UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

PRAXIS DE REDES Y SEGURIDAD

TESIS

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

JIMENEZ MORENO HUMBERTO

ROJAS ARTEAGA IRMA KARINA

DIRECTOR DE TESIS

M. EN C. MA. JAQUELINA LÓPEZ BARRIENTOS

Ciudad Universitaria, Enero 2015

Praxis de Redes y Seguridad

ÍNDICE

Introducción **8**
Objetivo General 9
Objetivos Particulares 9

1. Capítulo 1.- Necesidades del campo laboral **12**
1.1. Marcas de dispositivos 15
1.2. Tipos de redes 16
1.3. Conocimientos requeridos 17
1.4. Versiones IP 19
1.5. Problemas comunes de redes 20
1.6. Herramientas de seguridad 22
1.7. Biblipgrafia Capítulo 1 23

2. Capítulo 2.- Antecedentes de Redes y Seguridad **24**
2.1. Tipos de redes 27
2.1.1. Clasificación de las redes por cobertura geográfica 27
2.1.2. Clasificación de redes por topología 35
2.2. Modelo OSI 38
2.3. Métodos de direccionamiento 41
2.3.1. IPv4 41
2.3.2. IPv6 43
2.4. Asignación de direcciones estáticas y dinámicas 45
2.5. Dispositivos que interconectan una red 47
2.6. Protocolos de enrutamiento 51
2.6.1. Protocolos de enrutamiento estático 51
2.6.2. Protocolos de enrutamiento dinámico 52
2.7. Seguridad de redes 57
2.8. Identificación de amenazas y tipos de ataques 62
2.9. Bibliografía Capítulo 2 72

3. Capítulo 3.- Retos y Habilidades **73**
3.1. Estructura física de los dispositivos que interconectan las redes 75
3.2. Tipos de servidores 79
3.3. Redes LAN Virtuales 83
3.4. Firewall 87
3.5. Tendencias de las tecnologías de redes y seguridad 90
3.6. Sistemas de monitoreo 94
3.7. Sistemas de detección y prevención de intrusos 96
3.8. Bibliografía Capítulo 3 100

4. Capítulo 4.- Diseño y desarrollo de la asignatura **101**
4.1. Laboratorio1: Configuración de dispositivos que interconectan la red 105

4.1.1. Configuración básica de Switch 105
4.1.2. Configuración básica de Router 109
4.1.3. Configuración básica de Access Point 113
4.2. Laboratorio 2: Diseño e implementación de una red 117
4.2.1. Subnetting 117
4.2.2.VLSM 121
4.2.3. Configuración de direccionamiento 125
4.3. Laboratorio 3: Configuración de redes virtuales 130
4.3.1. Configuración básica de VLANs 130
4.3.2. Configuración de enrutamiento entre VLANs 134
4.4. Laboratorio 4: Configuración de protocolos de enrutamiento 138
4.4.1.RIP 138
4.4.2.OSPF 142
4.5. Laboratorio 5: Instalación y configuración de servicios 145
4.5.1. Configuración de un servidor FTP 145
4.5.2. Configuración de un servidor Web 147
4.6. Laboratorio 6: Servicios de autenticación y administración de usuarios 163
4.6.1. Servicios de Directorio Activo 163
4.6.2. Configuración de servidor RADIUS 170
4.7. Laboratorio 7: Configuración básica de dispositivos de seguridad 174
4.7.1. Configuración básica de Firewall 174
4.7.2. Configuración y publicación de servicios 180
4.7.3. Configuración de VPNs 183
4.8. Laboratorio 8: Tendencias en la tecnología 190
4.8.1. Control de la Web 2.0 190
4.8.2. Prevención de la pérdida de la información 195
4.8.3. Servicios en la nube 200
4.9. Laboratorio 9: Detección de amenazas y análisis de vulnerabilidades 202
4.9.1. Sistemas de detección y prevención de intrusos 202
4.9.2. Análisis de vulnerabilidades 209
4.10 Laboratorio 10: Monitoreo de dispositivos y aplicaciones de red 215
4.10.1 Trazas de monitoreo de networking 215
4.10.2 Análisis de tráfico 221
4.10.3 Trazas de auditoria y monitoreo 227
4.11 Laboratorio 11: Integración de los conocimientos adquiridos 233
4.11.1 Resolución de problemas y demostración de conocimientos Redes 233
4.11.2 Resolución de problemas y demostración de conocimientos Seguridad 237
4.12 Bibliografía Capítulo 4 242

Conclusiones **243**
Anexos **245**
Anexo A 246
Anexo B 260

Glosario de términos **265**

Introducción

En la actualidad las redes de datos juegan un papel muy importante en el ámbito de las comunicaciones, ya que han ido evolucionando en aspectos como en su extensión de área geográfica, así como en la cantidad de información que hay que almacenar y distribuir a través de ellas, un claro ejemplo de cómo fue creciendo fue la primera red Arpanet, la cual consistía en enlazar un conjunto de computadoras que ayudaba a descentralizar la información con la que contaba el gobierno de los Estados Unidos, posteriormente fueron aumentando las necesidades de las redes, así como los dispositivos que la formaban, adaptándose a las nuevas tecnologías, teniendo como resultado lo que hoy conocemos como Internet.

Conforme ha pasado el tiempo las redes han ido trascendiendo en nuestra vida cotidiana en actividades como son: transacciones empresariales, de entretenimiento, un medio de comunicación, educación, etc. Para que estas actividades sean posibles las redes deben cumplir con tres características principales: deben ser confiables, seguras y estar siempre disponibles, por lo tanto se necesita contar con profesionales capaces de administrar, configurar, crear, organizar, integrar, dirigir y controlar para que tengan un buen funcionamiento y así no se vean afectadas las diversas tareas que se basan en ellas.

Uno de los principales objetivos de la Facultad de Ingeniería en su carrera de Ingeniería en Computación en el módulo de Redes y Seguridad, es formar nuevos profesionistas que tengan la capacidad de hacer dichas tareas así como resolver problemas que se susciten día con día en las redes.

Nosotros como alumnos egresados y al tener un mayor panorama de los problemas que se presentan en la vida laboral, consideramos que las dos asignaturas que se imparten de manera curricular en la carrera de Ingeniería en Computación desde el plan de estudios con revisión en el año 2005 [Redes de Datos y Administración de Redes] brindan un conocimiento elemental y teórico de cómo funciona una red y su estructura, cabe señalar que las materias antes mencionadas cuentan con un laboratorio que ofrece 2 horas por semana cada una, las cuales no son suficientes para que los estudiantes conozcan a fondo el funcionamiento de los equipos, por tal motivo se les dificultaría hacer frente a los problemas que se les presenten ya que no tendrían algún acercamiento de tipo práctico con los dispositivos (Routers, Switchs, entre otros) que conforman una red.

Con base en lo anteriormente expuesto es que nos percatamos de la imperiosa necesidad de contar por lo menos con una asignatura más en el campo de las redes que le permita a los estudiantes profundizar en el conocimiento de las redes, sus diversas problemáticas y las posibles soluciones a distintos esquemas y requerimientos de las empresas u organizaciones además de adquirir las habilidades prácticas para la solución de problemas relacionados en los diversos campos de las redes como la seguridad, diseño, y administración entre otros.

Sugerimos que es necesario contar con una asignatura práctica que ayude al egresado a solucionar problemas y a familiarizarse con los equipos, independientemente de la marca del dispositivo, dicha asignatura debe contener un temario que describa de forma práctica: qué es, su funcionamiento, mantenimiento y las configuraciones en los diferentes

equipos utilizados que conforman una red, esta asignatura debe fomentar en el alumno un razonamiento con el cual pueda decidir cómo y por qué utilizar los distintos dispositivos, protocolos, y tecnologías que hacen posible la comunicación entre redes, ya sean aplicadas a una red local o a una red de área extensa, **todo con el objetivo de cumplir con las características que debe contar una red para que ésta sea funcional, práctica, segura, estar siempre disponible, confiable, integra, rápida y teniendo un amplio criterio para determinar cuál es la mejor opción para enfrentar cualquier situación que se nos presente.** Esta materia contará con una introducción por tema con el contenido necesario para retomar los conocimientos adquiridos en las asignaturas precedentes (Redes de Datos y Administración de Redes) y así abordar el contenido que se esté tratando, profundizando en él y enfocándose a la parte práctica de problemas, propuestas y soluciones.

Objetivo General

Diseñar y desarrollar el material necesario correspondiente a una asignatura en la cual los alumnos de la carrera de Ingeniería en Computación del Módulo de Redes y Seguridad aprendan a manipular equipos y aplicaciones que permitan abordar y dar solución a los problemas típicos en el área laboral y con ello adquirir la práctica necesaria para manejar diversas herramientas, así como la manipulación de equipos de diferentes desarrolladores. El alumno obtendrá conocimientos, habilidades y actitudes, por medio de la puesta en práctica de los conocimientos que ha adquirido en las asignaturas anteriormente cursadas que involucren a las redes de datos y seguridad informática, así como lo aprendido en esta asignatura, incitando su inquietud para que sigan ampliando sus conocimientos. Todo esto con el objeto de brindarle al alumno las herramientas necesarias para que sea más competitivo en el mundo laboral.

Objetivos Particulares

- Retomar los conocimientos adquiridos en las asignaturas anteriores.
- Crear un manual teórico-práctico.
- Incitar al alumno a que sea autodidacta.
- Que el alumno desarrolle un gusto por las redes de datos y seguridad informática.
- El alumno aprenderá a manipular los dispositivos mediante la práctica desarrollando una mayor destreza.
- Que se tome en cuenta la asignatura desarrollada en futuras revisiones del plan de estudios del Módulo de Redes y Seguridad.
- Ampliar el panorama de la configuración de los equipos independientemente de la marca.
- Describir los protocolos utilizados para redes de área local alámbrica e inalámbrica (LAN y WLAN) y de área extensa (WAN y WMAN).
- Implementar seguridad en los dispositivos de redes.

Metodología de trabajo

Para saber cuáles son los conocimientos que debe poseer el egresado para hacer frente a los problemas que surgen día con día, así como ser un profesional más competitivo, además identificar los tipos de problemas a los que se enfrentan las empresas o clientes y así poder brindar un mejor servicio.

- Revisar y retomar cuáles son los antecedentes que se tienen de las asignaturas cursadas anteriormente (Redes de Datos y Administración de Redes).

- Consultar estudios realizados por organizaciones y consultorías dedicadas a las Tecnologías de Información para saber cuáles son las tendencias que actualmente se presentan en este ámbito.

    - Problemas típicos que surgen en las redes.
    - Soluciones que se han efectuado a problemas reales propuestos por los especialistas en el campo de las redes.
    - Qué servicios y soluciones ofrecen los proveedores de servicios de red, consultorías, asociaciones (algunos de ellos son: IANA, IEEE, ITU, ETSI).
    - Configuración de equipos de diferentes proveedores.
    - Nuevas tecnologías que se están aplicando a las redes.

- Determinar cuáles son los temas que ayudarán a resolver los problemas que se presentan día con día en las redes y seguridad informática, basados en la información recopilada.

- Proponer una serie de prácticas que ayuden al alumno a:

    - Poner en práctica lo que han aprendido en las asignaturas antecesoras.
    - Implementar tecnologías diversas y protocolos, los cuales ayudarán a solucionar los posibles problemas existentes en una red.

- Probar las prácticas con alumnos del módulo de Redes y Seguridad los cuales tendrán acceso a los dispositivos físicamente así como la manipulación de éstos, ya que el objetivo principal de esta materia es que el alumno pueda tener un mayor acercamiento con los dispositivos y/o herramientas de software, además de demostrar que dichas prácticas sean comprensibles y de fácil implementación.

- Diseñar y Desarrollar prácticas que permitan manipular los dispositivos, programas, aplicaciones, y demás para la configuración, y la resolución de problemas cotidiano

Capítulo 1

Necesidades del campo laboral

Dentro de la industria de las comunicaciones en México, existen diversas empresas, entidades y consultorías que se dedican a brindar servicios de administración, configuración, creación, organización, integración, soporte, diseño, dirección y control de redes de datos, así como seguridad informática, dichas organizaciones demandan personal cada vez mejor preparado para enfrentar los problemas, realizar propuestas y cumplir con las necesidades que surgen día con día en el ámbito de las Tecnologías de la Información, por lo que se vuelve fundamental contar con especialistas que dominen las distintas tecnologías que están siendo aplicadas para el desarrollo de nuevas propuestas de mejora en los sistemas ya existentes, Implementaciones de tecnología que ayuden a mejorar el desempeño de la red, resolución de problemas que aqueje a la infraestructura, así como el mantenimiento preventivo y correctivo de los elementos que conforman la red.

Para realizar el presente proyecto se efectuó un sondeo basado en distintos artículos y publicaciones de entidades de consultoría y de investigación de las tecnologías de la información a nivel internacional, entre las que destacan: Gartner, IDC, NSS Labs, InfoSec Institute e Infoblox, esta investigación proporcionó un panorama más amplio de los conocimientos, tendencias y tecnologías que son utilizadas en el campo laboral. Entre los principales puntos investigados se encuentran:

- Fabricantes líderes utilizados para la LAN en organizaciones.
- Tecnologías empleadas en redes y seguridad informática.
- Problemas a los que se enfrentan con mayor frecuencia.
- Las herramientas de seguridad que implementan.
- Las habilidades básicas que el egresado debe dominar.

Una vez concluida la investigación, se observó que existen diferentes opciones de tecnologías que pueden ser empleadas por las organizaciones para el correcto funcionamiento de su red. Esto sirvió como base para determinar las habilidades y conocimientos necesarios para que el alumno egresado de la carrera de Ingeniería en Computación en el área de Redes y Seguridad cuente con los conocimientos necesarios para que enfrente los retos que en el ámbito laboral se lleguen a presentar, a continuación se presentan los temas que ayudan a lograr los objetivos propuestos para esta tesis.

1.1 Marcas de dispositivos

La situación en el campo de las redes en el área de Tecnologías de la Información actualmente se ha ido desarrollando rápidamente, la innovación tecnológica ofrece una amplia gama de opciones de dónde elegir en diversos aspectos como son: la convergencia de redes y servicios, la reducción de precios que hace accesibles los servicios a todo tipo de empresas, tecnologías complementarias empleadas, seguridad, configuraciones, entre otros. Estos factores combinados han hecho que las telecomunicaciones sean una de las industrias más dinámicas y de mayor crecimiento en el mundo. Actualmente existen diversas compañías que ofrecen una amplia diversidad de dispositivos los cuales satisfacen las necesidades actuales y futuras de cada organización con lo que respecta a las redes LAN ya sea cableada o inalámbrica.

Una vez recopilada la información se muestra a continuación la serie de fabricantes que Gartner determinó como la tecnología de redes de datos con mayor presencia en la industria internacional y haciendo el análisis de resultados, se observa que existen fabricantes de dispositivos de red dominantes, los cuales se muestran en la Figura 1.1.

Fabricantes líderes de acuerdo a Gartner en 2014	
Cisco	**Aruba**
HP Networking	**Dell**
Extreme (Enterasys Networks)	**Huawei**
Motorola Solutions	**D-Link**
Adtran	**Juniper Networks**
Aerobie	**Alcatel-Lucent**
Ximus	**Avaya**

Figura 1.1 – Marcas de los dispositivos utilizados en las empresas para red LAN cableada e inalámbrica.

Al examinar la gráfica tenemos que Cisco, HP y Aruba son las marcas predominantes en el mercado para 2014, haciéndolo así el líder en tecnología de redes para ese año, mientras su más cercano competidor es Dell y, seguido por otros fabricantes, como son: D-Lynk, Juniper, Extreme, Avaya, entre otros. No obstante, los egresados de Ingeniería en Computación en el área de Redes y Seguridad deben tener la habilidad de manipular, configurar, mantener y dar soporte a distintos dispositivos independientemente del fabricante al que se lleguen a enfrentar.

1.2 Tipos de red

Para satisfacer sus necesidades siempre crecientes, hoy en día las organizaciones evolucionan constantemente, por lo que es imprescindible contar con una infraestructura que sustente las redes de datos y así cumplir con sus tres características primordiales: eficiencia, seguridad y disponibilidad. Existen distintas maneras de clasificar las redes, dependiendo de sus características tales como: cobertura geográfica, tipo de conexión, relación funcional, topología, grado de difusión, grado de autentificación y servicios o funciones. De acuerdo en el último informe de Gartner 2014 se dice que "*el mercado de acceso a redes locales sigue evolucionando desde dos direcciones separadas, las redes cableadas y las redes wireless, hacia una única capa de acceso unificada*" y debido a esto es necesario que los alumnos conozcan estas dos vertientes en las que se está trabajando.

Tabla 1.1- Tipos de redes por extensión geográfica

Nombre	Tipo de acceso	Alcance	Estándares*
Redes de área personal Wireless WPAN	Acceso privado	<10 metros	IEEE 802.15 - Bluetooth
Redes de área local LAN	Acceso privado	10-100 metros	IEEE 802.3 - Ethernet
Redes de área local WLAN	Acceso privado	<100 metros	IEEE 802.11 a/b/g Wi-Fi
Redes de área metropolitana MAN	Acceso público	1-10 kilómetros	IEEE 802.6 DQDB
Redes de área metropolitana WMAN	Acceso público	<5 kilómetros	IEEE 802.16 a/e WiMax
Red de área amplia WAN	Acceso público	100-1,000 kilómetros	EIA/TIA-449
Red de área amplia WWAN	Acceso público	<15 kilómetros	IEEE 802.20 GSM, 3GPP, EDGE

*Los estándares mencionados son sólo algunos ejemplos para el tipo de red.

A pesar de que existen varios tipos de redes, la red LAN es la más predomina debido a que proporciona servicios y aplicaciones a personas dentro de una estructura organizacional de propiedad privada, por ejemplo en una casa o en una gran empresa.

Sin embargo cuando una compañía o una organización tienen distintas sedes en ubicaciones separadas por grandes distancias geográficas y necesita compartir información es necesario alquilar conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN).

1.3 Conocimientos requeridos

Uno de los principales objetivos que se tiene en la industria de las redes de datos y seguridad informática es mantener la infraestructura de red actualizada, de acuerdo a los requerimientos que surjan día con día en las necesidades del negocio, una de las consultorías a nivel mundial que se dedica a estudiar el comportamiento y las tendencias que en TI se suscitan es IDC, dicha organización realizó las predicciones para el 2015 cuyo nombre del reporte publicado es "Latin America Predictions 2015", teniendo los siguientes puntos como lo más importantes los cuales se tendrán como referencia para las empresas en Latino América en los próximos años. Véase Figura 1.2.

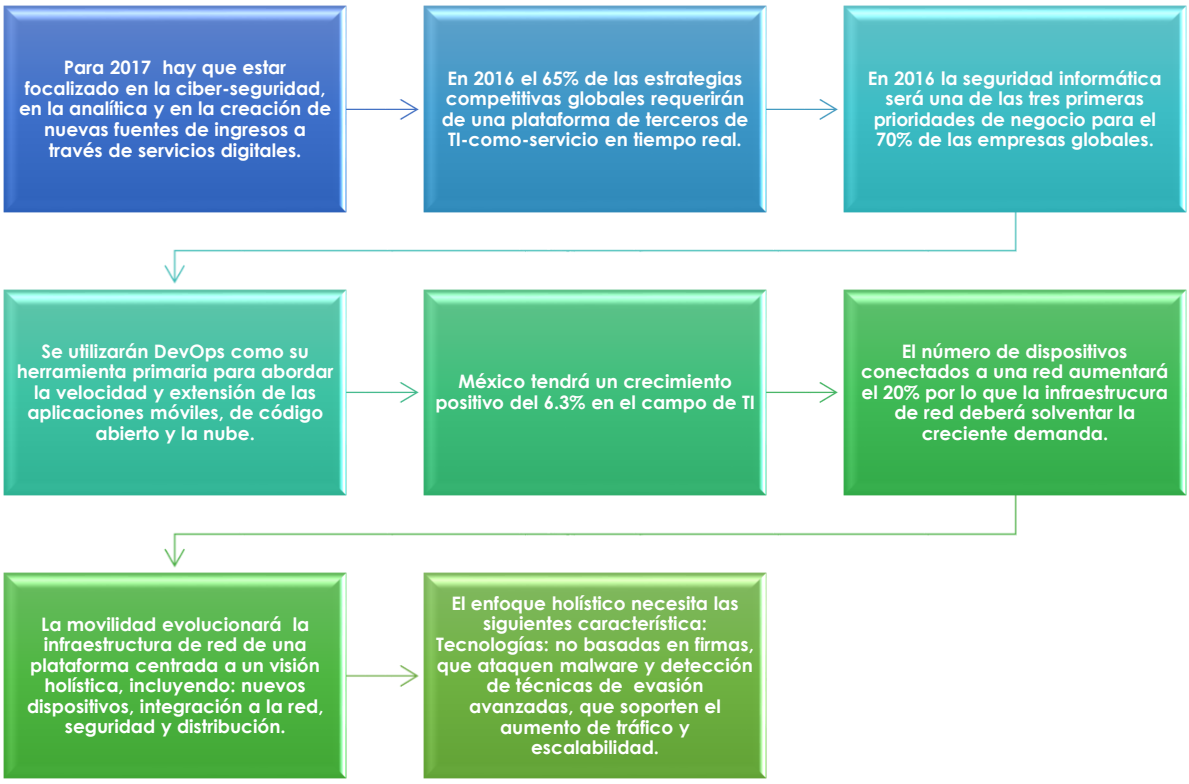


Figura 1.2 – Predicciones Latino América 2015

De acuerdo a los resultados obtenidos por IDC se observa que el egresado de la carrera de Ingeniería en Computación en el área de Redes y Seguridad, debe poseer diversos conocimientos los cuales le ayudarán a confrontar los nuevos requerimientos que en la industria se están incorporando, con base a ello, determinamos que de acuerdo a nuestra experiencia y a los informes leídos, alguno de los conocimientos que integraremos en esta propuesta de asignatura es para que el egresado practique los temas siguientes:

- Configuración de equipos que interconectan la red.
- Diseño e implementación de redes locales.
- Configuración de protocolos de enrutamiento.
- Instalación y configuración de servicios de autenticación y administración de usuarios.
- Configuración de herramientas de seguridad.
- Monitoreo de dispositivos y aplicaciones de red.
- Detección de amenazas y análisis de vulnerabilidades.

Una de las habilidades que se requiere adquirir es la configuración y manipulación de dispositivos administrables pertenecientes a una red como son Routers, Switches, Access Point, y Routers inalámbricos, principalmente. De igual forma uno de los aspectos que se vuelve relevante en las empresas es el monitoreo de red, esto se ha convertido en una labor cada vez más trascendental ya que permite visualizar el estado de los dispositivos y así tomar decisiones certeras para prevenir errores en la red.

Asimismo una parte fundamental para una empresa consiste en llevar una buena administración de su red para que ésta sea operativa, eficiente, segura, y con una planeación adecuada y debidamente documentada.

Otra de las responsabilidades a las que se enfrenta el egresado es a la administración y el mantenimiento de los servidores, ésta es una tarea de vital importancia que requiere dedicación y trabajo, debido a que en ellos se encuentra información relevante para las organizaciones y la alteración o pérdida de esto sería inexcusable.

Garantizar la integridad, confiabilidad y disponibilidad de la información que viaja a través de la red es una de las tareas más complicadas a las que se enfrentan los encargados de la seguridad, debido a que las redes se han vuelto más abiertas, extensas y ampliamente interconectadas, así, los métodos de protección deben ser cada vez más fuertes contra intrusos internos y externos, por eso el egresado debe de contar con bases sólidas para enfrentar los problemas de seguridad a los que se llegue a enfrentar.

Teniendo en cuenta las necesidades y los avances producidos en una sociedad sumamente compleja, resulta de gran importancia destacar tanto la transmisión de información, como la necesidad de que ésta llegue a destino en el momento preciso mediante el uso de las redes, por tal motivo se vuelve importante tener métodos por los cuales la información llegue a su destino a través de la mejor ruta y en el menor tiempo posible.

Cabe señalar que el objetivo de esta asignatura es proporcionarles a los alumnos las herramientas, habilidades y destrezas que le ayuden a proponer, resolver, mejorar e implementar los distintos escenarios a los que se enfrente en el campo laboral, sin embargo, los temas propuestos en esta asignatura pueden ser mejorados y actualizados con respecto a la experiencia y conocimiento de cada profesor.

1.4 Versiones IP

Para transmitir la información de una computadora a otra, es necesaria la presencia de mecanismos que se encarguen de identificar cada dirección de los dispositivos participantes en la transferencia de información a fin de que permita identificar y localizar no sólo a los participantes sino la mejor ruta que los interconecte entre sí. La dirección IP es el sistema básico de intercomunicación en la Red y el encargado de asigna esas direcciones de carácter numérico es la IANA, cabe mencionar que existen dos versiones de direcciones IP que son IPv4 e IPv6.

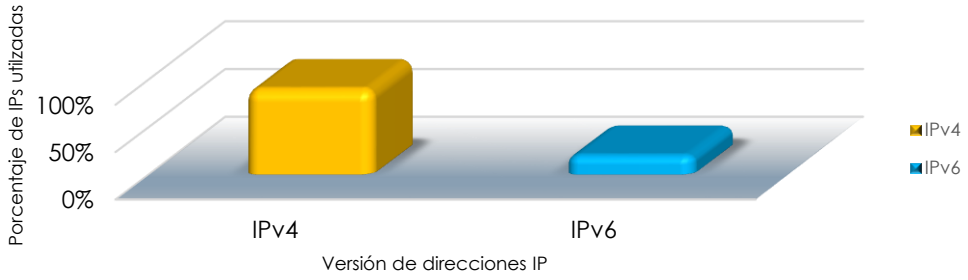


Figura 1.3 – Versiones de IPs

Como se observa en la Figura 1.3 las direcciones IPV4 son las predominantes en el campo de las redes, el problema de las direcciones IPV4 es que su rango es muy limitado debido a que esta dirección está conformada por 32 bits dando un total de 2^{32} direcciones utilizables, sin embargo, en el mes de Junio de 2014 fue anunciado que: "*Las direcciones de Internet basadas en el estándar IPv4 –un protocolo de comunicación entre computadoras– para América Latina han llegado a su fase de agotamiento, anunció el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), responsable de la asignación de recursos la región* y desplegar el protocolo IPv6 adquiere hoy más que nunca un sentido de urgencia, volviéndose inevitable e inaplazable si los proveedores de conectividad desean satisfacer la demanda de sus clientes y de nuevos usuarios. LACNIC y la comunidad de Internet han estado trabajando por años para este momento" afirmó el director de LACNIC, Raúl Echeberría." [1] .

Ahí es donde entra en juego IPv6, cuyo rango es mucho mayor, las direcciones IPv6 están compuestas por 128 bits, lo que permite generar un total de 2^{128} direcciones distintas, por lo tanto es importante que el egresado tenga conocimiento de esto y se familiarizarse con las direcciones de esta versión.

[1] *http://eleconomista.com.mx/tecnociencia/2014/06/15/las-direcciones-internet-ipv4-se-agotaron*

1.5 Problemas comunes en las redes

Configurar una red y hacer que ésta funcione correctamente puede ser una de las tareas más complicadas a las que un administrador de red se tiene que enfrentar, sin embargo no basta solo con configurar ya que a lo largo del tiempo en que la red está operando se presentarán situaciones que harán que la funcionalidad y eficiencia en las redes se vea afectada, por lo que es importante poseer una abstracción que permita resolver y detectar los diferentes conflictos que puedan surgir.

Conocer cuáles son los problemas que se presentan en la red de una organización dará la oportunidad de implementar algunas soluciones y estrategias siendo así capaces de detectar y responder a cualquier evento que se presente mientras ocurre y reaccionar ante ella.

En la investigación Infoblox publica cuáles son los problemas con mayor índice de concurrencia que se presentan en la red de una organización, éstos se exponen en la Figura 1.4

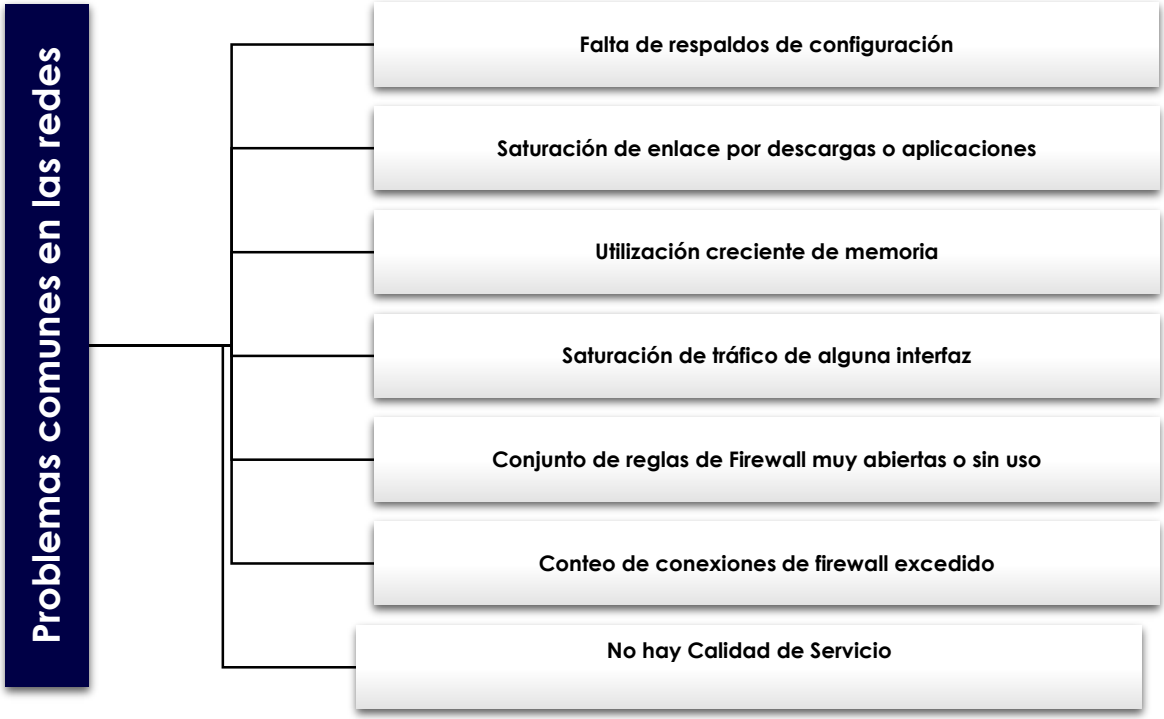


Figura 1.4 – Problemas comunes en las redes

- **Falta de respaldos de configuración:** Éste es uno de los principales problemas que se presentan en una red, debido a que si no se cuentan con respaldos periódicos, en una situación de contingencia puede ser determinante el tiempo de resolución de cualquier incidente.

- **Saturación de enlace por descargas o aplicaciones:** La saturación del enlace de Internet por uso indebido de este recurso impacta a la organización debido a que el corporativo debe brindar mayor velocidad para su correcto funcionamiento, el cual origina aumento de costos no previstos.

- **Utilización creciente de memoria:** Un error en el sistema operativo del dispositivo está consumiendo más memoria, haciendo que cuando el equipo no tenga más memoria libre, el dispositivo se reiniciará interrumpiendo todas aquellas aplicaciones que transitan por el equipo.

- **Congestión de tráfico de alguna interfaz:** El rendimiento de alguna aplicación impredecible con impacto en la productividad del usuario.

- **Conjunto de reglas de firewall muy abiertas o sin uso:** Hace que el rendimiento de un firewall se sea deficiente. Al tener reglas de seguridad muy abiertas o sin utilizar hacen que se creen posibles problemas de seguridad.

- **Conteo de conexiones de firewalll excedido:** Provoca que las nuevas conexiones a través del firewall fallen, las aplicaciones de negocio exhiben falta intermitente a cargas de firewall altas, las VPNs comienzan a fallar.

- **No hay QoS:** No se le da prioridad a aplicaciones de negocio importantes, lo que produce un rendimiento impredecible o deficiente durante horas e congestión de alguna interfaz.

1.6 Herramientas de seguridad

Garantizar que los activos existentes en la red de una empresa mantengan la confidencialidad, integridad, disponibilidad, autenticación, control de acceso, no repudio son los objetivos primordiales de la seguridad.

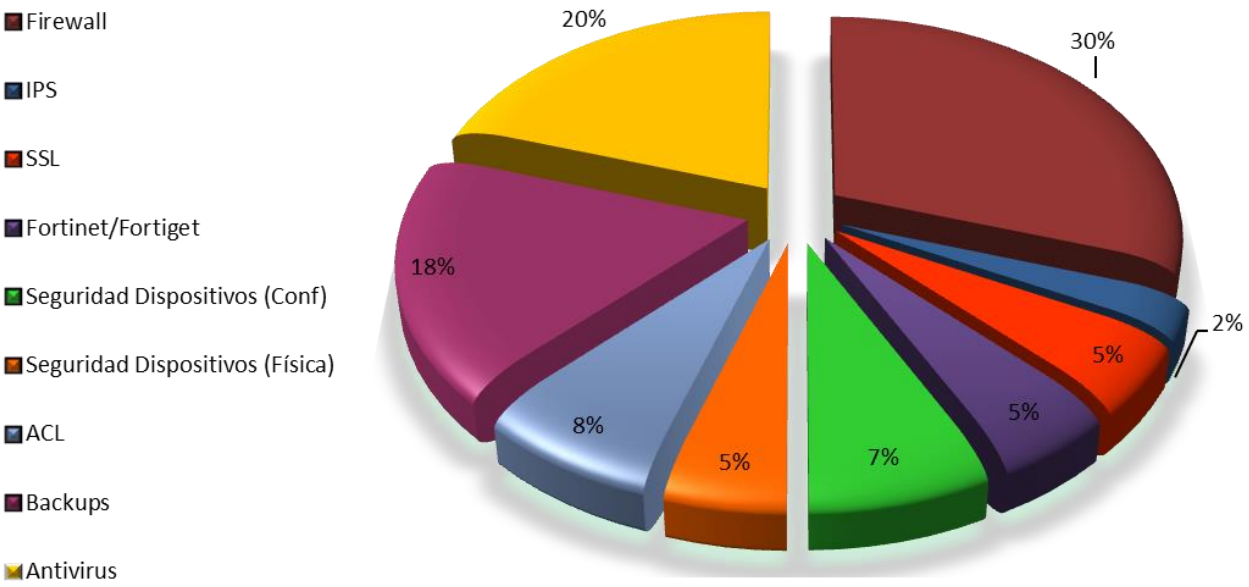


Figura 1.5 – Herramientas de seguridad

De acuerdo a estudios de NSS Labs, es necesario utilizar algunas herramientas de mayor uso en la actualidad, mismas que se muestran en la Gráfica 1.9, las cuales pueden ser:

- **Físicas.** Se refieren a la implementación de algún mecanismo de seguridad que esté destinado a proteger físicamente cualquier recurso del sistema, un ejemplo de ello es identificar si la persona que desea acceder está autorizada para consultar u operar equipo o información valiosa que existe en la organización.

- **Lógicas.** Consiste en la aplicación de procedimientos y barreras que resguarden el acceso a los datos y que sólo se realicen las acciones autorizadas

Uno de los mecanismos más importantes para asegurar una red interna de una que no es segura (por ejemplo internet) es la implementación de un Firewall ya que ejerce políticas de seguridad establecidas por la empresa, además sirve como defensa perimetral de la red, a pesar de ello no defiende de ataques o errores provenientes del interior ni tampoco ofrece protección una vez que es traspasado. Para ello existen otros mecanismos de seguridad como son antivirus, ACL, configuración en dispositivos intermedios, y demás.

Una de las medidas preventivas más necesarias son los backup, debido a que sirven como respaldo en caso de suscitarse algún problema con la información, son las pérdidas de información que pueden ser causadas por diversos factores como son:

- Error de hardware
- Error humano
- Error de software
- Virus
- Desastres naturales

Para mantener óptima la seguridad en la red es importante aplicar cada una de estas herramientas, que en conjunto hacen que la seguridad sea más fuerte y así sea más complicado dañar el activo. Una buena práctica de seguridad es tener auditorías de seguridad periódicas para poder descubrir las debilidades y vulnerabilidades y asimismo contrarrestarlas.

Bibliografía

Capítulo 1 Necesidades del campo laboral

Sánchez Onofre, Julio. (2014). Las direcciones de Internet IPv4 se agotaron para AL. El economista. Sitio Web: http://eleconomista.com.mx/tecnociencia/2014/06/15/las-direcciones-internet-ipv4-se-agotaron

Lacnic. (2014). No hay más direcciones IPv4 en América Latina y el Caribe. Sitio Web: http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac

Infoblox (2013) Los 25 problemas de red más comunes y su impacto en el negocio. http://www.infoblox.es/sites/infobloxcom/files/es/resources/infoblox-poster-top-25-network-problems-es.pdf

Ganguly Debashis. (2012). Network and Application Security Fundamentals and Practices. USA: CRC Press Taylor & Francis Group.

Llandez Abraham, Dávila Carlo, Ayvar David, Valer Diego, Florean Alejandro & Zergarra Daniel. (2014). I D C Latin America Predictions 2015.
Sitio Web: http://www.idclatin.com/campaign/predictions/

Zimmerman Tim, Lerner Andreu & Menezes Bill (2014) Gartner Magic Quadrant for the Wired and Wireless LAN Access Infrastructure 2014.
Sitio Web: https://www.gartner.com/doc/2781218/magic-quadrant-wired-wireless-lan

Capítulo 2

Antecedentes de Redes y Seguridad

Los conocimientos adquiridos a lo largo de la carrera de Ingeniería en Computación en el área de Redes y Seguridad, son las bases que el egresado necesita para entender de forma clara la operatividad de las redes de datos así como la seguridad de la información, ya sea en su administración, infraestructura, diseño y mantenimiento.

Con los avances tecnológicos los temas que se abordan en las asignaturas que conforman el módulo de redes y seguridad deben contar con conocimientos actualizados de tal manera que el alumno posea las herramientas necesarias para confrontar los requerimientos actuales.

Dentro del conjunto de conocimientos que se imparten en las asignaturas del módulo, se consideran de manera indispensable y relevante los temas que a continuación se presentan ya que son las bases fundamentales para todo ingeniero egresado de la carrera de Ingeniería en Computación en esta área:

- Tipos de redes
- Capas del modelo OSI
- Dispositivos que interconectan las redes
- Métodos de direccionamiento
- Asignación de direccionamiento
- Seguridad en redes
- Versiones IP
- Protocolos de enrutamiento

2.1 Tipos de redes

2.1.1 Clasificación de las redes por cobertura geográfica.

Una red se puede definir como un conjunto de computadoras o dispositivos (Figura 2.1) interconectados entre sí por un medio de transmisión (alámbrica o inalámbrica), por el cual comparten información, recursos y servicios. Las redes pueden clasificarse según su cobertura geográfica, topología y tipo de conexión.

Las redes de computadoras se clasifican por su extensión geográfica en tres tipos principalmente: redes de área local (LAN), redes de área metropolitana (MAN) y redes de área amplia (WAN), éstas pueden abarcar desde unos cuantos metros hasta grandes ciudades. A continuación se describen cada una de ellas.

Figura 2.1- Red de computadoras

Redes de área local (LAN)

Las redes de área local se conocen por sus siglas en inglés como LAN (Local Area Network), se caracterizan por ser redes privadas que se encuentran instaladas desde un edificio de oficinas hasta un campus de pocos kilómetros. La distancia que abarca está entre los 10m hasta 1Km. El objetivo de las redes es interconectar computadoras personales, recursos y servicios. Las redes LAN se clasifican de acuerdo a su tipo de conexión: alámbrica o inalámbrica.

Redes alámbricas o Ethernet

El organismos encargado de regular a las redes LAN es IEEE en su estándar 802.3, éste distingue a las redes LAN de otras en que las comunicaciones se restringen a un área geográfica limitada y en que pueden depender de un canal físico de comunicación con una velocidad alta y poca tasa de errores. Las características principales que definen a una red de área local son las siguientes:

- Las velocidades que alcanzan estas redes van desde 10Mbits/s hasta 10Gbit/s.
- Las tasa de error de transmisión de los bits es despreciable (Del orden de 1 bit de error por cada 100 millones de bit transmitidos)
- La administración de la red y de los recursos informáticos que la conforman es responsabilidad del administrador de red.

Las redes LAN utilizan un modo de transmisión/modulación, (Banda base o banda ancha), un protocolo de acceso al medio (TDMA, CSMA/CD,TokenPassing, o FDDI entre otros) y un medio de transmisión (cable de par trenzado, coaxial o fibra óptica) y una topología (bus, anillo, estrella, o malla).

A continuación en la Tabla 2.1 se presentan las diferentes normas en las que se divide el estándar 802.3, así como las especificaciones para el uso de fibra óptica en las redes establecida en el estándar 802.8.

Tabla 2.1 - Clasificación estándar 802.3					
Denominación	**Cable**	**Pares**	**Full Dúplex**	**Conectores**	**Distancia**
10BASE5	coaxial RG8, RG9 o RG11	1	No	´N´	500m
10BASE2	RG58 Coaxial delgado	1	No	BNC	185mm
10BASE-T	UTP Cat. 5, 5e, 6	2	Si	RJ-45	100m
100BASE-TX	UTP Cat. 5, 5e, 6	2	Si	RJ-45	100m
100BASE-T4	UTP Cat. 3, 4, 5,5e ,6	4	No	RJ-45	100m
100BASE-CX	STP	2	Si	8pin HSSDC	25m
1000 BASE-T	UTP Cat 5e, 6	4	Sí	RJ-45	100 m
10G BASE-T	UTP Cat 6a, 7	4	Sí	RJ-45, GG45	100 m
Cableado con Fibra Óptica según el estándar 802.8					
Medio	**Ventana**	**Luz**	**Fibra**	**Conector**	**Distancia**
10BASE-FL	1ª	Normal	62,5/125	ST	2 Km
100BASE-FX	2ª	Normal	62,5/125	SC	2Km
100BASE-SX	1ª	Láser	62,5/125 50/125	SC	275m, 550m
100BASE-LX	2ª	Láser	62,5/125 50/125 9/125	SC	550m 550m 5km

En la actualidad, algunos de estos estándares se han vuelto obsoletos, debido a la necesidad de compartir cada vez más rápido la información así como los recursos que existen en la red. El uso de cada uno de estos estándares depende de las necesidades a las cuales se enfrente el arquitecto de la red. Sin embargo la tendencia en estas redes, es la utilización de enlaces vía inalámbrica, todo esto para facilitar la movilidad de los usuarios, tanto en las empresas como en los hogares e incluso en sitios público.

WLAN (Wireless Local Area Networks)

Las redes inalámbricas de área local WLAN por sus siglas en inglés Wireless Local Area Network son redes que comúnmente cubren distancias de los 10 a los 100 metros. Esta cobertura permite una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia.

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de la empresa IBM en Suiza, el cual consistió en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados publicados por el IEEE, se pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Desde 1985 hasta 1990 se siguió trabajando más en la

fase de desarrollo, hasta que en Mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1Mbits/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de accesos también conocidos como Access Points que actúan como un concentrador o Hub que reciben y envían información vía radio a los dispositivos de clientes, que habitualmente son computadoras, impresoras o dispositivos móviles

EL estándar IEEE 802.11 o también llamado Wi-Fi fue definido por la IEEE en 1997 como un estándar que reemplazaría los cables de la conexión alámbrica Ethernet con una conexión inalámbrica. El estándar 802.11 de la capas Física incluye definiciones para el procedimiento de convergencia de la capa física (PLCP) y las subcapas dependientes del medio (PMD).

Las WLAN utilizan la tecnología Wi-Fi la cual envía datos utilizando ondas de radio, éstas se propagan en línea recta en varias direcciones al mismo tiempo y pueden atravesar obstáculos. Wi-Fi utiliza un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, a continuación en la Tabla 2.2 se muestran sus características principales.

Tabla 2.2- Clasificación Estándar 802.11

Estándar Wireless	802.11	802.11a		802.11b	802.11g	802.11n		802.11ac	
Lanzamiento	1997	1999		1999	2003	2009		2011	
Frecuencia [GHz]	2.4	5	3.7	2.4	2.4	2.4	5	5	
Bandwidth [MHz]	20	20		20	20	20	40	80	160
Velocidad [Mbps]	1 a 2	6 a 54		5.5 a 11	6 a 54	7 a 72	15 a 150	433 a 867	867 a 1.3 Gb
Rango Interior [m]	20	35	**	35	38	70		**	
Rango Exterior	100	120	5000	140	140	250		**	
Compatibilidad	**	Incompatible con 802.11b y g		**	Compatible con 802.11b	Compatible con 802.11b y g		En desarrollo	

** No está definido

Redes de área Metropolitana (MAN)

Redes MAN Ethernet

Desde que los equipos personales y las redes LAN se volvieron comunes, la demanda para el envío de la información ha ido en aumento, con ello han aparecido nuevas necesidades como la interconexión de las LAN geográficamente separadas. Para dar respuesta a esta situación se tenía el estándar IEEE 802.6 que define un tipo de red MAN llamado DQDB (por sus siglas en inglés Distributed Queue Dual Bus) el cual actualmente está en desuso debido a que cuando una estación desea transmitir tiene que confirmar primero la dirección del receptor y luego tomar el bus correspondiente. Esto generó un gran problema ya que una vez conformada la red, cada estación tiene que validar las direcciones de las otras estaciones, generando grandes demoras de tiempo.

Actualmente esta tecnología se sustituyó por la red MAN (Metropolitan Area Network) definida como MAN BUCLE, esta es una red de alta velocidad (banda ancha) que da cobertura a un área geográfica extensa la cual oscila entre 1 y 7 kilómetros , proporcionando la capacidad de integración de múltiples servicios mediante la transmisión multimedia (datos, voz y vídeo) sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia(entre 1-50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps hasta 75Mbps, sobre pares de cobre y 100Mbps hasta 10Gbps mediante Fibra Óptica.

Las Redes MAN BUCLE, se basan en tecnologías Bonding, de forma que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario. Esta tecnología ofrece servicios Ethernet de alta disponibilidad en distancias próximas a los 5 Km y la posibilidad de encapsulado de múltiples interfaces TDM.

Existen dos tipos de MAN: las privadas y las públicas. Un ejemplo de MAN privada sería un conjunto de edificios pertenecientes a una misma organización (bancos, tiendas departamentales, entre otros) con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa mediante los operadores públicos (ISP, proveedor de servicios de Internet). La Figura 2.2 muestra un ejemplo de red MAN privada.

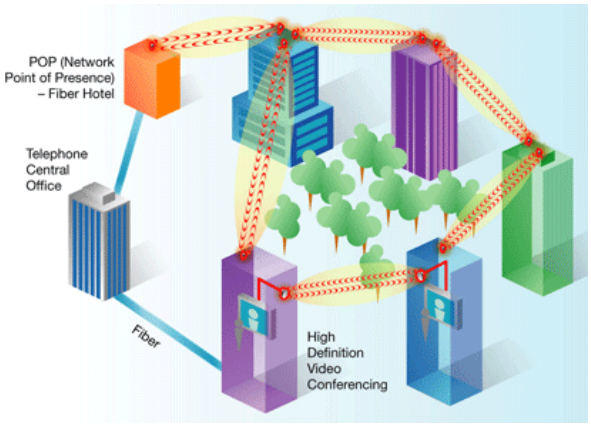


Figura 2.2 - Red MAN privada

Un ejemplo de MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

Redes MAN inalámbrica (WMAN)

Las redes metropolitanas inalámbricas (WMAN) también son conocidas como Bucle local inalámbrico (WLL: Wireless Local Loop), están definidas en el estándar IEEE 802.16 (WiMAX) el cual ofrecen una velocidad de transmisión de 1 a 10 Mbps con un alcance de hasta 60 kilómetros.

WiMAX son las siglas de "Worldwide Interoperability for Microwave Access", y es la marca que certifica que un producto está conforme a los estándares de acceso inalámbrico 'IEEE 802.16'. Estos estándares permitirán conexiones de velocidades similares al ADSL o cable módem, sin cables, y hasta una distancia de 50-60 km. Este nuevo estándar es compatible con otros anteriores, como el de Wi-Fi (IEEE 802.11).

La tecnología WiMAX es la base de las Redes Metropolitanas de acceso a Internet, sirve de apoyo para facilitar las conexiones en zonas rurales, y es utilizada en el mundo empresarial para implementar las comunicaciones en distintas sucursales localizadas por una extensión geográfica mayor a la que ofrece una WLAN. Véase la Figura 2.3.

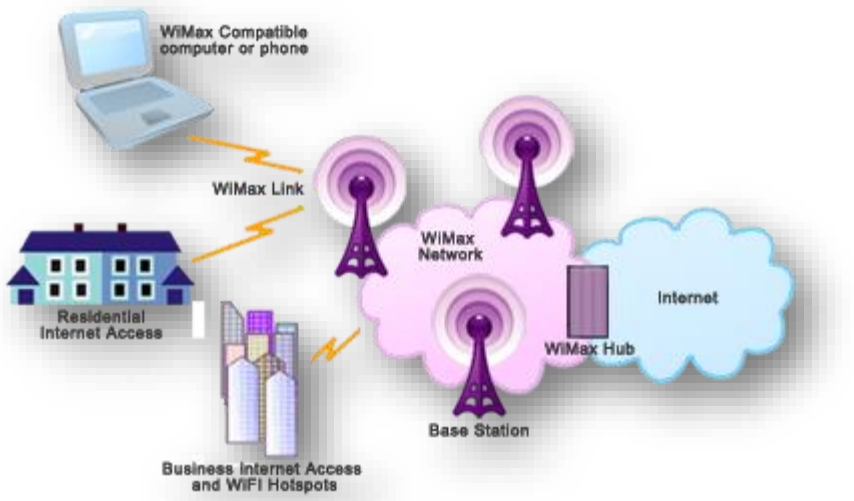


Figura 2.3 - Red WiMAX

WiMAX está diseñado principalmente como tecnología de "última milla" y se puede usar para enlaces de acceso, MAN o incluso WAN. Destaca principalmente por su capacidad como tecnología portadora, sobre la que se puede transportar diferentes protocolos como: IP, TDM, T1/E1, ATM, Frame Relay y voz, lo que la hace adecuada para entornos de grandes redes corporativas de voz y datos, así como para operadores de telecomunicaciones.

El estándar IEEE 802.16 está orientado a sistemas de acceso de radio de banda ancha (BWA: Broad band Wireless Access) punto a multipunto, que proporcionen a los usuarios tasas de transmisión elevadas (hasta 40 Mbps por canal) y puedan operar en condiciones NLOS (Non Line Of Sight: término referido cuando existe obstrucción en la línea de visión entre el receptor y emisor de la señal) con radios de cobertura de varios kilómetros.

A continuación se muestra en la Tabla 2.3 las características principales del estándar 802.16 en sus tres versiones.

Tabla 2.3 – Características del estándar 802.16			
	802.16	**802.16a**	**802.16e**
Espectro	10 - 66 GHz	< 11 GHz	< 6 GHz
Funcionamiento	Solo con visión directa	Sin visión directa (NLOS)	Sin visión directa (NLOS)
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Modulación	QPSK, 16QAM y 64 QAM	OFDM con 256 subportadoras QPSK, 16QAM, 64QAM	Igual que 802.16a
Movilidad	Sistema fijo	Sistema fijo	WiMAX Mobile
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máximo de 50 km)	2 - 5 km aprox.

Redes de área Extensa (WAN)

Redes WAN Ethernet

Las redes de área extensa son conocidas por sus siglas en inglés como WAN (Wide Area Network), este tipo de redes tienen un alcance que va desde los 100 hasta 1.000 Kilómetros aproximadamente, lo que le permite brindar conectividad a varias ciudades, incluso a un país o un continente. En la Figura 2.4 se observa cómo una red WAN interconecta dispositivos que se encuentran localizados en un área geográfica distinta.

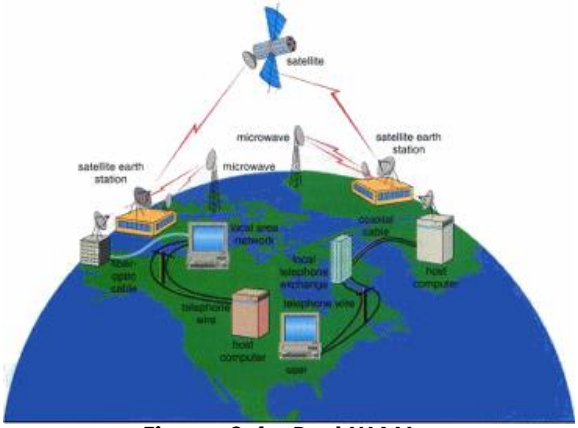


Figura 2.4 - Red WAN

Una red WAN utiliza conexiones dedicadas o conmutadas para conectar computadoras que se encuentran a grandes distancias, estas conexiones pueden realizarse a través de una red pública o una red privada. Las redes WAN pueden realizar su conexión a través de líneas dedicadas (Camino permanente entre dos puntos durante un tiempo determinado) suministradas por un proveedor de servicios de Internet o líneas conmutadas (no requiere conexiones permanentes, utilizan conexiones temporales entre múltiples puntos).

Tradicionalmente las WAN se implementaron usando alguna de las tecnologías siguientes, conmutación de circuitos (ISDN, Dial-up, POST, DDR, SW-56) o conmutación de paquetes (X.25), aunque actualmente se ha optado por las técnicas de retransmisión de tramas como Frame Relay y técnicas de retransmisión de celdas como Cell Relay o ATM, ambas técnicas son derivadas de la tecnología de conmutación de paquetes.

Las operaciones de una WAN se basan principalmente en la capa 1 y 2 del modelo OSI, los protocolos de la capa 1(capa física) describen el funcionamiento de las conexiones eléctricas, mecánicas, operativas y funcionales de los servicios brindados por un proveedor de servicios de comunicaciones. La capa de enlace de datos (capa 2 del modelo OSI), define el modo de encapsulación de los datos para su transmisión a lugares remotos, así como los mecanismos de transferencia de las tramas resultantes. En la Figura 2.5 se muestran los mecanismos que utilizan las redes WAN para la transición de la información.

Figura 2.5 - Servicios proporcionados por las redes WAN en el modelo OSI

Redes WAN Inalámbricas (WWAN)

Una Wireless WAN es una red de computadores que abarca un área geográfica relativamente extensa, permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red. Por medio de una WAN Inalámbrica se pueden conectar diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas como se muestra en la Figura 2.6. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

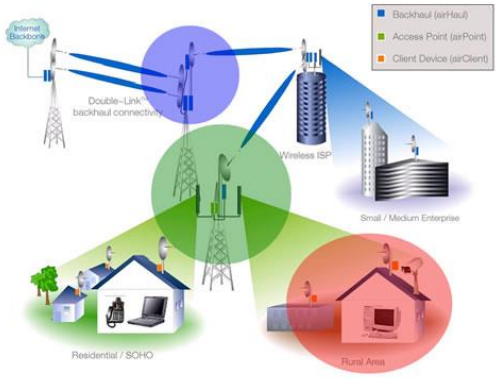


Figura 2.6 - Red WWAN

En sí, la forma más común de implementación de una red WAN es por medio de Satélites, los cuales enlazan una o más estaciones base, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites funcionan en tres bandas de frecuencias, llamadas C, Ku y Ka, las cuales trabajan en distintas frecuencias como las mostradas en la Tabla 2.4

Tabla 2.4 – Frecuencias a la que trabaja los satélites.

Banda	Frecuencia ascendente (GHz)	Frecuencia descendente (GHz)
C	5,925 - 6,425	3,7 - 4,2
Ku	14,0 - 14,5	11,7 - 12,2
Ka	27,5 - 30,5	17,7 - 21,7

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35,784 Km.

Las redes de área amplia inalámbricas transmiten los datos mediante señales de telefonía móvil, a través de un proveedor de servicios de este tipo, con velocidades de conexión iguales a las de acceso telefónico de 56Kbits/seg. Su alcance puede llegar hasta 30 km, lo que ofrece a los usuarios un modo de conectarse mientras se desplazan o están alejados de otra infraestructura de red. Las principales tecnologías que utilizan las redes WWAN son:

- GSM(Global System for Mobile Communication)
- DPRS (General Packet Radio Service)
- UMTS (Universal Mobil Telecommunication System)
- CDMA (Code Division Multiple Access)
- 3G
- 4G

2.1.2 Clasificación de las redes por Topología

El término Topología hace referencia a la forma en la que los dispositivos se interconectan ya sea de forma física y lógica dentro de una red, la manera en la que se conectan y comunican depende del número de dispositivos que la conforman, de modo que al diseñar una red debe plantearse una serie de preguntas:

- Cómo encontrar la formas más óptima y económica para interconectar las estaciones de trabajo y así proporcionar confiabilidad en la transmisión de la información a través de la red.
- Cómo evitar tiempos de latencia altos
- Cuál será el crecimiento futuro de la red

En los siguientes temas se abordarán las distintas topologías de red que hacen que una red sea funcional.

Topologías Físicas

La topología física se refiere a la disposición física de las máquinas, los dispositivos de red y el cableado. Así, dentro de la topología física se pueden diferenciar dos tipos de conexiones: punto a punto y multipunto.

- En las conexiones punto a punto existen varias conexiones entre parejas de estaciones adyacentes, sin estaciones intermedias.
- Las conexiones multipunto cuentan con un único canal de transmisión, compartido por todas las estaciones de la red. Cualquier dato o conjunto de datos que envíe una estación es recibido por todas las demás estaciones.

Existen varios tipos de topologías las cuales se pueden combinar para obtener una topología híbrida o mixta, las principales topologías son:

BUS

Es una topología de red en la que todas las estaciones están conectadas a un único canal de comunicación por medio de una interfaz de red, éste canal de comunicación es conocido como Bus, troncal o backbone, este puede ser de cable coaxial, par trenzado fibra óptica, además en sus dos extremos tiene resistencias denominado terminadores que además de indicar que no existen más computadoras en los extremos, permiten cerrar el bus, en la Figura 2.7 se observa este tipo de topología. La implementación de este tipo de topología es fácil de realizar, pero tiene la desventaja que si el bus se daña, toda la red deja de funcionar.

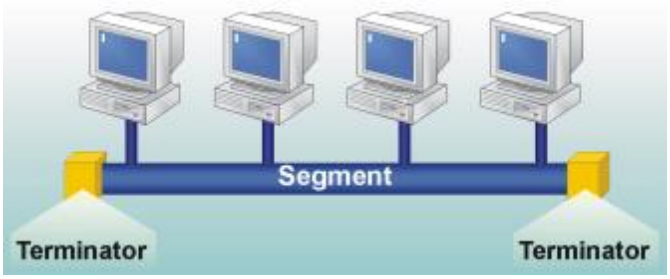


Figura 2.7 - Topología tipo bus

Estrella

En una topología estrella, todos los dispositivos de la red están conectados a un concentrador (Hub o Switch), el cual replica la información a todos los que se encuentran conectado, pero solamente lo recibe el dispositivo con la dirección destino. En la Figura 2.8 se muestra la distribución de una topología estrella.

Una de las ventajas de esta topología es que si un enlace llega a fallar el resto de la red no se ve afectada, sin embargo, si Hub falla la red deja de operar.

Figura 2.8 - Topología tipo estrella

Anillo

En esta topología cada nodo está conectado consecutivamente a otro nodo por enlaces punto a punto, formando un anillo por el cual viaja la información. En esta tipo de configuración, todos los dispositivos repiten la misma señal que fue enviada por el emisor y lo hace en un solo sentido de la red, el mensaje se transmite de dispositivo en dispositivo hasta que encuentra al destinatario. En la Figura 2.9 se muestra la topología. Una de las desventajas es que si algún dispositivo llega a fallar, éste podría hacer que toda la red dejara de funcionar.

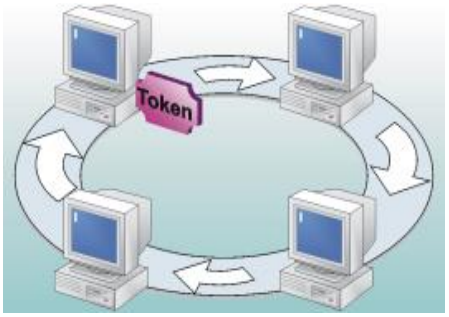


Figura 2.9 - Topología tipo anillo

Árbol

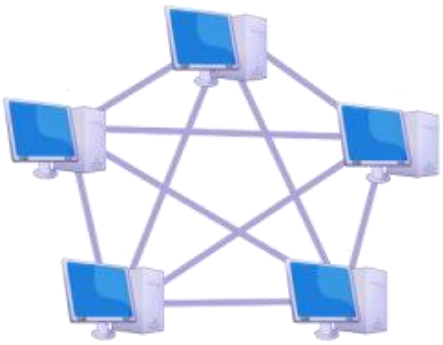
La topología en árbol o también denominada jerárquica es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red, sin embargo, no todos los dispositivos se conectan directamente al concentrador central.

Esta topología comienza en un punto denominado raíz (head end). Teniendo desde un mismo punto uno o más cables salientes en donde cada uno de ellos puede tener ramificaciones en cualquier otro punto.

Una red como ésta representa una red completamente distribuida en la que computadoras proporcionan la información a sus ramificaciones de forma contigua. En la Figura 2.10 se observa la estructura de esta topología.

Figura 2.10 - Topología Tipo árbol

Malla



En la topología malla los dispositivos están interconectados entre sí por medio de cables tal y como se muestra en la Figura 2.11, este tipo de configuración provee redundancia, esto quiere decir que si un segmento de cable falla, existe otro que permite mantener la comunicación. Una de las desventajas que posee esta topología, es que se necesita enormes cantidades de cableado para su implementación, y por consiguiente se vuelve muy costosa.

Figura 2.11 - Topología Tipo Malla

Esta topología a diferencia de las demás no requiere de un nodo central con lo que se reduce el mantenimiento, además este tipo de topología es auto-ruteable, es decir, que si un nodo llega a fallar los demás nodos evitan enviar datos a través de esta ruta, en consecuencia la red de malla se vuelve confiable.

Topologías lógicas

La topología lógica se define como la forma en la que los dispositivos transmiten la información a través de algún medio de comunicación. Existen dos tipos de topologías lógicas:

Broadcast

En esta topología los dispositivos que la conforman envían sus datos hacia todos los demás componentes conectados al mismo medio de red, donde las estaciones de trabajo no siguen ningún orden para utilizarla, sino que los dispositivos acceden a ella para transmitir los datos en el momento en que lo necesiten. Uno de los protocolos que funcionan de esta manera es Ethernet.

Topología transmisión de tokens

Controla el acceso a la red mediante la transmisión de un token a cada dispositivo de forma secuencial. Cuando el dispositivo recibe el token, éstos envían datos a través de la red. Si él no tiene ningún dato para enviar, transmite el token al siguiente y el proceso se vuelve a repetir. Ejemplos de redes que utilizan la transmisión de tokens son Token Ring, Token bus y la Interfaz de datos distribuida por fibra(FDDI).

2.2 Modelo OSI

A finales de los años 70, la Organización Internacional para la Normalización (ISO) comenzó a desarrollar un modelo conceptual para las conexiones de red, a éste se le puso el nombre de *Open Systems Interconnection Reference Model* mejor conocido como modelo de referencia de interconexión de sistemas abiertos (OSI). En 1984, este modelo pasó a ser el estándar internacional para las comunicaciones en las redes, al ofrecer un marco de trabajo conceptual que permitía explicar el modo en que los datos se desplazaban dentro de una red. El modelo de referencia OSI se divide en 7 capas las cuales se pueden observar en la Figura 2.12

Figura 2.12 - Modelo OSI

Este modelo define de forma precisa las funciones de cada capa. Cada una de ellas se comporta como un prestador de servicios para la capa inmediatamente superior. Para que una capa realice una petición o envío de datos al nivel equivalente del que intercambia, debe constituir una información y enviarla a través de todas las capas inferiores, cada una de las cuales añade un identificador específico convirtiéndose en una especie de serie. Una vez transferida, se decodifica la información y se libera la aplicación que originó el proceso. A continuación se explica brevemente el funcionamiento de cada una de las capas que conforman este modelo de referencia.

Física

En esta capa se lleva a cabo la transmisión de bits de un canal de comunicación. Los aspectos de diseño implica asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Los aspectos de diseño tienen que ver mucho con las interfaces mecánica, eléctricas y de temporización, además del medio físico de transmisión.

Enlace de datos

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que al llegar a la capa de red, aparezca libre de errores de transmisión. Esta tarea se realiza haciendo que el emisor fragmente los datos de entrada y los transmita de manera secuencial.

Por lo general, se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia esta regulación de flujo y el manejo de errores están integrados. La capa de enlace de datos se divide en dos subcapas:

- LCC – Control de enlace lógico
- MAC – Control de acceso al medio

Capa de red

La capa de red tiene como objetivo proporcionar los servicios de envío, enrutamiento o encaminamiento y control de congestionamiento de los datos de un nodo a otro en la red no importando su localización geográfica. Su propósito es establecer un diálogo con la red para especificar la dirección destino y solicitar ciertos servicios, con ello se logra la independencia a los niveles superiores respecto a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas. El protocolo utilizado es IP.

Capa de transporte

Esta capa mantiene el control de flujo de datos entre los nodos que establecen una comunicación, esto quiere decir que los datos no sólo deben entregar sin errores, sino además en la secuencia correcta. Otra de las funciones que tiene esta capa es optimizar el uso de los servicios de red, y en proporcionar la calidad del servicio solicitado.

Capa de Sesión

El nivel de sesión proporciona los mecanismos para controlar el diálogo entre los sistemas debido a que establece, mantiene y sincroniza la interacción de la comunicación. Dicha capa ofrece tres servicios:

- Control de diálogo
- Agrupamiento
- Recuperación

Capa de presentación

La capa de presentación define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas un conjunto de servicios de transformación de datos, en ella se define la sintaxis utilizada entre las entidades de aplicación, además proporciona los medios para seleccionar y modificar la presentación utilizada.

Capa de aplicación

La capa de aplicación es la encargada de proporcionar la interfaz entre las aplicaciones que utiliza el usuario para comunicarse y la red subyacente en la cual se transmiten los mensajes. Los protocolos de la capa de aplicación se utilizan para intercambiar la información de las aplicaciones que se ejecutan en los dispositivos origen y destino. Algunos de los protocolos que se utilizan en esta capa son:

- FTP
- DNS
- DHCP
- HTTP
- HTTPS
- NAT
- POIP
- SMTP
- SSH
- TELNET
- TFTP
- SYSLOG

2.3 Métodos de direccionamiento

Una dirección IP es un identificador lógico y único con el cual se reconoce un dispositivo dentro de una red de datos, en la actualidad se utilizan dos versiones de direccionamiento IPv4 e IPv6 las cuales se estudian a continuación.

2.3.1 IPv4

Esta versión tiene una longitud de 32 bits organizada en 4 grupos de 8 bits cada uno, esto ocurre en IPv4, donde la dirección IP se divide en dos partes: de red y de host.

La porción de red se utiliza para identificar un grupo de dispositivos que comparten el mismo protocolo de enlace dentro de un segmento de red, la parte de host hace referencia a todos aquellos dispositivos que se encuentran dentro de la misma red.

A medida que ha pasado el tiempo, los métodos de direccionamiento han tenido que evolucionar para adaptarse al constante crecimiento de las redes. A continuación se presentan los métodos de direccionamiento utilizados.

CLASSFULL

Las direcciones IP se clasifican en 5 diferentes clases, las cuales de acuerdo a ésta permiten cierto número de redes y host, a estas redes se les conoce como clase A, B, C, D y E, de las cuales hoy en día sólo se emplean las tres primeras. A esta clasificación de redes se le denomina direccionamiento con clase (classfull).

Las direcciones Clase A se diseñaron para admitir redes de tamaño grande o con gran número de host, las direcciones de clase A utilizan sólo el primer octeto para indicar la dirección de la red y los tres octetos restantes son para las direcciones de los host. Las direcciones de clase B l utilizan los 2 primeros octetos para direcciones de red y los dos últimos para direcciones de host. Para las direcciones de clase C son 3 octetos para la máscara de red y uno para host. Las clase D se utilizan para grupos de multicas y las E están reservadas para fines de investigación. En la Tabla 2.5 se muestra los distintos tipos de clases, así como la máscara típica de red que utilizan para las direcciones IPv4.

Tabla 2.5 – Clases de direcciones IPv4

CLASE	1 Octeto	2 Octeto	3 Octeto	4 Octeto	Rango de direcciones	Mascara de red por defecto	# de redes disponibles	# de hosts disponibles
A	00000000	00000000	00000000	00000000	0.0.0.0 - 127.0.0.0	255.0.0.0	128	16777214
B	10000000	00000000	00000000	00000000	128.0.0.0 – 191.255.0.0	255.255.0.0	16248	65534
C	11000000	00000000	00000000	00000000	192.0.0.0 – 223.255.2552.55	255.255.255.0	2097152	254
D	11100000	00000000	00000000	00000000	224.0.0.0 – 239.255.255.255			
E	11110000	00000000	00000000	00000000	240.0.0.0 – 255.255.255.255			

El direccionamiento classfull presenta algunas desventajas como son:

- Falta de flexibilidad en el direccionamiento interno.
- Ineficiente espacio de direcciones.
- Proliferación de las entradas de la tabla de enrutamiento.

CIDR

Classless Inter-DomainRouting que significa "Enrutamiento entre dominios sin clase" se encuentra descrito en el RFC 1519 desde el año 1993 por la IETF, este fue creado como una mejora en el modo de asignar direcciones IP para el rango de direcciones privadas, brindando una mayor flexibilidad y eficiencia al momento de distribuir las direcciones IP debido a que fragmenta las redes en subredes.

Este método utiliza la técnica de máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo con el tamaño que se necesita en lugar de hacerlo según la clase. Este tipo de asignación permite que el segmento asignado al prefijo de red y al del host se mueva en cualquier bit de la dirección no importando la clase a la que pertenezcan teniendo como efecto el subdividir o dividir en subredes cada segmento.

Subnetting

La función de subnetting es dividir una red de IP´s físicas en subredes lógicas, para que cada una de estas trabaje a nivel de envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

Subnetting permite una mejor administración, control de tráfico y seguridad al segmentar la red. También mejora el performance de la red al reducir el tráfico de broadcast, sin embargo una de las desventajas es el desperdicio de direcciones, sobre todo en los enlaces seriales.

Para llevar a cabo subnetting hay que tener en cuenta 2 características:

1. El número de usuarios por red y el número de redes que se necesiten. Cuanto más usuarios por red menos redes y cuanto más redes menos usuarios por red.
2. Por cada red que se desea, se dejan de utilizar 2 IP´s una asociada al broadcast y otra para el identificador de red.

Para hacer más fácil el cálculo de las subredes existen dos fórmulas, la primera es para averiguar cuántos bits se deben tomar de los hosts para tener un número determinado de subredes. La fórmula es la siguiente $\mathbf{2^x = y}$, donde **x** es el número de bits que se deben tomar de los host para hacer subredes, de manera que el resultado sea un número igual o mayor al número de subredes que es necesario crear ($\boldsymbol{y}$).

La segunda fórmula, es para saber cuántos bits se necesitan para tener un número determinado de hosts por red, la fórmula para llevar a cabo este cálculo es $\mathbf{2^x - 2 = y}$, donde x es el número de bits necesarios para tener $\boldsymbol{y}$ hosts por subred, se le resta 2 ya que como se había dicho antes éstas son para la dirección de broadcast y el ID de red, el resultado siempre tiene que ser igual o mayor al número de hosts que se necesitan por cada subred. Una de las desventajas que tiene este método de direccionamiento, es que todas las subredes son del mismo tamaño, y por lo tanto si se tiene una subred con pocos hosts, se desperdiciarán direcciones IP. Por tal motivo, se creó el método denominado VLSM.

VLSM

Las máscaras de subred de tamaño variable *(Variable Length Subnet Mask, VLSM)* representan una de las alternativas que se implementaron para solucionar el problema de agotamiento de direcciones IPV4. Una de sus principales funciones es descentralizar las redes consiguiendo que éstas sean seguras, jerárquicas y con una mejor distribución de las direcciones evitando el desperdicio excesivo de direcciones.

El método que emplea VLSM permite utilizar más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM maximiza la eficiencia del direccionamiento y con frecuencia se le conoce como división de subredes en subredes. A continuación en la Tabla 2.6 se ejemplifica el uso de VLSM en la máscara de red.

2.6 – Método de máscara de longitud variable

Sufijo	Host	CIDR	2^n=host	Binario=>Decimal
.255	1	/32	2^0	11111111
.254	2	/31	2^1	..... 1111111**0**
.252	4	/30	2^2	.....111111**00**
.248	8	/29	2^3	..... 11111**000**
.240	16	/28	2^4	..... 1111**0000**
.224	32	/27	2^5	..... 111**00000**
.192	64	/26	2^6	..... 11**000000**
.128	128	/25	2^7	..... 1**0000000**

VLSM además utiliza protocolos de enrutamiento como RIPv2, OSPF, IGRP, EIGRP, entre otros, lo cual permite a los administradores de red organizarlas y utilizarlas con libertad para usar distintas máscaras de subred para redes que se encuentran dentro de un sistema autónomo de red.

2.3.2 IPv6

Una dirección IPv6 está compuesta por 128 bits, divididos en ocho campos de 16 bits representados en notación Hexadecimal, cada uno de ellos están separados por dos puntos. Este tipo de direcciones está conformado por tres partes como se puede observar en la Figura 2.13.

Figura 2.13 – Dirección IPv6

Donde el **prefijo** describe la topología pública que es asignado por el PSI (Proveedor de servicios de Internet) O RIR (Registro regional de Internet), el **ID de subred** describe la topología privada o interna de una organización y el **ID de interfaz** el cual es configurado automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Direccionamiento IPv6

A comparación del protocolo IPv4, las direcciones IPv6 no utilizan métodos de direccionamiento ya que la estructura de la dirección es lo suficiente mente robusta para que esta sea única e irrepetible. IPv6 utiliza tres tipos de direcciones, los cuales llevan a cabo el direccionamiento, a continuación se describe cada una de ellas:

- **Direcciones Unicast:** Identifican a una única interfaz, es decir, un paquete enviado a una dirección Unicast será entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

- **Las direcciones Anycast** identifican un grupo de interfaces, de forma que un paquete enviado a una dirección Anycast será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de encaminamiento.

- **Las direcciones Multicast** identifican, al igual que las Anycast a un grupo de interfaces, pero un paquete enviado a una dirección Multicast es enviado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6, su misión ha sido suplantada por las direcciones multicast.

2.4 Asignación de direcciones estáticas y dinámicas

El tipo de direccionamiento que se utiliza en una red depende del número de host que la integren así como el tipo de dispositivos que la conforman. En su mayoría las redes están compuesta por dispositivos finales como PC, Teléfonos IP, impresoras, PDAs, tabletas, servidores y demás. Para ellos es necesario contar con algún método que asigne las direcciones IP a cada dispositivo teniendo en cuenta que una dirección IP es un identificador lógico el cual no puede ser repetido dentro de la red. A continuación se explican los dos métodos utilizados para la asignación de direcciones.

Direccionamiento Estático

En este tipo de asignación, el administrador de red debe configurar manualmente la dirección IP, la máscara de red, los DNS y el Gateway. Este tipo de direccionamiento es utilizado en dispositivos como impresoras, servidores, NAS, DAS, entre otros.

Existe otra forma de asignar direcciones IP´s estáticas, esto se hace mediante la dirección MAC, la cual es única para cada dispositivo que conforma la red. En este método el administrador de red construye una tabla la cual contiene las direcciones MAC de cada dispositivo y a cada una le asigna una dirección IP.

Una de las desventajas de utilizar este método de direccionamiento es que el administrador debe configurar manualmente cada dirección ya sea en la tabla de direcciones o en cada dispositivo y esto puede originar errores de captura y duplicidad de direcciones.

Direccionamiento Dinámico

Una computadora hoy en día puede estar conectada a más de una organización o pertenecer a una gran red en donde el número de usuarios es bastante alto, por lo que estar sujeto a una sola dirección IP ya no es viable para la movilidad que hoy en día se presenta en las organizaciones.

El direccionamiento dinámico se lleva a cabo cuando la dirección IP cambia constantemente sujeta a la disponibilidad de la red en la que se esté conectando, dicho mecanismo se establece con el protocolo DHCP ("*Dynamic Host Configuration Protocol*"), que se define como un conjunto de reglas que se encarga de proporcionar las direcciones IP y opciones de configuración en los dispositivos que se deseen conectar a la red, tal como se muestra en la Figura 2.14.

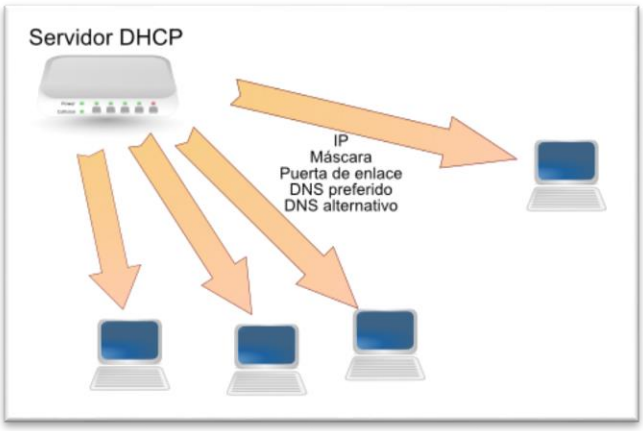


Figura 2.14 - Direccionamiento dinámico

La configuración básica que es enviada junto con la dirección IP es:

- Dirección IP y la máscara.
- La puerta de enlace predeterminada o Gateway.
- Servidores DNS.

Este protocolo es utilizado en las organizaciones cuando el número de dispositivos es grande, y por tal motivo la configuración manual se vuelve ineficiente.

2.5 Dispositivos que interconectan una red

En una red de computadoras existen distintos tipos de dispositivos que la componen, éstos son clasificados en dispositivos finales e intermedios. Como su nombre lo dice los dispositivos finales son aquellos con los que el usuario lleva a cabo el intercambio de información y de recursos, ya sea una impresora, laptop, computadora de escritorio, servidores, entre otros.

En cambio los dispositivos intermedios son aquellos que se encargan de interconectar y efectuar la comunicación entre los dispositivos finales. A continuación se da una breve explicación de cuál es su función y el modo en el que operan los dispositivos intermedios para entender la importancia de ellos, así como las ventajas y desventajas que tienen.

HUB

Un Hub es un dispositivo de capa uno el cual tiene la función de recibir la señal, regenerarla y enviarla a todos los puertos, el uso de éste crea un bus lógico, esto significa que la LAN utiliza medios de acceso múltiple. Los puertos utilizan un método de ancho de banda compartido y a menudo disminuyen el rendimiento en la LAN debido a las colisiones.

El Hub básicamente extiende la funcionalidad de la red para que el área de cobertura de esta sea mayor, es por esto que este dispositivo es considerado un repetidor. Hoy en día este tipo de dispositivos se han vuelto obsoletos debido a que su uso aumenta el dominio de colisiones y por tanto disminuye el performance de la red, en la Figura 2.15 se muestra el dominio de colisión de un Hub.

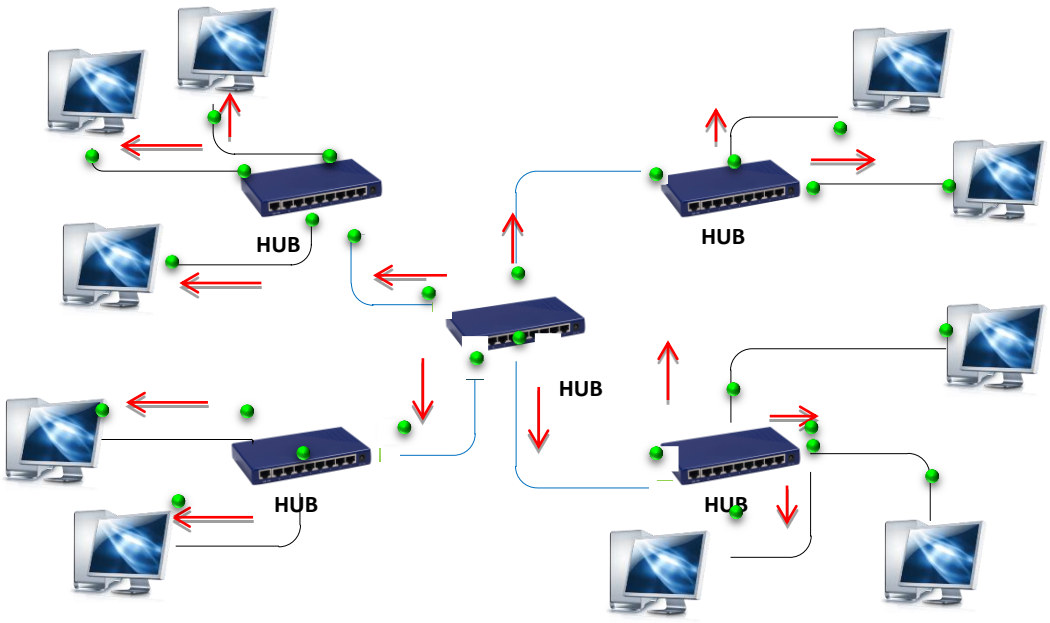


Figura 2.15 - Dominio de colisión HUB

Switch

El dispositivo Switch que traducido significa "interruptor" es utilizado en redes de área local en la que se necesita interconectar equipos relativamente cercanos por medio de cables. Su función principal es unificar redes entre sí, sin tener la necesidad de examinar a fondo la información debido a que sólo examina la dirección MAC de destino, creando puentes que tienen la posibilidad de dividir la red en varios segmentos con una velocidad de retransmisión alta.

De esta manera, el Switch originalmente es un dispositivo que opera en la capa 2 del modelo OSI, el cual tiene la característica en particular que aprende y almacena las direcciones MAC de este nivel por lo que siempre irán desde el puerto origen directamente al de destino, evitando colisiones y bucles de información. En la Figura 2.16 se muestra su dominio de colisión.

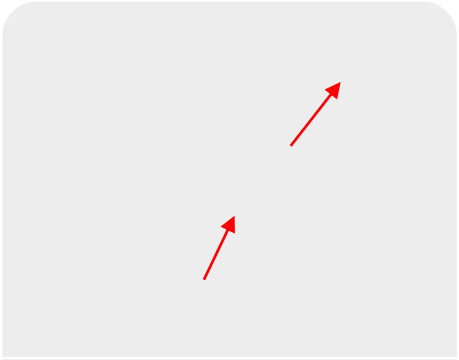


Figura 2.16 - Dominio de colisión Switch

Actualmente existe 3 tipos de Switches los cuales trabajan en distintas capas del modelo OSI, a continuación se explica en que consiste su funcionamiento:

- **Switch de capa 2:** Son los que funcionan como multi-puerto y su principal objetivo es dividir una LAN en múltiples dominios de colisión basando su decisión de envío en la dirección MAC destino que contiene cada trama de información.

- **Switch de capa 3:** Tiene las mismas funciones que un Switch de capa dos pero incorpora funciones de enrutamiento, soportando la definición de redes virtuales (VLAN) sin utilizar un Router.

- **Switch de capa 4:** Incorporan funcionalidades de Switch de capa 3, además de tener la capacidad de implementar políticas y filtros de información de acuerdo al protocolo que se está utilizando.

Router

Un Router es un dispositivo que trabaja en la capa 3 del modelo OSI, su función principal es el encaminar los paquetes destinados a redes locales y remotas. Para llevar a cabo esto, el Router utiliza tablas de enrutamiento para determinar el mejor camino para reenviar los paquetes. Cuando el Router recibe un paquete este examina la dirección IP destino a la cual está encaminado y busca en la tabla de enrutamiento la mejor coincidencia y manda el paquete por la interfaz en la cual se encuentra la red destino, en caso de que el Router no encuentra coincidencia en su tabla, este al envía a otro Router.

Además de encaminar los paquetes hacia la red destino, el Router ayuda a mejorar el tráfico de la red, dividiendo la red en dominios de Broadcast. Y así evitando las colisiones de paquetes dentro de la red. En la Figura 2.17 se muestra los dominios de broadcast.

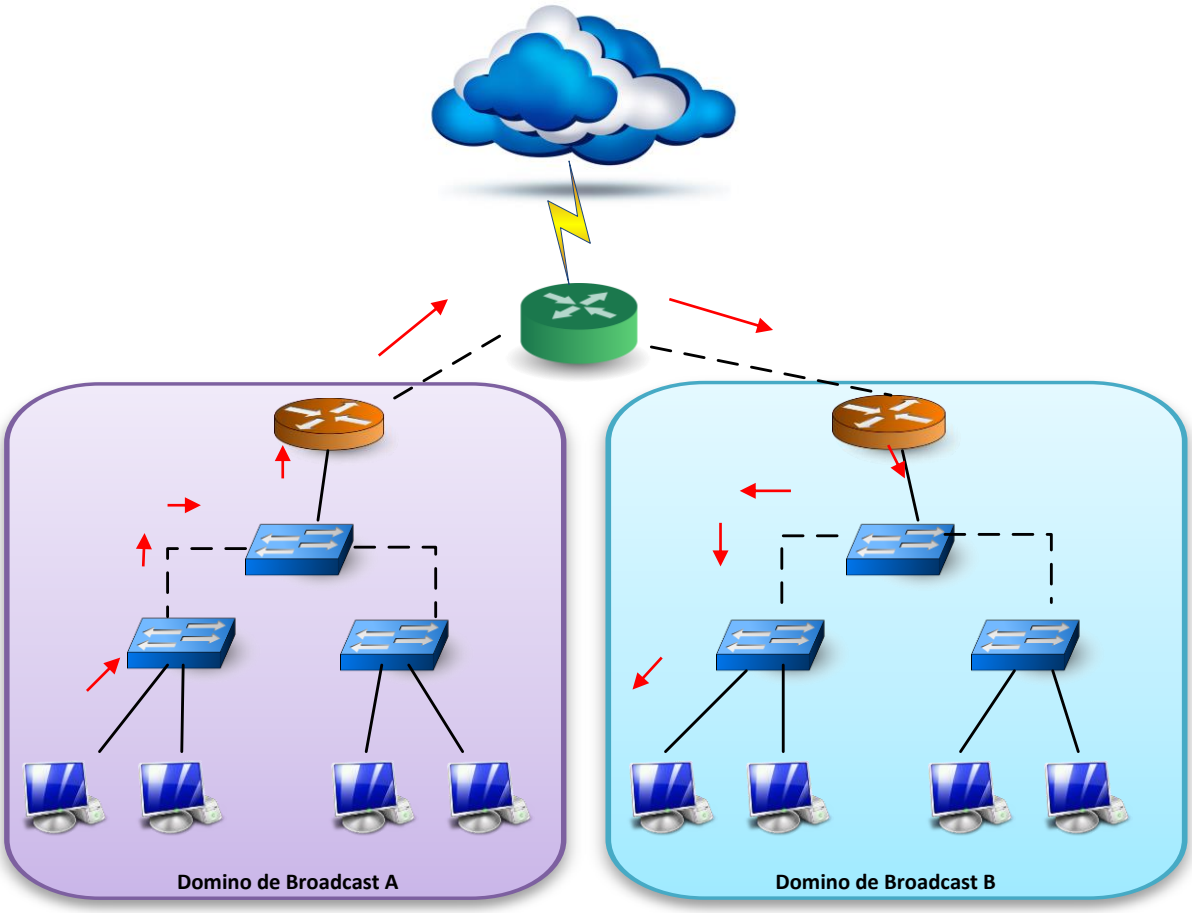


Figura 2.17 - Dominio de colisión Router

Access Point

Es un dispositivo que opera en la capa de enlace de datos, el cual es utilizado como una extensión de la red local cableada, 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.

Un AP no genera direcciones propias debido a que depende de un segmento de red dentro de la propia LAN, es la misma red pero con conexiones de distinto tipo, su uso es permitir que un grupo de dispositivos con tarjetas de red inalámbrica utilicen los servicios de la red local. Los Access Point tienen diversas formas de trabajar, las más conocidas son las siguientes:

Infraestructura (También conocido como AP o modo maestro): Esta es la forma de trabajar de los puntos de acceso para crear un servicio. La tarjeta de red crea una red con un canal y un nombre específico (llamado SSID), en este modo las tarjetas inalámbricas administran todas las comunicaciones de la red (autenticación de clientes inalámbricos, control de acceso al canal, repetición de paquetes, entre otros).

Las tarjetas inalámbricas en modo infraestructura sólo pueden comunicarse con tarjetas asociadas a ella en modo administrado. Un ejemplo de la arquitectura utilizada por un Access Point es la que se muestra en la Figura 2.18.

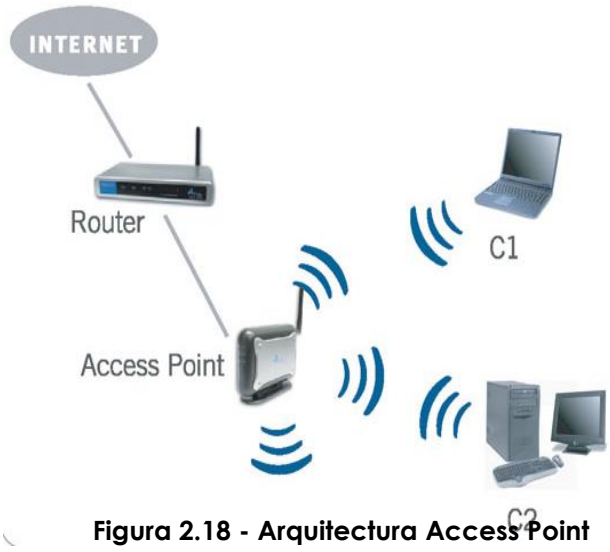


Figura 2.18 - Arquitectura Access Point

Ad-Hoc: Una red Ad-Hoc consiste en un grupo de computadoras que se comunican cada una directamente con las otras a través de las señales de radio sin usar un punto de acceso. Las configuraciones Ad-Hoc son comunicaciones de tipo punto a punto.

Modo administrado: Es denominado algunas veces como modo cliente. Las tarjetas inalámbricas en modo administrado sólo pueden unirse a una red creada por una tarjeta en modo maestro, y automáticamente cambiarán su canal para que corresponda con el de ésta.

Modo monitor: Es utilizado por algunas herramientas (Kismet) para escuchar pasivamente todo el tráfico de radio en un canal dado. En el modo monitor, las tarjetas inalámbricas no transmiten datos.

2.6 Protocolos de enrutamiento

Un protocolo de enrutamiento permite que un Router comparta información con otro, acerca de las redes que conoce, así como su cercanía a otros Router. La información que un Router obtiene de otro, mediante los protocolos, es usada para crear y mantener las tablas de enrutamiento.

Su objetivo principal es crear y mantener las tablas de enrutamiento, las cuales contiene las redes conocidas y los puertos asociados a cada red, así como la de sus vecinos. Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyendo la mejor ruta, además descarta de la misma las rutas que ya no se encuentran activas. Estas rutas aprendidas son utilizadas por el Router para enviar los paquetes de datos a su destino.

Los protocolos de enrutamiento se clasifican de acuerdo a su método de enrutamiento (Dinámico o Estático), protocolos de Gateway interior o exterior y demás, en la Figura 2.19 se muestra la clasificación general de los protocolos.

2.6.1 Protocolo de enrutamiento Estático

Este protocolo es la forma más sencilla y la que menos conocimientos exige para configurar tablas de enrutamiento, ésta es configurada manualmente por el administrador de red, el cual ingresa las rutas por donde los paquetes de datos son enviados a su destino. El principal problema que plantea este enrutamiento, es el mantenimiento de las tablas de

enrutamiento, ya que el Router por sí solo no puede adaptarse a los cambios que pueden producirse en la topología de la red.

2.6.2 Protocolo de enrutamiento Dinámicos

La función de un protocolo de enrutamiento dinámico es el intercambio entre Routers que les permite obtener una tabla de enrutamiento al día en forma automática, con el objetivo de encontrar el mejor camino posible en función de cada uno de los algoritmos utilizados por los protocolo de enrutamiento. Una de las principales ventajas que presentan, reside en el hecho de que una vez configurado no requiere alguna manipulación adicional por parte de los administradores de red para mantener actualizadas las tablas de enrutamiento de los diferentes Routers interconectados. Los protocolos de enrutamiento dinámicos se dividen en:

Protocolos de Gateway exterior

Es un protocolo utilizado para el intercambio de información de encaminamiento entre sistemas autónomos diferentes. Éste se basa en la consulta periódica, para monitorear la accesibilidad de los Routers vecinos y para sondear si existe la actualización de nuevas ruta. Actualmente, sólo existe un protocolo de este tipo llamado BGP (Border Gateway Protocol), el cual se explica brevemente a continuación.

BGP

Es un Protocolo de enrutamiento entre Sistemas Autónomos. La función principal es intercambiar información de acceso con otros Routers que tengan configurado BGP. Esta información de acceso incluye las rutas completas de los Sistemas Autónomos (AS) que los paquetes deben atravesar para llegar a estas redes. Esta información es suficiente para crear un gráfico de conexión de los AS y de los bucles de enrutamiento libres de loops que pueden ser eliminados, además incluye algunas políticas de decisión de enrutamiento.

A diferencia de los protocolos IGP, éste no utiliza métricas como número de saltos, ancho de banda, o retardo. En cambio, BGP toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

BGP 4

La versión 4 es un protocolo de Gateway exterior encargado de intercambiar información con otros sistemas. Esta información contiene las rutas necesarias para construir un mapa de acceso a la red; así, BGP4 es el protocolo utilizado por los ISP para tomar las decisiones de encaminamiento de Internet. Una de las características de este protocolo, es que soporta CIDR, así como la sumarización de rutas.

Protocolos de Gateway Interior

Se utiliza para el enrutamiento dentro de un sistema autónomo, este tipo de sistemas está definido para distintas redes LAN pertenecientes a una misma organización. Los IGP se clasifican dependiendo el algoritmo utilizado para encontrar la mejor ruta de encaminamiento, los protocolos en que se subdivide el protocolo de Gateway interior son: Protocolo vector distancia y protocolo de estado enlace.

Protocolos de Vector Distancia

Se denominan así por realizar la búsqueda del camino más corto determinando la dirección y la distancia a cualquier nodo de la red a través del conteo de saltos para llegar a su destino. Éstos operan a través de algoritmos de enrutamiento basados en vectores, los cuales envían copias periódicas de la tabla de enrutamiento de un Router a otro acumulando así vectores de distancia sin importar que se haya ejecutado alguna modificación. En la actualidad se tienen 4 protocolos que son clasificados dentro de este grupo, los cuales son: RIP, RIPv2, IGRP y EIGRP.

- **RIP**

Es un protocolo de enrutamiento de vector distancia muy utilizado en todo el mundo por su simplicidad en comparación a otros protocolos como: OSPF, BGP, IS-IS, el cual fue descrito por primera vez en el RFC 1058 por C. Hendrick de la Rutgers University en Junio de 1988.

RIP *(Routing Information Protocol)* es clasificado como un protocolo abierto que está basado en el algoritmo Bellman Ford el cual opera informando sobre qué redes son alcanzables para cada Router y la distancia a que éstas se encuentran, utilizando como métrica el número de saltos,los cuales son determinados al evaluar el número de Routers distintos que se han de atravesar para llegar al destino. Uno de los inconvenientes que se tienen al contar únicamente saltos, como cualquier protocolo de vector distancia es que no toma en cuenta datos como ancho de banda, congestión de enlace y demás.

Las principales características que definen este protocolo son:

- Es un protocolo de enrutamiento por vector distancia
- Las rutas que son publicadas con un conteo de saltos mayor a 15 son inalcanzables.
- Se transmiten mensajes cada 30 segundos.
- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependen de parámetros en tiempo real como retardos o carga de enlace.
- No admite subredes ni direcciones con máscara de longitud variable (VLSM).
- No admite CIDR.
- Los intercambios de información no están autenticados.
- Es compatible con la mayoría de los fabricantes de dispositivos.
- No permite usar múltiples rutas simultáneamente.

- **RIPv2**

A diez años de que se publicara la primera versión de RIP se publicó la versión 2 en Noviembre de 1998 por G. Malkin de la compañía Bay Networks el cual se describe en el RFC 2453 presentando las mismas características pero implementando una serie de avances muy importantes con su antecesor, las cuales son:

- Autenticación para la transmisión de información de RIP entre Routers contiguos.
- Utilización de máscaras de red, con lo que ya es posible la implementación de VLSM.
- Utilización de máscaras de red en la elección del siguiente salto, lo cual permite la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast.

- **IGRP**

De las siglas IGRP (Interior Gateway Routing Protocol) que traducido significa Protocolo de Enrutamiento de Gateway Interior es un protocolo de vector distancia con clase desarrollado por Cisco Systems en el año 1986. Fue diseñado para disminuir las limitaciones que RIP presentaba, proporcionando un mejor soporte para redes grandes con enlaces de diversos anchos de banda. IGRP calcula su métrica con base en diferentes atributos de ruta de red como: ancho de banda, retraso de red y el retraso basados en velocidad y capacidad de las interfaces.

Como RIP, IGRP utiliza publicaciones IP para comunicar la información de enrutamiento a los Routers vecinos, no obstante IGRP está designado como su propio protocolo de capa de transporte lo cual no depende de UDP o TCP para comunicar la información de la ruta de red.

IGRP ofrece tres mejoras importantes, las cuales son:

- La métrica de este protocolo puede admitir una red con un número máximo de 255 saltos de Router.
- Distingue entre los diferentes tipos de medios de conexión y los costos asociados a cada uno de ellos.
- Ofrece una convergencia de funcionalidad en la cual se envía la información sobre cambios en la red a medida que está disponible.

- **EIGRP**

Enchaced Interior Gateway Routing Protocol es una versión mejorada del protocolo IGRP desarrollado por Cisco en el año 1986, éste mantiene el mismo algoritmo de vector de distancia y la información de métrica original de IGRP; no obstante este protocolo ofrece tiempos de convergencia más rápidos, teniendo mejor escalabilidad y una gestión superior de los bucles de enrutamiento.
Una de sus grandes diferencias entre ambos es que EIGRP soporta CIDR y VLSM, lo que permite maximizar el espacio de direccionamiento de red. Como una característica particular EIGRP es considerado como un protocolo de enrutamiento híbrido que ofrece lo mejor de los algoritmos de vector distancia y del estado de enlace que lo hace un

protocolo de enrutamiento avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Protocolos de Estado Enlace

Este tipo de protocolo se basa en un conocimiento exacto de la topología de red sobre la que se quiere encaminar la información, manteniendo una tabla de enrutamiento que funciona con un algoritmo SPF (Shortest Path First) a partir de paquetes denominados de estado enlace que intercambian todos los Routers que estructuran la red para describir y determinar el estado de cada enlace. Una de sus principales características es que no intercambia toda la tabla de enrutamiento sino solamente información sobre los enlaces que cada Router tiene con sus adyacentes, los cuales están establecidos generalmente en el costo del enlace que se determina a partir de la velocidad de conexión. Un ejemplo de este protocolo es OSPF, el cual se describe enseguida.

- **OSPF**

Es un protocolo de enrutamiento de estado de enlace basado en un estándar abierto, de ahí su nombre "Open Shortest Path First" el cual fue creado por John J. Moy y descrito por primera vez en el RFC 1583, este protocolo utiliza un flujo de información y un algoritmo de Dijkstra para calcular las rutas más cortas posibles y se encarga de que todos los Routers de la red conozcan la topología del sistema autónomo (SA) completo.

OSPF a diferencia de los protocolos anteriores (RIP y RIPv2) permite una escalabilidad muy notable ya que no está limitado a un cierto número de saltos, además los tiempos de convergencia son considerablemente mejores ya que para el cálculo de costos y rutas toma en cuenta todos los factores relacionados con la red como: retraso, ancho de banda, velocidad, costo, entre otros.

OSPF utiliza la tecnología de estado del enlace, el cual mantiene una imagen común de la red e intercambia su información de enlaces desde su descubrimiento inicial hasta los cambios de la red. Las características que representan a este protocolo se describen en la Figura 2.20.

Figura 2.20 - Características OSPF

- **IS-IS**

Es un protocolo de enrutamiento IGP y de estado enlace, fue diseñado y desarrollado por DEC (Digital Equipment Corporation), este protocolo es utilizado por el protocolo del modelo OSI llamado CLNP (Connectionless Network Protocol). Aunque IS-IS fue desarrollado para implementar direcciones CLNP se adoptó para dar soporte al enrutamiento del protocolo IP.

Este protocolo utiliza una terminología distinta a la utilizada por el protocolo TCP/IP, en éste se manejan términos como:

- ES (End System) : Host
- IS (Intermediate System): Router
- Nivel 1: INTRA-área
- Nivel 2: INTER-área
- Nivel 1-2: realiza funciones tanto de nivel 1 y nivel 2

Para entender mejor el funcionamiento del protocolo se plantea el siguiente escenario:

Una red es considerada como un dominio que está dividido en áreas, donde cada sistema reside en un área. El enrutamiento ejecutado dentro del área es conocido como enrutamiento Nivel 1, y el que se efectúa entre áreas se determina como enrutamiento Nivel 2. Un sistema intermedio (IS) nivel 2 mantiene la información de las rutas a los destinos de las otras áreas. Un nivel 1 mantiene la información del enrutamiento dentro del área. Cuando un paquete lleva como destino otra área, el nivel 1 envía el paquete al nivel 2 más cercano dentro de su área. Sin importar el área de destino, donde el paquete viaja por caminos de enrutamiento nivel 1 hasta el destino. En la Figura 2.21 se muestra el escenario con el que se describe a IS-IS.

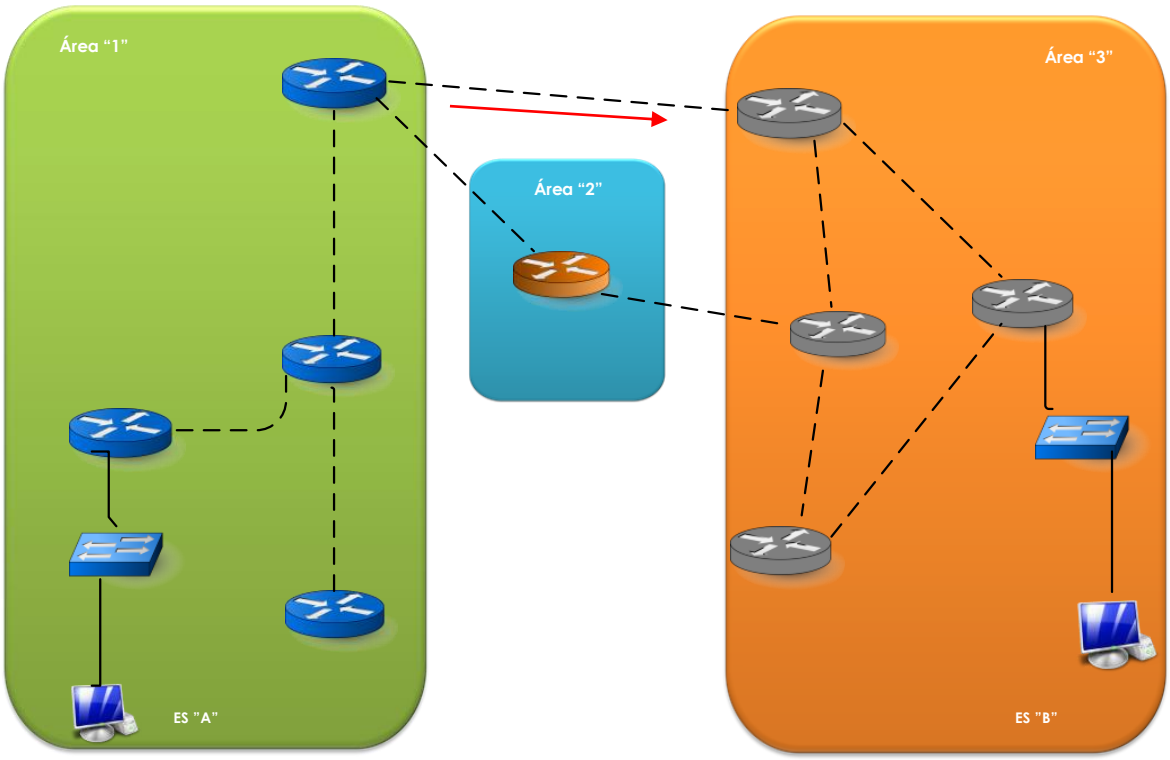


Figura 2.21 - Protocolo IS-IS

2.7 Seguridad en redes

Una de las grandes tareas a las que se enfrenta el administrador de la red, es mantener los activos de una organización seguros, para realizar esta tarea existen distintas normas, políticas y herramientas de seguridad que ayudan a mantener la red libre de amenazas.

Para conservar segura la red es necesario identificar los activos que deben ser protegidos, éstos puede ser lógicos o físicos, para salvaguardar su integridad deben ser evaluadas sus posibles vulnerabilidades, así como las amenazas a las que está expuestos, después de haber identificado lo anterior es necesario realizar una plan de trabajo donde se estipulen políticas, acciones a realizar, sanciones y demás tareas para mantener seguro el activo.

Fundamentos de seguridad

La palabra seguridad proviene del latín *securitas*, y de acuerdo a la definición dada por Real Academia Española se describe como la ausencia de riesgo, daño o peligro, es decir, sobresale la propiedad de que algo que es seguro posee las características de ser: firme, cierto e infalible. Sin embargo, este término puede tomar diversos sentidos según el área o campo a la que haga referencia. En el área de la tecnología de la información, la seguridad se establece en el término *seguridad informática* y su definición es la siguiente:

"*La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable*."[2]

Dentro de la seguridad informática se encuentran los elementos y técnicas tanto en Hardware como en Software, así como los dispositivos físicos y medios humanos que ayudan a proteger que un activo se encuentre seguro. No obstante, estas medidas de seguridad que serán aplicadas no garantizan estar libres de algún riesgo, amenaza o vulnerabilidad, por lo que se vuelve transcendental definir lo siguiente:

- **Cuáles son los elementos o activos** que componen los recursos que deben protegerse, los cuales son considerados como fundamentales para el funcionamiento vital de la organización.

- **Cuáles son los peligros, amenazas y vulnerabilidades** a los que se podrían enfrentar aquellos activos que componen el sistema, dichas acciones pueden ser intencionales, accidentales o provocadas.

- **Cuáles son las acciones o planes de trabajo** que deben efectuarse para prevenir, disuadir, reducir o controlar todas aquellas acciones malintencionadas, así mismo se realiza un estudio para decidir qué mecanismos y servicios de seguridad ayudarán a proteger al máximo los activos informáticos.

[2] Seguridad informática, **Purificación Aguilera López, Introducción a la seguridad, Editex. Página 9**.

Todos estos elementos que conforman el sistema de información puede ser perturbados debido a fallas de seguridad, si bien suelen considerar a los datos como el elemento más importante y vulnerable debido a que este activo no siempre es recuperable, ocasionando daños irreversibles a las organizaciones. Otro factor que se vuelve importante a considerar es que la mayoría de los problemas de seguridad son ocasionados por el factor humano.

Existen dos tipos de seguridad: activa o pasiva, a continuación se detalla cada una de ellas.

- **Seguridad Activa**

Este tipo de seguridad consiste en proteger mediante un conjunto de defensas y mecanismos al sistema de información frente a posibles contingencias.

- **Seguridad Pasiva**

Son las medidas de seguridad implementadas que dan aviso a los administradores de red sobre riesgos que existen en el sistema. Su objetivo es dar aviso sobre algún acontecimiento sospecho que esté ocurriendo en la red. Si llegara a ocurrir alguna falla o ataque el impacto es el menor posible debido a que se activan los mecanismos de recuperación. La seguridad debe contemplar todo aquel origen de eventos que amenace al activo informático, por lo que considerar seguridad a nivel físico o material o seguridad a nivel lógico o software se vuelve importante para mitigar posibles ataques.

Seguridad Física

Se llama seguridad física a aquella que "consiste en la *aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*"[3].

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del área de cómputo, así como los medios de acceso remoto implementados para proteger el hardware y medios de almacenamiento de datos. En la Figura 2.22 se muestra un ejemplo de seguridad física.

Figura 2.22 - Control de acceso biométrico

[3] *(1) HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.org*

Seguridad lógica

La seguridad lógica se encarga de asegurar la parte del software de un sistema de información, que trabaja con todo lo que no es tangible, es decir, los programas y los datos. La seguridad lógica se encarga de llevar un control de acceso al sistema informático, desde el punto de vista de software, en donde tiene como objetivo revisar que los usuarios o procesos que desean establecer comunicación con los recursos del sistema sean las personas autorizadas y aunque es casi imposible asegurar al 100% la información, con ello se pretende utilizar ciertas medidas para evitar daños a la información o a la privacidad de ésta. En la Figura 2.23 se muestra el diseño de mecanismos y herramientas de seguridad lógica.

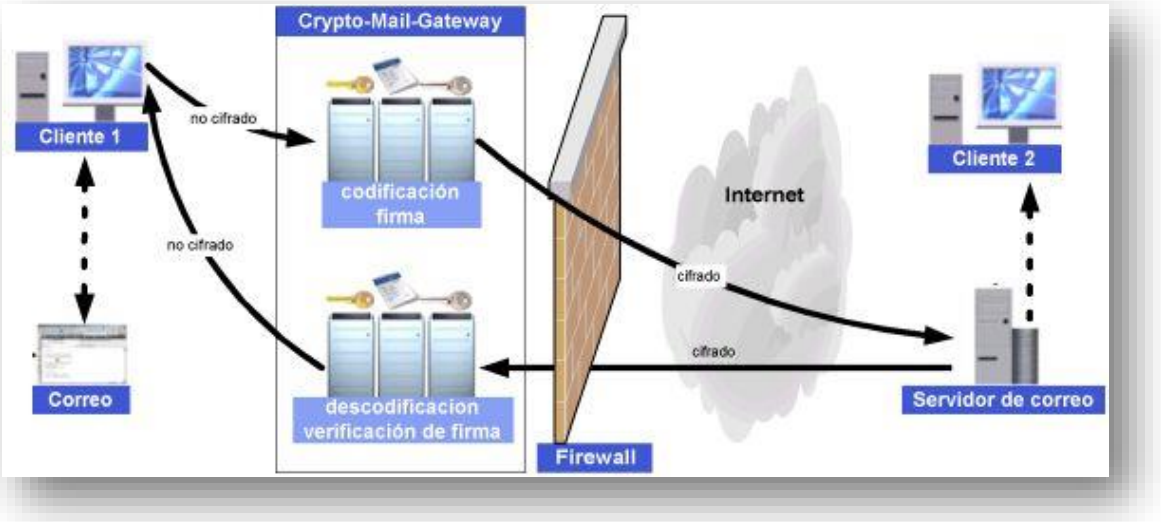


Figura 2.23 - Seguridad Lógica

Los daños producidos por la falta de seguridad, ocasionan pérdidas económicas, de credibilidad o de prestigio para la organización, su origen puede ser alguno de los siguientes:

-Fortuito: Son los errores cometidos accidentalmente ocasionados por los mismos usuarios, catástrofes naturales, averías en el sistema y demás.

-Fraudulentos: Son los daños causados por algún software malicioso, intrusos o por voluntad maliciosa de algún miembro de la empresa, robo o accidentes provocados con fines de lucro.

La seguridad informática debe cumplir con 6 servicios, los cuales son sumamente importantes ya que cada uno de ellos se refiere a todos los aspectos en los que debemos proteger nuestro sistema de información para considerarlo seguro. En seguida, se describe de manera detallada en qué consisten. En la Figura 2.24 se muestran los servicios de seguridad.

Figura 2.24 - Servicios de seguridad

- **Confidencialidad**

Es el servicio de seguridad que conforme a la OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus normas para la Seguridad de los Sistemas de información se define como: "El hecho de que los datos o información estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada." Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de la información son por ejemplo: el uso de cifrado de la información, uso de herramientas de control de acceso a los sistemas, y demás.

- **Autenticación**

La tarea de este servicio es confirmar que los usuarios sean quienes dicen ser, el cual asegura que la comunicación sea auténtica, esta es utilizada para proporcionar una prueba al sistema de que en realidad se es la entidad que se pretende ser. El sistema verifica la información que alguien provee contra la información que el sistema posee sobre ese usuario. Éste puede ser realizado a través de:

- Algo que se sabe: Es una contraseña, algún número de identificación. Al ingresar esta información al sistema, éste lo valida contra los datos que tiene almacenados en el sistema determinando si la autenticación es autorizada o no.
- Algo que se tiene: Es una tarjeta, una credencial, es algo que otorga la organización el cual es utilizado por el sistema para verificar la identidad del usuario.
- Algo que se es: Es una característica única e irrepetible, como por ejemplo la voz, el rostro, la huella digital, entre otros.

- **Integridad**

Este principio de seguridad garantiza la autenticidad, es decir, asegura que los datos no han sido alterados ni destruidos de modo no autorizado, es decir, permite comprobar que no se ha producido manipulación alguna en el mensaje original. La integridad de un mensaje se obtiene adjuntando al mismo otro conjunto de datos de comprobación de la integridad. Un ejemplo de ello es una función hash que genere una huella digital asociada a un mensaje es un mecanismo que aporta esta característica.

- **No repudio**

Es una transacción que no puede ser negada por ninguno de los intervinientes, es decir, este servicio proporciona al sistema de información una serie de evidencias irrefutables de la autoría de un hecho, un ejemplo de ello consiste en no poder negar haber originado una información que si emitió y en no poder negar su recepción cuando ha sido recibida.

- **Control de acceso**

Este servicio consiste en utilizar un proceso en el cual el sistema de información controla la interacción entre los usuarios y los recursos de red. Este mecanismo de seguridad permite implementar una política de seguridad, que está determinada por las necesidades y restricciones que la organización establece.

- **Disponibilidad**

Se encarga de garantizar el buen funcionamiento del sistema así como al accesos a sus servicios y recursos en todo momento. El programa MAGERIT lo define como "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado". Dicho servicio está unido a la fiabilidad de los componentes del sistema de información.

2.8 Identificación de amenazas y tipos de ataques

Cuando se habla de seguridad es necesario tener claro las diferencias entre que es una amenaza, vulnerabilidad y ataque, ya que es necesario identificar en que momento pasa cada una para dar frente y plantear una posibles solución. En los siguientes temas a tratar se definirá cada una de estos conceptos, así como las características que presenta cada una.

Amenaza

Es cualquier persona, circunstancia, evento o idea que pueden causar daño a un activo debido a una brecha existente en la seguridad. Las amenazas pueden clasificarse en:

- **Humana:** Este tipo de amenazas son iniciadas debido a la falta de conocimiento, negligencia o inconformidad de los usuarios finales respecto a las políticas establecidas por la organización.

- **Hardware:** se origina cuando existen fallas físicas en cualquier elemento del dispositivo que conforman al activo. Algunos de las amenazas identificadas de este tipo son: bajo rendimiento, pérdida del dispositivo físico por uso excesivo o funcionamiento incorrecto, entre otras.

- **De red:** Se refiere al tipo de amenaza que surge cuando el flujo de comunicación es interrumpido provocado por diversos factores como: flujo desmedido de información que circula a través del canal de comunicación, falla en algún dispositivo encargado de reenviar los datos o fallas en los medios de transmisión.

- **De tipo lógico:** Se presenta cuando alguna herramienta encargada de la seguridad de la red, ha sido implementada erróneamente, funciona inadecuadamente o no cumple con las expectativas de la seguridad necesarias para la organización. Al no cumplirse los puntos anteriores un atacante puede realizar robo de información, denegación de servicios y demás.

- **Desastres:** Son causadas por fuerzas naturales que no son controladas por el hombre tales como: incendios, terremotos, inundaciones y más.

Vulnerabilidad

Una vulnerabilidad es una brecha en un sistema que permite a un perpetrador comprometer la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Las vulnerabilidades son el resultado de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser

el resultado de las propias limitaciones tecnológicas. Las vulnerabilidades se clasifican en 6 tipos las cuales son:

- **Física:** Este tipo de vulnerabilidades se refiere al control de acceso físico al sistema.
- **Natural:** la vulnerabilidad natural se refiere a que grado puede verse afectado el sistema por desastres naturales o ambientales.
- **Hardware:** El no revisar las características de los dispositivos así como la falta de mantenimiento de estos, presenta una vulnerabilidad del tipo hardware.
- **Software:** El que un programa presente fallas o debilidades hace más fácil acceder a ellos y por lo tanto lo hace más vulnerable ante algún tipo de ataque que se puede presentar.
- **Red:** El mal planeamiento de una red no siguiendo los estándares de cableado estructurado y otro tipo de estándares, presentan una amenaza de riesgo potencialmente alta.
- **Humana:** Las vulnerabilidades de este tipo suelen ser las más comunes y las que menos se puede evitar ya que por más se traten de evitar no podemos cubrirse la mayoría algunos ejemplos de este tipo de vulnerabilidades pueden ser:

  - Ingeniería social
  - Mala comunicación con el personal
  - Contratar personas sin un perfil psicólogo y ético
  - El descuido

Ataque

Es la culminación de una amenaza, es decir, cuando una vulnerabilidad es aprovechada por un atacante para causar daño. Estas actividades pueden ser catalogadas en dos grupos:

- **Ataque activo:** Son aquellos que implica algún cambio en los datos, modificación en el flujo de información o la creación de un falso flujo de transmisión de datos.
- **Ataque pasivo:** Son en los que el atacante no realiza ninguna alteración en la información, es decir, solamente la observa, escucha, obtiene o monitorea mientras es transmitida.

Un ataque es clasificado en 4 categorías:

Interrupción: Un recurso del sistema es destruido o se vuelve no disponible. Ataque contra la disponibilidad. Se representa en la Figura 2.25.

Figura 2.25 – Ataque de Interrupción

Intercepción: Una entidad no autorizada consigue acceso a un recurso. Ataque contra la confidencialidad. Véase la Figura 2.26.

Figura 2.26 - Ataque de Intercepción

Modificación: Se lleva a cabo cuando un atacante logra modificar un activo atentando contra su integridad, en la Figura 2.27 se muestra un ejemplo de este tipo de ataque.

Figura 2.27 – Ataque de Modificación

Suplantación: Se presenta cuando una persona o proceso apócrifo se hace pasar por otro, por tal motivo este tipo de ataque está atentando contra la identidad. En la imagen 2.28 se ejemplifica este tipo de ataque.

Figura 2.28 – Ataque de Suplantación

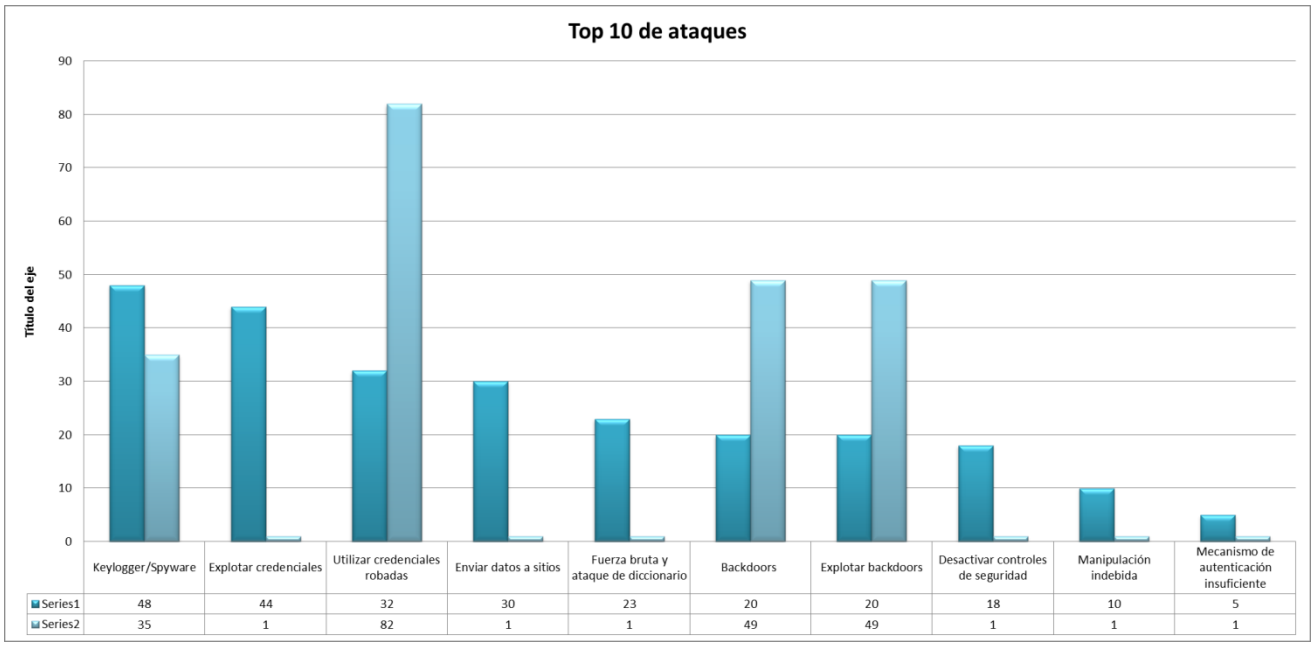
Tipos de ataques

Con el transcurso de los años, el avance en las tecnologías y las comunicaciones, han incitado el surgimiento de nuevas formas de ataque a los activos que son importantes para una empresa, actualmente Internet es uno de los medios preferidos por los atacante para efectuar este tipo de tareas.

A diferencia de lo que sucedía años atrás, donde un atacante debía tener amplios conocimientos en redes, informática y programación para ejecutar un ataque, hoy en día cualquier individuo que tenga acceso a un dispositivo con conexión a Internet puede realizar este tipo de acciones. Por tal motivo la seguridad física y lógica se vuelve crucial para mantener seguro los activos que se desean resguardar de amenazas internas o externas.

La principal preocupación que aqueja a las grandes y pequeñas empresas es saber si la red se encuentra preparada para enfrentar un ataque que pueda atentar contra los activos. Para ello los administradores de red deben estar constantemente actualizados en el ámbito de la seguridad, para saber qué nuevos ataques o amenazas han surgido.

Existen distintas consultorías que realizan publicaciones anuales con los ataques más utilizados, así como las vulnerabilidades a las que se encuentran expuestos los dispositivos que se encuentran en la red. Una de las consultorías que realiza este tipo de publicaciones es Verizon, que a principios del año 2012 publicó un documento en el cual enlista los principales ataques a los que están expuestas las grandes y medianas empresas. La información que se muestra en la Figura 2.29 muestra los principales ataques realizados durante el 2012.



	Keylogger/Spyware	Explotar credenciales	Utilizar credenciales robadas	Enviar datos a sitios	Fuerza bruta y ataque de diccionario	Backdoors	Explotar backdoors	Desactivar controles de seguridad	Manipulación indebida	Mecanismo de autenticación insuficiente
Series1	48	44	32	30	23	20	20	18	10	5
Series2	35	1	82	1	1	49	49	1	1	1

Puesto	Ataque	Categoría	% de Vulnerabilidad	% de Eventos Registrados
1	Keylogger/Farms-grober/Spyware	Malware	48	35
2	Explotar credenciales automátices o fáciles de adivinar	Hacking	44	1
3	Utilizar credenciales robadas	Hacking	32	82
4	Enviar daños a sitios /entidades externas	Malware	30	1
5	Fuerza bruta y ataque de diccionario	Hacking	23	1
6	Backdoors (permitir acceso/control remoto)	Malware	20	49
7	Explotar backdoor o canal de órdenes y control	Hacking	20	49
8	Desactivar o interferir con los controles de seguridad	Malware	18	1
9	Manipulación indebida	Fisico	10	1
10	Mecanismo de autenticación insuficiente	Hacking	5	1

Figura 2.29 – Top 10 Ataques Fuente: Verizon 2012

A continuación se detalla cada uno de los ataques que en el 2012 fueron los más concurridos.

Keylogger / Form-Grabber / Spyware - Empleo de credenciales robadas

Descripción	Malware que está diseñado para recopilar, vigilar y registrar acciones de los usuarios. Suele servir para reunir nombres de usuarios y contraseñas como parte de un ataque, también suele ser utilizado para capturar información de tarjetas bancarias en puntos de venta.

Puertas traseras (Backdoor)

Descripción	Son herramientas que proporcionan acceso remoto y control de los sistemas infectados. Las backdoors son capaces de superar los módulos de autenticación y otros mecanismos de seguridad normales y funcionan de manera encubierta.

Manipulación indebida

Descripción	La alteración o interferencia con el estado o el funcionamiento normal de un activo se refiere a métodos físicos más que alteraciones de la configuración del software o del sistema.

Phishing

Descripción	Es una técnica de ingeniería social en la que el atacante emplea una comunicación electrónica fraudulenta para convencer al usuario de que divulgue información, la mayoría de estos ataque parecen venir de una entidad legitima y lleva contenido que parece autentico, por lo regular este tipo de ataques se lleva a cabo mediante páginas web falsas.

Fuerza bruta

Descripción	Es un proceso automatizado que consiste en probar todas las combinaciones posibles de nombres de usuarios y contraseñas hasta encontrar alguna que de acceso al recurso

SQL Injection

Descripción	Es una técnica que explota la forma en la que las páginas web se comunican con la base de datos administrativa. El atacante puede inyectar en una base de datos comandos mediante los campos de entrada en un sitio web

Explotar credenciales automáticas y fáciles de imaginar

Descripción	Cuando una persona utiliza las contraseñas predeterminadas de algún programa que ha instalado o las contraseñas utilizadas son fáciles de adivinar debido a que no cumplen con los principios de seguridad para la creación de contraseñas seguras, el atacante aprovecha estas vulnerabilidades para tener acceso a los activos importantes para una empresa o persona.

Envío de datos a sitios

Descripción	La pérdida de información confidencial es uno de los principales problemas a los que se enfrentan las organizaciones, este tipo de ataque es originado por un atacante que se encuentra trabajando dentro de la empresa, el principal objetivo de este ataque es obtener información la cual puede ser utilizada con fines de lucro o extorsión.

Desactivar o inferir con los controladores de seguridad

Descripción	Cuando un usuario desactiva algún controlador que permite mantener seguro un activo, es aprovechado por el atacante para obtener información o hacer que el activo quede en estado de negación.

Políticas de seguridad informática

Las política de seguridad informática (PSI) definen las normas generales de una organización en materia de seguridad informática, en otras palabras, es la forma de dar a conocer tanto a los usuarios y administradores de la red, las reglas que el personal deberá seguir en relación con los recursos y servicios de red importantes para la organización. En ellas no se trata de describir técnicamente el funcionamiento de aquellos mecanismos de seguridad que van a ser empleados, ni de una expresión legal que involucre sanciones por alguna conducta, es más bien una descripción puntual de lo que deseamos proteger, de qué se va a resguardar y qué medidas van a ser tomadas para reducir al máximo cualquier conducta inadecuada.

Las políticas de seguridad son un conjunto de requisitos definidos por los responsables de un sistema, que indican en términos generales qué ésta y qué no está permitido en el área de seguridad durante la operación general del sistema, por lo que su diseño y redacción debe contener esta serie de características:

- Deben ser holísticas, es decir, debe cubrir todos los aspectos relacionados con la misma.
- Adecuarse a las necesidades y recursos.
- Ser atemporal.
- Definir estrategias y criterios generales que se adoptarán en distintas funciones y actividades.
- Cualquier política de seguridad ha de contemplar todos los elementos claves de la seguridad (Integridad, Disponibilidad, Confidencialidad, Control de acceso, No Repudio y Autenticidad).
- Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.
- Deben contemplar y evaluar los riesgos, el valor del sistema protegido y el costo de ser atacado
- Es importante adoptar el modelo "Todo lo que no esté específicamente prohibido está permitido" o "Todo está prohibido excepto lo que esté específicamente permitido".

Como se señaló anteriormente las PSI deben orientar las decisiones que se toman en relación con la seguridad. Por lo que se pide de una disposición de todos los miembros de la organización para conseguir una visión conjunta de lo que se considera primordial.
Las PSI han de considerar los siguientes elementos:

- Alcance de las políticas, es una invitación de la organización a todo el personal a reconocer la información como uno de sus principales activos.
- Objetivos y descripción clara de todos los elementos involucrados.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas a los cuales va a proteger el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios en relación a la información a la cual tiene acceso.
- Las PSI deben ofrecer explicaciones claras y comprensibles acerca de por qué deben tomarse ciertas decisiones así como transmitir por qué son importantes estos y otros recursos o servicios.
- Deben ser expresadas en un lenguaje en el que todas las personas involucradas puedan entender.

Y algo que se vuelve importante:

- Verificar el cumplimiento de la política, analizarla y perfeccionarla cada vez que se detecte un problema.

Sin embargo, antes de llevar a cabo el proceso de desarrollo de las políticas de seguridad de la información, es conveniente considerar la metodología que abordará puntos clave ya que en ellas se trata a las amenazas de la seguridad de la información y se especifican los procedimientos a adoptar en la organización. Para desarrollar una PSI se deben seguir estas cuatro fases, las cuales están interrelacionadas. Véase la Figura 2.30

Figura 2.30 – Fases de desarrollo de las políticas de información

1. Análisis y valoración de los riesgos

Esta fase consiste en realizar el análisis para identificar el estado en el que se encuentra la seguridad dentro de la organización y en ella se proponen medidas y controles que ayuden a cumplir los objetivos de negocio establecido. Su objetivo fundamental es determinar las amenazas a las que se encuentra susceptible la información, y los riesgos asociados a cada uno de ellos.

2. Construcción de las políticas

Esta fase se relaciona con el desarrollo de la política de seguridad y se centra principalmente, en conocer los contenidos adecuados de una política robusta, eficaz y eficiente. El documento en donde se definen las políticas de seguridad de la información debe distribuirse a todos los empleados y usuarios del sistema, así como asegurarse de su lectura.

3. Implementación de las políticas

En esta etapa se deben especificar todos los detalles de a quién, cuándo y dónde se aplica la política de seguridad de tal forma que se deben explicar los resultados esperados. En la Figura 2.31 se tiene el proceso de implementación.

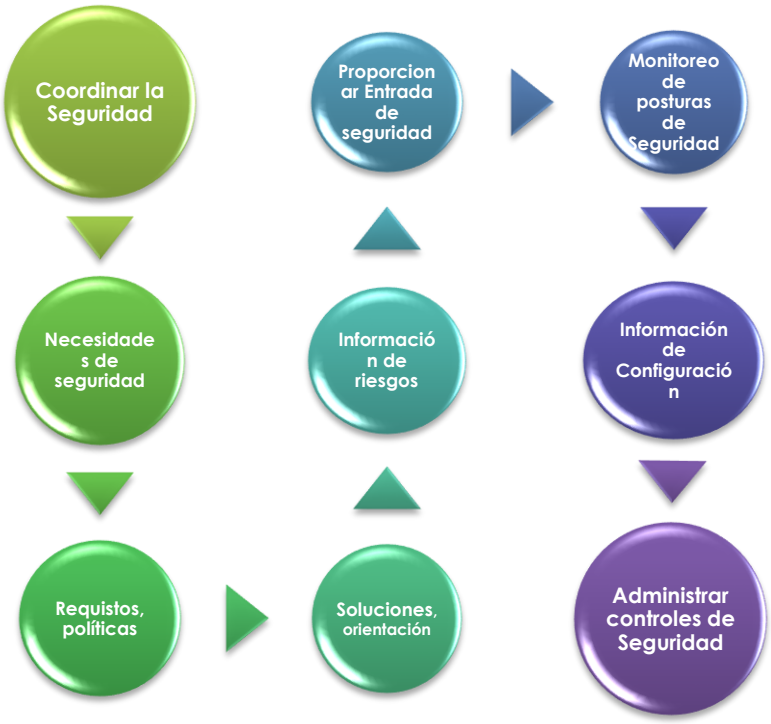


Figura 2.31 – Proceso de implantación de PSI

4. Mantenimiento de las políticas

En este módulo se establece que las PSI se deben de verificar y adecuar regularmente en relación a los avances tecnológicos, así como a la evolución de los ataques.

Mecanismos de seguridad

Los mecanismos de seguridad también conocidos como herramientas de seguridad o controles, son un conjunto de técnicas utilizadas para implementar un servicio, es decir, son aquellos que están diseñados para detectar, prevenir o recuperarse ante un ataque. Dichas herramientas efectúan varios servicios básicos de seguridad o combinaciones de ellos, en los que se especifica cómo deben ser ejecutados estos controles. Sin embargo, no existe un único mecanismo capaz de proteger a todo el sistema de información y debido a ello existen variados mecanismos dependiendo del método, de su función, del sistema y el factor de riesgo que lo amenazan.

Los mecanismos de seguridad con base en la norma ISO 7498-2 se pueden clasificar en general en dos categorías:

- **Mecanismos de seguridad generalizados,** no son específicos ni para servicios concretos. Un ejemplo de ellos son: responsabilidad-auditoría.
- **Mecanismos de seguridad específicos,** son utilizados para proporcionar servicios de seguridad como son: confidencialidad, integridad y autenticación, y son implementados en un nivel determinado de la arquitectura de comunicación en los siete niveles del modelo OSI.

De manera particular, los mecanismos también pueden ser clasificados por las acciones que realizan:

- **Disuasivos:** Este tipo de control trata de prevenir que se lleve a cabo una acción no autorizada mediante la concientización de las personas, colocando anuncios o letreros que prevenga al usuario que está violando alguna política de seguridad.
- **Preventivos:** Este mecanismo es el primer elemento con el cual se enfrenta un perpetrador cuando quiere realizar un ataque, por lo regular en una red este papel lo juegan los Firewall, antivirus, antiespam, y demás herramientas de seguridad.
- **Correctivos:** Cuando un ataque se culmina exitosamente, La principal tarea a la que se enfrenta el encargado de la seguridad en la red, es encontrar la solución al daño que se realizó durante el ataque. En la mayoría de las empresas una buena práctica es realizar respaldos de la configuración de los dispositivos, así como de la información de vital importancia, la cual puede ser restablecida si el perpetrador realizó algún cambio en la información o configuración.
- **De Detección:** Su función es identificar una amenaza antes de que esta se convierta en un ataque, para ello existen distintas herramientas como sistemas de detección de intrusos, Herramientas de correlación, IPS y demás.

Actualmente en el ámbito de la seguridad, existen distintas herramientas que ayudan a mantener segura y libre de amenazas la red de una empresa, para llevar acabo esto es necesario que los administradores de la red y los encargados de la seguridad se mantenga informados de cuáles son las herramientas líderes en el rubro que necesitan cubrir.

Para facilitar y determinar cuáles son las mejores herramientas existentes en la industria, se pueden consultar estudios realizados por empresas consultoras y de investigación de tecnologías de información, estas se encargan de realizar y proporcionar un análisis sobre que aplicaciones o tecnologías que actualmente existen en el ámbito de las rede y seguridad. Entre las empresas más importantes de consultoría y de investigación que realizan este tipo de estudios se encuentran: Gartner, IDC, NSS Lab, Infosec Institute, Frost and Sullivan, entre otra.

El método utilizado por Gartner es el denominado cuadrante mágico, el cual muestra de manera gráfica cuales son las mejores herramientas en el ámbito de las TIC. En la Figura 2.32 se observa un ejemplo del cuadrante mágico de Gartner respecto a Firewalls.

Figura 2.32 – Cuadrante mágico de Gartner

Bibliografía

Capítulo 2 Antecedentes de redes y seguridad

Gómez Joaquín. (2010). Servicios en Red España: Editex.

Romero María del Carmen, Barbancho Julio, Benjumea Jaime, Rivera Octavio y Ropero Jorge. (2010). Redes locales España: Paraninfo.

Herrera Enrique.(2003). Tecnologias y redes de transmision de datos México:Limusa

Boronat Fernando Seguí, Montagud Mario. (2013) Direccionamiento e interconexión de redes basada en TCP/IP : IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF Valencia: Universidad Politécnica de Valencia.

Díaz Gabriel, Alzórri Ignacio, Sancristóbal Elio, Alonso Manuel Castro. (2013**).** Procesos y herramientas para la seguridad de redes Madrid: Universidad Nacional de Educación a Distancia.

S.A.M Rizvi, V.K. Sharma. (2011). Introduction to computer networks.United Kindon: Oxford

Tanenbaum, Andrew S. (1996). *Computer Networks*. (Boston)Prentice-Hall.

Garcia Alfonso, Hurtado Cervigón, Alegre María del Pilar. (2011). Seguridad informática. Madrid: Paraninfo

Ganguly Debashis. (2012). Network and Application Security Fundamentals and Practices. USA: CRC Press Taylor & Francis Group.

Ramírez Sergio, Cervantes María. (2005). Introducción al IPv6. Universidad de la república Sitio web: http://www.rau.edu.uy/ipv6/queesipv6.html