surgido la necesidad de realizar el diseño y la implementación de soluciones que mantengan las redes y dispositivos seguros, disponibles, confiables y que trabajen eficientemente, utilizando las últimas tendencias en las tecnologías de la información.

Entre las herramientas que han surgido para satisfacer los requerimientos actuales de los usuarios y del área de TI, se tienen las siguientes tendencias que en el 2014 han tenido un gran auge.

Green IT (Virtualización)

Hace referencia al uso eficiente y responsable de las tecnologías que componen la infraestructura de red tomando en cuenta las afectaciones al medio ambiente, y basando sus principios en minimizar el impacto ambiental que el uso de estos dispositivos conlleva.

El concepto Green IT reúne todas las tendencias encaminadas a definir, impulsar e incentivar la eficiencia energética en la tecnología. Uno de los mecanismos que adoptan este principio es la virtualización de sistemas, la cual consiste en compartir recursos de cómputo en distintos ambientes permitiendo la separación del hardware y el software, lo cual posibilita a su vez que múltiples sistemas operativos, aplicaciones o plataformas de cómputo se ejecuten simultáneamente en un solo dispositivo.

El uso de este tipo de tecnología ayuda a:

- Administración de recursos centralizada y reducidos.
- Recuperación de los sistemas en casos de fallos.
- Minimizar las Vulnerabilidad.
- Reducción en el uso de espacio físico, al tener menos servidores físicos, los centros de IT optimizan el espacio de los data center dedicados a ellos.

Cloud Computing

La llamada computación de nube (Cloud computing) es el término que se le da a la tendencia de basar las aplicaciones en servicios alojados de forma externa, es decir, ofrece recursos informáticos remotos a las empresas, a través de Internet moldeándose a las necesidades cambiantes de ésta. Es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa sin importar el lugar donde se encuentren.

Este paradigma incorpora el software como servicio, como en la Web 2.0 y otras tendencias tecnológicas recientes, que tienen en común el que confían en Internet para satisfacer las necesidades de los usuarios, los beneficios que ofrece son los siguientes:

- Integración probada de servicios Web. La tecnología de Cloud Computing se integra con mucha mayor facilidad y rapidez con el resto de las aplicaciones empresariales, ya sean desarrolladas de manera interna o externa.
- Prestación de servicios a nivel mundial. La infraestructura de Cloud Computing proporciona mayor capacidad de adaptación, recuperación de desastres completa y reducción del impacto en tiempos de inactividad.
- Una infraestructura que es totalmente implementada en Cloud Computing no necesita instalar ningún tipo de hardware.
- Lleva a cabo una implementación más rápida y con menos riesgos. En este tipo de proyectos se empieza a trabajar muy rápidamente gracias a que las aplicaciones en tecnología de Cloud Computing están disponibles en cuestión de semanas o meses, incluso con un nivel considerable de personalización o integración.
- Contribuye al uso eficiente de la energía. Es decir, sólo utiliza la energía requerida para el funcionamiento de la infraestructura.

La tecnología Cloud Computing ofrece cualquier tipo de trabajo o acción que se realiza en un sistema informático como servicio, de esta forma tanto infraestructura, plataforma (Software) son ofrecidos como servicios por los proveedores de Cloud. Sin embargo cuando se habla de esta tecnología se debe tener en cuenta que se pueden elegir entre tres tipos de servicios y que cada uno de ellos representa una estrategia distinta a la hora de gestionar las TI. En la Figura 3.7 se muestran los tipos de servicios ofrecidos en la nube.

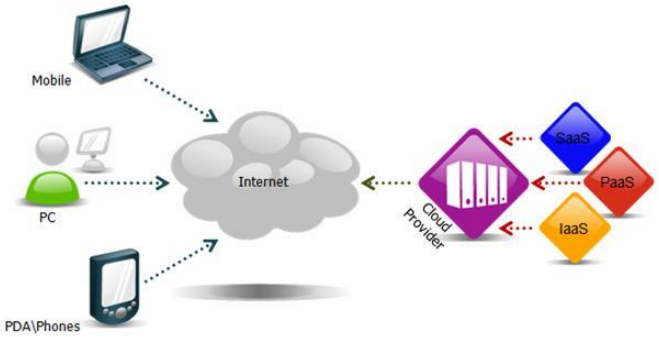


Figura 3.7 – Tipos de servicios ofrecidos por Cloud Computing

Tipos de servicios del Cloud Computing

- **SaaS**

Por sus siglas en inglés *Software As a Service* es una forma económica en la que las empresas interactúen con aplicaciones por Internet sin tener que instalar programas en sus propios dispositivos ni tampoco la obtención de licencias, el proveedor se encarga del mantenimiento, operatividad y soporte de software. Google Docs, Zoho, Office365 y Zcaler son algunos ejemplos de SaaS

Existen diversos tipos de software que se prestan para el modelo SaaS. Típicamente el software realiza una tarea simple sin tener la necesidad de interactuar con otros sistemas, lo que hace ideal para un sistema de este tipo. Algunas de las aplicaciones son:

- Gestión de relación con los clientes (CRM).
- Video Conferencia.
- Gestión de servicios de TI.
- Análisis Web.
- Gestión de contenido Web, entre otras.

SaaS provee software basado en Web, que está disponible comercialmente. Desde que el software sea gestionado desde un sitio central, los clientes pueden acceder a sus aplicaciones desde cualquier lugar donde haya conexión a Internet.

- **PaaS**

Plattform As a Service que traducido significa Plataforma Como Servicio, el cual es ofrecido por el proveedor de Cloud como una solución para el diseño, desarrollo, test, distribución y hospedaje de software y base de datos, incluye todas las facilidades al programador y pone en marcha aplicaciones todo en un sólo proceso. PaaS da servicio de integración de la base de datos, seguridad, escalabilidad, almacenaje, copias de seguridad, y demás. PaaS se encuentra en tres diferentes tipos de sistema:

- Complementos para aplicaciones: Permiten la personalización de aplicaciones SaaS existentes, por lo regular los desarrolladores y usuarios requieren pagar suscripciones para la aplicación del SaaS para este complemento.

- Ambientes Stand-Alone: Estos ambientes no incluyen dependencia de algún tipo de licenciamiento, técnicas o financieras sobre aplicaciones SaaS específicas y son utilizadas para desarrollos generales.

- Ambientes para entrega de aplicaciones únicamente: éstos soportan servicios a nivel de almacenamiento, estos no incluyen la capacidad de desarrollar, depurar y realizar pruebas.

- **IaaS**

  IaaS se refiere a Infrastructure as a Service, en este modelo el proveedor alquila infraestructura informática como servicio de modo que el costo total depende de la cantidad de recursos consumidos, esto quiere decir, que cuando la demanda aumenta más recursos son proporcionados por el proveedor, en cambio, cuando la demanda de recursos disminuye la cantidad de recursos asignados a la infraestructura se reduce apropiadamente. Los recursos físicos son administrador por el proveedor del servicio mientras que el sistema operativo y aplicaciones implementadas sobre esos componentes son administrados por el usuario.

Filtrado Web y DLP

Las tecnologías Web 2.0 tienen como característica principal ser interactivas y dinámicas, por tal motivo se han transformado en una plataforma central de aplicaciones comerciales. No obstante, el uso de la Web 2.0 implica nuevos riesgos ya que el contenido dinámico generado por los usuarios hace que las tecnologías de seguridad tradicionales, como los antivirus y filtrado de URLs resulten ineficientes, estas tecnologías tampoco pueden ofrecer control sobre información confidencial saliente.

La información es el activo más importante de toda organización. La manera en la que es creada, consultada y transmitida ha cambiado radicalmente, por esta razón es necesario adecuar la seguridad, ya que si alguna información sensible llega a filtrarse, la empresa pierde la confianza del consumidor. Este problema se vuelve más complejo debido a la rápida proliferación de dispositivos informáticos móviles, el uso extendido de dispositivos periféricos y el fácil acceso a software de intercambio de archivos; todo ello crea más oportunidades para la fuga de información. Para solucionar este tipo de problemas, existen distintas herramientas que ayudan a tener un control más preciso de las aplicaciones que existen en Internet, así como un control más estricto en la manipulación de la información que se encuentra circulando a través de la red empresarial. A continuación se presenta algunas aplicaciones existentes

- **Filtrado URL y aplicaciones:** es utilizada para realizar el bloqueo de contenido Web y aplicaciones, apoyándose de una base de datos que contiene un gran número de URL categorizadas de acuerdo al propósito de cada página y aplicación, además de analizar el contenido de cada una de ellas.

- **Prevención de pérdida de datos:** es un término de seguridad que identifica, monitorea y protege los datos que están en uso, detiene las filtraciones de datos sensibles que realiza el usuario de manera accidental o mal intencionado. Hoy en día toda organización debe ser capaz de identificar todos aquellos datos confidenciales, realizar un seguimiento de los mismo y protegerlos, ya sea que estén almacenados, utilizados o en tránsito. Esta tarea resulta más complicada debido a los crecientes factores de riesgo, como la movilidad y el uso generalizado de unidades de almacenamiento, correo electrónico y mensajería instantánea.

3.6 Sistemas de monitoreo

Hoy en día, las redes de las organizaciones se han vuelto cada vez más complejas y heterogéneas además que las exigencias de su correcta operación se han vuelve cada vez más crítica para toda organización. Las redes cada vez soportan más aplicaciones y servicios que requieren una mayor infraestructura, además que su crecimiento constante y la incorporación de nuevas tecnologías van ocasionando el degrado del desempeño de la red y el aumento en las medidas de seguridad.

Debido a la gran importancia que tienen las redes en la productividad y eficiencia de las organizaciones, es importante contar con un análisis y monitoreo de las mismas que aseguren su correcto funcionamiento. Esta acción se ha vuelto importante y de carácter proactivo para evitar problemas que puedan afectar la productividad de las empresas. Para ellos existen distintas aplicaciones que facilitan el trabajo de los administradores de la red, estas pueden ser utilizadas en un NOC (Network Operation Center), Y un SOC (Security Operation Center), a continuación se explica cada uno de estos.

NOC (Network Operation Center)

Es un sistema de operaciones centralizado que permite el monitoreo de los dispositivos que conforman una red tales como servidores, Firewall, Switch, Routers, AP, Equipos de escritorios y demás dispositivos, los cales son monitoreados para verificar su:

- funcionamiento de interfaces.
- unidades de almacenamiento.
- Disponibilidad.
- tiempo de respuesta.
- pérdidas de paquetes.
- en los enlaces se puede verificar el consumo de ancho de banda, tráfico. disponibilidad y latencia.

Las herramientas que son utilizadas para un NOC por lo regular ocupan el protocolo SNMP (Simple Network Management Protocol) que es utilizado para supervisar el rendimiento de los equipos monitoreados, así como diferentes parámetros que el equipo contenga dentro de su MIP.

El NOC es responsable de monitorear las redes en función de alarmas o condiciones que requieran atención especial para evitar impacto en el rendimiento de estas y el servicio a los usuarios finales. De ser necesario, el NOC también escalará al personal apropiado de forma que sea resuelto en el tiempo establecido. Entre los servicios que brinda un NOC están:

- Vigilancia de las operaciones de todos los enlaces.
- Vigilancia de todos los dispositivos de red.
- Vigilancia del funcionamiento de equipos de infraestructura.

- Vigilancia para el control de la seguridad de instalaciones.
- Informes inmediatos sobres las incidencias monitoreadas.
- Reportes cotidianos y efectivos sobre el estado de la red y demás elementos monitoreados.

SOC (Security Operations Center)

Es un Centro de Operaciones de Seguridad el cual tiene como objetivo garantizar y proteger a la red de cualquier amenaza que atente contra la disponibilidad de los activos que conforman la red. El SOC se encuentra conformado por especialistas altamente capacitados y certificados en las herramientas y productos más sofisticados en la industria de seguridad informática. También ayuda a prevenir el acceso no autorizado, así como el manejo de incidentes de seguridad usando diversos procesos y procedimientos establecidos por las empresas u organizaciones. El SOC ofrece un análisis continuo de riesgos y garantiza la protección contra intrusos, Los servicios que se ofrecen son:

- Análisis proactivo y administración del sistemas.
- Administración de los dispositivos y políticas de seguridad.
- Diseño e implementación de soluciones de seguridad.
- Auditoría interna.
- Presentación de informes.
- Alertas de seguridad.
- Análisis de seguridad.
- Análisis de vulnerabilidades.
- Asistencia Técnica.

3.7 Sistemas de detección y prevención de intrusos.

Los sistemas de información son parte fundamental en nuestra vida cotidiana, cada día se incrementa el número de actividades relacionadas con la transferencia y almacenamiento de información en formato electrónico, y a su vez el número de amenazas informáticas ha aumentado de forma alarmante debido a que están orientadas a obtener, destruir o negar la información que circula en este canal de comunicación.

Como consecuencia, la seguridad en la información es un aspecto al que debe prestarse mucha atención, la mayoría de las acciones se enfocan en la prevención, sin embargo no es algo que garantice totalmente que la red se encuentre segura debido a que depende de múltiples factores, los cuales abarcan desde el campo de la programación, los mecanismos y políticas de seguridad hasta llegar al usuario final. De tal modo, que la detección y el tiempo de respuesta ante intrusiones es de suma importancia.

Con base en lo descrito anteriormente se han diseñado mecanismos orientados al conocimiento de las amenazas de la red, las metodologías de los sistemas de prevención y detección de intrusos.

IDS

Los sistemas de detección de intrusos (IDS) son el proceso mediante el cual se monitorea los contenidos del flujo de información que viaja a través de la red, además de realizar la búsqueda y en determinados casos el rechazo de posibles ataques, los IDS pueden combinar hardware y software, y normalmente se instalan en los dispositivos más externos de la red. Estos sistemas están compuestos por tres elementos fundamentales básicos, los cuales se muestran en la Figura 3.8

- Una fuente de información que proporciona eventos del sistema.
- Un monitor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados.

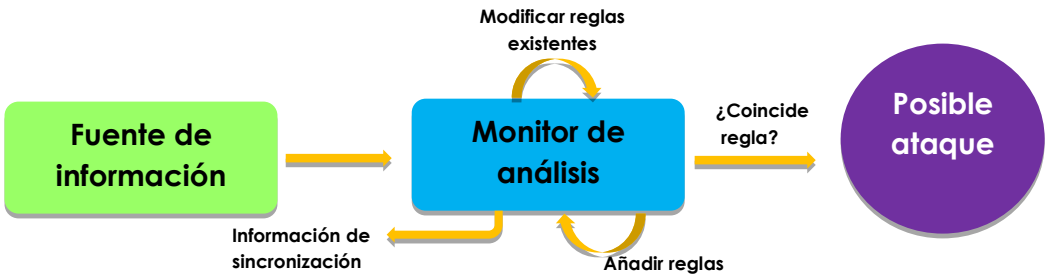


Figura 3.8 – Proceso de funcionamiento de un IDS

La detección de intrusos es la evolución de las auditorías convencionales, esto significa que examina y analiza los eventos generados por los sistemas operativos y otros elementos. La revisión de los eventos se lleva a cabo entre otros motivos para asegurarse de que no se han quebrantado las políticas de seguridad. Este tipo de mecanismo se clasifica según la actividad y el tipo de análisis que realizan.

a) Según la actividad que realizan:

- **Basados en red:** Monitorean una red, suelen ser elementos pasivos que no sobrecargan la red, como por ejemplo un analizador de protocolos, el cuan tiene como objetivo el analizar todo el tráfico que pasa por la red.

- **Basados en host:** Monitorean un host o un conjunto de ellos, los cuales permiten un control más detallado, registrando los procesos y usuarios implicados en las actividades registradas por el IDS. Consumen registros del host e incrementan el flujo de información a través de la red.

- **Basados en aplicación:** Registran la actividad de una determinada aplicación.

- **Basados en objetivos:** Este tipo difiere del resto, debido a que generan sus propios registros, utiliza funciones de cifrado para detectar posibles alteraciones de sus objetivos, y contrastan los resultados con las políticas. Este método es especialmente útil cuando se utilizan contra elementos que, por sus características, no permiten ser monitoreados de otra forma.

- **Del tipo híbrido:** Combinan dos o más actividades de las antes mencionadas. Cada vez es más frecuente encontrarse con herramientas de detección de intrusiones híbridos debido a que se tiene una mejor cobertura y posibilidades de detección.

b) Según el tipo de análisis que realizan:

- **Basadas en firmas:** De forma similar a los antivirus, estos tipos de IDS monitorean la red en busca de patrones que permitan identificar un ataque ya conocido. Estos tipos de IDS requieren que las bases de datos de firmas de ataques se encuentren constantemente actualizadas.

- **Basadas en anomalías:** En este caso, el IDS busca comportamientos anormales en la red como por ejemplo un escaneo de puertos, IP Spoofing, paquetes malformados, entre otros.

La siguiente Figura 3.9 muestra un esquema general de un IDS basado en anomalías.

Figura 3.9 - Esquema general de un IDS

Además del análisis basado en firmas y en anomalías, también existe el análisis de integridad. Este método es utilizado por las herramientas que verifican la integridad de los datos, que complementan a los IDS. Este mecanismo detecta cambios en la información u objetos, utilizando mecanismos robustos de encriptación tales como la función hash.

Otro factor que se debe considerar a la hora de llevar a cabo el monitoreo de intrusos es el tiempo de análisis de ejecución el cual puede ser:

- Por lotes o también conocido como Batch Mode, se realiza en cada intervalo de tiempo el procesamiento de una porción de los datos recibidos, enviando las posibles alarmas de intrusiones después de que se hayan suscitado.

- Análisis en tiempo real, en este mecanismo los datos son examinados en el tiempo en que son recibidos o con un retardo mínimo. La aparición de este análisis ocurre gracias a las respuestas automáticas.

IPS

Son herramientas que están diseñadas para detener las amenazas de Internet o de redes externas antes de que afecten a la red de una organización, este análisis de prevención comienza a partir de la identificación y bloqueo de patrones específicos de ataque. Un IPS (Intrusion Prevention System) o Sistema de Prevención de Intrusos ofrece una plataforma para la convergencia de seguridad global que permite minimizar la necesidad de soluciones puntuales, y brindar una mayor confiabilidad ante las amenazas

y ataques que pueden ocurrir. Esta tecnología es considerada por algunos como una extensión de los IDS, pero en realidad es otro tipo de control de acceso.

Las principales funciones de los sistemas de prevención de intrusos son:

- La identificación de actividad maliciosa.
- Llevar un registro de información sobre las actividades sospechosas.
- Detiene las amenazas antes de que tengan repercusión sin sacrificar el rendimiento de la red.
- Ofrece protección a medida que van evolucionando las amenazas.
- Realiza un informe de actividades.

Este sistema funciona por medio de módulos, los cuales establecen políticas de seguridad para proteger el equipo o la red de un ataque. Los IPS se categorizan dependiendo de la forma en la que detectan el tráfico como:

- **Basada en Firmas:** Tiene la capacidad de reconocer una determinada cadena de bytes modificada por un ataque, si esta coincide con alguna que tenga en su base de datos de firmas, entonces lanza una alerta que notifica que se ha encontrado un posible ataque. Para tener un adecuado funcionamiento se debe confirmar que las firmas estén continuamente actualizadas.

- **Basada en Políticas.** En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

- **Basada en Anomalías:** Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. En este tipo de detección el IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación.

- **Honeypot:** Es un equipo que induce a los atacantes a realizar un ataque a un dispositivo señuelo, el cual recolecta información que sirve para estudiar los métodos utilizados por el atacante e incluso identificarlo, y de esa forma reforzar las políticas de seguridad existentes.

Bibliografía

Capítulo 3 Retos y habilidades

O´Flaherty Christian.(2009). IPv6 para Todos: Guía de uso y aplicación para diferentes entornos. Buenos Aires Argentina. Capitulo Argentina de ISOC

Iñigo Jordi, Barceló José María, Cerdá Llorenc, Peig Enric, Abella Jaume. (2008). Estructura de redes de computadores. Barcelona. UOC

Santos Manuel. (2013). El switch: cómo funciona y sus principales características. 14 Febrero del 2014, de Redes Telemáticas Sitio web: http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

Iñigo Jordi, Barceló José María, Cerdá Llorenc, Peig Enric, Abella Jaume. (2008). Estructura de redes de computadores. Barcelona: UOC

Blanco Antonio, Huidobro José Manuel. (2006). Redes de área local: administración de sistemas informáticos. Madrid: Paraninfo