UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Material de Apoyo para Redes de Datos Seguras

MATERIAL DIDÁCTICO

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Mauricio Urbina Garrido

ASESORA DE MATERIAL DIDÁCTICO

M. en C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2020

Introducción

Desde el comienzo de los tiempos, con la evolución del ser humano, han surgido necesidades entre los grupos formados. Una de las necesidades básicas es la de comunicarse para compartir y recibir información. Un ejemplo de forma de comunicación, que fue muy utilizada en el pasado, es el correo postal en el cual es necesario que todo emisor (remitente) redacte una carta en papel para ser enviada a través del sistema postal hacia el destinatario, para lo que el sistema se apoya de manera importante con la participación de carteros que entregan en el domicilio indicado la correspondencia que el sistema de correos ha enviado a la zona destino. Posterior a este sistema, se utilizó ampliamente el teléfono que fue patentado por Alexander Graham Bell en el año de 1876, y fue a través de éste que las comunicaciones entre dos lugares relativamente lejanos entre sí pudieron comunicarse de una forma más rápida, segura y eficaz.

Con el paso del tiempo, las formas de comunicarse han cambiado. Es así como las redes de datos que se fueron formando se adaptaron a las nuevas tecnologías con el propósito de mantenerse funcionales, y adicionalmente, tratar de mantener las comunicaciones seguras.

La forma de comunicación más importante para la época de los 60s y 70s, donde la tecnología avanzaba de manera rápida, fue la implementación de la red ARPANET, precedente de la Internet, cuya función era la comunicación entre cuatro nodos en la costa este de Estados Unidos. Ésta forma de comunicación fue evolucionando y actualmente es utilizada por distintos tipos de usuarios como universidades, empresas y gobiernos para la compartición de información y recursos.

En el presente trabajo, se muestran y definen los conceptos y los procesos actuales para el establecimiento de una comunicación a través de medios digitales, los cuales son la forma en que las redes de datos y comunicaciones se llevan a cabo alrededor de todo el mundo.

Otro aspecto importante, es la seguridad en el proceso e implementación de las redes de datos. Actualmente, la seguridad es un punto notable que se debe de considerar en cualquier fase de nuestra vida cotidiana. Sin embargo, en cuanto a las redes de datos se refiere, las comunicaciones pueden llevar consigo cualquier tipo de información, personal, militar o cuentas bancarias, por ejemplo. Es por esto que se considera necesario saber qué tipo de información circulará a través de la red para que, conociendo la importancia de la información, se implementen las medidas de seguridad necesarias a fin de proteger la información de terceros que no deben de tener acceso a ésta.

Así, el cuidado de las redes desde su instalación, configuración y gestión es una de las tareas primordiales que realizan los Ingenieros en Computación, y que desde su formación universitaria deben conocer y aprender.

Con este compromiso de formar recursos altamente calificados, es que en el plan de estudios de la carrera de Ingeniería en Computación se tiene la asignatura Redes de Datos Seguras y para que los estudiantes cuenten con material que les sea de apoyo y utilidad en su formación profesional en esta valiosa área del conocimiento es que se desarrolla el presente trabajo.

Este trabajo, que es un material de apoyo enfocado de manera particular en la asignatura antes mencionada, por los contenidos que la conforman y la manera en que son tratados, se tiene la confianza de saber que serán de mucha utilidad tanto para quienes cursen asignaturas relacionadas con las redes de datos seguras, como para los docentes que imparten asignaturas de áreas afines.

Cabe mencionar que, si bien las redes de datos son de suma importancia, estas deben ser administradas y gestionadas para que los recursos que se obtienen a través de ellas sean utilizados correctamente y aprovechados en su total, ya que, de no ser así, se corre el riesgo de que la red se alente, se vuelva insegura, e incluso deje de funcionar. Es por esto que se vuelve muy importante que se hable de la administración de redes, que si bien, no se trata en esta asignatura, es indispensable conocer de ella, motivo por el que se decidió incorporar un panorama general de la administración en un anexo de este documento.

Objetivo General:

El objetivo de este trabajo es desarrollar material de apoyo para alumnos y docentes de la carrera de Ingeniería en Computación, con el fin de que tengan un complemento a sus clases correspondientes a la asignatura de Redes de Datos Seguras y afines.

Así, para alcanzar el objetivo planteado es que el material está organizado por capítulos, y cada uno de estos está dedicado a un contenido que forma parte del plan de estudios de la asignatura. Para desarrollar los contenidos, se llevó a cabo una amplia investigación de los temas que componen a la asignatura, cuya bibliografía está referenciada en la sección de fuentes de información, y cabe mencionar que se buscó que las imágenes que aparecen en este documento fuesen principalmente de uso libre, sin embargo, es pertinente decir que en algunos casos se consideró que la imagen más representativa correspondía a una publicada en algún documento del cual se puso claramente la fuente de donde fue tomada esa imagen.

En el contenido del trabajo se encuentra en primer lugar el capítulo 1, en el que se definen conceptos y se muestran ejemplos sobre los distintos tipos de redes, su evolución en cuanto a cobertura, y los principales fundamentos sobre seguridad.

En el capítulo 2 se describen los estándares, arquitecturas y organismos de estandarización para redes de datos y seguridad, así como el modelo OSI y el modelo TCP.

En el capítulo 3 se describen los distintos medios de transmisión terrestres y aéreos, los estándares de la capa física del modelo OSI y el cableado estructurado, así como los distintos tipos de interconexión, siendo los más relevantes en esta capa el repetidor y el hub. Además, se hará un énfasis en las recomendaciones básicas para la instalación del cableado estructurado.

En el capítulo 4 se analizan los diferentes tipos de protocolos, métodos y estándares de la capa de enlace, así como su aplicación en dispositivos físicos de este nivel y la seguridad que es recomendable seguir para éstos.

En el capítulo 5 se describen y desarrollan ejemplos de métodos para el diseño y configuración de redes de datos seguras por medio de subneteo y protocolos de enrutamiento estático y dinámico.

En el capítulo 6 se definen los diferentes tipos de protocolos, métodos y estándares que se utilizan en la capa de transporte del modelo OSI, así como la relevancia de los protocolos TCP y UDP y los puertos lógicos.

En el capítulo 7, correspondiente a la capa de sesión se muestran los distintos tipos de servicios, como la transmisión de datos entre las capas de transporte y de presentación, así como la relevancia que tiene esta capa del modelo OSI.

En el capítulo 8 se analizan los distintos tipos de representación de datos, así como técnicas de compresión y cifrado de éstos para mantener la seguridad de la información.

En el capítulo 9, correspondiente a la capa de aplicación del modelo OSI, se describen los servicios web, así como los distintos protocolos para la compartición y transferencia de archivos, sesión remota entre dispositivos, protocolos de autenticación y mecanismos de seguridad en esta capa.

Adicionalmente, se incluyen dos anexos, el primero de ellos que trata sobre la administración de redes y que ya se comentó su importancia, y el segundo que contiene material referente al cableado estructurado, mencionando las características más importantes a considerar, así como recomendaciones en la implementación.

Cabe mencionar que los materiales fueron revisados por un grupo de estudiantes quienes emitieron su opinión al respecto y se realizaron modificaciones con base en los comentarios recibidos.

Finalmente, las conclusiones muestran los resultados de la elaboración y utilización de este material de apoyo a la docencia.

Índice temático.

Índice Temático

Índice temático.

Índice temático.

Índice de Figuras

Índice temático.

Índice temático.

Índice temático.

Índice de Tablas

Tema 1

Conceptos básicos

Objetivo: El alumno explicará las funciones principales de las redes de datos a través de las típicas estructuras y posibles formas de enviar información, así como los conceptos básicos de seguridad.

1.1 Redes de comunicaciones de datos. Panorama general.

¿Qué es una red de datos?

Una red de datos es un conjunto de dispositivos y software conectados entre sí mediante vías o medios de transmisión que comparten recursos, datos e información entre ellos de manera segura, eficiente y confiable. Su objetivo es brindar confiabilidad a la información, obtener una buena relación costo/beneficio y la transmisión de usuarios distantes de manera segura, eficiente y confiable. Una red de datos debe de ser capaz de procesar, generar, almacenar, distribuir y compartir datos y recursos. En la figura 1.1.1 se pueden observar distintos ejemplos de redes de datos implementadas en distintas áreas.

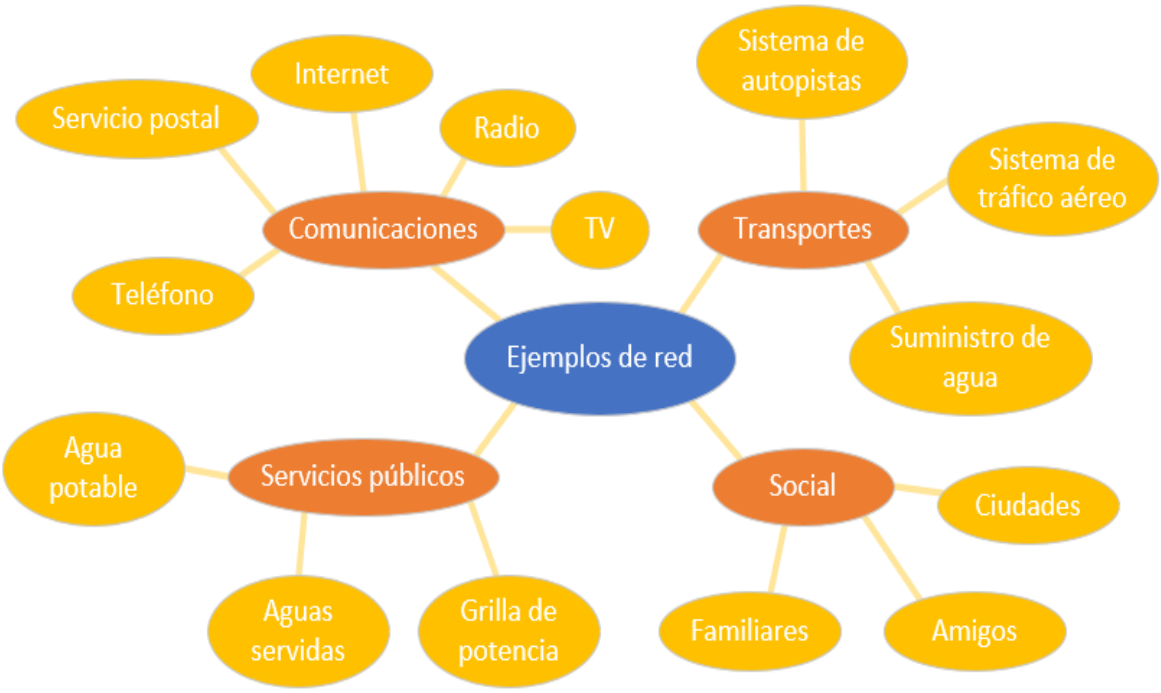


Figura 1.1.1. Ejemplos de redes en distintas áreas.

Las estructuras de las redes de datos están basadas en estándares y protocolos. De acuerdo a su implementación, será el diverso uso de aplicaciones que se le puedan dar. Existen estándares específicos para lugares comerciales, empresas, edificios o para usos básicos como compartir archivos de texto o multimedia. En la figura 1.1.2 se representa una red de datos que conecta una red local de computadoras que a la vez requiere del servicio de correo electrónico.

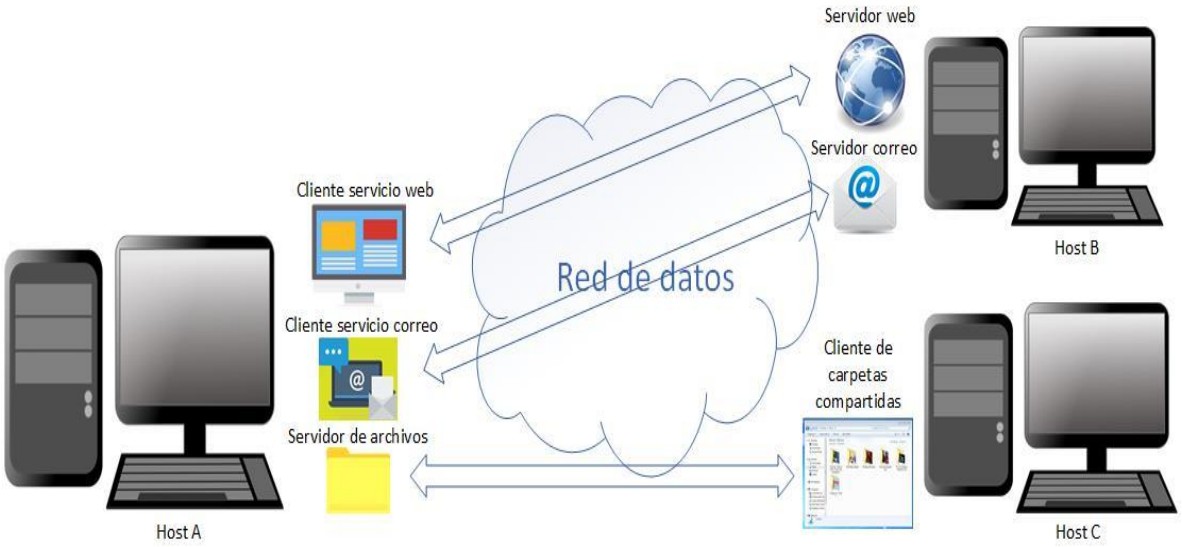


Figura 1.1.2. Red de datos para servicio de email.

De acuerdo a su uso, también es como se considera la forma física de implementación y el tipo de seguridad que se configurará para la red. Por ejemplo, en una red interna, esto es, la red de un usuario, empresa, u organización, se puede usar un servidor o un equipo de cómputo que controle y monitoree a todas las demás para el uso de recursos o para compartir datos, tal como se muestra en la figura 1.1.3.

Figura 1.1.3. Ejemplo de una red interna.

Algunos ejemplos de implementación de redes para diversos propósitos pueden ser:

Una red global implementada de acuerdo a las necesidades de una gran compañía, la cual requiere contar con comunicación entre sus diversas sucursales a lo largo del mundo en diferentes países. La red puede ser utilizada para comunicación, compartir datos estadísticos, financieros, o de productividad, entre otros. Una posible representación de alguna empresa puede verse ejemplificada en la figura 1.1.4.

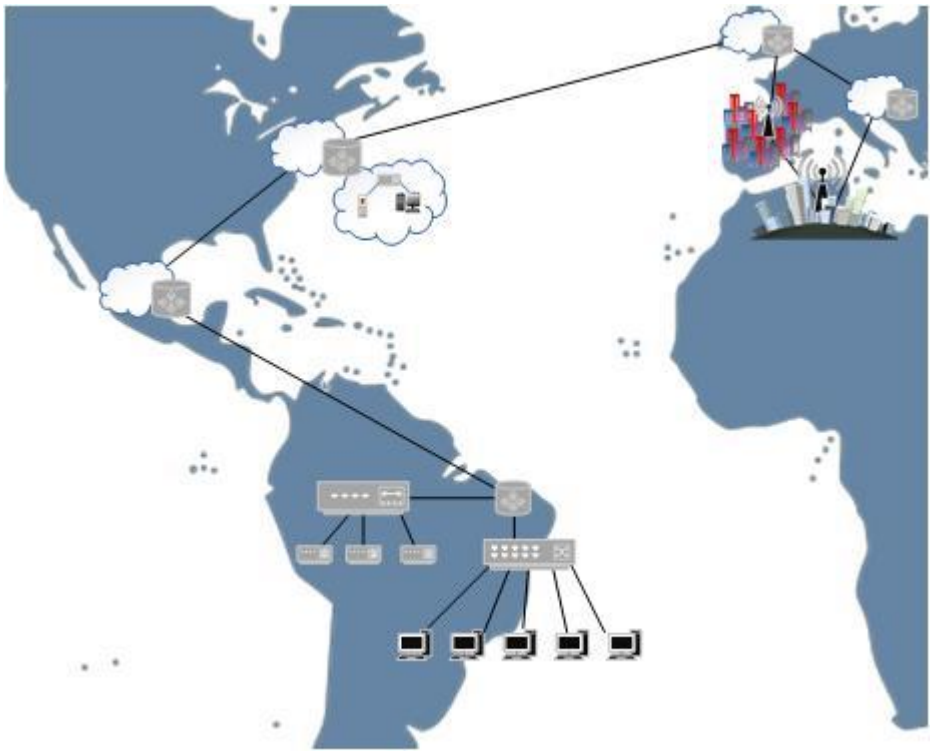


Figura 1.1.4. Ejemplo de una red global.

Una red interna en las oficinas de una empresa, la cual puede tener un controlador central de acuerdo al departamento que se maneje (por ejemplo, ventas, producción, atención al cliente). La red se diseñará de acuerdo a las necesidades de la empresa para que ésta pueda compartir sus datos internamente. Un ejemplo de esta implementación está representado en la figura 1.1.5.

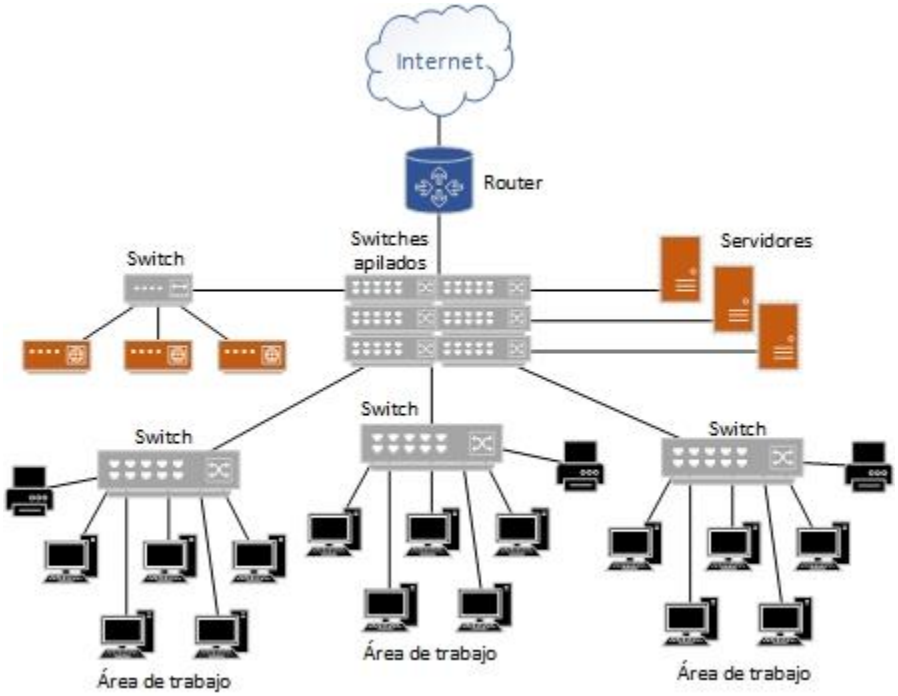


Figura 1.1.5. Ejemplo de una red interna de oficinas.

Elementos de una red de datos.

Dispositivos. Hay de dos tipos de acuerdo a su función:

- Dispositivos para gestionar el acceso y las comunicaciones en una red, regularmente al proveedor de servicios de internet (ISP).
- Dispositivos de usuario final, es decir, todos los equipos que los usuarios utilizan para conectarse a la red a fin de hacer uso de ella.

Medio. El medio es la conexión que hace posible que los dispositivos se relacionen entre sí. Los medios de transmisión de datos o medios de comunicación en redes pueden clasificarse por tipo de conexión como guiados o no guiados.

Información. Comprende todo elemento intercambiado entre dispositivos, y se refiere a los datos de interés para el usuario final, así como los requeridos para el establecimiento de la transmisión, así, son los datos tanto de gestión de acceso y comunicación, como de usuario final (texto, imágenes, música, video, entre otros).

Recursos. Un recurso es todo aquel elemento que forma parte de la red, y que puede ser identificado y accedido directamente. Puede tratarse de un recurso físico para la comunicación del usuario con la red o de un recurso lógico, tales como archivos compartidos en otra computadora dentro de la red o un servicio que se desea consumir, como está representado en la figura 1.1.6.

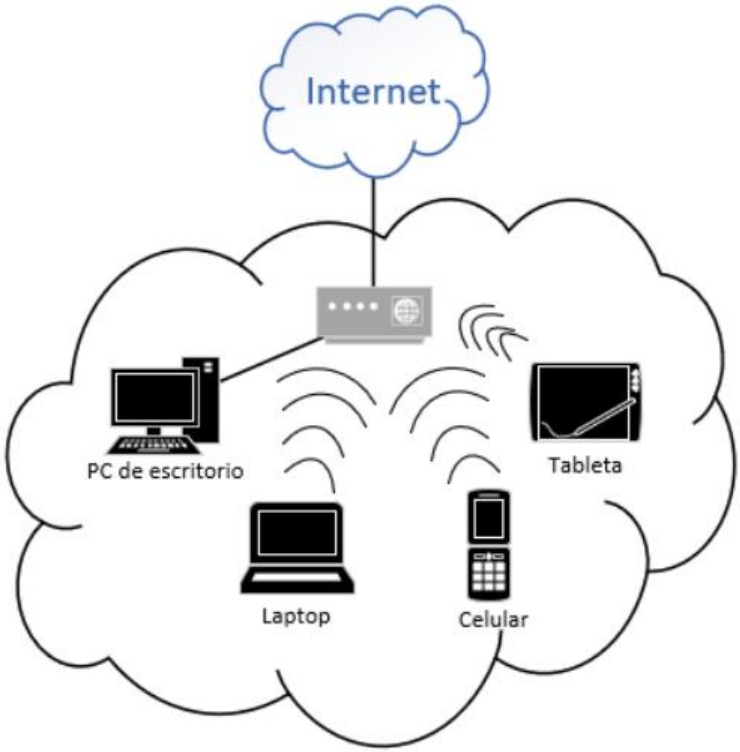


Figura 1.1.6. Red doméstica o residencial.

1.2 Beneficios de las redes locales. Usos y aplicaciones.

Una red de área local, es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, y escuelas, por ejemplo.

Beneficios

- Acceso simultáneo a programas e información.
- Equipos periféricos compartidos (impresoras, escáner, entre otros).
- Comunicación personal más eficiente (email, foros, entre otros).
- Procesos de respaldo más efectivos.
- Permite mejorar la seguridad y control de la información que se utiliza.

1.3 Topologías. Importante consideración de diseño.

La topología es la forma en que los dispositivos que forman parte de la red están conectados entre sí. Los diversos tipos de topologías que existen son los siguientes:

a) Estrella. Los equipos de la red están conectados a un nodo central y todas las comunicaciones se han de hacer necesariamente a través de éste. Su estructura se representa en la figura 1.3.1.

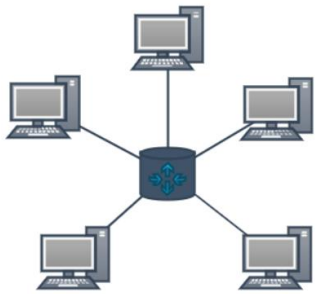


Figura 1.3.1. Red en estrella.

Toda topología según la interconexión de los dispositivos presenta ventajas y desventajas, en este caso se presentan en la tabla 1.3.1.

***Tabla 1.3.1. Ventajas y desventajas de una red en topología estrella*.**

Ventajas	Desventajas
● Si un equipo falla, se desconecta del nodo central sin afectar el rendimiento de la red. ● Agregar o quitar equipos a la red es muy sencillo. ● Es de mejor organización.	● Si el nodo central falla, esto imposibilita la comunicación entre los equipos de la red. ● El crecimiento de la red depende directamente de la capacidad del nodo central para aceptar más equipos conectado a él.

b) Árbol. La conexión en árbol es parecida a una serie de redes en estrella interconectadas entre sí, de ahí que también reciba el nombre de estrella o de estrellas o estrella jerárquica. Tiene un nodo de enlace troncal desde el que se ramifican los demás nodos. Su estructura se representa en la figura 1.3.2 y sus ventajas y desventajas en la tabla 1.3.2.

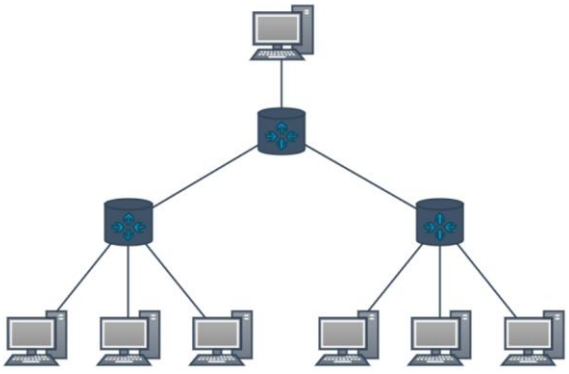


Figura 1.3.2. Red en árbol.

Tabla 1.3.2. Ventajas y desventajas de una red en topología árbol.

Ventajas	Desventajas
• Permite priorizar y aislar las comunicaciones de distintas computadoras.	• Si falla un nodo o enlace de nivel superior, la sección entera queda aislada del resto de la red. • Si el segmento principal falla, se viene abajo toda la red.

c) Anillo. Esta topología consiste en que cada dispositivo se comunica directamente con otros dos presentes en la red, y así todos los dispositivos que la forman se comunican formando un círculo. La información viaja de nodo a nodo, y cada uno de estos a lo largo del "anillo" maneja cada paquete de datos. Su estructura se representa en la figura 1.3.3 y sus ventajas y desventajas en la tabla 1.3.3.

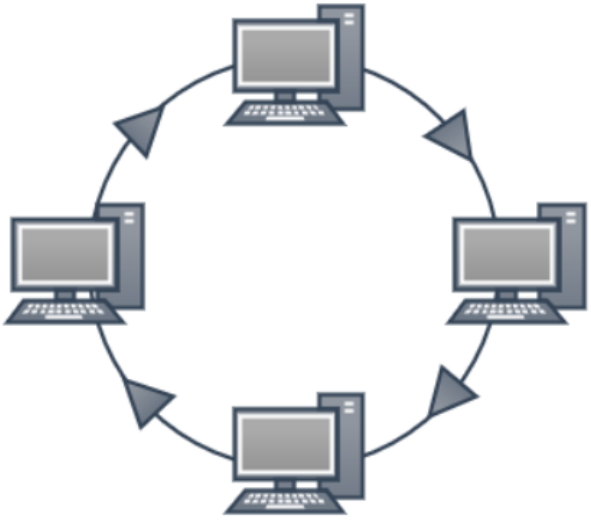


Figura 1.3.3. Red en anillo.

Tabla 1.3.3. Ventajas y desventajas de una red en topología anillo.

Ventajas	Desventajas
● Cada equipo actúa como un repetidor, regenerando la señal y enviándola al siguiente equipo conservando la potencia de la señal. ● Los datos fluyen en una sola dirección.	● Si falla un canal entre dos nodos, falla toda la red. ● Conforme aumenta el número de equipos participantes aumenta el tiempo de transmisión. ● Todos los nodos “ven” la información que circula por la red.

d) Bus. Todos los equipos están conectados a la misma línea o medio de transmisión de datos mediante un cable. Su estructura se representa en la figura 1.3.4 y sus ventajas y desventajas en la tabla 1.3.4.

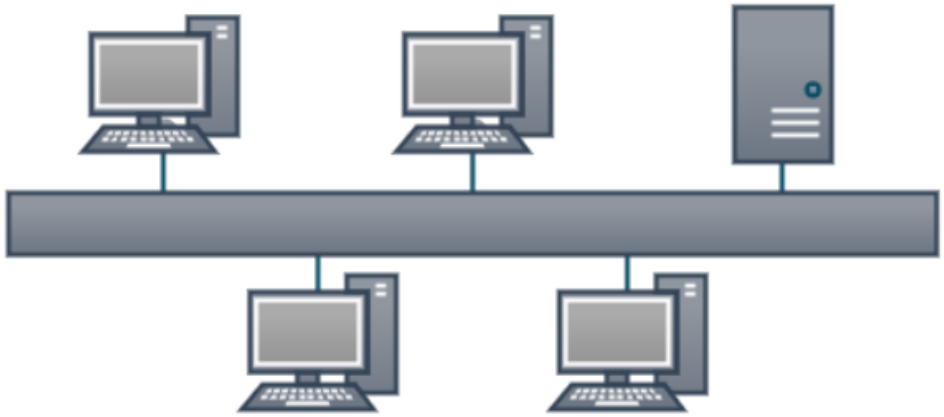


Figura 1.3.4. Red en bus.

Tabla 1.3.4. Ventajas y desventajas de una red en topología bus.

Ventajas	Desventajas
● Facilidad de implementación y funcionamiento.	● Altamente vulnerable, si una conexión es defectuosa, se afecta toda la red. ● Si el número de equipos conectados al bus es grande, puede afectar el rendimiento de la red.

e) Malla. Cada nodo está conectado a los demás nodos. De este modo es posible llevar los mensajes de un nodo a otro por un camino directo y sin escalas. Su estructura se representa en la figura 1.3.5 y sus ventajas y desventajas en la tabla 1.3.5.

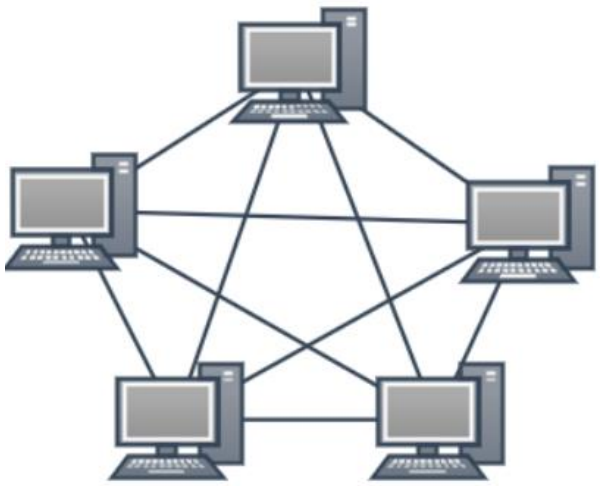


Figura 1.3.5. Red en malla.

Tabla 1.3.5. Ventajas y desventajas de una red en topología malla.

Ventajas	Desventajas
• Si un medio de transmisión falla, otro transporta el tráfico y la red sigue funcionando. • Proporciona múltiples rutas a través de la red. • Si un cable o nodo falla o desaparece, no afecta en absoluto a los demás nodos.	• Requiere más enlaces de comunicación en comparación de otras topologías, por lo que puede resultar más costosa. • Los equipos de cómputo deben tener una alta capacidad de comunicación y procesamiento de datos para soportar la conexión con todos los equipos de la red.

f) Híbrida. Combina características de dos o más tipos de topologías diferentes, y regularmente esto ocurre al interconectar diferentes redes entre sí. Su estructura se representa en la figura 1.3.6 y sus ventajas y desventajas en la tabla 1.3.6.

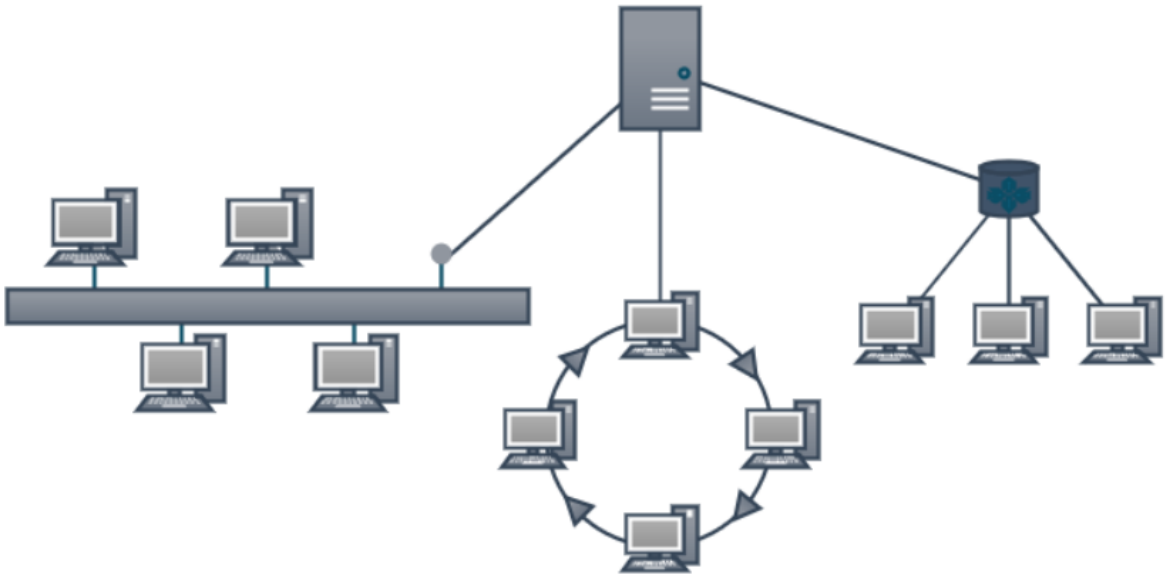


Figura 1.3.6. Red híbrida.

Tabla 1.3.6. Ventajas y desventajas de una red en topología híbrida.

Ventajas	Desventajas
• Si un solo equipo falla, no afecta al resto de la red.	• Si una parte de la red está en estrella y falla su nodo central, se afecta a esa parte de la red.

1.4 Evolución de las redes de datos. Principales características: cobertura geográfica, velocidad, control de errores, enlaces, historia ALOHA y X.25.

LAN (Red de Área Local – Local Area Network)

Las redes de área local suelen ser redes limitadas a la conexión de equipos dentro de un único espacio, oficina, piso, edificio o conjunto de edificios cercanos entre sí, y que estos son de propiedad privada. La figura 1.4.1 representa un ejemplo una red LAN de un edificio para oficinas.

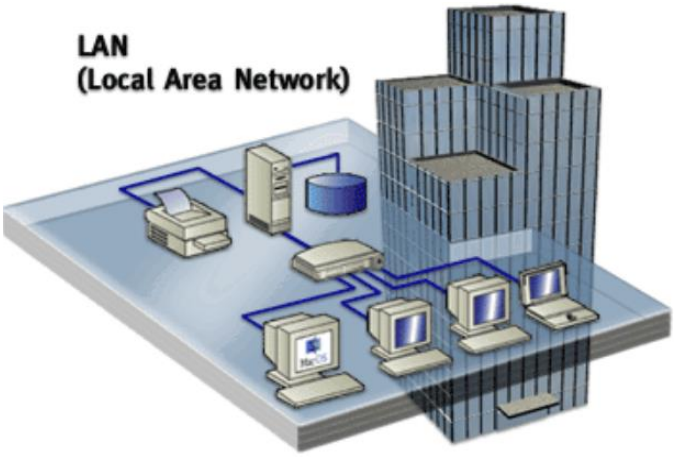


Figura 1.4.1. Red LAN.

MAN (Red de Área Metropolitana – Metropolitan Area Network)

Las redes MAN están diseñadas para la conexión de equipos para dar cobertura a una ciudad entera o campus. Una red MAN puede ser una única red que interconecte varias redes de área local LAN's resultando en una red mayor como por ejemplo el campus de Ciudad Universitaria. La figura 1.4.2 representa la conexión de redes LAN dentro de una ciudad para comunicarse entre sí.

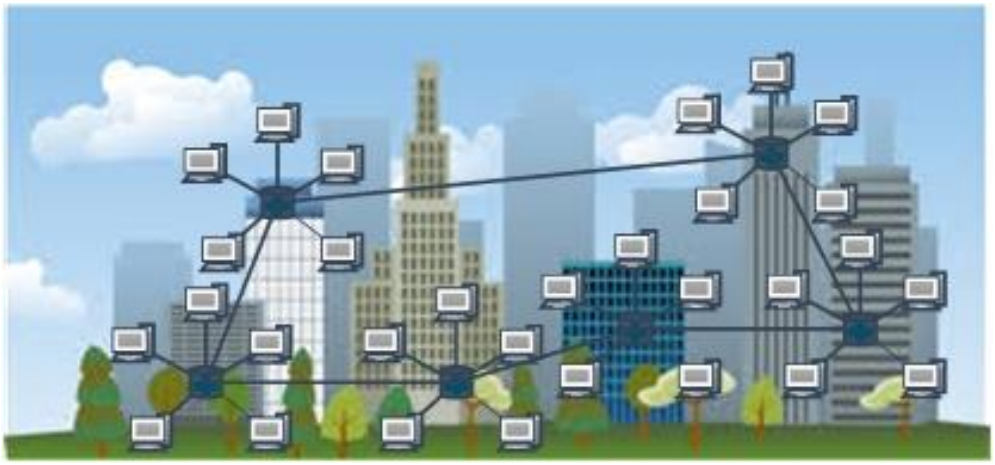


Figura 1.4.2. Red MAN.

PAN (Red de Área Personal – Personal Area Network)

Las redes de Área Personal son las de menor tamaño, son de alcance muy limitado y se utilizan para interconectar dispositivos personales muy cercanos entre sí y de manera inalámbrica, tal y como se representa en la figura 1.4.3.

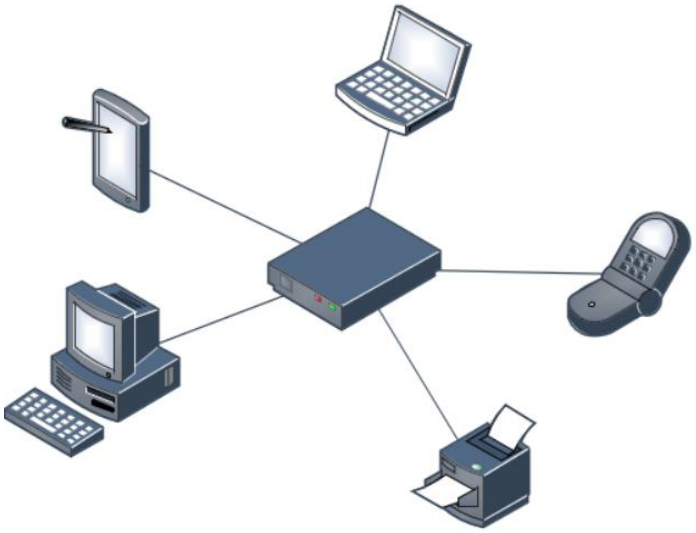


Figura 1.4.3. Red PAN.

WAN (Red de Área Amplia – Wide Area Network)

Las redes WAN son aquellas que proporcionan un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional), tal y como se representa en la figura 1.4.4. Una red WAN generalmente está conformada por redes de servicio público y redes privadas y pueden extenderse alrededor del globo terráqueo.

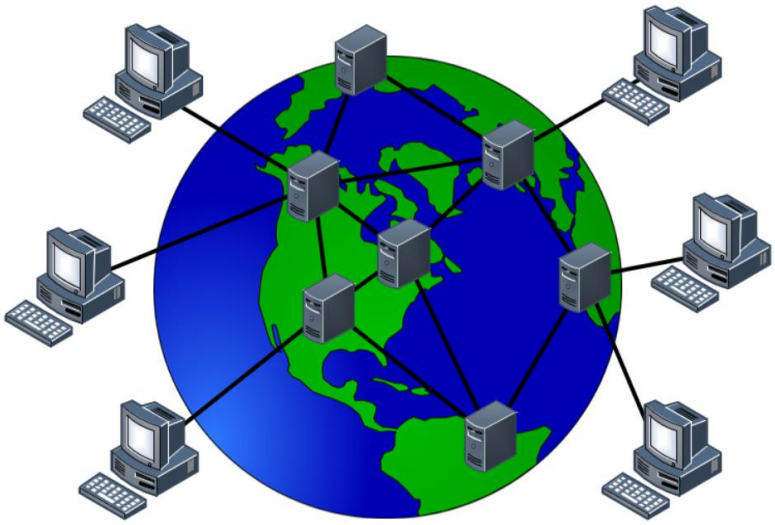


Figura 1.4.4. Red WAN.

GAN (Red de Área Global – Global Area Network)

Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Area Networks) y las agrupan mediante cables submarinos internacionales o transmisión por satélite. Una representación de este tipo de red se puede observar en la figura 1.4.5.

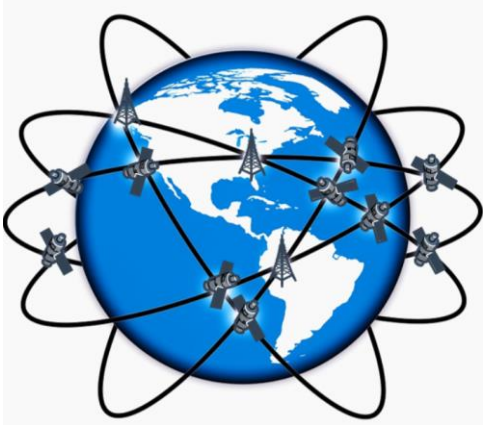


Figura 1.4.5. Red GAN.

VLAN (Red de Área Local Virtual – Virtual LAN)

Es un método para crear redes virtuales dentro de una misma red física. Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectadas al mismo conmutador, aunque se encuentren físicamente conectadas a diferentes segmentos de una red de área local (LAN) y esto gracias a la configuración que se hace en cada switch, tal y como se trata de representar en la figura 1.4.6.

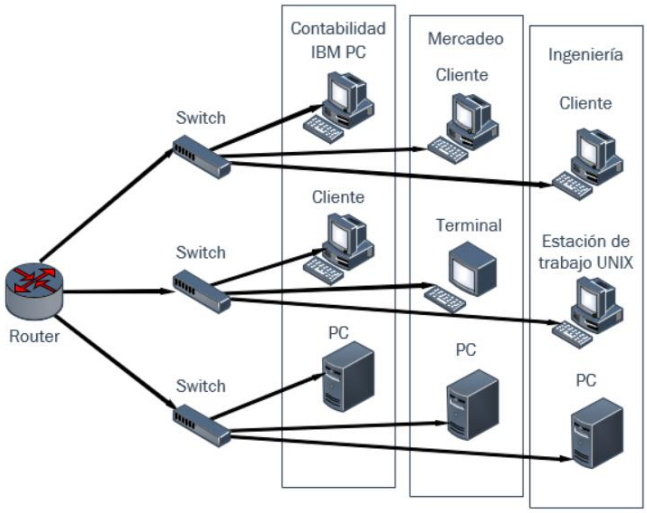


Figura 1.4.6. Red VLAN.

A continuación, se muestran en la tabla 1.4.1 la cobertura geográfica de cada uno de los tipos de redes mencionados.

Tabla 1.4.1. Cobertura geográfica de las redes.

Tipo de red	*Distancia entre procesadores de red*	*Área que cubre el tipo de red*
PAN	1 – 5 metros	m^2
LAN	5 metros – 1km	habitación – edificio conjunto de edificios cercanos entre sí
MAN	1 kilómetro - 10 kilómetros	campus – ciudad
WAN	100 kilómetros - 1000 kilómetros	país – continente
GAN	Más de 1000 km	mundo

Existen diferentes tipos de enlaces para la comunicación entre un nodo de una red con otro dispositivo de la misma red. Dichos tipos de enlaces son:

Enlace punto a punto. Normalmente se refiere a redes en las que el intercambio de datos se realiza entre dos puntos específicos de la red de manera directa. Si se trata de una red cableada es precisamente el cable de conexión que enlaza dos equipos entre sí como se vio en la topología en anillo, en tanto que si se trata de una inalámbrica estos puntos pueden ser las antenas de wifi, de radiofrecuencia o de telecomunicaciones, como se muestra en la figura 1.4.6.

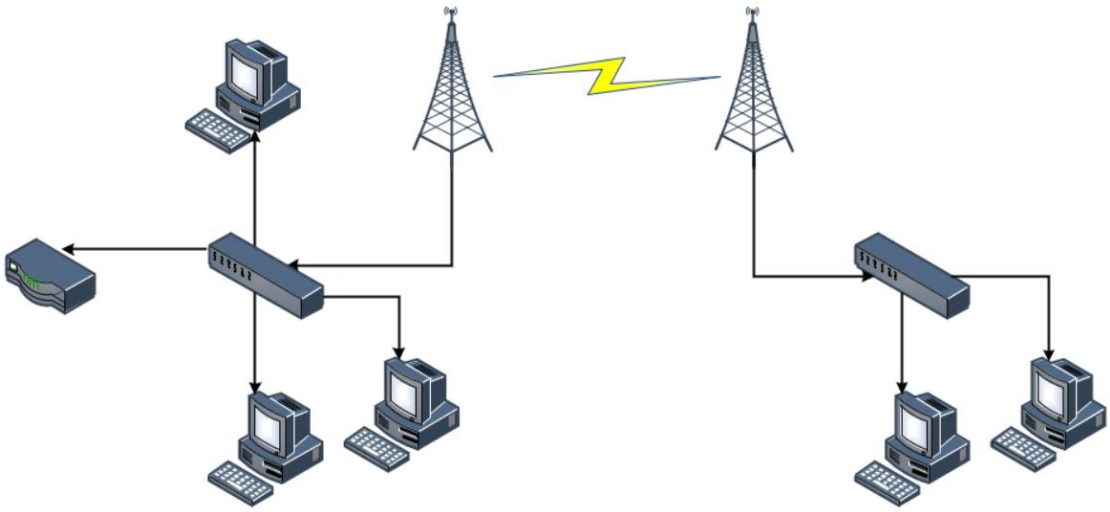


Figura 1.4.7. Enlace punto a punto.

Enlace Multipunto. Normalmente se refiere a redes en las que el intercambio de datos se realiza desde un punto hacia el resto de los elementos o puntos que conforman la red, y viceversa, esto es, todos los puntos pueden comunicarse con el elemento central como en la topología en estrella cuando se trata de una red cableada, o como se aprecia en la figura 1.4.7 cuando se trata de una red inalámbrica.

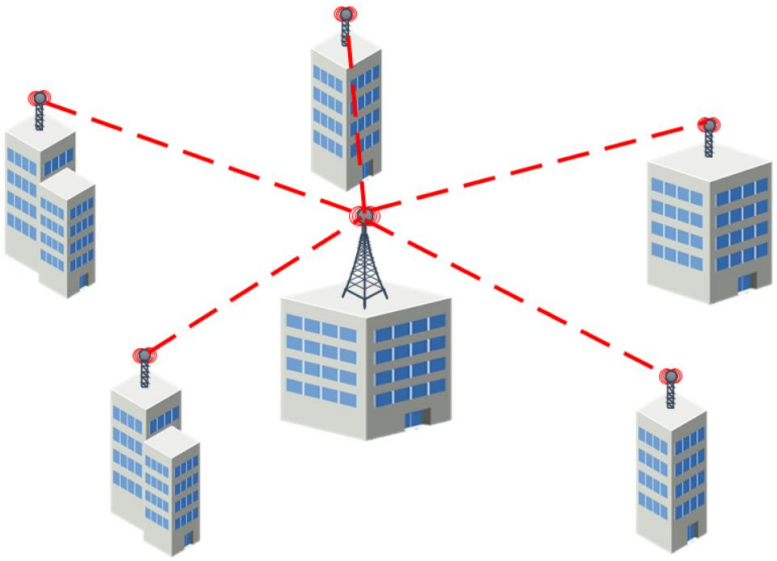


Figura 1.4.8. Enlace multipunto.

La comunicación entre dos nodos terminales de la red sólo puede darse de dos formas distintas:

Half Dúplex. Sólo se puede enviar información en un solo sentido a la vez, es decir, sólo un nodo a un tiempo puede estar enviando información al otro nodo, y si el otro nodo requiere enviar información también, éste debe de esperar a que termine el proceso para que se libere el canal de envío de información y pueda enviar la información que requiere (véase figura 1.4.8).

Figura 1.4.9. Comunicación half dúplex.

Full Dúplex. En comparación con half dúplex, el envío de información puede ser simultáneo entre dos nodos, es decir, no tienen que esperar a que la transmisión del otro nodo termine para enviar la suya (véase figura 1.4.9).

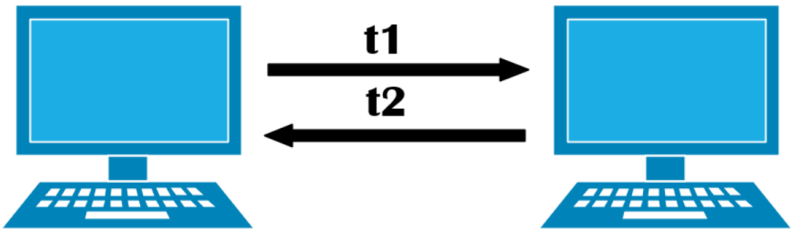


Figura 1.4.10. Comunicación full dúplex.

1.5 Fundamentos de seguridad

La seguridad informática se define como el conjunto de métodos y herramientas destinados a proteger los sistemas ante cualquier amenaza.

Consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red.

Las medidas de seguridad de cualquier red de datos de forma generalizada implican las siguientes medidas:

- **Autenticación.** Confirma que la identidad de una o más entidades conectadas a una o más entidades sea verdadera.
- **Control de acceso.** Provee protección contra uso no autorizado de los activos de un sistema, permitiendo que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.
- **Confidencialidad.** Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.
- **Integridad.** Asegura que los datos almacenados en los equipos y/o transferidos en una conexión no sean modificados.
- **Disponibilidad.** Asegura que la información sea accedida cuando se requiera por la gente, sistema o proceso con acceso a ella.
- **No repudio.** Este servicio protege contra usuarios que quieran negar falsamente haber enviado o recibido un mensaje.

Tres de estos aspectos conforman la “Triada de la seguridad de la información”, éstos son confidencialidad, integridad y disponibilidad. Su representación puede verse en la figura 1.5.1.

Figura 1.5.1. Triada de la seguridad de la información.

Seguridad física

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema.

Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos deliberados.

Estas medidas se pueden ver en los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Seguridad lógica

Se refiere a que la información sólo pueda ser accedida parcialmente según el puesto de la persona, de modo que solo el administrador del sistema y alguno otro alto funcionario tenga acceso completo, eso previene fraudes y otros daños.

Algunas de las medidas de seguridad más comunes para la protección de los datos e información de una de red de dato son:

- Firewalls (sistema que protege a un ordenador o red de ordenadores contra intrusiones)
- Proxys (bloqueos por dominio e IP's)
- IDS (Sistema de Detección de Intrusos)
- IPS (Sistema de Prevención de Intrusos)
- Soluciones anti spam
- Antivirus

Es recomendable establecer múltiples capas de seguridad, ya que, si un incidente llegara a ocurrir, exista un mayor número de elementos preventivos que protejan a la información.

Conceptos generales

A continuación, se definen los conceptos más utilizados en el área de la seguridad informática.

Seguridad. Conjunto de protecciones que permiten resguardar un bien.

Atacantes. Individuo o elementos que amenazan contra la integridad y seguridad de un activo o un sistema.

Ataque: Acciones organizadas e intencionadas causadas por una o más entidades para ocasionar daño o problemas a un sistema o red.

Amenazas. Todo aquello que puede causar daño, modificación o pérdida en los activos de una organización.

Incidente: Es cualquier evento que afecte la continuidad del negocio y atente contra la confidencialidad, integridad o disponibilidad de la información.

Activo de información. Es todo aquello con valor para una organización y que necesita protección, tales como información, aplicaciones, procesos, servicios, infraestructura y personal.

Vulnerabilidad. Es un defecto o falla de seguridad en los sistemas que una o varias amenazas podrían aprovechar para causar un posible daño a ciertos activos o a toda la organización.

Vulnerabilidad de día cero. Son desconocidas por el fabricante (de una aplicación o sistema) y sus usuarios, hasta el día que se presentan los ataques dirigidos.

Riesgo. Posibilidad de la ocurrencia de un evento no deseado. En seguridad informática, es la probabilidad de que una amenaza logre explotar una vulnerabilidad, representando un impacto a la organización. El riesgo está presente mientras no se corrija la vulnerabilidad o, de ser posible, se erradique la amenaza.

Impacto. Consecuencias o efecto producido por un ataque.

Mecanismos de seguridad. Dispositivos o elementos para resguardar la información entre la red privada y la red externa.

Seguridad perimetral. Abarca equipos que van desde el último punto de administración hasta las estaciones finales.

En muchas ocasiones, los ataques a sistemas de seguridad son realizados por programas de computadora, llamados scripts, realizados con ese propósito. Para estos casos, existen términos especiales, los cuales son los siguientes:

Exploit. Es el medio que un atacante utiliza para aprovechar una vulnerabilidad con la finalidad de atacar un activo. Puede ser una secuencia de comandos o un fragmento de datos.

Payload. Son las acciones posteriores a explotar una vulnerabilidad. Generalmente son tareas automatizadas para un determinado objetivo.

Shellcode. Es una secuencia de bytes (opcodes) que representan instrucciones en ensamblador. Son parte esencial de muchos exploits, puesto que representan el payload. Se usa para ejecutar un código arbitrario, aunque históricamente se emplea para abrir un Shell en el sistema vulnerado.

Tema 2

Estándares y arquitecturas

Objetivo: El alumno explicará los estándares y protocolos de redes de datos a través de los diferentes modelos de comunicaciones y de seguridad

Estándares. Normas que permiten implementar, brindar o apoyar en un objetivo particular; y deben seguirse para que se cumpla de la mejor forma posible el objetivo.

Permiten la comunicación entre diferentes tipos de equipos e incrementan el mercado para los productos que se apegan a las normas establecidas.

Normas de facto (del hecho). Son normas que aparecieron y se desarrollaron sin ningún plan formal.

Normas de jure (por ley). Estándares formales y legales adaptados por algún organismo de estandarización autorizado.

2.1 Organismos de estandarización. Objetivos, miembros, grupos de trabajo, organismos, etc.

Existen estándares nacionales e internacionales para la implementación de redes. Dichos estándares son regulados por las siguientes organizaciones:

ISO (Organización Internacional de Normalización – International Organization for Standardzation)

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional. Su logotipo se muestra en la figura 2.1.1.

Figura 2.1.1. ISO. https://www.iso.org/home.html

IEEE (Insitute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos)

Fundado en Nueva York el 13 de mayo de 1884 por un grupo de profesionales como Thomas A. Edison y Alexander Graham Bell. El propósito principal es fomentar la innovación tecnológica, y la excelencia, para el beneficio de la humanidad. Definió los estándares de redes de área local (LAN). La mayoría de los estándares fueron establecidos por el Comité en los 80´s cuando apenas comenzaban a surgir las redes entre computadoras personales. Su logotipo se muestra en la figura 2.1.2.

Figura 2.1.2. IEEE.

https://www.ieee.org/

NOM (Normas Oficiales Mexicanas)

Figura 2.1.3. NOM.

Es una serie de normas cuyo objetivo es regular y asegurar valores, cantidades y características mínimas o máximas en el diseño, producción o servicio de los bienes de consumo entre personas morales y/o personas físicas, sobre todo los de uso extenso y de fácil adquisición por parte del público en general, poniendo atención en especial en el público no especializado en la materia. Su logotipo se muestra en la figura 2.1.3.

http://www.economia-noms.gob.mx/noms/inicio.do

TIA (Telecommunications Industry Association – Asociación de la Industria de las Telecomunicaciones)

Figura 2.1.4. TIA.

Representa los intereses de la industria mundial de tecnologías de la información y la comunicación (TIC). Los miembros de la industria incluyen compañías relacionadas con telecomunicaciones, banda ancha, telefonía móvil inalámbrica, tecnología de la información, redes, cable, satélite, comunicaciones unificadas y comunicaciones de emergencia. Cuenta con acreditación ANSI y se usar principalmente en el mercado norteamericano. Su logotipo se muestra en la figura 2.1.4.

https://www.tiaonline.org/

EIA (Electronic Industries Association – Asociación de Industrias Electrónicas)

Figura 2.1.5. EIA.

Son asociaciones de comercio que desarrollan y publican juntas una serie de estándares que abarcan el cableado estructurado de voz y datos para las LAN. Estos estándares de la industria evolucionaron después de la desregulación de la industria telefónica de los EE.UU. en 1984, que transfirió la responsabilidad del cableado de las instalaciones al dueño del edificio. Su logotipo se muestra en la figura 2.1.5.

ANSI (American National Standards Institute – Instituto Nacional Estadounidense de Estándares)

Figura 2.1.6. ANSI.

Es una organización encargada de supervisar el desarrollo de normas para los servicios, productos, procesos y sistemas en los Estados Unidos. El ANSI forma parte de la Organización Internacional para la Estandarización (ISO). Su logotipo se muestra en la figura 2.1.6

https://www.ansi.org/

ITU (Unión Internacional de Telecomunicaciones)

Atribuyen el espectro radioeléctrico y las órbitas de satélite a escala mundial, elaboran normas técnicas que garantizan la interconexión continua de las redes y las tecnologías, y mejoran el acceso a las TIC de las comunidades insuficientemente atendidas de todo el mundo. Su logotipo se muestra en la figura 2.1.7.

Figura 2.1.7. ITU. https://www.itu.int/es/Pages/default.aspx

BROADBAND FORUM

Es un consorcio industrial sin fines de lucro dedicado a desarrollar especificaciones de redes de banda ancha. Su logotipo se muestra en la figura 2.1.8.

https://www.broadband-forum.org/

Figura 2.1.8. BROADBAND FORUM.

2.2 Modelo OSI de acuerdo al estándar 7498-1

El modelo OSI es un modelo de referencia que describe cómo se transmite la información de una aplicación de software en un dispositivo a través del medio de transmisión hasta una aplicación de software en otro dispositivo. La representación de este modelo se encuentra en la figura 2.2.1.

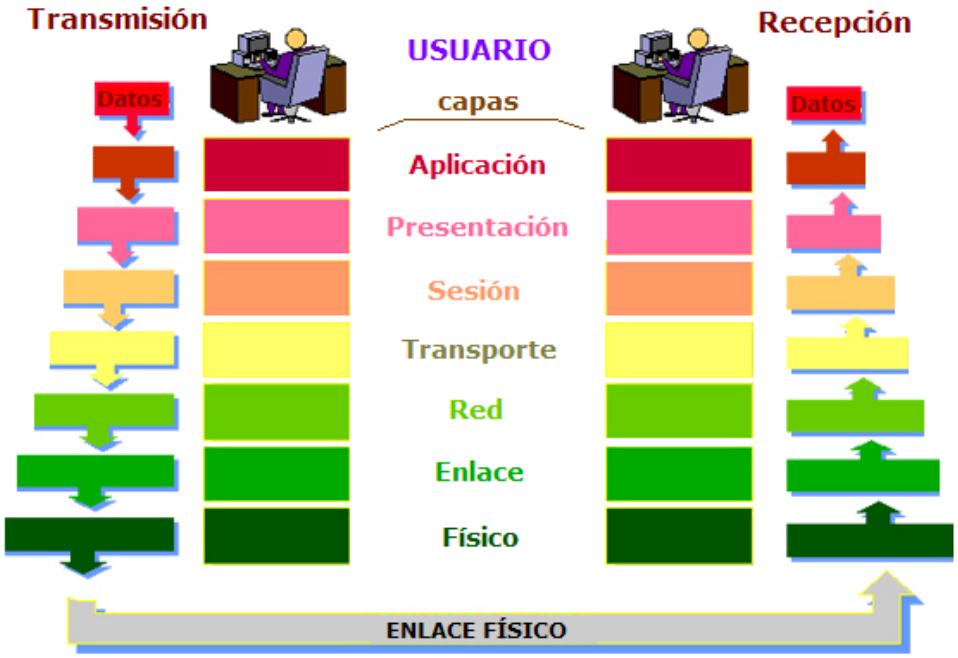


Figura 2.2.1. Las 7 capas del modelo OSI.

Objetivo

Permitir la comunicación entre sistemas de distintas marcas sin necesidad de combinar la lógica del hardware o el software subyacente.

Utilidad

Permite comprender y diseñar una arquitectura de red flexible, robusta e interoperable.

Capas del modelo OSI.

Compuesto por siete capas independientes pero relacionadas entre sí.

1. Capa física

Cubre las interfaces físicas entre dispositivos y las reglas bajo las cuales cadenas de bits son tratadas y transferidas de un dispositivo a otro.

Se definen características como:

- Niveles de voltaje, luz o frecuencia
- Topología física
- Modulación y multiplexaje
- Velocidades de transferencia de información
- Distancias máximas de transmisión
- Conectores físicos
- Codificación de línea

2. Capa de enlace de datos

Controla la capa física y provee los mecanismos necesarios que convierten a las comunicaciones entre dos nodos en una comunicación confiable. Verifica que los datos transferidos lleguen a su destino como fueron enviados y define los métodos de acceso al medio físico.

3. Capa de red

Se encarga de encaminar los paquetes hasta su destino a través de la mejor ruta y resuelve problemas concernientes al control de flujo y de gestionamiento.

Entre las principales actividades están:

- Buscar el mejor camino por paquete o por mensaje.
- Realizar las funciones de encaminamiento que permitan múltiples enlaces de datos en una red.
- Realizan un direccionamiento lógico.

4. Capa de transporte

En el proceso de salida del bloque de datos hacia su destino en otro equipo ubicado en otra red, la función de este nivel es aceptar los datos de la capa de sesión, dividirlos en unidades más pequeñas y asegurar que todos lleguen a su destino a través de diferentes máquinas o procesos, de manera que en el proceso de recepción su tarea es reensamblar todos los fragmentos antes de enviar los datos a la capa de sesión.

Entre sus principales responsabilidades están:

- Segmentación y re ensamblado de mensajes
- Control de flujo y de conexión
- Manejo de direcciones de puerto
- Administración de circuitos virtuales
- Control de errores y solicitud de retransmisión.

5. Capa de sesión

Define el procedimiento para iniciar la comunicación entre dos procesos a nivel de presentación. Permite establecer una comunicación, mantenerla para el intercambio de datos y finalmente concluirla, de ahí que su objetivo es asegurar que habiéndose establecido una sesión, ésta se mantenga de principio a fin.

Sus funciones son:

- Establecer y gestionar un camino de comunicación.
- Establecer la sesión, controlar la comunicación y sincronizar el diálogo.
- Indica quién “habla”, “cuando” y por “cuánto tiempo”.
- Dirigir el diálogo entre las entidades participantes.

6. Capa de presentación

Proporciona la sintaxis de los datos intercambiados entre los procesos.

Asegura la legibilidad de la información enviada por un sistema desde su capa de aplicación hasta la capa de aplicación del sistema receptor, realiza el cifrado de información y la compresión de datos.

7. Capa de aplicación

Contiene todos los protocolos de alto nivel que proveen los servicios que requieren los usuarios a través de las aplicaciones de red de propósitos diversos. Sus responsabilidades son:

- Proporcionar servicios distribuidos a los procesos de aplicación de los usuarios.

- Identificar a socios de comunicación.
- Determinar la disponibilidad de recursos de la red.
- Sincronizar la comunicación de aplicaciones.
- Proporciona servicios de directorios.

2.3 Arquitectura de seguridad de OSI estándar 7498-2

Para brindar la seguridad deseada es necesario instalar herramientas de seguridad que nos ayuden a lograr el objetivo: la seguridad de la información. Para lo cual es necesario tener presente que un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización.

El estándar ISO 7498-2 define un servicio de seguridad como el servicio proporcionado por un nivel de un sistema abierto que garantiza la seguridad de los sistemas abiertos o a las transferencias de datos en dichos sistemas. Estos servicios están divididos en cinco categorías:

- **Autenticación.** Verifica que la entidad que requiere el servicio sea quien dice ser (cifrado/firma digital).
- **Control de acceso.** Este servicio provee protección contra uso no autorizado de los activos de un sistema.
- **Confidencialidad.** Sólo las personas o entidades correspondientes pueden leer y entender el mensaje (cifrado).
- **Integridad.** Verifica que la información permanece sin haber sido modificada por una entidad no autorizada (cifrado).
- **No repudio.** Asegurar que una entidad no rechace su participación en una comunicación.

No existe un único mecanismo capaz de proveer todos los servicios, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información, y entre los más destacados se encuentran los siguientes:

- **Intercambio de autenticación.** Corrobora que una entidad, ya sea origen o destino de la información, es la deseada.
- **Cifrado.** Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados a través de lo cual proporciona confidencialidad a la información.
- **Integridad de datos.** Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad

(Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

- **Firma digital.** Este implica el cifrado, por medio de una clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios, de manera que el mensaje se procesa en el receptor y la autenticidad del emisor.
- **Control de acceso.** Consiste en permitir que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.
- **Tráfico de relleno.** Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- **Control de encaminamiento.** Permite enviar determinada información por determinadas zonas consideradas clasificadas, así como habilitar la posibilidad de solicitar otras rutas en caso de que se detecten persistentes violaciones de integridad en una ruta determinada.
- **Unicidad.** Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados, pero independientemente de cuántos sean y cómo se integren, los mecanismos de seguridad siempre deberán contener tres componentes principales:

- Información secreta, como claves y contraseñas, conocida por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado y descifrado, y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué, a quién y cuándo.

De igual manera, es importante hacer notar que los sistemas de seguridad requieren una gestión de seguridad la cual comprende dos grandes rubros:

1. Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
2. La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

2.4 Modelo TCP/IP

Es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red, el cual fue desarrollado en la década de los 70s. Las siglas TCP/IP significan Transmisson Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. En la figura 2.4.1 se realiza la comparación entre el modelo OSI y el modelo TCP/IP.

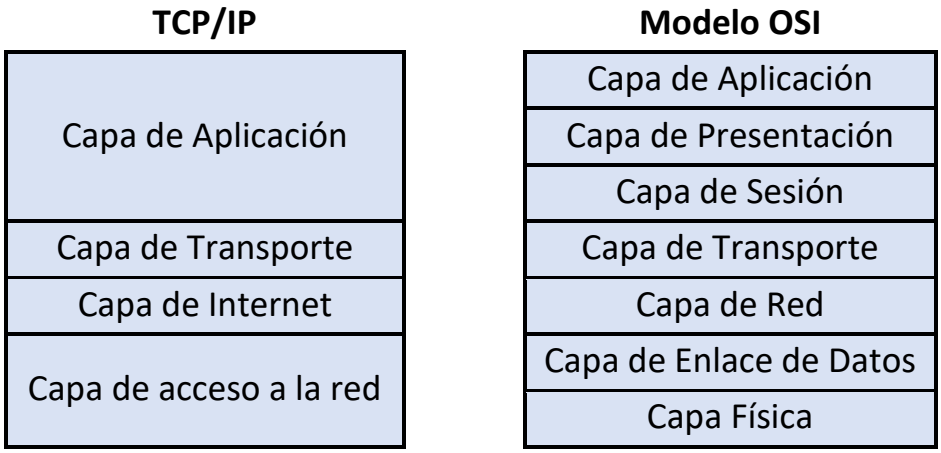


Figura 2.4.1. Comparación del modelo OSI con el modelo TCP/IP.

Capas del modelo TCP/IP

Capa de acceso a la red o interfaz de red

Especifica las características del hardware que se utilizará para la red, así como la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.

Esta capa acepta los datagramas IP y los transmite como tramas a través de un hardware de red específico, por ejemplo, redes Ethernet o de Red en anillo.

Capa de red o internet

Es responsable de proporcionar el paquete de datos (datagrama).

La capa de red de Internet pone el paquete en un datagrama de IP (Internet Protocol), pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (directamente a un destino o a una pasarela) y pasa el datagrama a la capa de interfaz de red.

Capa de transporte

Brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión. Comprende a los protocolos TCP y UDP.

Recibe los datos de la aplicación, los divide en partes más pequeñas llamadas *paquetes*, añade una dirección de destino y, a continuación, pasan los paquetes a la siguiente capa del modelo, la capa de red de Internet.

Capa de aplicación

Incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, entre otras).

Los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, UDP (User Datagram Protocol) o TCP (Transmission Control Protocol).

Seguridad en TCP/IP

La familia de protocolos TCP/IP puede ser vulnerada con base en dos conceptos inherentes a su diseño:

1. El formato de los paquetes de los diferentes protocolos: Además de la propia información transportada, la información contenida en cada uno de los campos de las cabeceras de los protocolos proporciona una fuente muy valiosa de conocimiento.

2. El modo de funcionamiento de los protocolos: Las etapas asociadas a cada proceso en los protocolos, así como el método de actuación en las diferentes situaciones posibles, ofrecen la información necesaria para analizar la existencia de vulnerabilidades.

2.5 Otros modelos (SNA, DNA, Netware, Appletalk)

SNA

Systems Network Architecture (SNA), es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hosts o mainframe — grandes ordenadores y servidores muy robustos que soportan millones de transacciones que por lo general son utilizados en bancos.

Originalmente fue diseñado para permitir la comunicación con un host. Cada red o subred era controlada por este host. Los ordenadores se podían comunicar con dicho host pero sin embargo no podían establecer comunicación directa con otros ordenadores. Este estilo de red recibe el nombre de subárea SNA. El nuevo diseño de red permite sin necesidad de host la comunicación punto a punto.

SNA define los estándares, protocolos y funciones usadas por los dispositivos para permitirles la comunicación entre ellos en las redes SNA.

La arquitectura SNA es un modelo que presenta similitudes con el modelo de referencia OSI (ver figura 2.5.1). Se compone de las siguientes capas:

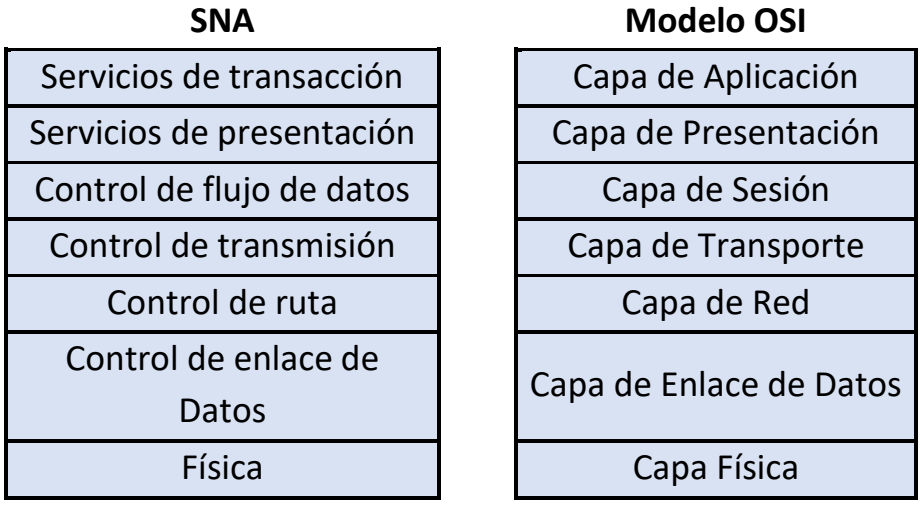


Figura 2.5.1. Comparación del modelo OSI con el modelo SNA.

Física: SNA no define protocolos específicos para su capa física. Se puede emplear cualquier otro estándar.

Control de Enlace de Datos (DLC - Data link control): Define varios protocolos incluidos el SDLC (Synchronous Data Link Control) y el protocolo de comunicación Token Ring Network para LAN entre iguales (peers).

Control de Ruta (Path control): Implementa mucha de las funciones de la capa de red OSI.

Control de Transmisión (Transmission control): Proporciona un servicio de conexión extremo-extremo o end-to-end fiable, además de servicios de cifrado y descifrado.

Control de Flujo de Datos (Data flow control): Entre otras cosas, controla el proceso de petición y respuesta, determina de quién es el turno para la comunicación e interrumpe el flujo de datos.

Servicios de Presentación (Presentation services): Especifica los algoritmos de transformación de datos para cambiarlos de una forma a otra, sincroniza las transacciones y coordina los recursos compartidos.

Servicios de Transacción (Transaction services): Proporciona servicios de aplicación en forma de programas que implementan el procesamiento distribuido o servicios de gestión.

DNA

Digital Network Arquitecture, es una arquitectura de Red creada por la compañía Digital Equipment Corporation (DEC). Introducida en 1975, DNA fue diseñada para servidores DEC's fuera de línea para el pasado, presente y futuro de las comunicaciones de sus productos.

La arquitectura de red DNA provee dos opciones de implementaciones. La primera es una Aplicación OSI la cual está conforme a las siete capas del modelo de referencia OSI (ver figura 2.5.2). La segunda, que es conocida como aplicación DNA, usa las cuatro capas inferiores del modelo de referencia OSI con la capa de Control de Sesiones de DNA para reemplazar las capas superiores del modelo OSI.

DNA	Modelo OSI
Capa de Aplicación	Capa de Aplicación
Capa de Presentación	Capa de Presentación
Capa de Sesión	Capa de Sesión
Capa de Transporte	Capa de Transporte
Capa de Red	Capa de Red
Capa de Enlace de Datos	Capa de Enlace de Datos
Capa Física	Capa Física

Figura 2.5.2. Comparación del modelo OSI con el modelo DNA.

Capa Física. Esta capa define cómo la información será transmitida para y de qué componentes físicos de red. DNA soporta completamente los estándares de la capa física OSI.

Capa Enlace de Datos. Esta capa es la responsable de proveer una comunicación confiable de rutas entre los dispositivos conectados. Algunos de los protocolos usados DNA son conforme al OSI.

Capa de Red. Esta capa es la responsable para el "routing" de los datos entre dispositivos en la red. Esto se realiza dinámicamente. DNA soporta los estándares OSI para una variedad de topologías.

Capa de Transporte. Es la responsable para enviar mensajes para un nodo final de la red a otro y soporta los estándares OSI a este nivel.

Capa de Sesión. La aplicación OSI soporta los estándares para habilitar diálogos entre usuarios. La aplicación DNA reemplaza este nivel con la Sesión de Control DNA.

Capa de Presentación. OSI soporta todos los estándares para asegurar que esta información sea entregada en una forma entendible. La aplicación DNA reemplaza este nivel con el Control de Sesión DNA.

Capa de Aplicación. Esta capa provee un enlace para la capa de transporte DNA hacia la capa de aplicación. Estas funciones de comunicación incluyen lo siguiente:

- Traducción Nombre-Dirección el cual permite a los usuarios referirse a objetos remotos por nombre. Esto provee una transparencia creciente de la red.
- Selección de protocolo para incrementar la flexibilidad de la red.
- Control de acceso para incrementar seguridad de la red

Netware

Es un sistema operativo para LAN desarrollado por Novell Corporation. NetWare es un producto de software que corre sobre distintos tipos de LANs, desde redes Ethernet a IBM con topología de anillo. Provee a los usuarios y programadores con una interfaz consistente que es independiente del hardware utilizado para transmitir los mensajes. Su comparación con el modelo OSI se puede observar en la figura 2.5.2.

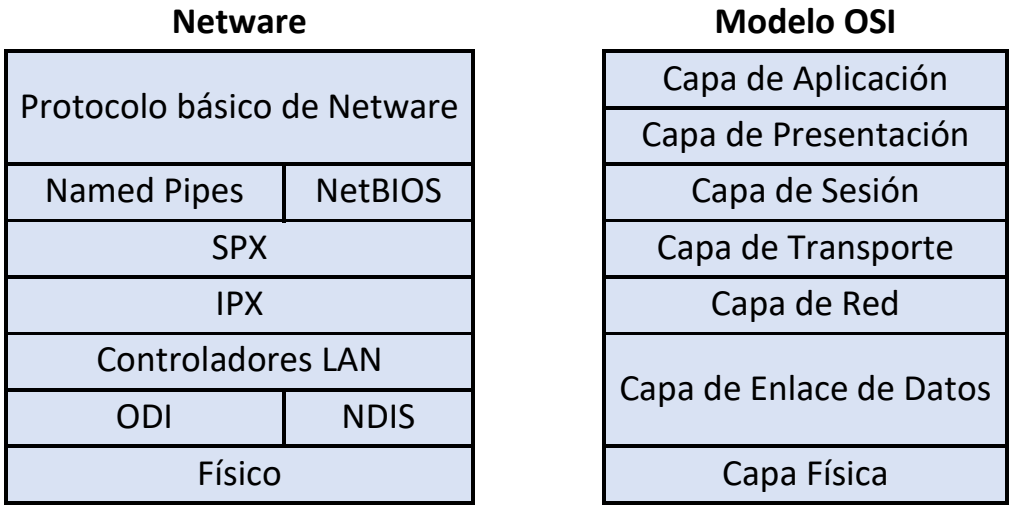


Figura 2.5.3. Comparación del modelo OSI con el modelo Netware.

Capa Física. Similar al modelo OSI. Netware provee soporte para las versiones más conocidas de Ethernet, Token Ring y ARCnet.

Capa de enlace de Datos. Dividida en ODI y NDIS. ODI (Open Data Link Interface) es una estructura de protocolo independiente el cual provee soporte simultáneo de diferentes protocolos en la red. NDIS (Network Drive Interface Specification) es una interfaz para tarjetas de red desarrollada por Microsoft cuya función es conectar redes distintas. NDIS o ODI pueden coexistir en una estación, de modo que los usuarios podrán acceder a redes NetWare. El propósito de ODI y NDIS es escandalizar la interfaz de controladores y tarjetas de red. De este modo, no se necesita controladores separados para cada tipo de protocolo que se desee ejecutar en la tarjeta.

Capa de Red. En esta capa Netware construyó IPX (Internetwork Packet Exchange) para los protocolos de red Peer to Peer, que son los medios primarios para proporcionar servicios a los dispositivos clientes en un ambiente de Netware.

Capa de Transporte. Se cuenta con el SPX (Sequenced Packet Exchange) que en algún tiempo se refirió como una comparación del protocolo IPX. SPX ofrece una conexión orientada de comunicaciones, mientras SPX usa IPX para la entrega de mensajes, este garantiza la entrega de paquetes y conserva la secuencia de paquetes para mantener una conexión entre los dispositivos de comunicación.

Capa de Sesión. Netware vuelve a dividir en dos esta sesión: Named Pipes and NetBios. Named Pipes es una interfaz de alto nivel para entregar datos entre procesos ejecutándose en diferentes computadoras conectadas en la red. NetBios es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

Capa de Aplicación. NCP (Netware Core Protocol) es el principal protocolo para la transmisión de la información entre el servidor Netware y los clientes. IPX es un protocolo que usa mensajes portadores de NCP. Algunos de los servicios que ofrece son: Petición de Inicio de Sesión, Acceso a servicios de impresión, Acceso a Archivos, Permitir recursos, Administración de las redes y seguridad, Comunicación Inter-Servidores.

Appletalk

Appletalk representa una serie de especificaciones que describe las conexiones de computadoras Macintosh, impresiones y otros recursos o computadoras dentro de una red. AppleTalk es una pila de protocolos dentro de las 7 capas del modelo de referencia OSI y usa los mismos nombres (ver figura 2.5.4). Algunas de estas capas tienen múltiples protocolos definidos.

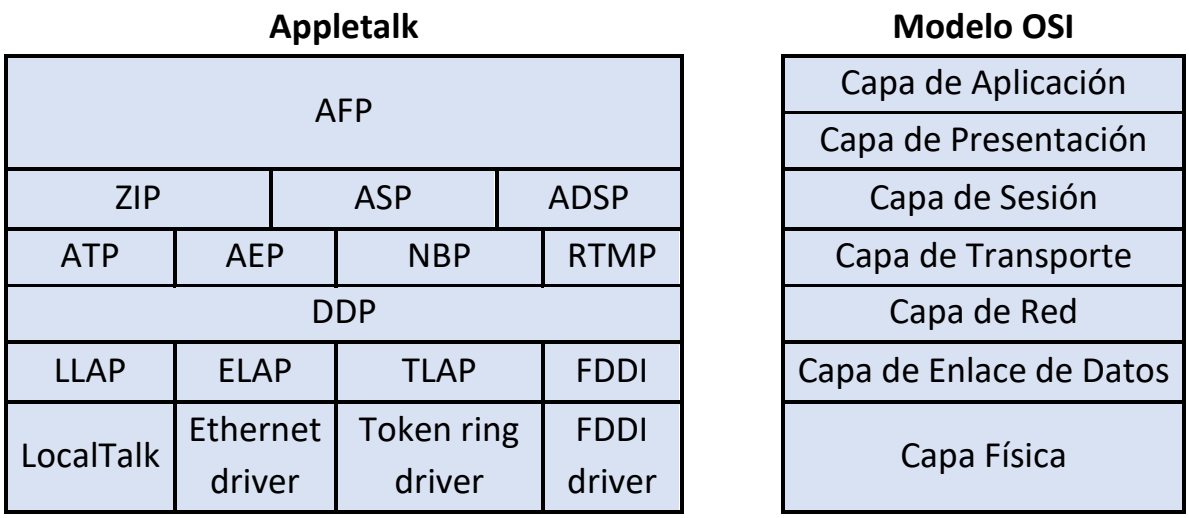


Figura 2.5.4. Comparación del modelo OSI con el modelo Appletalk.

Capa Física y Enlace de Datos. La capa de enlace de datos y la capa física proporcionan conectividad. La comunicación entre sistemas en red puede ser a través de un cable físico hecho de alambre o fibra óptica, o puede ser a través de transmisión por infrarrojos o microondas. Además de estos, el hardware puede incluir un controlador de interfaz de red (NIC), si se usa uno. El hardware o los medios de transporte y los controladores de dispositivo para el hardware comprenden la capa física. LocalTalk, token ring, Ethernet y la interfaz de datos distribuidos de fibra (FDDI - Fiber Distributed Data Interface) son ejemplos de tipos de hardware de red que admite AppleTalk.

El hardware físico proporciona nodos en una red con un medio de transmisión de datos compartido llamado enlace (link). La capa de enlace de datos incluye un protocolo que especifica los aspectos físicos del enlace de datos y el protocolo de acceso al enlace, que maneja la logística de enviar el paquete de datos a través del medio de transporte. AppleTalk está diseñado para ser independiente del enlace de datos, lo que permite el uso de varios tipos de hardware y sus protocolos de acceso al enlace.

Capa de Red. Especifica el enrutamiento de red de paquetes de datos entre nodos y las comunicaciones entre redes, lo que se conoce como internetworking. El Protocolo de entrega de datagramas (DDP - Datagram Delivery Protocol) es implementado en la capa de red. Es un protocolo de datagrama sin conexión que proporciona la entrega de mejor esfuerzo. Esto significa que DDP transfiere datos como paquetes discretos y que no incluye soporte para garantizar que todos los paquetes enviados se reciban en el destino o que los paquetes que se reciben estén en el orden correcto. Los protocolos de nivel superior que utilizan los servicios de DDP proporcionan este tipo de confiabilidad.

Capa de Transporte. Esta capa aísla algunos de los aspectos físicos y funcionales de una red de paquetes de las tres capas superiores. Proporciona responsabilidad de extremo a

extremo, asegurando que todos los paquetes de datos enviados a través de la red sean recibidos y en el orden correcto.

Este es el proceso que se conoce como entrega confiable de datos e implica proporcionar un medio para identificar la pérdida de paquetes y suministrar un mecanismo de retransmisión. También proporciona servicios de gestión de conexión y sesión.

Los siguientes protocolos AppleTalk se implementan en la capa de transporte:

- Protocolo de enlace de nombre (NBP - Name-Binding Protocol)
- Protocolo de transacciones AppleTalk (ATP - AppleTalk Transaction Protocol)
- Protocolo AppleTalk Echo (AEP - AppleTalk Echo Protocol)
- Protocolo de mantenimiento de la tabla de enrutamiento (RTMP - Routing Table Maintenance Protocol)

Además de estos protocolos de capa de transporte, el Protocolo de transmisión de datos AppleTalk (ADSP - AppleTalk Data Stream Protocol) incluye funciones que abarcan tanto las capas de transporte como las de sesión. ADSP proporciona una entrega confiable de datos, y en esa capacidad cubre los requisitos de la capa de transporte.

Capa de Sesión. Algunas de las funciones que proporciona la capa de sesión son el control de flujo, el establecimiento de puntos de sincronización para verificaciones y la recuperación para la transferencia de archivos, full-duplex y half-diálogos dúplex entre procesos, y aborta y reinicia.

Los protocolos AppleTalk implementados en la capa de sesión son:

- El Protocolo de flujo de datos AppleTalk (ADSP - AppleTalk Data Stream Protocol), que proporciona sus propios servicios de capa de transporte basados en flujo que permiten cuadros de diálogo full-duplex.
- El Protocolo de sesión AppleTalk (ASP - AppleTalk Session Protocol), que utiliza los servicios basados en transacciones de ATP para transportar los comandos de la estación de trabajo a los servidores.
- El Protocolo de información de zona (ZIP - Zone Information Protocol), que proporciona a las aplicaciones y procesos acceso a los nombres de zona. Cada nodo en una red pertenece a una zona.

Capa de Presentación. La capa de presentación supone que ya existe una ruta o conexión de extremo a extremo a través de la red entre las dos partes que se comunican, y le preocupa la representación de valores de datos para transferencia, o la sintaxis de transferencia. En el modelo OSI, el Protocolo de archivo AppleTalk (AFP - AppleTalk Filing Protocol) abarca las capas de presentación y aplicación. AFP proporciona una interfaz entre una aplicación y un servidor de archivos. Utiliza los servicios de ASP, que, a su vez, es cliente de ATP.

AFP permite que una estación de trabajo en una red AppleTalk acceda a archivos en un servidor de archivos AFP, como un servidor de archivos AppleShare. Cuando el usuario abre una sesión con un servidor de archivos AppleShare a través de Internet, aparece cualquier aplicación que se ejecute en la estación de trabajo que use rutinas de administrador de archivos como si los archivos en el servidor de archivos estuvieran ubicados en una unidad de disco conectada a la estación de trabajo.

Capa de Aplicación. El software escrito en esta capa se beneficia de los servicios de todas las capas subyacentes. No hay un protocolo AppleTalk que asigne directamente a esta capa, aunque algunas de las funciones del Protocolo de archivo AppleTalk (AFP - AppleTalk Filing Protocol) cumplen con esta capa.

Tema 3

Capa física

Objetivo: El alumno definirá y explicará los diferentes medios de transmisión y las ventajas de cada uno de ellos mediante los estándares IEEE y ANSI/TIA/EIA involucrados en la capa física a fin de utilizar las normas del cableado estructurado con el propósito de diseñar una red de datos segura

Esta capa del modelo OSI cubre las interfaces físicas entre dispositivos y las reglas bajo las cuales cadenas de bits son tratadas y transferidas de un dispositivo a otro.

Se definen características como:

- Niveles de voltaje, luz o frecuencia
- Topología física
- Modelación y multiplexaje
- Velocidades de transferencia de información
- Distancias máximas de transmisión
- Conectores físicos
- Codificación de línea

3.1 Medios de transmisión

Medios de transmisión terrestres o guiados

Constituidos por cables que se encargan de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

Par trenzado

El cable de par trenzado es una forma de conexión en la que dos conductores son entrelazados para cancelar las interferencias electromagnéticas (IEM) de fuentes externas y la diafonía de los cables adyacentes. Un ejemplo de éste puede verse en la figura 3.1.1.

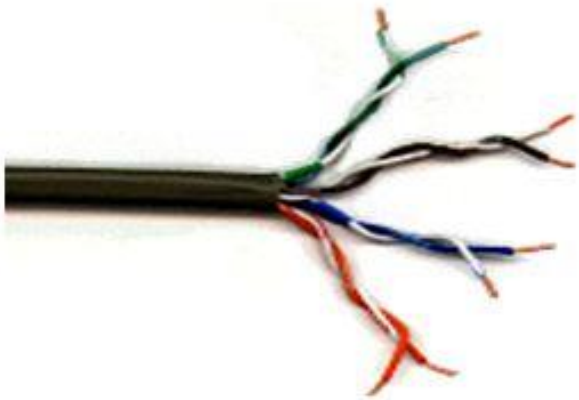


Figura 3.1.1 Ejemplo de cable de par trenzado.

Todos los cales requieren ser identificados por tres características principales que en las jerarquías de multiplexación se denotan como sigue:

Capacidad de transferencia	BANDA	tipo de cable

Donde la capacidad de transferencia puede ser dada en Kbps, Mbps, Gbps, por ejemplo. La banda es igual a la transmisión de una señal en un canal, y la banda ancha es lo mismo que muchas señales en diferentes canales (hasta su número máximo de canal). Y el tipo de cable se refiere a la distinción entre cables de cobre o de fibra óptica. Por ejemplo:

1000BASE-T se refiere a un cable con capacidad de transferencia de 1Gbps (1000Mbps), que transmite en banda base y que se trata de par Trenzado, este tipo de cable se identifica como UTP categoría 6 y transmisión a 250 MHz.

Para transmisiones a mayor frecuencia se requieren cables de calibre más grueso, mayor blindaje y más vueltas de par por pulgada para reducir el ruido e interferencias.

Cable UTP (Unshield Twisted Pair - Par Trenzado sin Blindaje)

En la actualidad es el tipo de cable de red más utilizado, debido fundamentalmente a su precio. Este tipo de cable no posee ninguna otra protección contra interferencias que no sea su cubierta de PVC. La conexión se hace mediante el llamado conector tipo RJ45.

Categorías

Categoría 1. Es el más adecuado para las comunicaciones telefónicas. No es adecuado para transmitir datos o para trabajarlos en una red. Se utiliza sobre todo en instalaciones de cableado.

Categoría 2. Es capaz de transmitir datos de hasta 4 Mbps. Se trata de cable nivel 2 y se usó en las redes ARCnet (arco de red) y Token Ring (configuración de anillo) hace algún tiempo. El CAT 2 al igual que el CAT 1, no es adecuado para la transmisión de datos en una red.

Categoría 3. Es capaz de llevar a la creación de redes 100BASE-T y puede ayudar a la transmisión de datos de hasta 16 MHz con una velocidad de hasta 10 Mbps. No se recomienda su uso con las instalaciones nuevas de redes.

Categoría 4. Soporta transmisiones de hasta 20 MHz. Es confiable para la transmisión de datos por encima del CAT 3 y puede transmitir datos a una velocidad de 16 Mbps. Se utiliza sobre todo en las redes Token Ring.

Categoría 5. Ayuda a la transmisión de hasta 100 MHz con velocidades de hasta 1000 Mbps. Es un cable UTP muy común y adecuado para el rendimiento 100BASE T. Se puede

utilizar para redes ATM, 1000BASE T, 10BASE T, 100BASE T y token ring. Estos cables se utilizan para la conexión de computadoras conectadas a redes de área local.

Categoría 5e. Es una versión mejorada sobre el de nivel 5. Sus características son similares al CAT 5 y es compatible con transmisión de hasta 10 MHz. Es más adecuado para operaciones con Gigabit Ethernet y es una excelente opción para red 1000BASE T.

Cabe mencionar que las categorías hasta aquí mencionadas ya no están en uso en la actualidad.

Categoría 6. Puede soportar hasta 250 MHz de transmisión. Se trata de la sexta generación del cable Ethernet. Este cable con alambres de cobre puede soportar velocidades de 1 GB. Es adecuado para redes 1000BASE T, 100BASE T y 10BASE T y posee estrictas reglas acerca del ruido del sistema y la diafonía.

Categoría 6A. Permite trabajar a velocidades de hasta 10Gbps dentro de un entorno Ethernet, pudiendo también llevar otras señales como servicios básicos de telefonía, TokenRing y ATM. Diseñado para transmisión a frecuencias de hasta 500MHz.

Categoría 7. Es otro proyecto de norma que admite la transmisión de hasta 600 MHz. CAT 7 es un estándar Ethernet de cable de cobre 10G que mide más de 100 metros. Es compatible con CAT 5 y CAT 6 y tiene reglas más estrictas que CAT 6 sobre el ruido del sistema y la diafonía.

Categoría 8. Proporciona dos pares de conductores con velocidades máximas de señal a 2GHz, cuatro veces más que el ancho de banda del cable Categoría 6A. La infraestructura de cableado Categoría 8 está pensada para soportar distancias cortas de unos 30 metros máximo, lo que implica que se puede implementar únicamente en entornos de data center (no está pensado para cableado horizontal el cual necesita 100 metros). Multiplica por cuatro el ancho de banda especificado para el UTP, este importante incremento en el ancho de banda es utilizado por la aplicación del 40GBASE-T para cuadruplicar la velocidad máxima de transporte de datos anterior del BASE-T (de 10 a 40 Gbps).

Cable STP (Shielded Twisted Pair - Par Trenzado Blindado)

La diferencia fundamental entre este cable de red y el cable UTP es el nivel de protección contra ruidos e interferencias externas, mucho más efectivo. Esto se logra cubriendo cada par mediante una malla protectora e interconexión a tierra, ambos elementos que actúan a manera de pantalla ante cualquier perturbación. Todas estas medidas, además de proteger mejor las señales que viajan en el interior del cable de red, también hacen del cable mucho más caro.

FTP (Foiled Twisted Pair - Par trenzado Apantallado)

Podría decirse que el cable FTP es un cable similar al UTP, ya que sus pares no se encuentran apantallados, pero a diferencia del UTP, el cable FTP posee una pantalla que le permite mejorar el nivel de protección ante interferencias externas (véase figura 3.1.2). Otra característica relevante del cable FTP es que puede usar los mismos conectores RJ45 utilizados en el cable UTP.

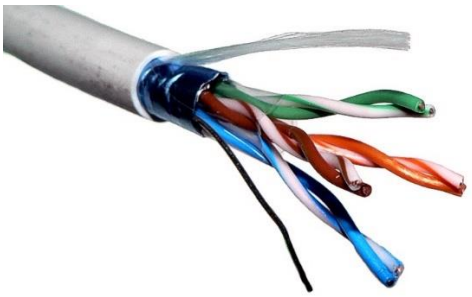


Figura 3.1.2. Cable FTP

Cable coaxial

El cable coaxial transporta señales con rango de frecuencias más altos que los cables de pares trenzados. El cable coaxial tiene un núcleo conductor central formado por un hilo sólido o enfilado, habitualmente de cobre, recubierto por un aislante de material dieléctrico que, a su vez, está recubierto de una hoja exterior de metal conductor, malla o una combinación de ambos, también habitualmente de cobre (véase figura 3.1.3). La cubierta metálica exterior sirve como blindaje contra el ruido y como un segundo conductor. Este conductor está recubierto por un escudo aislante, y todo el cable por una cubierta de plástico.

Figura 3.1.3. Cable coaxial.

Fibra óptica

La fibra óptica es un enlace hecho con un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el núcleo de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total. La fuente de luz puede ser láser o un led.

La fibra óptica es una guía de ondas dieléctrica que opera a frecuencias ópticas. Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor (véase figura 3.1.4).

Figura 3.1.4. Fibra óptica.

Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total.

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

Estructura (véase figura 3.1.5)

- ***Elemento central dieléctrico.*** Este elemento central que no está disponible en todos los tipos de fibra óptica, es un filamento que no conduce la electricidad (dieléctrico), que ayuda a la consistencia del cable entre otras cosas.
- ***Hilo de drenaje de humedad.*** Su finalidad es que la humedad salga a través de él, dejando al resto de los filamentos libres de humedad.
- ***Fibras.*** Esto es lo más importante del cable, ya que es el medio por dónde se transmite la información. Puede ser de silicio (vidrio) o plástico muy procesado. Aquí se producen los fenómenos físicos de reflexión y refracción. La pureza de este material es lo que marca la diferencia para saber si la fibra puede ser utilizada para transmitir datos o no. Una simple impureza puede desviar el haz de luz, haciendo que este se pierda o no llegue a su destino. En cuanto al proceso de fabricación es muy interesante y hay muchos vídeos y material en la red, pero básicamente las hebras (microns de ancho) se obtienen al exponer tubos de vidrio al calor extremo y por medio del goteo que se producen al derretirse, se obtienen cada una de ellas.
- ***Loose Buffers.*** Es un pequeño tubo que recubre la fibra y a veces contiene un gel que sirve para el mismo fin haciendo también de capa oscura para que los rayos de luz no se dispersen hacia afuera de la fibra.
- ***Cinta de Mylar.*** Es una capa de poliéster fina que hace muchos años se usaba para transmitir programas a PC, pero en este caso sólo cumple el rol de aislante.

- ***Cinta antillana.*** Es un cobertor que sirve para proteger al cable del calor y las llamas.
- ***Hilos sintéticos de Kevlar.*** Estos hilos ayudan mucho a la consistencia y protección del cable, teniendo en cuenta que el Kevlar es un muy buen ignífugo, además de soportar el estiramiento de sus hilos.
- ***Hilo de desgarre.*** Son hilos que ayudan a la consistencia del cable.
- ***Vaina.*** La capa superior del cable que provee aislamiento y consistencia al conjunto que tiene en su interior.

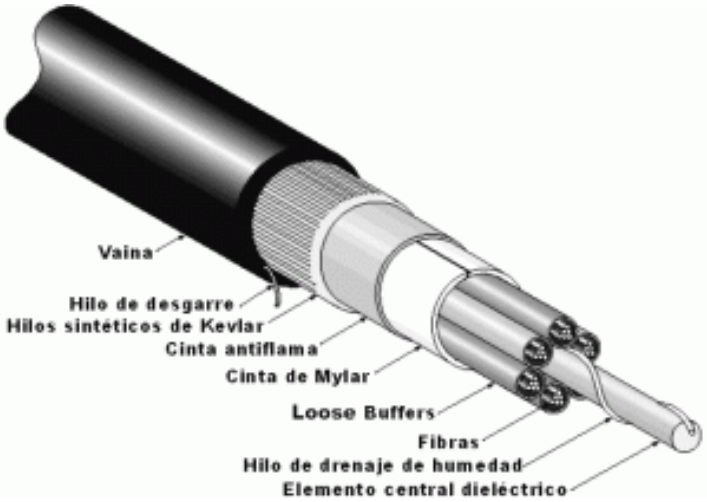


Figura 3.1.5. Estructura de la fibra óptica.
(Obtenido de: https://www.fibraopticahoy.com/fibra-optica-que-es-y-como-funciona/)

Características

- ***Cobertura más resistente:*** la cubierta contiene un 25% más material que las cubiertas convencionales.
- ***Uso dual (interior y exterior):*** La resistencia al agua y emisiones ultravioleta, la cubierta resistente y el funcionamiento ambiental extendido de la fibra óptica contribuyen a una mayor confiabilidad durante el tiempo de vida de la fibra.
- ***Mayor protección en lugares húmedos:*** Se combate la intrusión de la humedad en el interior de la fibra con múltiples capas de protección alrededor de ésta, lo que proporciona a la fibra, una mayor vida útil y confiabilidad en lugares húmedos.
- ***Empaquetado de alta densidad:*** Con el máximo número de fibras en el menor diámetro posible se consigue una más rápida y más fácil instalación, donde el cable debe enfrentar dobleces agudos y espacios estrechos. Se ha llegado a conseguir un cable con 72 fibras de construcción súper densa cuyo diámetro es un 50% menor al de los cables convencionales.

Cada uno de los distintos tipos de cables funcionan para distintos propósitos, por lo tanto, cada uno tiene diferentes características en cuanto a rendimiento, por lo cual, en la tabla 3.1.1 se representa la impedancia de los distintos tipos de cable de acuerdo a su calibre.

Tabla 3.1.1. Calibre e impedancia de cables.

Cable	Calibre	Impedancia
Cable Coaxial estándar Ethernet	12 mm	50 Ω
Cable coaxial Ethernet delgado	6 mm	50 Ω
Cable coaxial tipo RG 62	6 mm	93 Ω
Cable coaxial tipo RG 59	6 mm	75 Ω
UTP	52 mm	100 Ω
STP	30 mm	100 Ω o 150 Ω
FTP	7 mm	120 Ω
Fibra óptica	50 – 125 µm cada fibra 10 fibras: 8 – 10 mm 64 fibras: 15 – 20 mm	

Medios de transmisión aéreos o no guiados

Los medios no guiados o comunicación sin cable transportan ondas electromagnéticas sin usar un conductor físico, sino que se radian a través del aire, por lo que están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas. En este tipo de medios tanto la transmisión como la recepción de información se lleva a cabo mediante antenas.

Redes inalámbricas

Es un término que se utiliza para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos lógicos. Una de sus principales ventajas es referente a los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos, pérdida o robo de información.

Microondas

Las emisiones pueden ser de forma analógica o digital, pero han de estar en la línea visible, tal y como se representa en la figura 3.1.6. Tienen una dirección, un enfoque. Puede tener un ángulo o muy cerrado o muy amplio. Mientras más cerrado es más larga la distancia que alcanza. Mientras más amplio, se tiene una mayor área de cobertura, pero el alcance es corto.

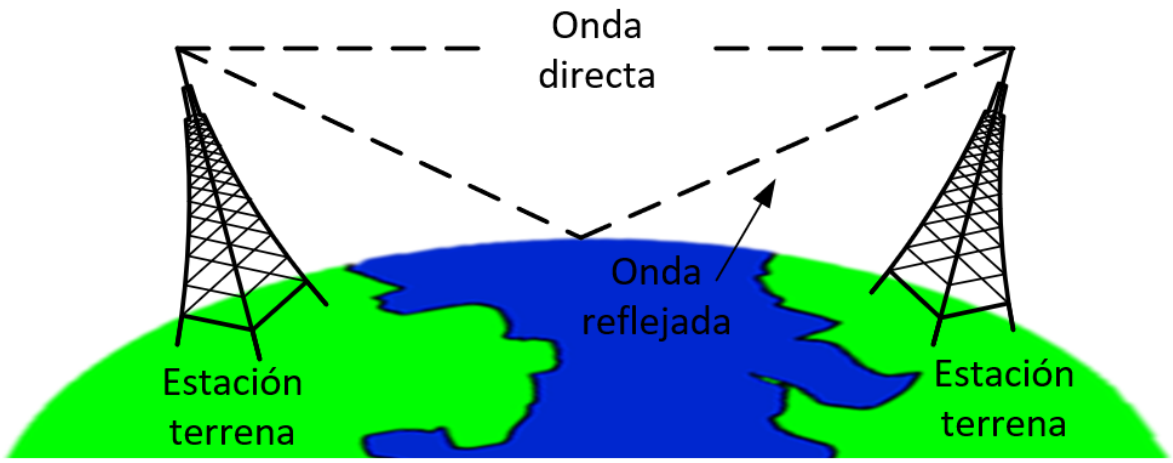


Figura 3.1.6. Transmisión por microondas.

Existen una variedad de sistemas de microondas funcionando a distancias que varían de 24 a 6400 kilómetros, los sistemas de microondas de servicio intraestatal o alimentador se consideran en general de corto alcance, porque se usan para llevar información a distancias relativamente cortas, por ejemplo, hacer una radiocomunicación entre ciudades que se encuentran en un mismo país. Los sistemas de microondas de largo alcance son los que se usan para llevar información a distancias relativamente mucho más largas, por ejemplo, en aplicaciones de rutas interestatal y de red primaria.

La distancia cubierta por enlaces de microondas puede ser incrementada por el uso de repetidoras, las cuales amplifican y re direccionan la señal, es importante destacar que los obstáculos de la señal pueden ser salvados a través de reflectores pasivos.

Enlaces satelitales

Sus ventajas son la libertad geográfica y su alta velocidad, pero como desventaja tienen como gran problema el retardo de las transmisiones debido a que deben viajar grandes distancias. Su funcionamiento se representa en la figura 3.1.7.

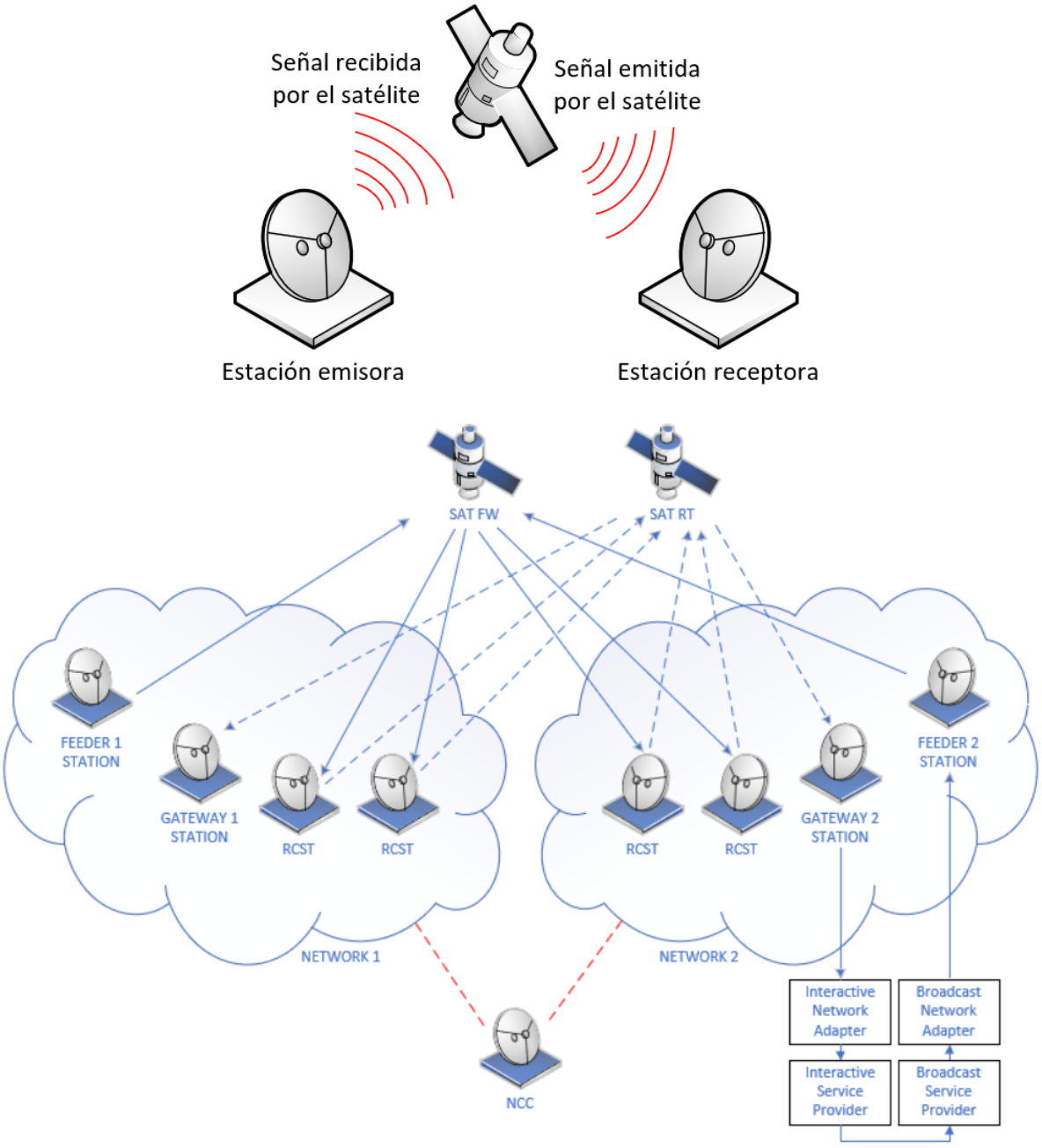


Figura 3.1.7. Enlace satelital.

Los satélites pueden estar localizados a distintas alturas, lo que puede llegar a ser útil dependiendo del tipo de comunicación que se quiera brindar (ver figura 3.1.8).

- **LEO (Low Earth Orbit):** Conocida como "órbita baja", situada entre los 160 y 2,000 kilómetros de altura. Entre más baja es la órbita, los objetos se mueven a mayor velocidad respecto de la superficie terrestre. Aquí se encuentran la gran mayoría de los satélites meteorológicos o de observación.
- **MEO (Medium Earth Orbit):** Órbita intermedia, entre 2,000 y 36,000 kilómetros de altura. Usada por satélites de observación, defensa y posicionamiento, como las redes satelitales de GPS.
- **GEO (Geoestationary Orbit):** Órbita geoestacionaria, que está a 35680 kilómetros de la superficie terrestre y tiene un período orbital de 24 horas (coincidiendo con la duración del día sideral).
- **Órbita Molnya:** Órbita desarrollada por Rusia, especialmente usada por los países cercanos al círculo polar ártico. Es altamente elíptica con visibilidad desde las zonas polares. Permite a los países nórdicos establecer satélites de comunicaciones para las regiones donde los geoestacionarios no pueden llegar.
- **HEO (High Earth Orbit):** Son todas las órbitas altas, que se ubican más allá de las órbitas geoestacionarias, a más de 36,000 kilómetros y con períodos orbitales mayores a 24 horas.
- **SSO (Sun Sincronous Orbit):** Órbita sincrónica solar, un caso particular de órbita polar, que permite que un objeto ubicado en ella, pase todos los días, sobre un determinado lugar, a la misma hora. Eso se logra usando una órbita polar, controlando la precesión de la órbita de modo que se ajuste de forma sincrónica a la posición del sol durante todo el año.

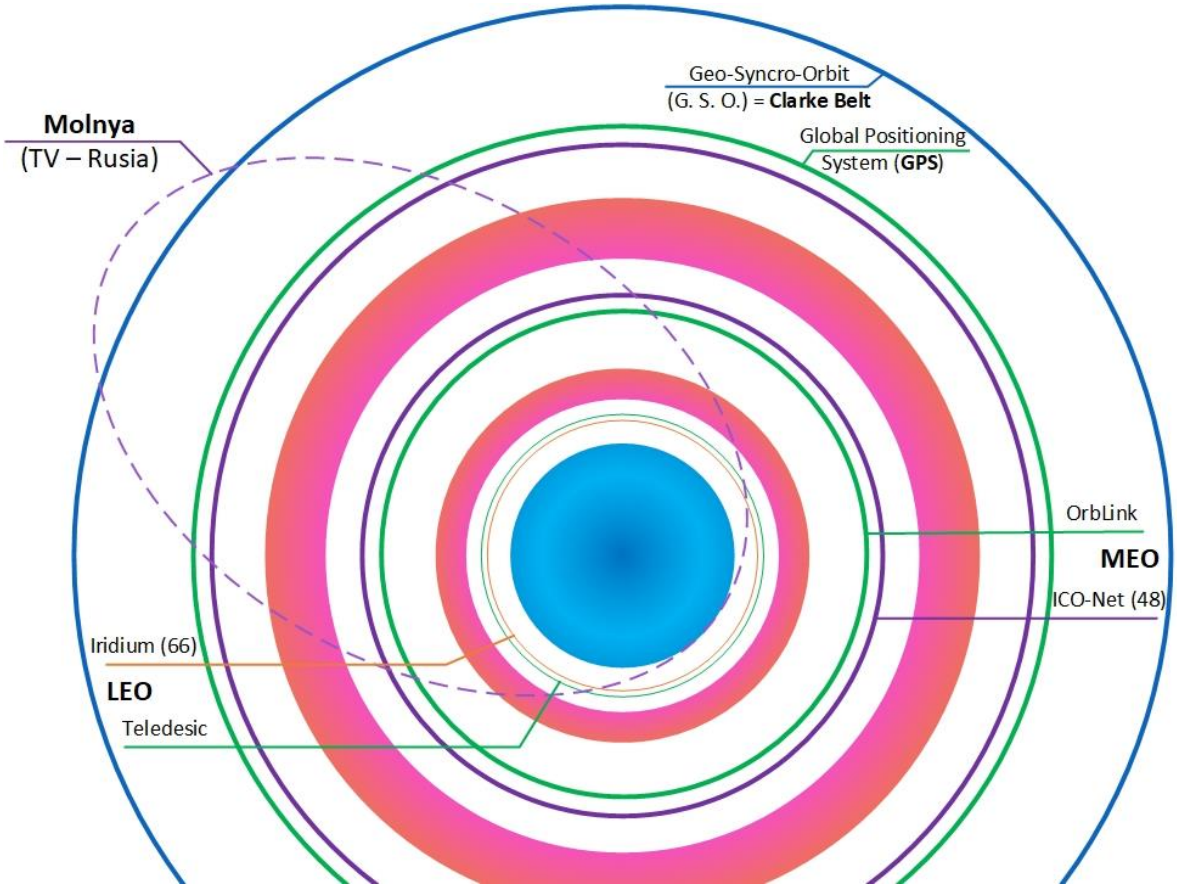


Figura 3.1.8. Tipos de satélites y sus órbitas.

Rayo láser

Las ondas de láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector (ver figura 3.1.9). Hasta 4 kilómetros de distancia con una velocidad de transmisión de 1500 Mbps.

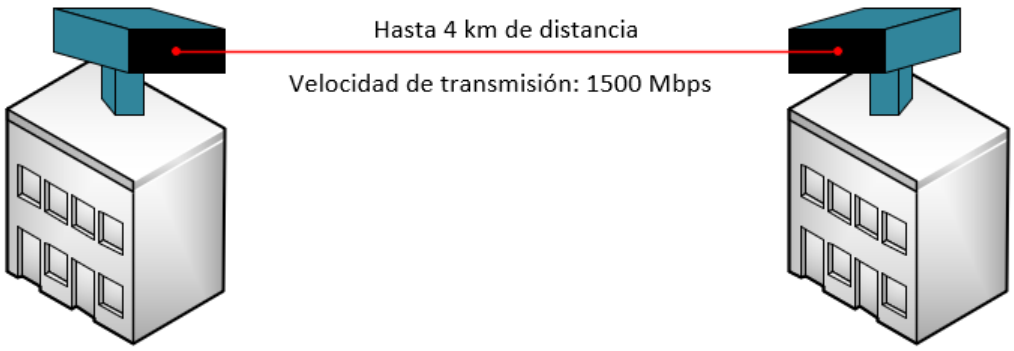


Figura 3.1.9. Enlace por rayo láser.

Infrarrojo

Poseen las mismas técnicas que las empleadas por la fibra óptica, pero son por el aire. Son una excelente opción para las distancias muy cortas (ver figura 3.1.10). Ofrece transferencia de datos inalámbrica punto a punto en su línea de visión, con un alcance de aproximadamente uno o dos metros y velocidades de transferencia de datos de hasta 4 Mbit/s.

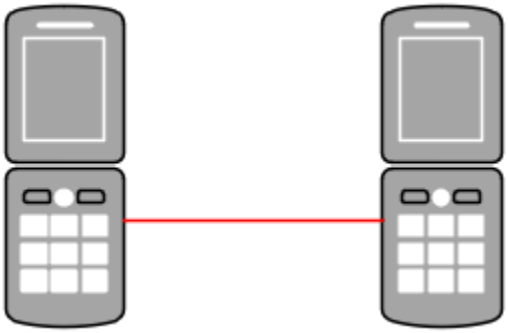


Figura 3.1.10. Enlace por infrarrojo.

3.2 Estándares de la capa física: RS-232, RS-422, RS-449

RS-232, Transmisión Balanceada (Single Ended)

Esta norma fue diseñada para comunicación punto a punto, en donde se tiene una computadora (en la norma RS-232 se le denomina DTE, Data Terminal Equipment) que se encuentra transmitiendo hacia un equipo esclavo (en la norma conocido como DCE, Data Communications Equipment) ubicado a distancias no mayores a 15 metros (aunque en la práctica alcanza distancias de hasta 50 metros) y a una velocidad máxima de 19,200 bps. Este tipo de trasmisión se le conoce como "single ended" porque usa en el cable un solo retorno (GND). Es un modo de trasmisión muy simple, pero también vulnerable al ruido aditivo en la línea y por esa razón es empleada para comunicación a distancias cortas.

En general, en la transmisión RS-232, las cadenas de datos son caracteres ASCII, los cuales incluyen los códigos de letras, números y signos de puntuación, además de caracteres especiales. Se trata de un estándar orientado a la trasmisión de texto.

RS-422

Cuando se requieren mayores distancias y velocidades de transmisión, entonces deben de emplearse las normas RS-422 y RS-485. Además, estas normas permiten también la transmisión multipunto, es decir una computadora central conectada con varias UTR

(Unidad Terminal Remota). Dado que la computadora central típicamente tiene como salida la interfaz RS-232, se hace necesaria la conexión de un módulo convertidor RS-232 a RS-422/485, para implementar una red.

La transmisión diferencial permite velocidades de hasta 10 Mbps, sobre distancias de hasta 1.3 kilómetros. Se usan dos señales para transmitir y dos para recibir, además de la tierra, la cual es normalmente conectada al blindaje del cable. En cada par, viaja la señal de transmisión y su complemento. En el receptor, la señal original se obtiene restando una de la otra. Esta técnica reduce grandemente el ruido generado en la línea, ya que éste se induce por igual en ambas líneas del par y es al final cancelado. Este tipo de transmisión debe de hacerse siempre sobre cable del tipo par trenzado.

RS-422 usa 4 señales y puede emplearse para comunicación punto a punto o multipunto. En su aplicación más simple, una computadora central se comunica con una UTR empleando un protocolo master-slave, full dúplex.

RS-449

El RS-449 especifica las características mecánicas y funcionales de la interfaz entre Equipo Terminal de Datos (DTE) y Equipo Terminal de Circuito de Datos (DCE), puede utilizarse en velocidades de hasta 2 Mbps, en cables de hasta 60 metros. Los componentes estándar para el uso junto con el RS-449 son el RS-422 para señales balanceadas, y el RS-423 para señales no balanceadas.

3.3 Cableado estructurado

El cableado estructurado es la infraestructura de cable destinada a transportar a lo largo y ancho de una red LAN los datos que requieran compartir los usuarios, tal y como se representa en la figura 3.3.1.

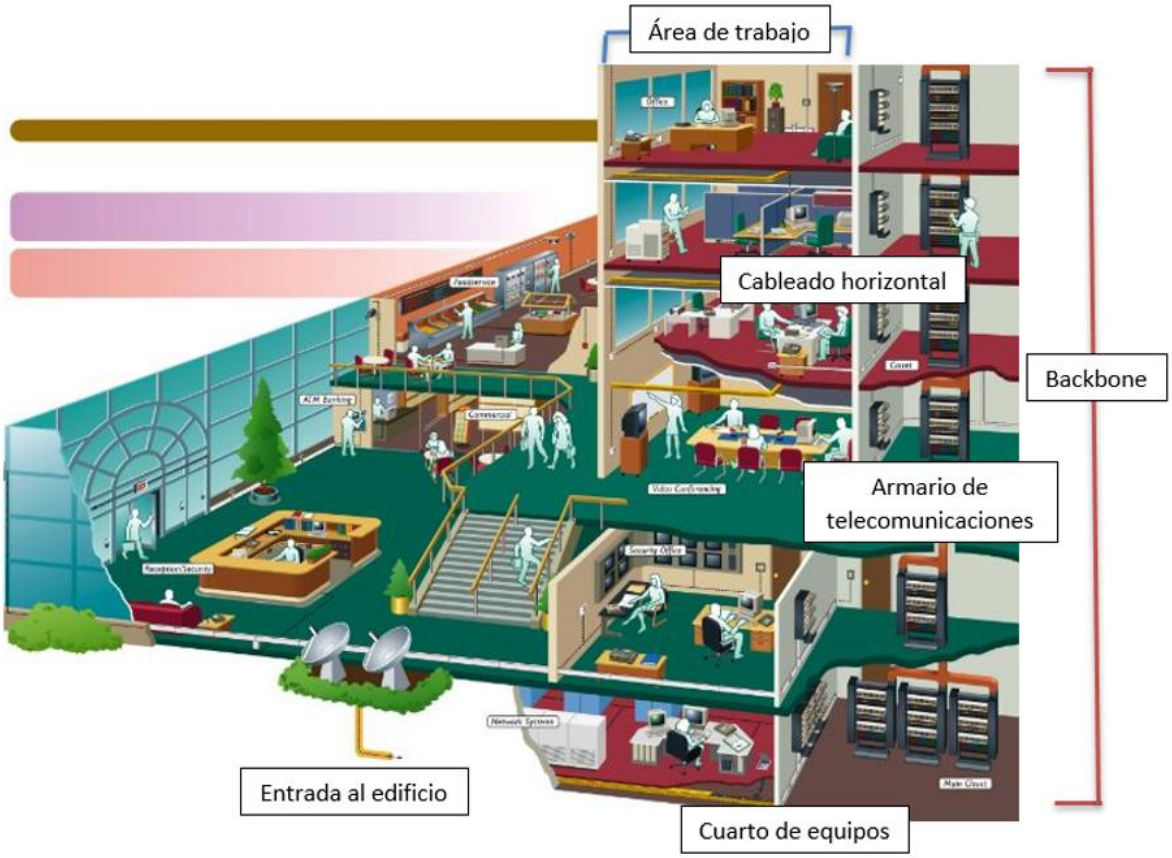


Figura 3.3.1. Cableado estructurado.

En este tema se explicará de forma básica las partes del cableado estructurado, sin embargo, en el Anexo B titulado "Cableado estructurado" se profundizará más en las recomendaciones necesarias para la instalación de este.

Estándar EIA/TIA 568

Estándar del cableado de Telecomunicaciones en Edificios Comerciales. Esta norma establece dos estándares (A y B) para el cableado ethernet 10Base-T, determinando qué color corresponde a cada pin del conector RJ45 como se aprecia en las figuras 3.3.2 y 3.3.3 y las tablas 3.3.1 y 3.3.2.

Tabla 3.3.1. Estándar 568-A.

Pin #	Par #	Función	Color del Cable
1	3	Transmite	Blanco/Verde
2	3	Recibe	Verde/Blanco
3	2	Transmite	Blanco/Naranja
4	1	Telefonía	Azul/Blanco
5	1	Telefonía	Blanco/Azul
6	2	Recibe	Naranja/Blanco
7	4	Respaldo	Blanco/Marrón
8	4	Respaldo	Marrón/Blanco

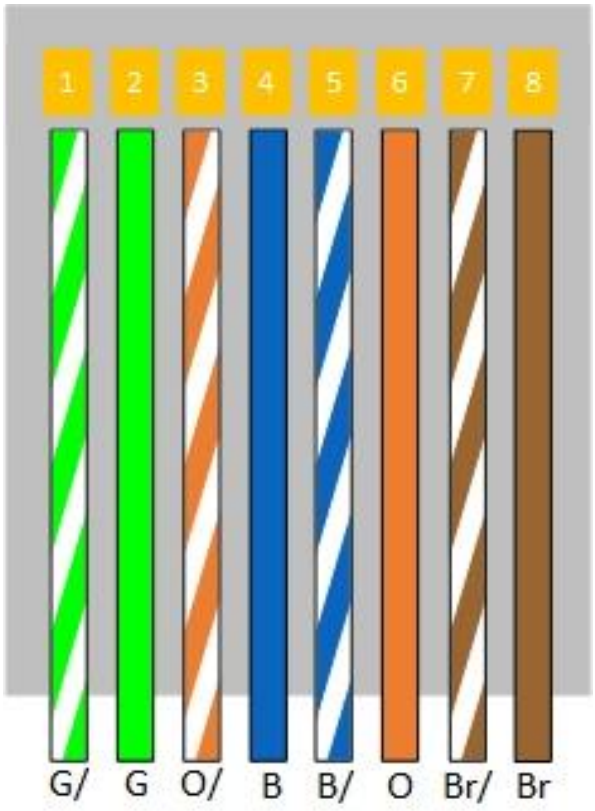


Figura 3.3.2. Estándar 568-A.

Tabla 3.3.2. Estándar 568-B.

Pin #	Par #	Función	Color del Cable
1	2	Transmite	Blanco/Naranja
2	2	Recibe	Naranja/Blanco
3	3	Transmite	Blanco/Verde
4	1	Telefonía	Azul/Blanco
5	1	Telefonía	Blanco/Azul
6	3	Recibe	Verde/Blanco
7	4	Respaldo	Blanco/Marrón
8	4	Respaldo	Marrón/Blanco

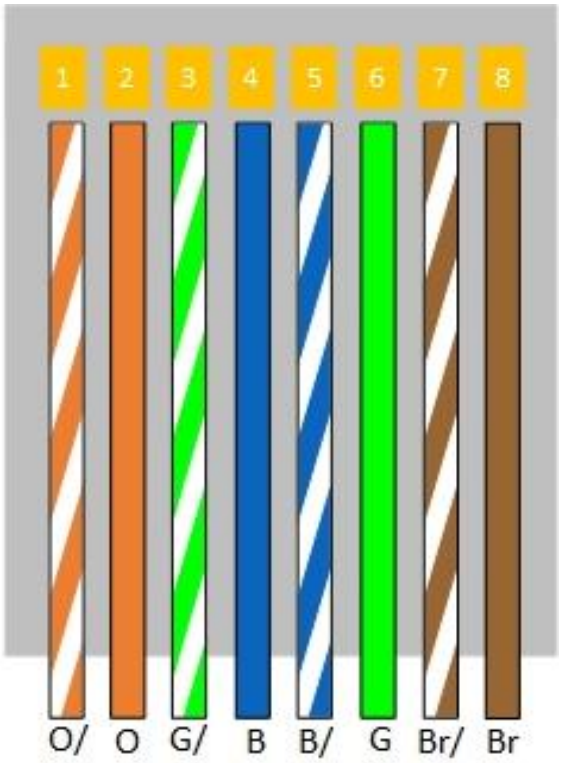


Figura 3.3.3. Estándar 568-B.

Cabe mencionar que los cables que se utilizan para interconectar los equipos, típicamente son llamados patch cord, los cuales se arman respetando el mismo estándar (A o B) en ambos extremos del cable. Estos cables se utilizan para:

- Conectar una estación de trabajo a la roseta que se encuentra en el área trabajo de una instalación de cableado estructurado.
- Conectar el patch panel con un hub o un switch en el armario de telecomunicaciones.
- Conectar directamente una estación de trabajo a un hub o un switch.

Se le denomina como cable cruzado al patch armado utilizando el estándar A en un extremo y el B en el otro. Estos cables se utilizan para:

- Conectar hubs o switch entre sí.
- Conectar dos estaciones de trabajo aisladas, a modo de una mini-LAN.
- Conectar una estación de trabajo y un servidor sin necesidad de un hub.

La norma garantiza que las redes que se apeguen a ella, soportarán todas las aplicaciones de telecomunicaciones presentes y futuras en un rango de 10 años, mediante una administración sencilla y sistemática de los cambios y reubicaciones de personal y equipos que se requieran.

Provee flexibilidad:

- Independencia del fabricante
- Facilita movimientos, adiciones y cambios
- Conectividad de sistema abierto

Mejor retorno de inversión:

- Mayor vida del sistema
- Menor costo del ciclo de vida

Como se aprecia en la figura 3.3.1, son seis los subsistemas que conforman el cableado estructurado de toda red a instalarse en un edificio, y cada uno de estos subsistemas se describen a continuación:

Entrada al edificio

Consta de los cables, hardware de conexión, dispositivos de protección, hardware de transición y equipo necesario para conectar e instalar los servicios externos con la red local.

Cuarto de equipos

Unen la entrada del edificio con el backbone, deben ser colocados en lugares cálidos, con temperaturas entre 21º y 23º C.

Backbone – Cableado vertical

Conecta los cuartos de telecomunicaciones, armarios e instalaciones de entrada. Cada cable sale de cada equipo a los armarios de telecomunicaciones.

Armario de telecomunicaciones

Punto de transición entre las vías de acceso o de backbone y de distribución horizontal. Sirve al piso en donde se encuentran, debe de estar dedicado a la función de telecomunicaciones.

Cableado horizontal

Es aquel que une la salida del armario de telecomunicaciones en cada piso con el área de trabajo. Debe tener un máximo de 100 metros, donde 90 metros son del patch panel del switch a la roseta. Los 10 metros restantes corresponden a 5 metros del backbone al switch y los otros 5 metros de la roseta al equipo de trabajo.

Área de trabajo

Es el espacio en donde el ocupante interactúa con los dispositivos de telecomunicaciones. Un mínimo de una salida de telecomunicaciones por área de trabajo.

Estándar EIA/TIA 569

Estándar para ductos y espacios de Telecomunicaciones en Edificios Comerciales que puedan soportar un ambiente de productos y proveedores múltiples. Esta norma indica los siguientes elementos para espacios y recorridos de telecomunicaciones en construcciones:

- **Recorridos entre los Edificios.** Están compuestos de recorridos de cables subterráneos, enterrados, aéreos o en túneles.
- **Estación de Trabajo.** Espacio interno de un edificio donde un ocupante actúa entre sí con dispositivos de telecomunicaciones.
- **Tomas de Telecomunicaciones.** Localización del punto de conexión entre el cable horizontal y los dispositivos de conexión del cable en el área de trabajo.
- **Recorridos Horizontales.** Implican en infraestructuras para instalación de cable de telecomunicaciones proveniente del armario e las mismas y destinado a una toma o conector de telecomunicaciones. Pueden ser de dos tipos: canaleta debajo del piso, piso de acceso, conducto eléctrico, bandejas y tuberías de cableado, cielo raso y perímetro.

- **Armarios de Telecomunicaciones.** Dedicado exclusivamente a la infraestructura de las telecomunicaciones. Equipos e instalaciones extraños a las telecomunicaciones no se deben instalar en estos armarios, ni pasar a través o entrar en los mismos.
- **Sala de equipos.** Espacio destinado para equipos de telecomunicaciones. Acomoda solamente equipos directamente relacionados con el sistema de telecomunicaciones y los sistemas de apoyo ambiental.

Estándar EIA/TIA 598-A

Estándar que establece el modo de agrupación de las fibras para la fibra óptica. Cada grupo será compuesto por 2, 4, 6 o hasta 12 fibras ópticas.

Los 12 colores son:

1 - Azul	4 - Café	7 - Rojo	10 - Morado
2- Naranja	5 - Gris	8 - Negro	11 - Rosa
3 - Verde	6 - Blanco	9 - Amarillo	12 - Agua

Cuando el primer grupo ya se ha utilizado por completo, se creará otro grupo teniendo en cuenta la clasificación según la norma:

Grupo 1 - Azul y sus 12 colores	*Grupo 7* - Rojo y sus 12 colores
Grupo 2 - Naranja y sus 12 colores	*Grupo 8* - Negro y sus 12 colores
Grupo 3 - Verde y sus 12 colores	*Grupo 9* - Amarillo y sus 12 colores
Grupo 4 - Café y sus 12 colores	*Grupo 10* - Morado y sus 12 colores
Grupo 5 - Gris y sus 12 colores	*Grupo 11* - Rosa y sus 12 colores
Grupo 6 - Blanco y sus 12 colores	*Grupo 12* - Aqua y sus 12 colores

De esta manera podemos tener desde 2 fibras hasta 144 fibras en un solo cable.

Estándar EIA/TIA 606

Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales. Habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tengan que habilitar o deshabilitar.

Estándar EIA/TIA 607

El sistema de puesta a tierra es muy importante en el diseño de una red ya que ayuda a maximizar el tiempo de vida de los equipos, además de proteger la vida del personal a

pesar de que se trate de un sistema que maneja voltajes bajos. Aproximadamente el 70% de anomalías y problemas asociados a sistemas distribución de potencia son directa o indirectamente relacionados a temas de conexiones y puestas a tierra. A pesar de esto, el sistema de puesta a tierra es uno de los componentes del cableado estructurado más obviados en la instalación.

El estándar que describe el sistema de puesta a tierra para las redes de telecomunicaciones es ANSI/TIA/EIA-607. El propósito principal es crear un camino adecuado y con capacidad suficiente para dirigir las corrientes eléctricas y voltajes pasajeros hacia la tierra. Estas trayectorias a tierra son más cortas de menor impedancia que las del edificio.

Los términos básicos para entender un sistema de puesta a tierra en general son:

- **Puesta a tierra (grounding).** Es la conexión entre un equipo o circuito eléctrico y la tierra.
- **Conexión equipotencial a tierra (bonding).** Es la conexión permanente de partes metálicas para formar una trayectoria conductora eléctrica que asegura la continuidad eléctrica y la capacidad de conducir de manera segura cualquier corriente que le sea impuesta.
- **Conductor de enlace equipotencial para telecomunicaciones (BCT).** Es un conductor de cobre aislado que interconecta el sistema de puesta a tierra de telecomunicaciones al sistema de puesta a tierra del edificio. Por lo tanto, une el TMGB con la puesta a tierra del sistema de alimentación. Debe ser dimensionado al menos de la misma sección que el conductor principal de enlace de telecomunicaciones (TBB). No debe llevarse en conductos metálicos.
- **Barra de tierra principal de telecomunicaciones (TMGB).** Es una barra que sirve como una extensión dedicada del sistema de electrodos de tierra (pozo a tierra) del edificio para la infraestructura de telecomunicaciones. Todas las puestas a tierra de telecomunicaciones se originan en él, es decir que sirve como conexión central de todos los TBB's del edificio. Las consideraciones del diseño son:
  - Usualmente se instala una por edificio.
  - Generalmente está ubicada en el cuarto de entrada de servicios.
  - En el cuarto de equipos, en cualquiera de los casos se tiene que tratar de que el BCT sea lo más corto y recto posible.
  - Montada en la parte superior del tablero o caja.
  - Aislada del soporte mediante aisladores poliméricos (50 mm mínimo).
  - Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y 100 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.

- **Barra de tierra para telecomunicaciones (TGB).** Es la barra de tierra ubicada en el cuarto de telecomunicaciones o de equipos que sirve de punto central de conexión de tierra de los equipos de la sala. Las consideraciones del diseño son:
  - Cada equipo o gabinete ubicado en dicha sala debe tener su TGB montada en la parte superior trasera.
  - El conductor que une el TGB con el TBB debe ser cable 6 AWG. Además, se debe procurar que este tramo sea lo más recto y corto posible.
  - Hecha de cobre y sus dimensiones mínimas 6 mm de espesor y 50 mm de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.
  - Aislada mediante aisladores poliméricos.
- **Conductor central de enlace equipotencial de telecomunicaciones (TBB).** Es un conductor aislado de cobre utilizado para conectar todos los TGBs al TMGB. Su principal función es la de reducir o ecualizar todas las diferencias de potencial de todos los sistemas de telecomunicaciones enlazados a él. Las consideraciones del diseño son:
  - Se extiende a través del edificio utilizando la ruta del cableado vertical.
  - Se permite varios TBBs dependiendo del tamaño del edificio (véase figura 3.3.4).
  - Se deberá usar un conductor de cobre aislado cuya sección acepte estas medidas.
  - El estándar ha establecido una relación entre la longitud del cable y el calibre de éste para diseñar el conductor como se muestra en la tabla 3.3.4.

Tabla 3.3.3. Dimensionamiento del TBB.

Longitud del TBB (m)	Calibre (AWG)
Menor a 4	6
4 - 6	4
6 - 8	3
8 - 10	2
10 – 13	1
13 – 16	1/0
16 – 20	2/0
Mayor a 20	3/0

Deben evitarse empalmes, pero si de todas maneras existen, éstos deben estar ubicados en algún espacio de telecomunicaciones.

Es importante mencionar que los conectores usados en la TMGB y los usados en la conexión entre el TBB y el TGB, deberán ser de compresión de dos perforaciones. Mientras que la conexión de conductores para unir equipos de telecomunicaciones a la

TMGB o TGB pueden ser conectores de compresión por tornillo de una perforación, aunque no es lo más recomendable debido a que pueden aflojarse por cualquier movimiento (véase figura 3.3.5).

Todos los elementos metálicos que no lleven corriente en el sistema de cableado estructurado deberán ser puestos a tierra, como por ejemplo los racks.

Cualquier doblez que se tenga que realizar a los cables no debe ser mayor a 2,54 cm.

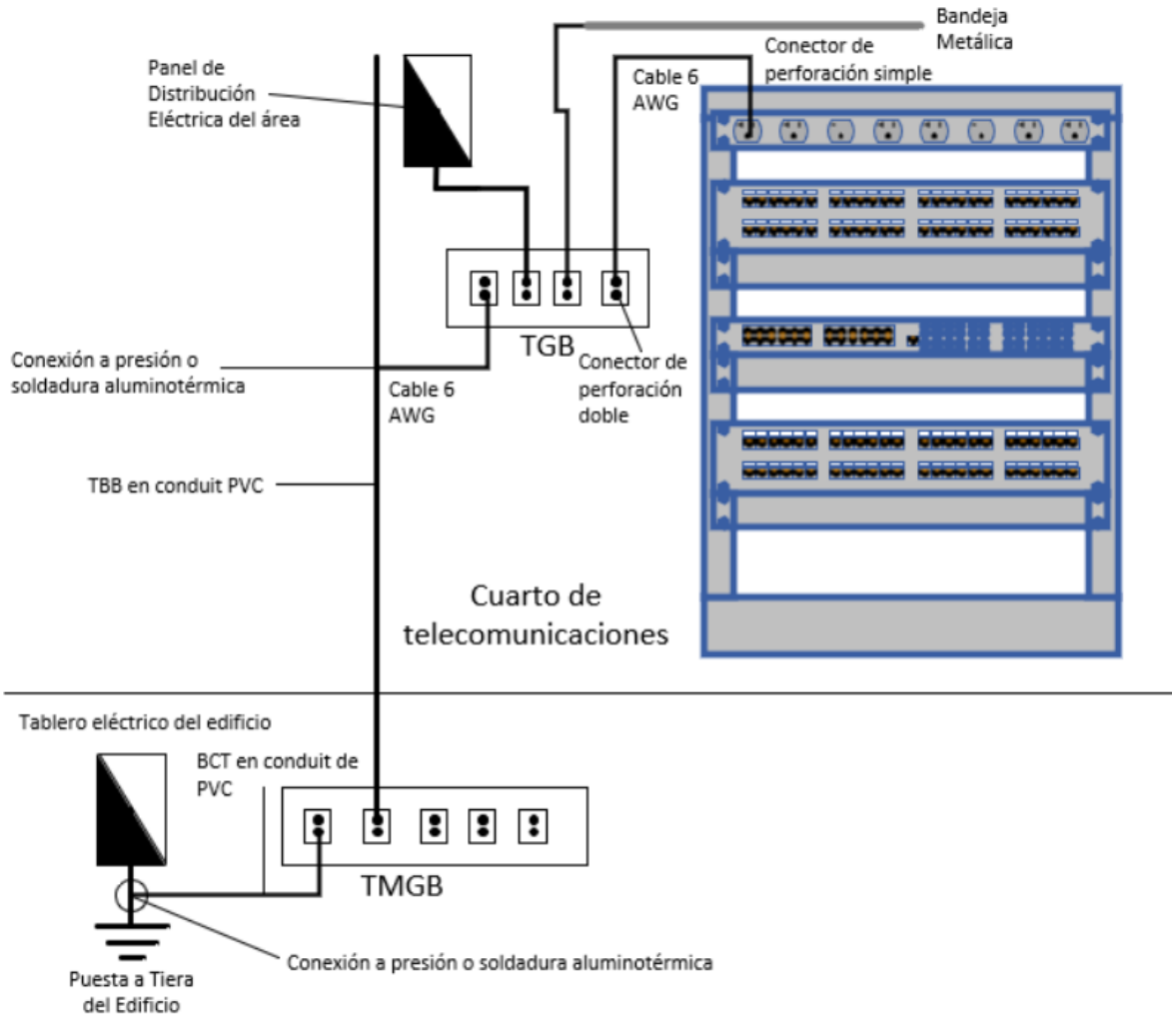


Figura 3.3.4. Puesta a tierra para telecomunicaciones.

3.4 Dispositivos de interconexión

Activos

Son aquellos equipos que se encargan de distribuir en forma activa la información a través de la red. Además, se encargan de distribuir banda ancha a determinada cantidad de equipos.

Pasivos

Se utilizan para interconectar los enlaces de una red de datos.

Repetidor

Es un dispositivo sencillo utilizado para regenerar una señal entre dos nodos de una red. De esta manera, se extiende el alcance de la red (véase figura 3.4.1).

Figura 3.4.1. Repetidor.

Hub

Es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples ordenadores y regenerar la señal (véase figura 3.4.2).

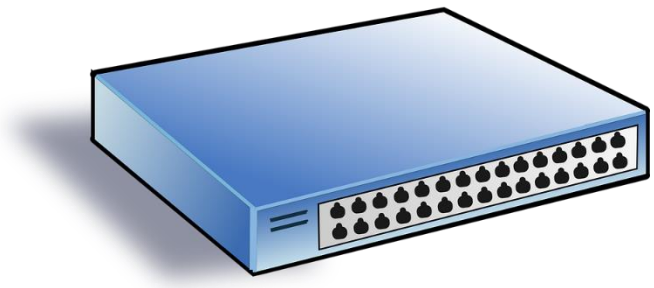


Figura 3.4.2. Hub.

Patch Cord

Es el cable que va de la toma terminal a la estación de trabajo o del panel de parcheo al hub (véase figura 3.4.3).

Figura 3.4.3. Patch cord.

Gabinete

Su función es alojar equipamiento electrónico, informático y de comunicaciones (véase figura 3.4.4).

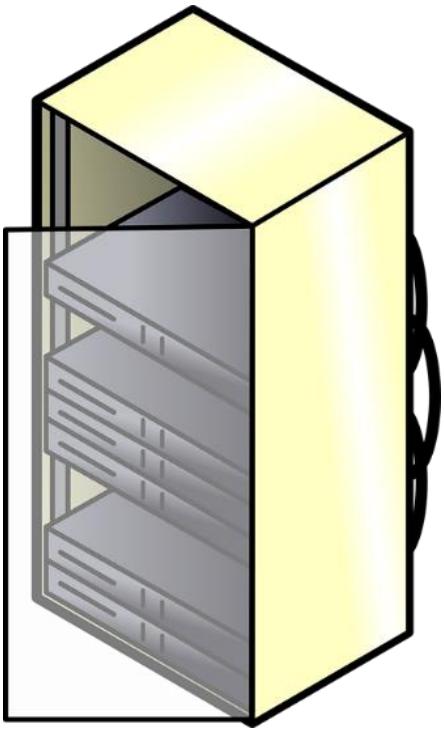


Figura 3.4.4. Gabinete.

Rack

Es el equipo donde se agrupa o ubican los hubs, paneles de parcheo, switchs, y routers principalmente (véase figura 3.4.5).

Figura 3.4.5. Rack.

Patch Panel

Es el recolector central de los cables que vienen de las áreas de trabajo al armario de comunicaciones. Generalmente van fijadas a un rack (véase figura 3.4.6).

Figura 3.4.6. Patch panel.

Conector RJ45

Es una interfaz física comúnmente usada para conectar redes de cableado estructurado (véase figura 3.4.7).

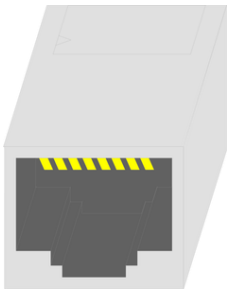


Figura 3.4.7. Conector RJ45.

Canaleta

Son canales plásticos que protegen el cable de tropiezos y rupturas, dando además una presentación estética al cableado interno del edificio (véase figura 3.4.8).

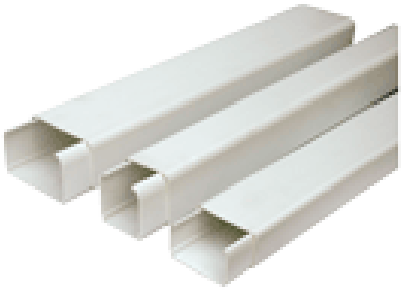


Figura 3.4.8. Canaleta.
(Tomada de: www.psolera.com)

3.5 Seguridad a nivel de capa física

Cuando se habla de seguridad física se hace referencia a todos aquellos mecanismos de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

Control de acceso físico

Desde una perspectiva de seguridad informática, a este nivel debemos preocuparnos por impedir que terceros no autorizados ingresen a las instalaciones. Entre otras medidas, encontramos la implementación de un sistema de alarma, de vigilancia y la disposición de barreras y dispositivos de control de acceso a las facilidades donde se encuentra desplegada la red.

Otro riesgo a considerar es la "amenaza interna", es decir, personal autenticado realizando acciones no autorizadas, o que persiguen un fin perjudicial. La disposición de los cables no debe permitir escuchas indebidas, y para ello se vuelve necesario restringir el acceso a la sala de telecomunicaciones, y proteger el cableado y equipos para que no puedan ser intencionalmente dañados con el objeto de provocar un ataque a la disponibilidad del servicio.

Para evitar todo este tipo de problemas, es recomendable implementar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe es necesario detectar los accesos no autorizados cuanto antes e instalar los mecanismos de seguridad pertinentes).

- Utilización de guardias
- Utilización de detectores de metales
- Utilización de sistemas biométricos
- Verificación autómata de firmas
- Seguridad con animales

En muchos casos es suficiente con controlar el acceso a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles.

Para la detección de accesos se emplean medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, aunque en muchos entornos es suficiente con qué las personas que utilizan los sistemas se conozcan entre sí y sepan quién tiene y no tiene acceso a las distintas salas y equipos, de modo que les resulte sencillo detectar a personas desconocidas o a personas conocidas que se encuentran en sitios no adecuados.

Desastres naturales

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves

consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.

Algunos desastres naturales a tener en cuenta:

- Terremotos y vibraciones
- Tormentas eléctricas
- Inundaciones y humedad
- Incendios

Terremotos

Hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas o grandes vibraciones:

- No situar equipos en sitios altos para evitar caídas
- Evitar la colocación elementos móviles sobre los equipos para evitar que caigan sobre ellos
- Separar los equipos de las ventanas para evitar que caigan por ellas o que objetos lanzados desde el exterior los dañen
- Utilizar fijaciones para elementos críticos
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones

Inundaciones

Esta es una de las causas de mayores desastres en centros de cómputo. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas:

- Construir un techo impermeable para evitar el paso de agua desde un nivel superior
- Acondicionar las puertas para contener el agua que bajase por las escaleras.

Firestopping (contención del fuego)

Es reestablecer la integridad de las estructuras y ensambles arquitectónicos para que contengan el fuego (paredes y pisos entre otros) cuando las barreras sean penetradas por:

- Tubos
- Ductos
- Cables
- Ductos internos
- Charolas de cable
- Otros elementos

Clasificaciones de las Barreras Anti-fuego

- **Clasificación F (Horas).** No permite que las flamas pasen a través de la barrera anti-fuego.
- **Clasificación T (Temperatura).** Limita el aumento de temperatura.
- **Clasificación L (Fuga de Aire).** Indica que la barrera provee una detención efectiva de humo.

Información en los Sistemas de las Barreras de Anti-fuego

- **Mecánicos.** Consisten de componentes elastoméricos pre-fabricados moldeados para ajustarse alrededor de cables estándar, tubos y conductos.
- **No-mecánicos.** Masilla, calafateo, cememtitious, hojas intumescentes, tiras para envolturas, espuma de silicón, almohadillas pre-fabricadas.

Instalaciones

Para la implementación de la seguridad en una red, se debe de tener como primer énfasis la seguridad en instalaciones físicas.

Instalación de las tomas de corriente. Esta tarea suele realizarla un electricista, pero desde el punto de vista del proyecto se debe asegurar de que haya suficientes tomas de corriente para alimentar todos los equipos de comunicaciones.

Figura 3.5.1. Tomas de corriente.

Instalación de rosetas y jacks. Es la instalación de los puntos de red finales desde los que se conectarán los equipos de comunicaciones sirviéndose de latiguillos. La mayor parte de estas conexiones residirán en canaletas o en armarios de cableado.

Figura 3.5.2. Roseta.

Tendido de los cables. Se trata de medir la distancia que debe recorrer cada cable y añadirle una longitud prudente que permita trabajar cómodamente con él antes de cortarlo. Debemos tener cuidado de verificar que el cable que se utilizará tenga la certificación necesaria.

Conexión de los cables en los patch panels y en las rosetas utilizando las herramientas de crimpado apropiadas. A esto se le denomina cross-connect.

Probado de los cables instalados. Cada cable construido y conectado debe ser previamente probado para asegurarse de que cumplirá correctamente su función.

Etiquetado y documentación del cable y conectores. Todo cable debe ser etiquetado en ambos extremos, así como los conectores de patch panels y rosetas, de modo que queden identificados unívocamente.

Figura 3.5.3. Etiquetado de cables.
(Obtenida de: https://www.conectronica.com/cableado-estructurado/etiqueta-giratoria-para-cableado)

Instalación de los adaptadores de red. Gran parte de los equipos informáticos vienen ya con la tarjeta de red instalada, de no ser este caso, se debe de instalar uno.

Instalación de los dispositivos de red. Se trata de instalar los concentradores, conmutadores, puentes y encaminadores. Algunos de estos dispositivos deben ser configurados antes de prestar sus servicios.

Configuración del software de red en clientes y servidores de la red.

Para trabajar con seguridad hay que tomar en cuenta las normativas laborales de seguridad en el trabajo.

El correcto funcionamiento del sistema de cableado es tan importante que en muchas instalaciones se exige la certificación de cada uno de los cables, es decir, se compara la calidad de cada cable con unos patrones de referencia propuestos por un estándar. En el

caso de los cables de cobre, la norma comúnmente utilizada es la ANSI/TIA/EIA-TSB-67 del año 1995, la norma EIA/TIA 568 y su equivalente norma ISO IS11801.

La certificación de una instalación significa que todos los cables que la componen cumplen con esos patrones de referencia y, por tanto, se tiene la garantía de que cumplirán con las exigencias para las que fueron diseñados.

Las consideraciones del EIA/TIA 568 especifican los siguientes elementos:

- Requerimientos mínimos para el cableado de telecomunicaciones.
- Topología de la red y distancias máximas recomendadas.
- Parámetros determinantes del rendimiento.

En esta norma se incluyen otras como la TSB36A que determina las características de los cables de pares trenzados de 100 ohmios, la norma TSB40A que indica las características de los conectores RJ45 y sus conexiones, o la norma TSB53 que especifica los cables blindados de 150 ohmios y sus conectores.

La organización internacional TIA/EIA contempla un conjunto de estándares para el cableado estructurado:

TIA/EIA-568-B.1. Estándar Con requisitos generales para el cableado de telecomunicaciones en edificios comerciales.

TIA/EIA-568-B.2. Componentes de cableado de par trenzado.

TIA/EIA-568-B.3. Componentes de cableado de fibra óptica.

TIA/EIA-568-B. Estándares de cableado.

TIA/EIA-569-A. Estándares sobre recorridos y espacios de telecomunicaciones para edificios comerciales.

TIA/EIA-570-A. Estándar para el cableado de comunicaciones en zonas residenciales y pequeño comercio.

TIA/EIA-606. Estándar de administración de la infraestructura de telecomunicaciones en edificios comerciales.

TIA/EIA-607. Especificación de requisitos de conexión a tierra.

Tema 4

Capa de enlace de datos

Objetivo: El alumno analizará los diferentes tipos de protocolos, métodos y estándares utilizados en la capa de enlace, así como su aplicación en dispositivos físicos de esta capa.

Esta capa del modelo OSI es la responsable del intercambio de datos entre un host cualquiera, y la red a la que está conectado, permitiendo una correcta comunicación entre las capas superiores (Red, Transporte y Aplicación) y el medio físico de transporte de datos. Su principal objetivo es la de proveer una comunicación segura entre dos nodos pertenecientes a una misma red o subred, para ello se encarga de la notificación de errores, de la topología de la red y el control de flujo en la transmisión de las tramas.

4.1 Subcapa LLC del estándar IEEE 802 para redes de área local

La capa LLC (Control de Enlace Lógico – Logical Link Control) define el protocolo de control de enlaces lógicos del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación. La capa de Enlace de Datos en el protocolo OSI esta subdividida en las subcapas de Control de Acceso a Medios (MAC) y de Control de Enlaces Lógicos (LLC).

Su trabajo es ocultar las diferencias entre las variantes 802 con la finalidad de que sean imperceptibles para la capa de red. Y es responsable de la transferencia fiable de los datos a través del medio de transmisión de datos, la cual se realiza mediante tramas que son las unidades de información para el intercambio de datos en la capa de enlace.

Los requisitos que cubre la capa de enlace de datos son:

1. **Sincronización de la trama:** comprende los procesos necesarios para adquirir, mantener y recuperar la sincronización de carácter u octeto.
2. **Control de flujo:** se encarga de vigilar y tomar los acuerdos necesarios para que en el intercambio de datos el emisor no sature al receptor.
3. **Control de errores:** su objetivo es proporcionar detección y corrección de errores en el envío de tramas entre los participantes de un intercambio de datos.
4. **Direccionamiento:** su tarea es ingresar en la trama las direcciones de origen y destino del hardware de control de acceso, esto es, la dirección de la tarjeta de red de cada equipo, a la que también se le conoce como dirección física o dirección MAC.
5. **Bloque de datos + información de control:** es indispensable que viajen conjuntamente en la misma trama los datos propios del intercambio y la información necesaria para controlar el intercambio y que la transferencia sea exitosa.
6. **Gestión de enlace:** atiende a dos tipos de comunicaciones, las que atienden a un centralizado como es el caso de la topología en estrella; y las que corresponden a un sistema distribuido como es el caso de las topologías bus y anillo, por ejemplo.

Los servicios que proporciona son:

Servicios sin conexión y sin acuse de recibo. El transmisor manda tramas al destino. Uso. si la frecuencia de errores es muy baja o el tráfico es de tiempo real (voz).

- **Servicio sin conexión y con acuse de recibo**. El receptor manda un acuse de recibo al transmisor por cada frame recibido.
- **Servicio orientado a conexión con acuse de recibo**. Provee un flujo confiable de bits. Se establece conexión antes de enviar datos. Los frames se enumeran y todos se reciben una vez y en orden correcto.

Protocolos de enlace para redes alámbricas (Ethernet)

CSMA/CD

En CSMA/CD (Carrier Sense Multiple Access with Collision Detection) como su nombre lo indica, el control de acceso al medio de transmisión se encarga de la detección de colisiones, el dispositivo monitorea los medios para detectar la presencia de una señal de datos (ver figura 4.1.1). Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si posteriormente se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet usan este método.

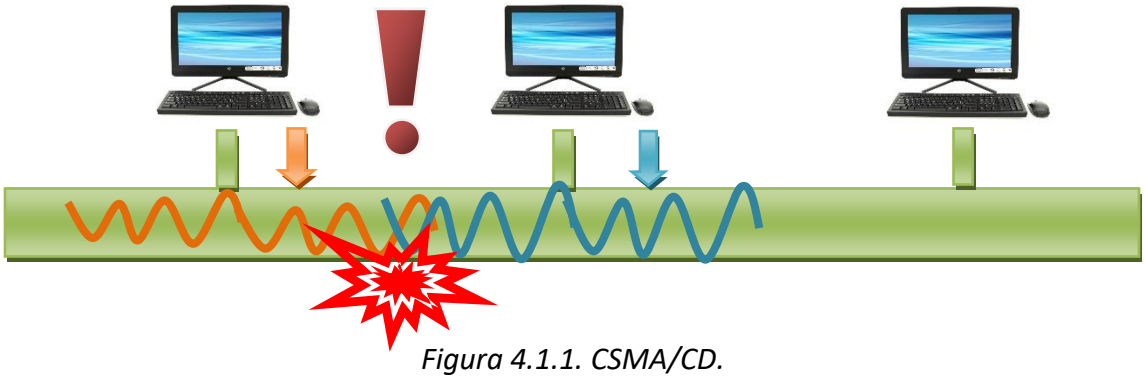


Figura 4.1.1. CSMA/CD.

En CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) como su nombre lo indica, el control de acceso al medio de transmisión se encarga de la prevención de colisiones, el dispositivo examina los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. El dispositivo luego envía los datos. Este método es utilizado por las tecnologías de redes inalámbricas.

Ethernet

Ethernet es una tecnología para redes de datos por cable que vincula software y/o hardware entre sí. Esto se realiza a través de cables de redes LAN, de ahí que Ethernet sea concebido habitualmente como una tecnología LAN. Así, Ethernet permite el intercambio

de datos entre terminales como, por ejemplo, ordenadores, impresoras, servidores, distribuidores, entre otros. Conectados en una red local, estos dispositivos establecen conexiones mediante el protocolo Ethernet y pueden intercambiar paquetes de datos entre sí. El protocolo actual y más extendido para ello es IEEE 802.3.

Ethernet fue desarrollado a principios de los 1970, época en la que solo se utilizaba como sistema interno de red en la empresa Xerox, y no fue hasta principios de los ochenta que Ethernet se convirtió en un producto estandarizado. Con todo, aún habría que esperar hasta mediados de la década para que empezara a utilizarse más ampliamente. Fue cuando los fabricantes comenzaron a trabajar con Ethernet y con productos relacionados. Así, dicha tecnología contribuyó de manera significativa a que los ordenadores personales revolucionaran el mundo laboral. El estándar IEEE 802.3 tan popular actualmente se utiliza, por ejemplo, en oficinas, viviendas particulares, contenedores y portadores (carrier).

Mientras que la primera versión de esta tecnología solo tenía una velocidad de 3 Mbit/s, los protocolos Ethernet actuales permiten alcanzar velocidades de hasta 1 000 megabits por segundo. Por otro lado, los estándares Ethernet antiguos se restringían a un solo edificio, mientras que hoy en día pueden alcanzar hasta los 10 km gracias a la utilización de la fibra de vidrio. En el transcurso de su desarrollo, Ethernet ha tenido el rol dominante entre las tecnologías LAN y ha destacado entre sus numerosos competidores. La conocida como Ethernet en tiempo real es en la actualidad un estándar industrial para aplicaciones de comunicación.

Trama Ethernet (ver figura 4.1.2)

?	1	6	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección Destino	Dirección Origen	Tipo	Datos	Secuencia de verificación de trama

Figura 4.1.2. Trama Ethernet.

Preámbulo. Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.

Inicio de trama (SOF). Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.

Direcciones destino y origen. Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección

única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).

Tipo (Ethernet). Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

Longitud (IEEE 802.3). Indica la cantidad de bytes de datos que sigue este campo.

Datos. Incluye los datos enviados en la trama. En las especificaciones IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama).

Secuencia de verificación de trama (FCS). Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese.

El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes. El número de nodos que comparten el medio, la carga de trabajo o información que desee enviar cada uno de los nodos y la distancia o longitud del medio compartido (si es aéreo, sería más bien el rango de frecuencia usado se tiene define en el estándar ethernet que se esté utilizando.

Estándares IEEE 802 para redes alámbricas

La tabla 4.1.1 muestra las características de los distintos tipos de estándar de ethernet.

Tabla 4.1.1. Comparativa de los estándares Ethernet.

Estándar de Ethernet	Denominación	Velocidad de datos	Tecnología de cables	Año de publicación
802.3	10Base5	10 MB/s	Cable coaxial	1983
802.3a	10Base2	10 MB/s	Cable coaxial	1988
802.3i	10Base-T	10 MB/s	Cable de par trenzado	1990
802.3j	10Base-FL	10 MB/s	Cable de fibra óptica	1992
802.3u	100Base-TX100Base-FX100Base-SX	100 MB/s	Cable de par trenzado, cable de fibra óptica	1995
802.3z	1000Base-SX1000Base-LX	1 GB/s	Cable de fibra óptica	1998
802.3ab	1000Base-T	1 GB/s	Cable de par trenzado	1999
802.3ae	10GBase-SR, 10GBase-SW,	10 GB/s	Cable de fibra óptica	2002

	10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW, 10GBase-LX4			
802.3an	10GBase-T	10 GB/s	Cable de par trenzado	2006
802.3ba	40GBase-SR4/LR4 100GBase-SR10/LR4/ER4	40 GB/s 100 GB/s	Optimizado por láser MMF o SMF	2010
802.3bq	40GBase-T	40 GB/s	Cable de par trenzado	2015

Protocolos de enlace para redes inalámbricas (Wi-Fi)

Las redes inalámbricas son aquellas en la que los extremos de la comunicación no se encuentran unidos por un medio de propagación físico, sino por ondas electromagnéticas a través de aire.

CSMA/CA

CSMA (Carrier Sense Multiple Access – Acceso múltiple con escucha de señal portadora) es un algoritmo de acceso al medio compartido. Trata de reducir el riesgo de colisión y al mismo tiempo introduce un plan de actuación en caso de que se produzca (ver figura 4.1.3). Lo más importante a cumplir en estos procesos de comunicación establece que dos o más dispositivos no pueden realizar envíos al mismo tiempo.

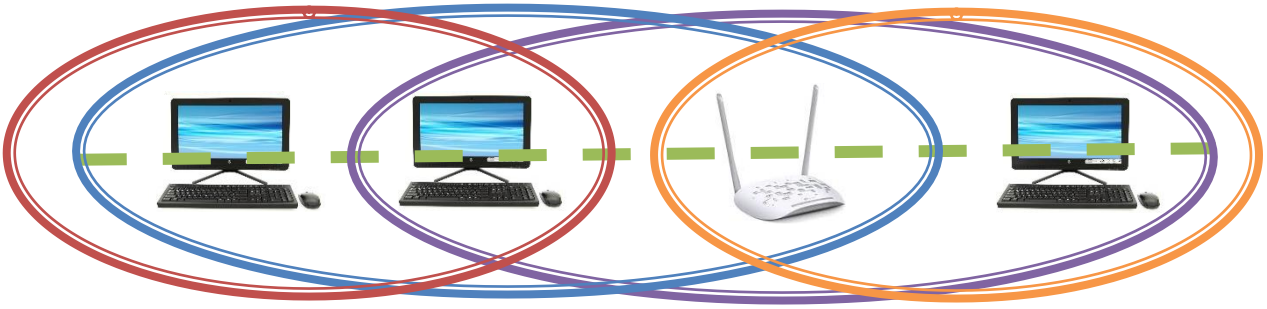


Figura 4.1.3. CSMA/CA.

Estándares IEEE 802 para redes inalámbricas

El estándar internacional 802.11 define las características de una red de área local inalámbrica. WiFi es conocida como Wireless Fidelity, que se retiene al estándar 802.11, creado en 1997 por la IEEE.

Estándar 802.11a. Creado en 1999. Soporta velocidades de hasta 54 Mbps y trabaja a una frecuencia de 5 GHz. Su técnica de modulación es OFDM (Orthogonal Frequency Division Multiplexing – Multiplexación por División de Frecuencia Ortogonales). Requiere línea de vista, por lo que necesita un número elevado de repetidores para cubrir una zona. No traspasa muros, por lo que es de alcance reducido.

Estándar 802.11b. Se publicó en 1999. Se pueden seleccionar tasas de transmisión entre 1, 2, 5.5 y 11 Mbps. Tiene un alcance de 100 a 300 metros, trabaja en la banda de frecuencia de 2.4 GHz. La técnica de modulación que utiliza es DSSS (Direct Sequence Spread Spectrum – Espectro Esparcido de Secuencia Directa). Tiene un mayor alcance que el 802.11a ya que sus ondas son fácilmente absorbidas por paredes, pero sufre interferencias de productos que operan en la misma banda, como microondas, teléfonos inalámbricos, monitores de bebé, dispositivos bluetooth, entre otros.

Estándar 802.11e. Su calidad de servicio se utiliza para transmisión de datos, voz o video.

Estándar 802.11f. Su inter operatividad de puntos de acceso funciona entre dispositivos de distintos fabricantes.

Estándar 802.11g. Aprobado en 2003. Utiliza la banda de los 2.4 GHz, con una tasa máxima de trasferencia de 54 Mbps y una velocidad real de 24.7 Mbps. Es compatible con el estándar 802.11b y utiliza las mismas frecuencias.

Estándar 802.11h. Define la administración del espectro de la banda de los 5 GHz para uso en Europa y Asia Pacífico.

Estándar 802.11i. Su seguridad opera con base en cifrado y autenticación. Los datos de las tramas se cifran antes de ser enviados. Los usuarios son autenticados antes de que se les permita hacer uso de la red inalámbrica.

Estándar 802.11n. Se aprobó en septiembre de 2009. Su velocidad es de 300 Mbps. Trabaja en bandas de frecuencia de 5 y 2.4 GHz. El formato de la trama de este estándar se representa en la figura 4.1.4.

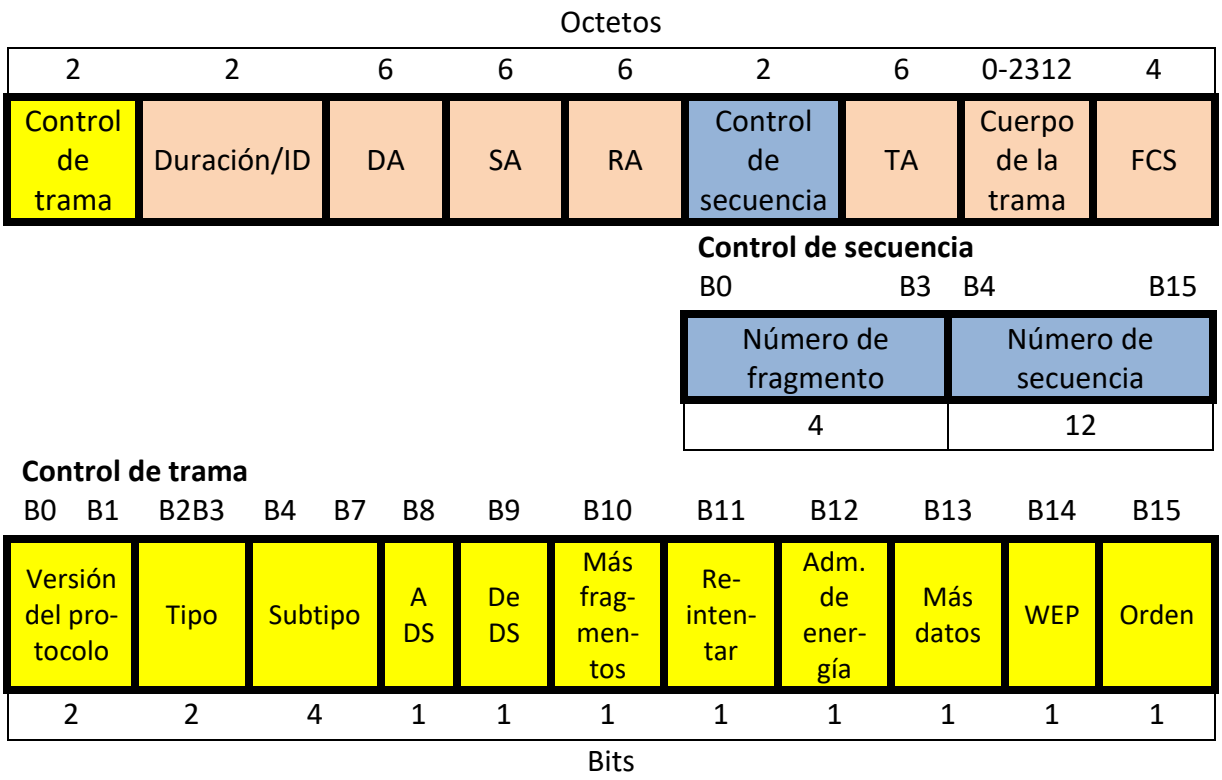


Figura 4.1.4. Formato de Trama 802.11.

Control de Trama: Tiempo que se ocupará en la transmisión de la trama y su confirmación.
DA: Origen.
SA: Destino.
RA: AP Origen.
Control de secuencia: Para numerar fragmentos: 12 bits para identificación de trama y 4 para fragmento.
TA: AP Destino.
Cuerpo de la trama: 2312 bytes de carga útil.
FCS: Para control de errores.

Control de Trama

Versión de protocolo: permite que 2 versiones operen al mismo tiempo.
Tipo: Datos, Control, Administración.
Subtipo: RTS (solicita), CTS (acepta), ACK (confirma +).
A DS – De DS: la trama va hacia o viene del Sistema de Distribución.
Más Fragmentos
Reintentar: Retransmisión de la trama.

Administración de energía: lo utiliza la estación base para poner al receptor en modo hibernación o sacarlo de él.
Más datos: el emisor tiene más tramas para el receptor.
W: especifica que la trama se ha codificado utilizando un algoritmo de seguridad.
O: indica al receptor que debe procesar las tramas en orden estricto.

Estándar 802.16

El nombre comercial para el estándar 802.16 es WiMax (Worldwide Interoperability for Microwave Access). Es un protocolo para redes de área metropolitana (MAN), utiliza la arquitectura punto-multipunto. Fue publicado en el año 2002, trabaja en el rango de 10 a 66 GHz. Necesita línea de visión directa, con una capacidad de hasta 134 Mbps.

Estándar 801.16a. Publicado en el año 2003. Trabaja en el rango de 2 a 11 GHz, con sistemas sin línea de vista y con línea de vista.

Estándar 801.16b. Incrementó el espectro de 5 a 6 GHz. Se caracterizó por aportar una fuerte calidad de servicio.

Estándar 801.16c. Publicado en 2003. Opera en el rango de frecuencias de 10 a 66 GHz. Mejoró la interoperabilidad.

Estándar 801.16-2004. Versión fija del estándar WiMax, opera en frecuencias de 2 a 11 GHz, velocidad de transmisión de 70 Mbps.

Estándar 801.16e. Versión móvil de WiMax, publicado en 2005. Permite utilizar el sistema de comunicaciones inalámbricas con terminales en movimiento (ver figura 4.1.5).

Componentes de una red WiMax

Consta de dos componentes principales:

1. **Estación base WiMax**
   - Torre WiMax
   - Brinda una cobertura a un área de 7500 km^2
2. **Un receptor WiMax**
   - Debe contener una antea por separado para recibir la señal (tarjeta de red inalámbrica)

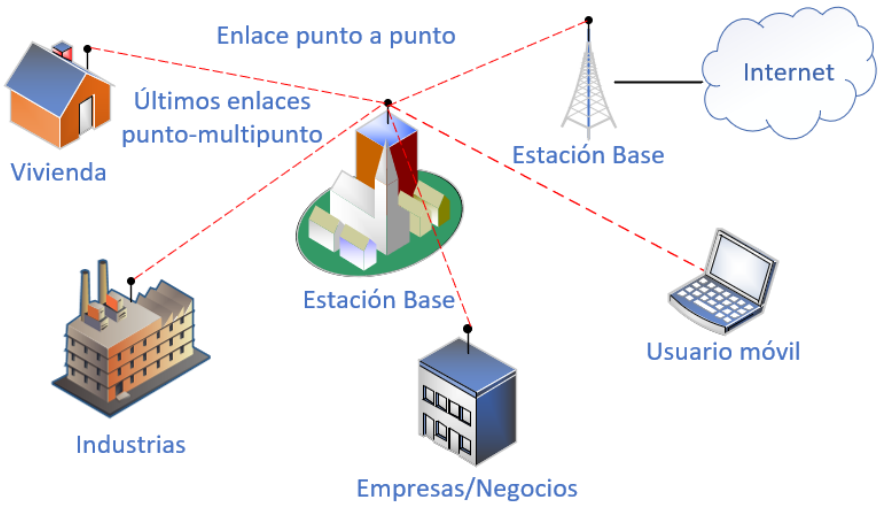


Figura 4.1.5. Estructura WiMax.

Características

- **Gran ancho de banda.** Una sola base puede admitir de manera simultánea conexiones tipo DSL.
- **Es independiente de protocolo.** Puede transportar IP, ethernet y otros. Eso hace que sea compatible con otros estándares como WiFi, ethernet o token ring.

Seguridad

- Medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos DES y RSA.
- Operación en un amplio rango de frecuencias de los 450 MHz a los 5.8 GHz (inicialmente en Latinoamérica en 2.3, 2.5 y 3.5 GHz).

Ventajas

- Veloccidad: 50 km a 70 Mbps
- Modos de ahorro de energía “sleep”
- Excelente cobertura en esquemas sin línea de vista
- Transmite VoIP, dayos o videos y tiene soporte de IPv6, QoS y VoIP.

Desventajas

- Implementación complicada
- Falta de un marco regulatorio
- Requerimientos de algoritmos y funciones de procesamiento complejos
- Limitación de potencia para proveer interfaces con otros sistemas y el alto consumo de batería

Estándar 802.15

El Estándar IEEE 802.15 se enfoca básicamente en el desarrollo de estándares para redes tipo WPAN o redes inalámbricas de corta distancia. Al igual que Bluetooth el 802.15 permite que dispositivos inalámbricos portátiles como PCs, PDAs, teléfonos, pagers, entre otros, puedan comunicarse e ínter operar uno con el otro. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11x, de alguna manera la IEEE definió este estándar para permitir la interoperabilidad de las redes inalámbricas LAN con las redes tipo PAN.

Bluetooth es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

Seguridad

Las redes inalámbricas están mucho más expuestas que las LAN's normales a problemas de seguridad. Algunos mecanismos que ayudan a mejorar la seguridad son:

- Desactivar el anuncio del SSID en modo broadcast. En este caso los usuarios deben conocer el SSID para conectarse a la red. No es un mecanismo seguro pues el SSID se transmite no cifrado en los mensajes de conexión.
- Filtrar por dirección MAC. Tampoco es seguro porque otras estaciones pueden cambiar su MAC y poner una autorizada cunado el verdadero propietario no está conectado.
- El 802.11 original contempló un mecanismo de seguridad basado en el protocolo WEP (Wired Equivalent Privacy).
- WEP es vulnerable e inseguro. El comité 802.11 ha sido muy criticado por su estandarización.
- Para resolver esas deficiencias se ha desarrollado el estándar 802.11i, aprobado en julio de 2004.
- Entretanto la WiFi Alliance ha desarrollado dos 'anticipos' de 802.11i que son el WPA (Wi-Fi Protected Access) y el WPA2.
- 802.11i, WPA y WPA2 se apoyan en otro estándar, el 802.1x (port based control) aprobado en el 2001

La seguridad solo es posible con técnicas criptográficas.

4.2 Subcapa MAC del estándar IEEE 802 para redes de área local

Se llama dirección MAC al identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto identificar dispositivos de red. Es individual, y única para cada dispositivo, determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación.

Un listado de las direcciones MAC que emplean algunos fabricantes puede encontrarse en el siguiente enlace: http://standards-oui.ieee.org/oui/oui.txt

4.3 HDLC, SDLC y Hand-shaking

SDLC (Synchronous Data Link Control)

SDLC (control síncrono de enlace de datos) es un protocolo utilizado para transferir información síncrona de código transparente serie por bit a través de una línea de comunicaciones.

El origen de este producto data de 1973, y el objetivo de su creación fue el soporte de comunicación entre los cajeros automáticos de los bancos. El protocolo SDLC está presente en numerosos componentes de comunicaciones de IBM.

El SDLC emplea conjuntamente los métodos síncronos, orientado al bit y Vuelta-atrás-N. Controla una sola línea configurada como punto a punto, multipunto o bucle. Funciona con líneas full-dúplex, half-dúplex, conmutadas o privadas. Permite operaciones dúplex multipunto en los que una estación puede transmitir a otra estación mientras recibe datos de una tercera.

El SDLC emplea variantes de la técnica sondeo/selección. La estación maestra es responsable del control de la línea. Dicha estación inicia todas las transmisiones (tal como un sondeo) de las estaciones secundarias con un comando. Estas respondes enviando una respuesta. La estación maestra puede ser a su vez una estación secundaria para otra estación maestra.

SDLC tiene los siguientes significados:

- Una forma de control de línea de comunicaciones que utiliza mandatos para controlar la transferencia de datos por una línea de comunicaciones.

- Una disciplina de comunicaciones que cumple subconjuntos de los procedimientos de control de comunicaciones de datos avanzadas (ADCCP) de ANSI (American National Standards Institute) y el control de enlace de datos de alto nivel (HDLC). Estos estándares pertenecen a la ISO.

SDLC soporta los protocolos de comunicaciones tradicionales del iSeries, como APPC, pero no soporta TCP/IP.

Trama SDLC

Los mensajes DLC se transmiten por la línea en un formato específico llamado trama (ver figura 4.3.1). Los indicadores del comienzo y del final consisten cada uno en un octeto cuya configuración es 01111110. Esos indicadores sirven como referencia de comienzo y final de un mensaje, al igual que un campo FCS. El indicador de final puede servir de indicador de comienzo para la siguiente trama. Se pueden repetir indicadores entre tramas para mantener la línea en estado activo.

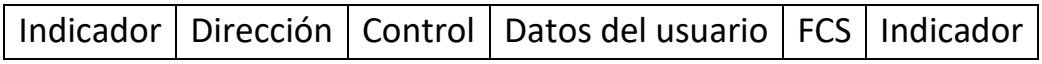


Figura 4.3.1. Trama SDLC.

El SDLC es transparente con respecto al alfabeto y tan sólo es especial la secuencia de bits del indicador. La lógica de control no permitiría que la secuencia 01111110 pueda transmitirse en otros lugares de la trama. En el extremo transmisor, el SDLC examina el contenido de la trama (excluyendo los indicadores) e inserta un 0 a continuación de cualquier sucesión de cinco unos consecutivos que tenga lugar dentro de la trama. El extremo receptor recibe la trama, reconoce los dos indicadores y elimina cualquier 0 que vaya a continuación de cinco unos consecutivos. Por ello, el SDLC no es dependiente de un alfabeto específico tal como el ASCII o el EBCDIC. El SDLC requiere para su correcto funcionamiento que todos los campos de la trama sean múltiplos de ocho bits, una vez que los cero de relleno han sido eliminados (ver tabla 4.3.1).

El campo de dirección viene a continuación del indicador de comienzo. La dirección identifica la estación secundaria. El SDLC también permite direccionar un determinado número de estaciones en la línea (dirección de grupo) así como todas las estaciones (dirección de radiodifusión). Un mensaje de sondo identifica la estación secundaria sondeada. Una respuesta también contiene la dirección de la estación secundaria.

El campo de control define la función de la trama y, por tanto, invoca la lógica SDLC en las estaciones transmisora y receptora. Este campo es un octeto y puede estar en uno de tres formas:

- Las tramas con Formato Sin Numeración (U, Unnumbered) se emplean con propósitos de control tales como a inicialización de estaciones secundarias, desconexión de estaciones, prueba de estaciones y control de los modos de respuesta de las estaciones.
- Las tramas con Formato de Supervisión (S) se emplean para reconocer afirmativamente (ACK) y negativamente (NAK) daos del usuario (tramas de información). Las tramas de supervisión no contienen datos de usuario. Se emplean para confirmar datos recibidos, informar de posibles condiciones de ocupación o de disponibilidad, y también para informar de errores de numeración de tramas.
- Las tramas de Transferencia de Información (I) contienen los datos del usuario.

El siguiente campo de la trama es el campo secuencia de verificación de trama (FCS, Frame Check Sequence). Este campo contiene una secuencia de 16 bits calculada a partir de los contenidos de los campos de dirección, control e información de las estaciones transmisoras. El receptor realiza un proceso similar para determinar si se han introducido errores durante la transmisión. El receptor no aceptará una trama errónea.

Tabla 4.3.1. Características de los comandos de respuesta SDLC.

Comando Respuesta	Formato	Campo de control				Respuesta	Campo I prohibido	Inicializa NR y NS
UI	U	000	P/F	0011	X	X		
RIM	U	000	F	0111		X	X	
SIM	U	000	P	0111	X		X	X
SNRM	U	100	P	0011	X		X	X
DM	U	000	F	1111		X	X	
DISC	U	010	P	0011	X		X	
UA	U	011	F	0011		X	X	
FRMR	U	100	F	0111		X		
BCN	U	111	F	1111		X	X	
CFGR	U	110	P/F	0111	X	X		
RD	U	010	F	0011		X	X	
XID	U	101	P/F	1111	X	X		
UP	U	001	P	0011	X		X	
TEST	U	111	P/F	0011	X	X		
RR	U	Nr	P/F	0001	X	X	X	
RNR	S	Nr	P/F	0101	X	X	X	
REJ	S	Nr	P/F	1001	X	X	X	
I	I	Nr	P/F	Ns 0	X	X		

Campo de control

Los bits menos significativos, es decir, los situados del lado derecho, identifican el formato de la trama (11 para el formato sin numeración; 10 para el formato de supervisión; 0 para las tramas de información). El resto de los bits define el tipo de función específicas de la trama (ver tabla 4.3.1):

- ***UI (Unumbered Information, Información Sin Numerar):*** Este comando permite la transmisión de datos en una trama sin numerar (por ejemplo, fuera de secuencia).
- ***RIM (Request Initialization Mode, Petición de Inicialización):*** La trama RIM en una petición, de una estación secundaria a una estación maestra, de comando SIM.
- ***SIM (Set Initialization Mode, Puesta en Modo Inicialización):*** Este comando se emplea para inicializar la sesión maestra-secundaria. La respuesta esperada en este caso es UA.
- ***SNRM (Set Normal Response Mode, Inicialización en Modo Normal de Respuesta):*** Pone la estación en NRM (Modo Normal de Respuesta). El NRM impide a la estación secundaria enviar alguna trama no solicitada. Esto significa que la estación central controla todo el flujo de mensajes en el enlace.
- ***DM (Modo Desconectado):*** Esta trama se transmite desde una estación secundaria para indicar que está en modo desconectado.
- ***DISC (Disconnect, Desconectado):*** Este comando enviado desde la estación maestra pone a la estación secundaria en el modo desconectado normal. Este comando es valioso para líneas conmutadas; el comando realiza una función similar a descolgar un teléfono.
- ***UA (Unnumbered Acknowledgment, Reconocimiento No Numerado):*** Es un ACK a un comando SIM, DISC o SNRM.
- ***FRMR (Frame Reject, Trama Rechazada):*** La estación secundaria envía esta trama cuando encuentra una trama inválida. Esta trama no se emplea para indicar un error en bits del campo Secuencia de Verificación de Trama, sino en situaciones más especiales tal como el caso de una trama demasiado larga para la capacidad de los tampones de una estación secundaria o un campo de control erróneo.
- ***BCN (Beacon, Guía)***
- ***CFGR (Configuración)***
- ***RD (Request Disconnect, Petición de Desconexión):*** Petición de una estación secundaria para ser desconectada.
- ***XID (Exchange Station Identification, Intercambio de Identificación de Estación):*** Este comando pide la identificación de una estación secundaria. Se emplea en entornos de conmutación para identificar a la estación que solicita un servicio.
- ***UP (Unnumbered Polls, Sondeo No Numerado)***

- ***TEST (Prueba):*** Esta trama se emplea para pedir respuestas de prueba de la estación secundaria.
- ***RR (Recieve Ready, Preparado Para Recibir):*** Indica que una estación maestra o secundaria está preparada para recibir. También se emplea para reconocer afirmativa (ACK) o negativamente (NAKK) tramas de información.
- ***RNR (Recieve not Ready, No Preparado Para Recibir):*** Indica que una estación maestra o secundaria está ocupada temporalmente. También se emplea para reconocer afirmativamente (ACK) o negativamente (NAK) tramas de información.
- ***REJ (Reject, Rechazo):*** Esta trama se puede emplear para pedir explícitamente la transmisión o retransmisión de trama de información. Este comando o respuesta es muy útil cuando se pierde el orden el orden en la secuencia de tramas.

Transmisión en Bucle

El SDLC tiene también capacidad para llevar a cabo sondeo distribuido. La configuración, denominada transmisión en bucle, permite a la estación maestra (controladora del bucle) enviar tramas de comando a cualquiera o tras las estaciones que formen parte del bucle. Cada estación secundaria decodifica el campo de dirección de cada trama y, si corresponde, acepta la trama. También se pasa la trama a la estación siguiente.

Una vez que la estación controladora del bucle ha finalizado la transmisión de las tramas de comando, envía ocho ceros consecutivos para señalar a las estaciones secundarias la finalización de las tramas. A continuación, transmite unos continuamente para asegurar que éstos han completado el bucle.

Para la transmisión de bucle se emplean los siguientes formatos adicionales:

- ***UP (Unnumbered Pols, Sondeo No Numerado):*** Esta trama es útil para operaciones de bucle, ya que proporciona a la estación secundaria la posibilidad de responder al sondeo. El sondeo puede entonces transmitirse alrededor del bucle y ser empleado por todas las estaciones sin tener en cuenta los números de secuencia (Ns ó Nr) anteriores.
- ***CFGR (Configuración):*** Este comando posibilita diversas funciones de configuración (poner una estación en modo de sólo recepción, poner estaciones fuera de línea).
- ***BCN (Beacon, Guía):*** Esta trama se emplea para resolver los problemas que puedan existir con la seña portadora; para determinar qué punto del recorrido está causando el problema. Da lugar a que la estación secundaria suprima la transmisión de la portadora o a que ésta se comience a transmitir de nuevo después de haberla suprimido.

Los sondeos no numerados sirven para provocar el envío de tramas de las estaciones secundarias de la línea y pueden enviarse desde la estación maestra una vez que la secuencia continua de unos haya completado el bucle.

HDLC (High Level Data Control)

El HDLC es una especificación de protocolo de línea orientado al bit, de la Organización Internacional de Estándares (ISO) y es la base para desarrollar numerosos protocolos ampliamente usados en la capa de enlace.

Características Básicas

Para satisfacer las demandas de diversas aplicaciones, HDLC define tres tipos de estaciones, dos configuraciones del enlace y tres modos de operación para la transferencia de los datos.

Los tres tipos de estaciones son:

- **Estación primaria.** Es la responsable de controlar el funcionamiento del enlace. Las tramas generadas por la estación primaria se denominan órdenes.
- **Estación secundaria.** Funciona bajo el control de la estación primaria. Las tramas generadas por la estación secundaria se denominan respuestas. La primaria establece un enlace lógico independiente con cada una de las estaciones presentes en la línea.
- **Estación combinada.** Combina las características de las primarias y de las secundarias, pudiendo generar tanto órdenes como repuestas.

Las dos posibles configuraciones del enlace son:

- **Configuración no balanceada.** Está formada por una estación primaria y una o más secundarias. Permite tanto transmisión full-duplex como half-duplex.
- **Configuración balanceada.** Consiste en dos estaciones combinadas. Permite igualmente transmisión full-duplex y half-duplex.

Los tres modos de transferencia de datos son:

- **Modo de respuesta normal (NRM, Normal Response Mode).** Se utiliza en la configuración no balanceada. La estación primaria puede iniciar la transferencia de datos hacia la secundaria, pero la secundaria sólo puede transmitir datos con base en respuestas a las órdenes emitidas por la primaria.
- **Modo balanceado asíncrono (ABM, Asynchronous Balanced Mode).** Se utiliza la configuración balanceada. En este modo, cualquier estación combinada puede iniciar la transmisión sin necesidad de recibir permiso por parte de la otra estación combinada.
- **Modo de respuesta asíncrono (ARM, Asynchronous Response Mode).** Se utiliza en la configuración no balanceada. La estación secundaria puede iniciar la transmisión sin tener permiso explícito de la primaria. La estación primaria sigue teniendo la responsabilidad del funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores y la desconexión lógica.

El modo NRM se usa en líneas que disponen de múltiples conexiones, en las que se conectan varios terminales a un computador central; el computador sondea cada una de las entradas correspondientes a los distintos terminales. NRM también se usa a veces en enlaces punto a punto, principalmente si el enlace conecta un terminal u otros periféricos a un computador.

ABM es el más utilizado de los tres modos; puesto que en ABM no se precisa realizar sondeos, la utilización de enlaces punto a punto full-duplex resulta más eficiente con este modo.

ARM se utiliza en contadas ocasiones, pudiendo usarse en ciertas situaciones particulares en las que la estación secundaria necesita a transmisión.

Estructura de la trama

HDLC emplea transmisión síncrona. Todos los intercambios se realizan con base en tramas, siendo suficiente un único formato de trama para todos los tipos de intercambios de datos e información de control (ver figura 4.3.2).

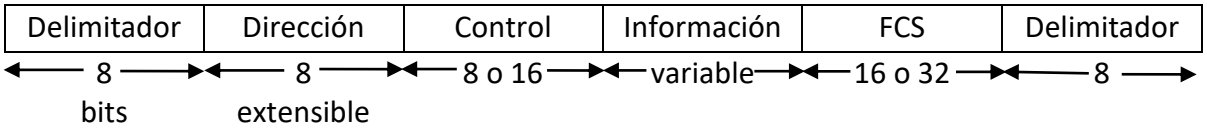


Figura 4.3.2. Estructura de la trama HDLC.

Los campos de delimitación, de dirección (ver figura 4.3.3) y de control (ver figuras 4.3.4 y 4.3.5), que preceden al campo de información, se denominan cabecera. Los campos FCS y de delimitador, que están a continuación del campo de información, se denominan cola.

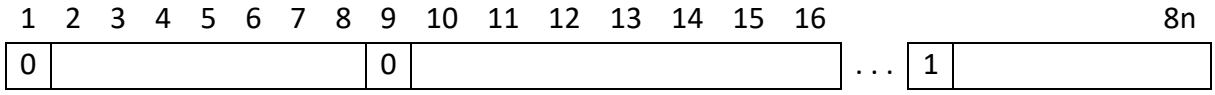


Figura 4.3.3. Campo de dirección ampliado.

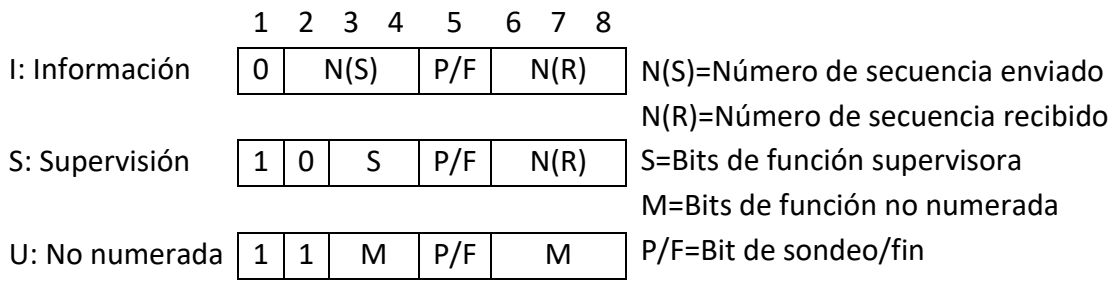


Figura 4.3.4. Formato del campo de control de 8 bits.

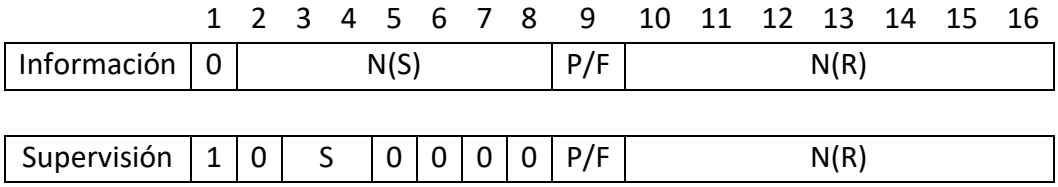


Figura 4.3.5. Formato del campo de control de 16 bits.

Campos de delimitación

Los campos de delimitación están localizados en los dos extremos de la trama y ambos corresponden al patrón de bits 01111110. Se puede usar un único delimitador como final de trama y comienzo de la siguiente simultáneamente. A ambos lados de la interfaz usuario-red, los receptores estarán continuamente intentando detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama. Mientras se está recibiendo una trama, la estación sigue intentando detectar esa misma secuencia para determinar el final de la trama. Debido a que el protocolo permite cualquier combinación de bits (es decir, no se impone restricción alguna en el contenido de los campos), no hay garantía de que la combinación 01111110 no aparezca en algún lugar dentro de la trama, destruyendo de este modo la sincronización de las mismas. Para evitar este problema, se utiliza un procedimiento denominado inserción de bits. En la transmisión de los bits existentes entre los delimitadores de comienzo y de fin, el emisor insertará un 0 extra siempre que se encuentre con la aparición de cinco 1 consecutivos. El receptor, tras la detección del delimitador de comienzo, monitorizará la cadena de bits recibida de tal manera que cuando aparezca una combinación de cinco 1 seguidos, el sexto bit se analiza como sigue. Si dicho bit es 0, se eliminará sin más. Si el sexto bit es un 1 y el séptimo es un 0. La combinación se considera como un delimitador. Si los bits sexto y séptimo son ambos igual a 1, se interpreta como una indicación de cierre generada por el emisor.

El empleo del procedimiento de inserción de bits permite que en el campo de datos aparezca cualquier combinación arbitraria de bits. Esta propiedad se denomina transparencia en los datos (ver figuras 4.3.6 y 4.3.7).

Patrón original: 11111111111011111101111110
Tras la inserción de bits: 111110111110110111110101111010

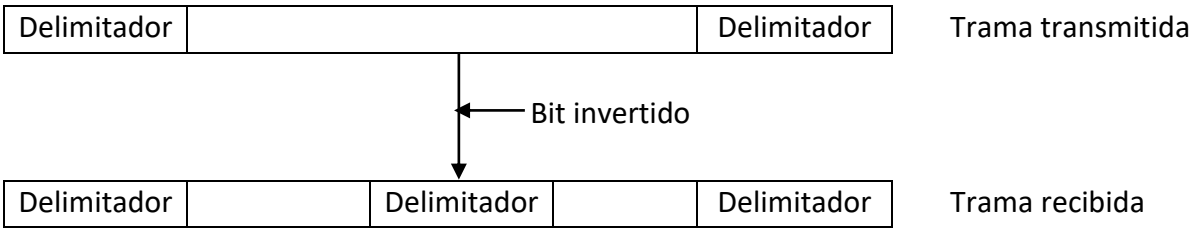


Figura 4.3.6. Un bit invertido divide una trama en dos.

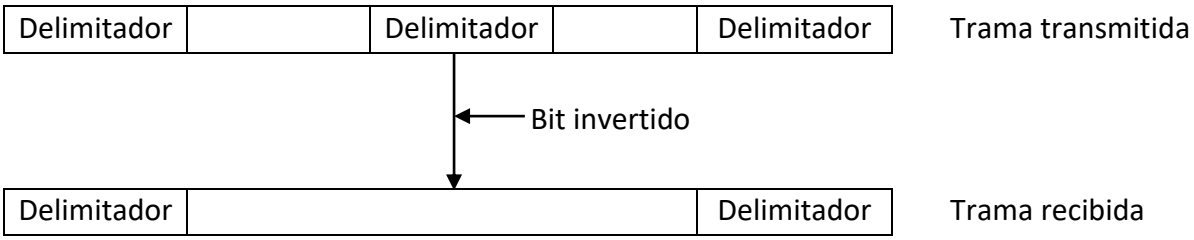


Figura 4.3.7. Un bit invertido funde dos tramas en una.

Campo de dirección

El campo de dirección identifica la estación secundaria que ha transmitido o va a recibir la trama. Este campo no se necesita en enlaces punto a punto, aunque se incluye siempre por cuestiones de uniformidad. El campo de dirección consta normalmente de 8 bits, si bien, tras una negociación previa, se puede utilizar un formato ampliado en el que la dirección es múltiplo de siete bits. El bit menos significativo de cada octeto será 1 o 0 en función de si es o no, respectivamente, el último octeto del campo de dirección. Los siete bits restantes de cada octeto constituyen la dirección propiamente dicha. Un octeto de la forma 11111111 se interpreta como una dirección que representa a todas las estaciones, tanto en el formato básico como en el ampliado. Este tipo de direccionamiento se utiliza cuando la estación primaria quiere enviar una trama a todas las secundarias.

Campo de control

En HDLC se definen tres tipos de tramas, cada una de ellas con un formato diferente para el campo de control.

Las tramas de información (tramas-I) transportan los datos generados por el usuario (esto es, por la lógica situada en la capa superior, usuaria de HDLC). Además, en las tramas de información se incluye información para el control ARQ de errores y de flujo.

Las tramas de supervisión (tramas-S) proporcionan el mecanismo ARQ cuando no se usa la incorporación de las confirmaciones en las tramas de información (piggybacking).

Las tramas no numeradas (tramas-U, del inglés unnumbered) proporcionan funciones complementarias para controlar el enlace. El primero o los dos primeros bits del campo de control se utilizan para identificar el tipo de trama. Los bits restantes se organizan en subcampos.

Todos los formatos posibles del campo de control contienen el bit sondeo/fin (P/F, poll/final), cuya utilización es dependiente del contexto. Normalmente, en las tramas de órdenes se denomina bit P y se fija a valor 1 para solicitar (sondear) una trama de respuesta a la entidad HDLC par. En las tramas de respuesta, este bit se denomina F y se fija a valor 1 para identificar la trama de respuesta devuelta tras la recepción de una orden.

Obsérvese que el campo de control básico en las tramas-S y en las tramas-I utiliza números de secuencia de 3 bits. Mediante una orden que fije el modo adecuado, en estas tramas se puede hacer uso de un campo de control ampliado en el que los números de secuencia sean de 7 bits. Las tramas-U tienen siempre un campo de control de 8 bits.

Campo de información

El campo de información sólo está presente en las tramas I y en algunas tramas-U. Este campo. puede contener cualquier secuencia de bits, con la única restricción de que el número de bits sea igual a un múltiplo entero de octetos. La longitud del campo de información es variable y siempre será menor que un valor máximo predefinido.

Campo de secuencia de comprobación de trama

La secuencia de comprobación de trama (FCS, Frame Check Sequence) es un código para la detección de errores calculado a partir de los bits de la trama, excluyendo los delimitadores. El código que se usa normalmente es el CRC-CCITT de 16 bits. También se pue de utilizar un campo FCS de 32 bits, que haga uso del polinomio CRC-32, si así lo aconseja la longitud de la trama o las características de la línea.

Funcionamiento

El funcionamiento de HDLC consiste en el intercambio de tramas-I, tramas-S y tramas-U entre dos estaciones. En la tabla 4.3.2 se definen las órdenes y respuestas posibles para los distintos tipos de tramas.

Tabla 4.3.2. Órdenes y respuestas para las tramas HDLC.

Nombre	Órdenes/ Respuesta	Descripción
Información (I)	C/R	Intercambio de datos de usuario
Supervisión (S)		
Receptor preparado (RR)	C/R	Confirmación positiva; preparado para recibir tramas I
Receptor no preparado (RNR)	C/R	Confirmación positiva; no preparado para recibir
Rechazo (REJ)	C/R	Confirmación negativa; vuelta atrás N
Rechazo selectivo (SREJ)	C/R	Confirmación negativa; rechazo selectivo
No numerada (N)		
Establecimiento de modo de respuesta normal/ampliado (SNRM/SNRME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo de respuesta asíncrono normal ampliado (SARM/SARME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo asíncrono balanceado normal/ampliado (SABM/SABME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo inicialización (SIM)	C	Inicialización de las funciones de control del enlace en las estaciones especificadas en la dirección
Desconexión (DISC)	C	Finalización de la conexión lógica del enlace
Confirmación no numerada (UA)	R	Aceptación de confirmación de una de las órdenes de establecimiento de modo
Modo desconectado (DM)	R	La estación que responda se encuentra en el modo desconectado
Solicitud de desconexión (RD)	R	Solicitud de una orden DISC
Solicitud de modo inicialización (RIM)	R	Se necesita inicializar; solicitud de la orden SIM
Información no numerada (UI)	C/R	Usada para intercambiar información de control
Sondeo no numerado (UP)	C	Usada para solicitar información de control
Reset (RSET)	C	Usada para recuperación, reinicia N(R) y N(S)
Identificación de intercambio (XID)	C/R	Usada para solicitar/informar el estado
Test (TEST)	C/R	Intercambio de campos de información idénticos para test
Rechazo de trama (FRMR)	R	Informa de la recepción de una trama inaceptable

El funcionamiento de HDLC implica tres fases (ver figura 4.3.8):

1. Inicio. El inicio lo puede solicitar cualquiera de los dos extremos con base en la transmisión de una de las seis órdenes previstas para fijar el modo. Esta orden tiene tres objetivos:

1. Avisa al otro extremo sobre la solicitud de la iniciación.
2. Especifica cuál de los tres modos (NRM, ABM, ARM) se está solicitando.
3. Indica si se van a utilizar números de secuencia de 3 o de 7 bits.

Si el otro extremo acepta la solicitud, la entidad HDLC transmitirá una trama de confirmación no numerada (UA, Unnumbered Acknowledgment) al extremo iniciante. Si la solicitud se rechaza, se envía una trama de modo desconectado (DM, Disconnected Mode).

2. Transferencia de datos. Cuando la iniciación haya sido solicitada y aceptada, se habrá establecido una conexión lógica. A partir de entonces, ambos extremos pueden comenzar a enviar datos mediante el uso de tramas-I, empezando por el número de secuencia 0. Los campos N(S) y N(R) de una trama-I contendrán los números de secuencia con los que se lleva a cabo el control de flujo y de errores. La entidad HDLC numerará la secuencia de tramas-I de forma ordenada módulo 8 o módulo 128, dependiendo de si se utilizan, respectivamente, 3 o 7 bits; para ello se usará el campo N(S). El campo N(R) se utiliza para llevar a cabo la confirmación de las tramas-I recibidas; de esta forma, se facilita que la entidad HDLC indique al otro extremo el siguiente número de trama-I que espera recibir.

Las tramas-S también se usan para controlar el flujo y los errores. La trama RR (receptor pre parado) confirma la última trama-I recibida mediante la indicación de la siguiente trama-I que se espera recibir. La trama RR se usa cuando no hay tráfico (tramas-I) en sentido contrario en el que se puedan incluir las confirmaciones. La trama RNR (receptor no preparado) confirma una trama-I, como lo hace la RR, pero a la vez solicita a la entidad situada al otro extremo del enlace que suspenda la transmisión de tramas-I; cuando la entidad que envió la trama RNR esté de nuevo pre parada, enviará una RR. La trama REJ (rechazo) sirve para iniciar el procedimiento ARQ con vuelta atrás N. A través de ella se indica que la última trama-I recibida se ha rechazado y, en consecuencia, se solicita la retransmisión de todas las tramas-I con números de secuencia posteriores a N(R). La trama SREJ (rechazo selectivo) se usa para solicitar la retransmisión de una única trama.

3. Desconexión. Cualquiera de las dos entidades HDLC pares puede iniciar la desconexión, tanto por iniciativa propia (si es que ha habido algún tipo de fallo) como tras la petición cursada por capas superiores. HDLC lleva a cabo la desconexión mediante el envío de una

trama DISC (desconexión, DISConnect). La entidad remota puede aceptar dicha desconexión mediante la devolución de una trama UA, e informando a su capa 3 sobre la finalización de la conexión. Cualquier trama-I pendiente de confirmación puede perderse, en cuyo caso será responsabilidad de las capas superiores su recuperación.

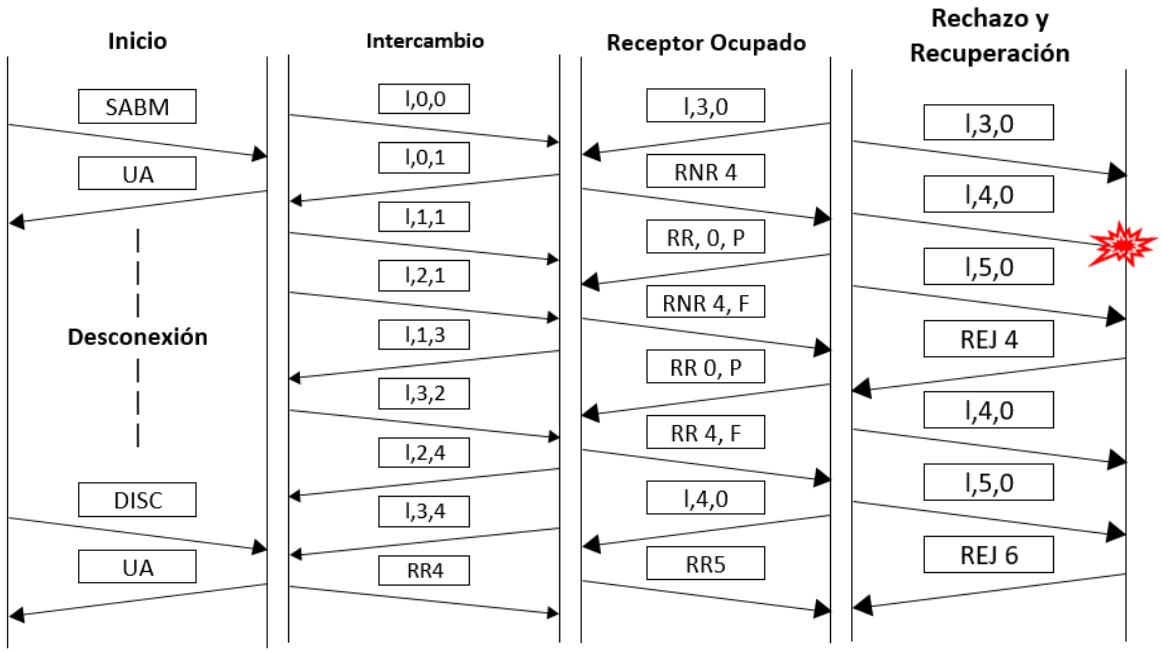


Figura 4.3.8. Acciones de HDLC.

Hand-shaking

Es el proceso de intercambio de información privada. Cuando un usuario entra en una página web para intercambiar información y ésta es a su vez es privada, con SSL (Secure Socket Layer) o con el protocolo https, se ejecuta un proceso llamado popularmente como Handshake, o apretón de manos. Se hace una similitud con los negocios cuando se realiza este gesto entre dos empresarios que tal vez no se conocían pero que van a entablar una relación de confianza.

En primer lugar, es el usuario o cliente quien envía al servidor datos sobre el número de cliente, el cifrado y la clave aleatoria, así como otro tipo de información que requieren los servidores.

El servidor a su vez reenvía los datos, de manera que el cliente obtiene la información que pedía. Así mismo envía el certificado digital que posee.

Entonces es el browser del cliente el que comprueba la autenticación. Le avisa a la persona por ejemplo si el servidor no está respaldado por nadie y otro tipo de problemas.

Hay entidades que son certificadoras pero que tienen una encriptación débil, por ejemplo. Si finalmente sí puede darse la conexión y está autenticado, se procede a la conexión.

Usando los datos generados por este apretón de manos, por el handshake, se crea el premaster secret para la sesión. Se cifra a través de la llave pública que es creada por el certificado digital. En ocasiones el servidor también puede pedir autenticación al cliente, por ejemplo, una contraseña.

Los dos protagonistas de la conexión generarán sus claves simétricas que serán usadas para cifrar y descifrar la información. De esta manera la conexión se permitirá una conexión íntegra y segura.

Este proceso de conexión se puede ver representado en la figura 4.3.9.

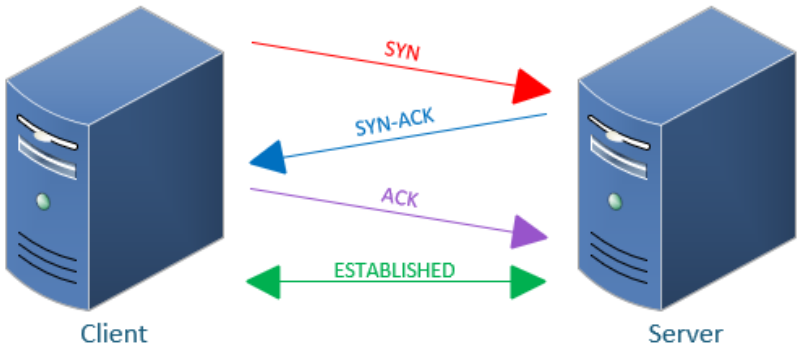


Figura 4.3.9. Hand-shaking.

4.4 Dispositivos de interconexión

Puente

Los puentes, también llamados “bridges” dan la conexión mejor que los repetidores, ya que éstos acceden paquetes de información para leer tanto la dirección de origen como la dirección destino, si el destino está dentro de la red deja el paquete en la misma; de no ser así, deja que salga de la red para que pueda llegar a su destino.

Para que los puentes puedan lograr esto, es muy importante saber las direcciones locales y remotas, por lo que el puente debe tener una tabla de direcciones que se lo indique. Una ventaja que tienen los puentes sobre los repetidores es que, para el usuario, los puentes permiten tener varias redes conectadas como una sola red extendida que permite acceso a recursos nuevos, segmentan el tráfico en la red dejando pasar sólo la información que debe.

Existen cuatro tipos de puentes:

Puentes Transparentes. Permite la conexión entre dos redes que utilizan los mismos protocolos tanto en la capa física como en la capa de enlace de datos. En caso de tener dos redes conectadas por un medio de un puente de este tipo (ver figura 4.4.1) su funcionamiento consta de los siguientes pasos:

1. El puente lee las direcciones destino de todos los mensajes transmitidos por los dispositivos de la red A.
2. El puente ignora todos los mensajes dirigidos a dispositivos ubicados en la red A.
3. El puente acepta todos los mensajes dirigidos a dispositivos ubicados en la red B y, utilizando los protocolos comunes, envía estos mensajes a la red B.
4. El puente realiza las mismas funciones para todos los mensajes transmitidos por la red B.

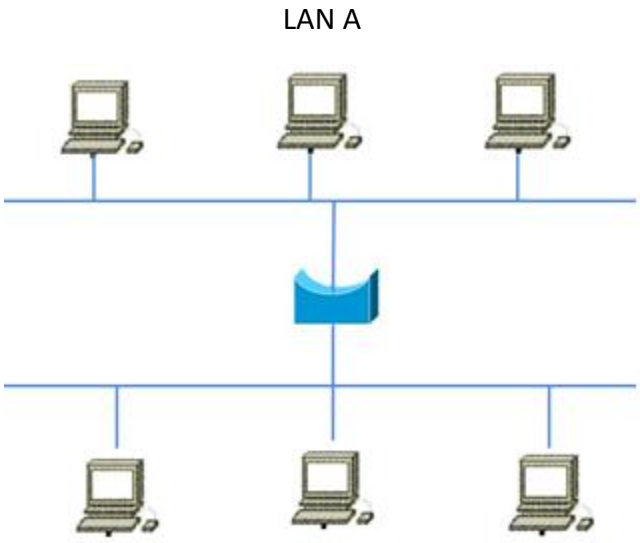


Figura 4.4.1. Puente transparente.

Para que esto se pueda llevar a cabo se requiere que el puente conozca la ubicación de los dispositivos, esto se puede hacer por configuración manual o por una función directa del equipo.

Esta última lee las direcciones origen de cada mensaje recibido y actualiza una base de datos que lista cada dirección y datos adicionales. Se lee la dirección de cada paquete de información que se transmite y se compara con las existentes en la base de datos decidiendo si se ignora o se manda a otra red.

Puentes Traductores. Este puente es una versión del puente transparente, ya que también realiza conexiones a redes que utilizan distintos protocolos en las capas físicas y enlace de datos. En la figura 4.4.2 se puede observar uno de estos puentes conectando una red Ethernet con una Token Ring, basándose en los siguientes pasos:

1. El puente utiliza los protocolos de la red A para leer la dirección destino de todos los mensajes transmitidos por los dispositivos ubicados en la red A.
2. El puente ignora todos los mensajes dirigidos a dispositivos ubicados en la red A.
3. El puente acepta todos los mensajes dirigidos a dispositivos ubicados en la red B y, utilizando los protocolos de esta red, transforma el mensaje para poderlo transmitir a la red B.
4. El puente hace lo mismo con los mensajes transmitidos en la red B.

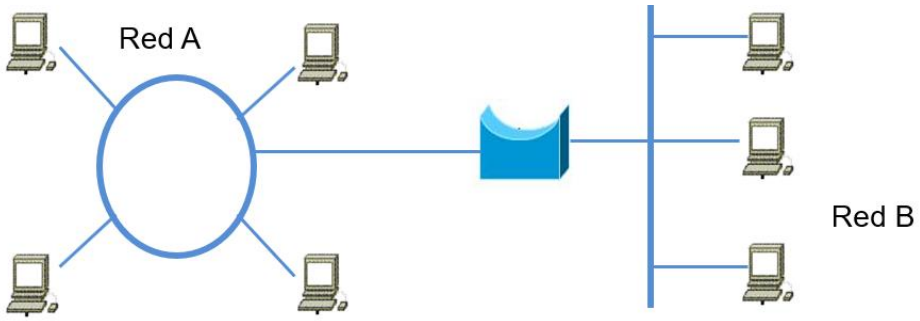


Figura 4.4.2. Puente traductor.

Puentes con encapsulamiento. Este puente a diferencia del puente traductor, encapsula los mensajes en un nuevo formato, viajan por el "backbone" y se desencapsulan hasta llegar a su destino (ver figura 4.4.3). Los pasos a seguir para mandar un mensaje de la red A a la red B son los siguientes:

1. El puente 1, usando los protocolos de la red A, lee la dirección destino de todos los mensajes transmitidos por dispositivos ubicados en la red A.
2. El puente 1 ignora todos los mensajes dirigidos a dispositivos ubicados en la red A.
3. El puente 1 acepta todos los mensajes dirigidos a otras redes, coloca el mensaje en un Frame de FDDI y lo envía a través del backbone.
4. El puente 2 recibe el mensaje, quita los encabezados del Frame y revisa la dirección destino. Como el destino no le pertenece, ignora el mensaje.
5. El puente 3 recibe el mensaje, quita los encabezados del Frame y revisa la dirección destino. Como está dirección si le pertenece, utiliza los protocolos de Ethernet para obtener el paquete.
6. El puente 4 recibe el mensaje, quita los encabezados del Frame y revisa la dirección destino. Como destino no le pertenece, ignora el mensaje.
7. El puente 1 elimina el mensaje encapsulado de backbone de FDDI.

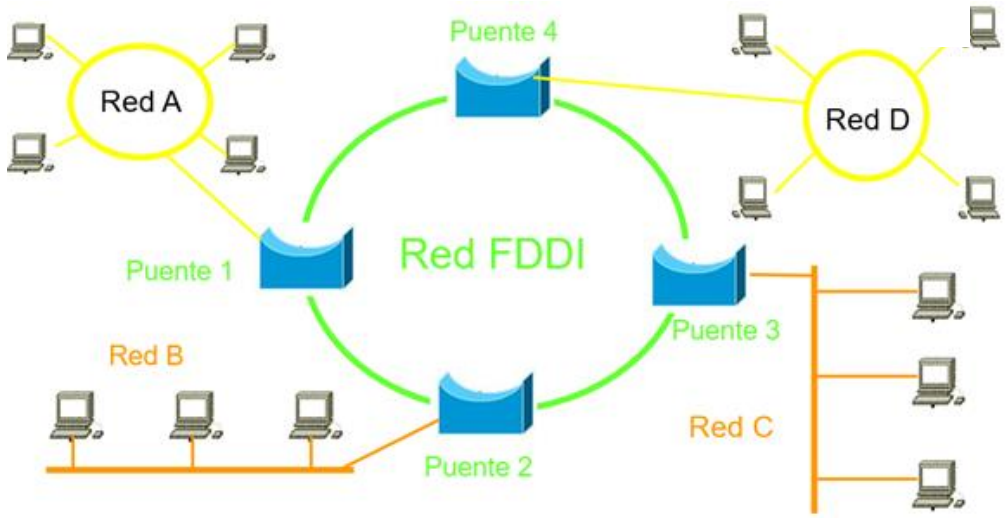


Figura 4.4.3. Puente con encapsulamiento.

Puente del routing origen (Source Routing Bridge). Este término fue utilizado por IBM para describir un método de "puenteo" en redes Token Ring, el cual requiere que un paquete exploratorio proporcione la información necesaria para hacer llegar un mensaje a su destino. Aquí los puentes no requieren almacenar una base de datos con direcciones, ya que se basan en la información contenida en el frame del mensaje, por lo que deben "descubrirse" las rutas más convenientes.

En la figura 4.4.4 se muestran cinco redes Token Ring conectadas por tres puentes, para enviar un mensaje de la red 1 a la red 5 tendríamos que hacer lo siguiente:

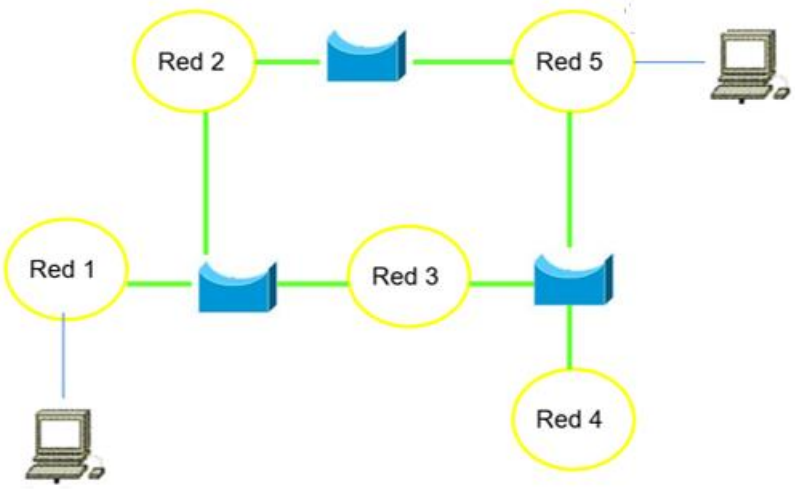


Figura 4.4.4. Puente del routing origen.

1. El dispositivo origen de la red 1 envía un paquete de exploración, el cual tiene un formato especial que es reconocido inmediatamente por el puente.

2. Al recibir este paquete, el puente graba en el mismo el número de conexión por la cual llegó y su identificación en una sección de la envoltura del paquete (campo de información de routing).
3. El puente envía este paquete a través de todas las conexiones, excepto por la que llegó. Originando así copias del paquete explorador.
4. El destino de la red 5 recibe varios paquetes exploradores, cada uno indicando la ruta que siguió, eligiendo el más adecuado ya sea por rapidez o por ser el más directo, después, envía una respuesta a la red 1, indicándole la ruta adecuada.
5. El dispositivo en la red 1 almacena esta información para que siempre que envíe un mensaje a la red 5 utilice esta ruta, empaquetando la información en un formato especial que reconozca el puente.
6. El puente recibe estos paquetes y lee la información que contienen para saber por dónde debe de enviarlo.

Switch

El término conmutar (switching) se usa cuando se describe en muchos tipos de tecnología de redes. En cada caso, en un único conjunto de hardware (véase figura 4.4.5), software, procesos y protocolos guían las operaciones de conmutación de la red. Los tipos de conmutación incluyen:

- LAN switching
- Conmutación en ATM
- Conmutación en Frame Relay
- Conmutación en capa 3 en el modelo OSI
- Conmutación de Redes Telefónicas

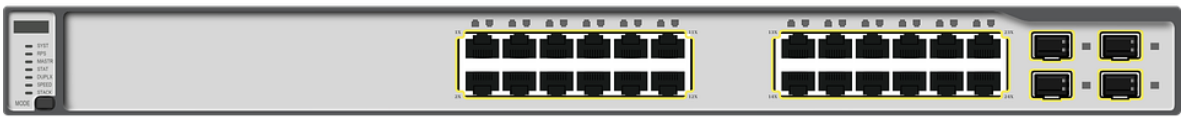


Figura 4.4.5. Switch.

El proceso de LAN switching opera en la capa dos del modelo OSI, aplicando eso hacia delante con las tecnologías hacia los frames de la capa 2. Por esta razón el LAN switching es también conocido como:

- Switching en Capa 2
- Switching en capa MAC
- Switching en capa de enlace de datos
- Vínculo Mutipuerto

Los switches LAN son dispositivos multipuertos que transfieren los frames entre sus puertos basándose en su información que contiene los frames, como sigue:

1. Un frame llega a un puerto del switch, referido como el puerto entrante o saliente.
2. El switch examina la dirección destino MAC contenida en el frame.
3. El frame se transmite fuera del puerto conectado al dispositivo destino, referid como el puerto saliente o de salida. SI la dirección destino esta indefinida, el frame se transmite fuera de todos los puertos con excepción del puerto de entrada.

NIC (Network Interface Card – Tarjeta de Interfaz de Red)

Una tarjeta de red es un dispositivo que permite la conexión en red de varios ordenadores. Una imagen de ésta se muestra en la figura 4.4.6. A través de esta red se pueden transferir datos y compartir recursos entre varios ordenadores. Al unir en red varios ordenadores se crea una red de trabajo LAN.

Figura 4.4.6. Tarjeta de Interfaz de Red.

Los ordenadores conectados en red se pueden comunicar entre sí utilizando diferentes protocolos para transferir paquetes de datos entre las diferentes máquinas de la red (nodos). La tarjeta de red actúa como un intérprete permitiendo a cada ordenador recibir y enviar datos a la red de trabajo. Con las tarjetas de red se pueden configurar redes tanto cableadas como inalámbricas.

Uno de los protocolos más comunes en redes de trabajo es Ethernet. Existen otros menos utilizados como puede ser el protocolo Token Ring. Cuando se monta una red LAN se ha de instalar una tarjeta de red en cada ordenador que se vaya a conectar a la red y cada una debe usar la misma arquitectura y protocolo. No se puede configurar una red basada en arquitectura Ethernet y conectar un ordenador con una tarjeta de red que utilice un protocolo diferente.

Una tarjeta de red se instala en un slot disponible en la placa base del ordenador. También existen tarjetas de red que se pueden instalar mediante conexión USB. La tarjeta de red asigna una dirección MAC a cada ordenador de la red. Las tarjetas de red además pasan los datos de formato en paralelo, utilizado por los procesadores de los ordenadores, a formato en serie, necesario para la transferencia de datos.

4.5 Seguridad a nivel de capa enlace

Los switches son los dispositivos más importantes en este nivel, y por tanto la seguridad del enlace se centra en la correcta configuración de estos aparatos. Se debe acompañar el bloqueo del acceso físico con la inutilización lógica de aquellos puertos que están sin ser usados para impedir conexiones fraudulentas que puedan llevar a escuchas indebidas, ataques de saturación de las tablas o envenenamiento ARP.

Además, esta capa también abarca la correcta elección de protocolos seguros para la comunicación. Por ejemplo, en el caso de un medio inalámbrico, se deberán utilizar protocolos WPA2 o WPA siempre que sea posible, por sobre WEP.

El filtrado MAC consiste en asignar manualmente una dirección MAC a un puerto específico.

Las VLANs guardan un rol crítico en la seguridad del sistema, contribuyendo a la segmentación de la red y la separación del tráfico, permitiendo una mayor organización del mismo y favoreciendo su rápido análisis.

Uso de protocolos WEP, WPA, WPA2

WEP (Wired Equivalent Privacy – Privacidad Equivalente al Cableado)

WEP fue desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wi-Fi en septiembre de 1999. WEP tenía como objetivo ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, hay muchos problemas de seguridad bien conocidos en WEP, que también es fácil de romper y difícil de configurar.

A pesar de todo el trabajo que se ha hecho para mejorar el sistema, WEP sigue siendo una solución altamente vulnerable. Los sistemas que dependen de este protocolo deben ser actualizados o reemplazados en caso de que la actualización de seguridad no sea posible. WEP fue oficialmente abandonada por la Alianza Wi-Fi en 2004.

WEP es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución

manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

En el sistema WEP se pueden utilizar dos métodos de autenticación:

Autenticación de Sistema Abierto. El cliente WLAN no se tiene que identificar en el Punto de Acceso durante la autenticación. Así, cualquier cliente, independientemente de su clave WEP, puede verificarse en el Punto de Acceso y luego intentar conectarse. En efecto, la no autenticación (en el sentido estricto del término) ocurre. Después de la autenticación y la asociación, el sistema WEP puede ser usado para cifrar los paquetes de datos. En este punto, el cliente tiene que tener las claves correctas.

Autenticación mediante Clave Compartida. WEP es usado para la autenticación. Este método se puede dividir en cuatro fases:

1. La estación cliente envía una petición de autenticación al Punto de Acceso.
2. El punto de acceso envía de vuelta un texto modelo.
3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.
4. El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

A primera vista podría parecer que la autenticación por Clave Compartida es más segura que la autenticación por Sistema Abierto, ya que éste no ofrece ninguna autenticación real. Sin embargo, es posible averiguar la clave WEP estática interceptando los cuatro paquetes de cada una de las fases de la autenticación con Clave Compartida. Por lo tanto, es aconsejable usar la autenticación de Sistema Abierto para la autenticación WEP (nótese que ambos mecanismos de autenticación son débiles).

WPA (Wi-Fi Protected Access – Acceso protegido Wi-Fi)

Durante el tiempo en que el estándar de seguridad inalámbrica 802.11i estaba en desarrollo, WPA se utilizó como una mejora de seguridad temporal para WEP. Un año antes de que WEP fuera oficialmente abandonado, WPA fue formalmente adoptado. La mayoría de las aplicaciones WPA modernas usan una clave previamente compartida (PSK), más a menudo conocida como WPA Personal, y el Protocolo de Integridad de Clave Temporal o TKIP para encriptación. WPA Enterprise utiliza un servidor de autenticación para la generación de claves y certificados.

WPA, al igual que WEP, después de ser puesto a prueba de concepto y las demostraciones públicas aplicadas resultó ser bastante vulnerable a la intrusión. Sin embargo, los ataques que representaron la mayor amenaza para el protocolo no fueron los directos, sino los que se hicieron en Configuración de Wi-Fi Segura (WPS) - Sistema auxiliar desarrollado para simplificar la vinculación de dispositivos a puntos de acceso modernos.

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuera bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se "entienden", entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que se conoce el contenido del paquete de autenticación y se conoce su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

Desgraciadamente WPA no está exento de problemas. Uno de los más importantes sigue siendo los DoS o ataques de denegación de servicio. Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Este mecanismo de defensa utilizado para evitar accesos no autorizados a la red puede ser un grave problema.

WPA2 (Wi-Fi Protected Access version 2 – Acceso protegido Wi-Fi versión 2)

La mejoría más importante de WPA2 sobre WPA fue el uso del Estándar de cifrado avanzado (AES) para el cifrado. AES es aprobado por el gobierno de EE.UU. para cifrar la información clasificada como de alto secreto, por lo que debe ser lo suficientemente bueno para proteger las redes domésticas.

En este momento, la principal vulnerabilidad a un sistema WPA2 es cuando el atacante ya tiene acceso a una red WiFi segura y puede acceder a ciertas teclas para realizar un ataque a otros dispositivos de la red. Dicho esto, las sugerencias de seguridad para las vulnerabilidades WPA2 conocidas son principalmente importantes para las redes de niveles de empresa, y no es realmente relevante para las pequeñas redes domésticas.

Lamentablemente, la posibilidad de ataques a través de Configuración de Wi-Fi Segura (WPS), sigue siendo alta en los actuales puntos de acceso capaces de WPA2, que es el problema con WPA también. Y aunque forzar el acceso en una red asegurada WPA / WPA2 a través de este agujero tomará alrededor de 2 a 14 horas sigue siendo un

problema de seguridad real y WPS se debe inhabilitar y sería bueno si el firmware del punto de acceso pudo ser reajustado a una distribución para no apoyar WPS, para excluir por completo este tipo de ataque.

Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (access point, punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque de DoS específico a WPA.

Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las claves PSK son vulnerables a ataques de diccionario.

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos, así como su integridad y autenticidad.

Tema 5

Capa de red

Objetivo: El alumno aplicará métodos y estándares para el diseño y configuración de redes de datos seguras.

El objetivo de la capa de red es encontrar la mejor ruta o camino para los paquetes de datos se dirijan a su destino, y llegar a él puede requerir varios saltos a través de encaminadores de ruta (ver figura 5.1.1), los cuales utilizan algoritmos de encaminamiento para cumplir con su tarea.

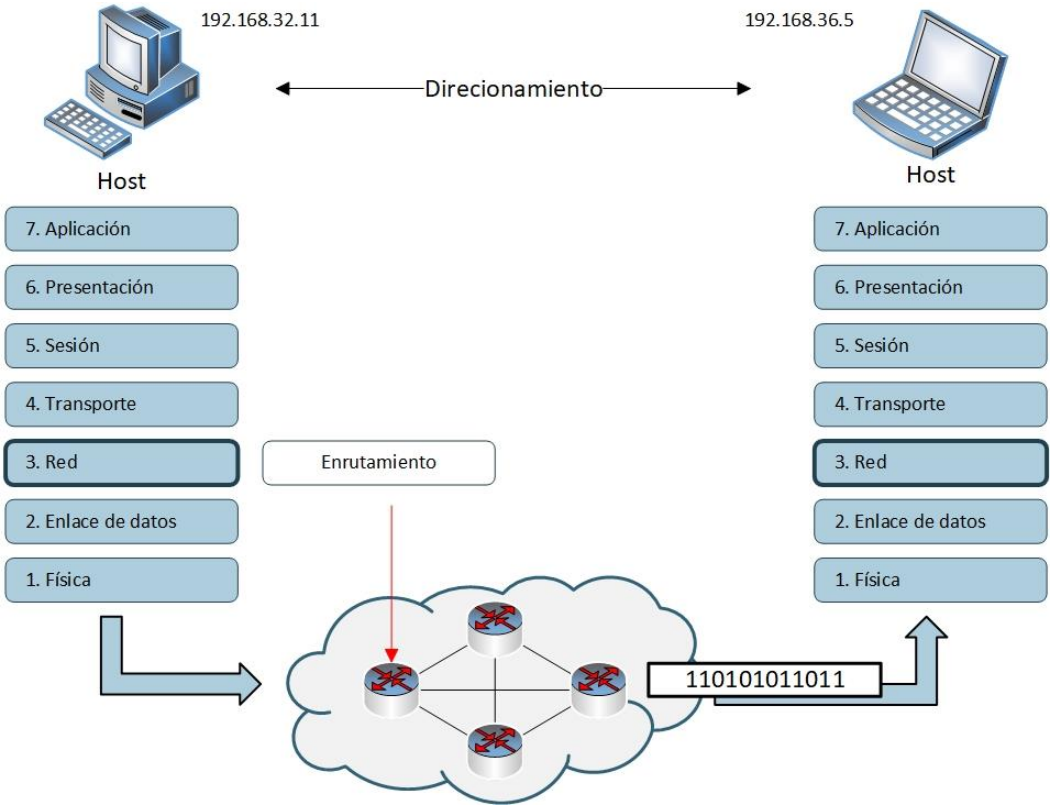


Figura 5.1.1. Diagrama del modelo OSI con énfasis en la capa de Red.

La capa de red provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la capa de red utiliza cuatro procesos básicos:

- Direccionamiento
- Encapsulamiento
- Enrutamiento
- Desencapsulamiento

Entre las principales actividades están:

- Buscar el mejor camino por paquete o por mensaje.
- Realizar las funciones de encaminamiento que permitan la comunicación a múltiples enlaces de datos en una red.
- Realizan un direccionamiento lógico.

5.1 Dispositivos de interconexión: router

Los routers son dispositivos que operan en la capa de red (ver figura 5.1.2) y su tarea es encontrar la mejor ruta para que los datos viajen a su destino de la forma más directa y en el menor posibles. Esto hace que sus operaciones sean diferentes que los repetidores y los puentes MAC. Ambos de estos dispositivos son usados para conectar redes que sean idénticas con respecto del acceso al medio usado.

Figura 5.1.2. Router.

Sin embargo, la información es transferida basándose en las direcciones MAC. Esto también hace que estos dispositivos de protocolo independiente, especifique que ellos son independientes de los protocolos que trabajen en la capa MAC.

Los routers son capaces de proveer conectividad en un nivel superior para mezclar ambientes MAC de manera que se trabaja con un protocolo en la capa superior mediante direcciones lógicas. Esto permite que las conexiones de los segmentos de red sean diferentes.

Sin embargo, se debe notar que las redes que se interconectan comparten algún protocolo similar en dicha pila, los routers no son capaces de traducir un protocolo. El router debe ser equipado con software apropiado para cada protocolo que sea soportado.

Una interred se basa en routers y está compuesta de diferentes subredes lógicas. Cada uno de los segmentos de red se conectan a través de un router que mantiene su identidad lógica.

Los routers pueden ser usados para interconectar redes sobre redes locales o amplias. Sea crítico el diseño de la instalación de interred y de grandes WANs usando enlaces de las telecomunicaciones.

El rol del router es dirigir paquetes a lo largo de la red de manera eficiente, y encontrar la ruta económica en redes acopladas cuando estas sean rutas muy redundantes desde el dispositivo origen al dispositivo destino.

Funcionalidad

Los routers son considerados dispositivos activos. Son activos en el sentido que son requeridos para que haga varias decisiones acerca de cada paquete manejado.

La funcionalidad del router puede estar categorizada dentro de tres áreas que son las siguientes:

- Permitir la unión de redes heterogéneas (diferentes)
- Asegurar que las redes sean capaces de manejar el tráfico de carga
- Escoger la mejor ruta de comunicación a través de la red

Uniendo redes

Los routers deben ser capaces de trabajar con esquemas diferentes de direcciones, de tamaños de frames y tasas de datos.

Los frames "largos" son administrados para que los routers fragmenten frames "largos" en paquetes pequeños, cada uno de los paquetes obtienen un número de secuencia el cual será utilizado para reensamblar el frame al llegar al receptor final.

5.2 Protocolo IP

Los protocolos son conjuntos de normas para formatos de mensaje y procedimientos que permiten a las máquinas y los programas de aplicación intercambiar información. Cada máquina implicada en la comunicación debe seguir estas normas para que el sistema principal de recepción pueda interpretar el mensaje.

TCP/IP proporciona los protocolos que son necesarios para satisfacer los requisitos de la RFC 1100, Protocolos oficiales de Internet, así como otros protocolos utilizados comúnmente por los sistemas principales de la comunidad de Internet.

El protocolo IP (Internet Protocol) tiene información de direccionamiento para el encaminamiento de paquetes (ver figura 5.2.1).

Tiene dos responsabilidades principales:

1. Entregar datagramas a través de la red basado en el mejor esfuerzo.
2. Ofrecer la fragmentación y el re ensamblado de datagramas para soportar los enlaces de datos con tamaños diferentes de las Unidades de Transmisión Máxima (MTU).

0 - 3	4 - 7	8 - 15	16	17	18	19 - 31
Versión	IHL	Tipo de servicio	Longitud total			
Identificación				DF	MF	Desplazamiento
Tiempo de vida		Protocolo	Checksum			
Dirección fuente						
Dirección destino						
Opciones						

Figura 5.2.1. Cabecera de la trama IP.

Versión. En este campo se define la versión de IP que se está utilizando, 0100 (IPv4) o 0110 (IPv6).

Internet Header Length. Indica la longitud del encabezado en palabras de 32 bits. Normalmente es de 20 bytes. Sin embargo, al ser un campo de 4 bits la longitud del encabezado puede ser de 64 octetos.

Tipo de Servicio. Distingue las clases de servicios que por cierto no es muy utilizado. Sólo usa los últimos 4 bits y sólo uno puede estar encendido. Si todos los bits se encuentran apagados indican un servicio normal.

Largo o Longitud Total. Este campo indica la longitud total del datagrama IP en butes, como es un campo de 16 bits, la longitud de un datagrama IP puede ser de hasta 65535 bytes.

Identificación. Este campo lleva un número generado por el nodo para que el host destino identifique a qué datagrama pertenece el fragmento recién llegado (cuando existe fragmentación en el trayecto del datagrama).

Banderas. Para fines de fragmentación, consiste en 3 bits:

1. No está definido
2. **DF (Don´t Fragment)**. Si está encendido indica que el datagrama no puede ser fragmentado.
3. **MF (More Fragments).** Indica que existen más fragmentos para este datagrama.

Offset o Desplazamiento del Fragmento. Indica qué tanto se ha desplazado el fragmento, así, identifica en qué parte del datagrama va el paquete de datos en relación con el comienzo de los datos en relación con el comienzo de los datos originales (cuando el datagrama tuvo que ser fragmentado).

Tiempo de Vida. Este campo indica el número máximo de saltos que un datagrama puede dar (255), en cada salto el número de este campo se decrementa en 1, cuando este campo

tiene un valor 0 y no se ha alcanzado el destino el datagrama se descarta y el nodo fuente es informado con un mensaje ICMP.

Protocolo. Identifica el protocolo de capa superior que está encapsulado en el datagrama IP.

Checksum. Sólo para la cabecera IP, y es útil para la detección de errores generados por palabras de memoria erróneas en los routers.

Dirección Fuente. Dirección IP origen

Dirección Destino. Dirección IP destino

Opciones. Son de longitud variable y se utiliza el campo cuando se considera necesario (www.iana.org/assignments/ip-parameters)

Direcciones IP

Las direcciones IP, son los identificadores utilizados por el protocolo para que los paquetes alcancen su destino.

IPv4

El protocolo IPv4 utiliza 32 bits para representar una dirección IP (ver figura 5.2.2), los cuales son divididos en 4 octetos de 8 bits cada uno, separados por puntos y representados en formato decimal.

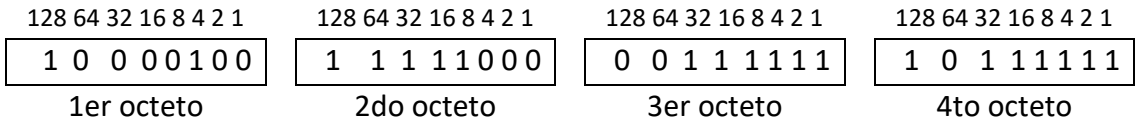


Figura 5.2.2. Representación en bits de una dirección IPv4.

El esquema de direccionamiento IP es jerárquico, esto es, para buscar una dirección IP primero se busca la red que la contiene y después el host al que identifica esa IP. Para la identificación de determinadas direcciones, existen direcciones especiales para poder identificarlas fácilmente (ver figura 5.2.3).

00000000000000000000000000000000	Este host
0000 … 0000 | Host	Un host de esta red
11111111111111111111111111111111	Broadcast – difusión en la red local
Red | 1111 … 1111	Difusión hacia otra red
127 | Cualquier secuencia de bits	Loopback – dirección local para pruebas

Figura 5.2.3. Direcciones especiales de IPv4.

De los 32 bits utilizados para la dirección: una porción se utiliza para identificar a la red y otra para identificar al host (ver figura 5.2.4).

Existen diferentes formatos de dirección:

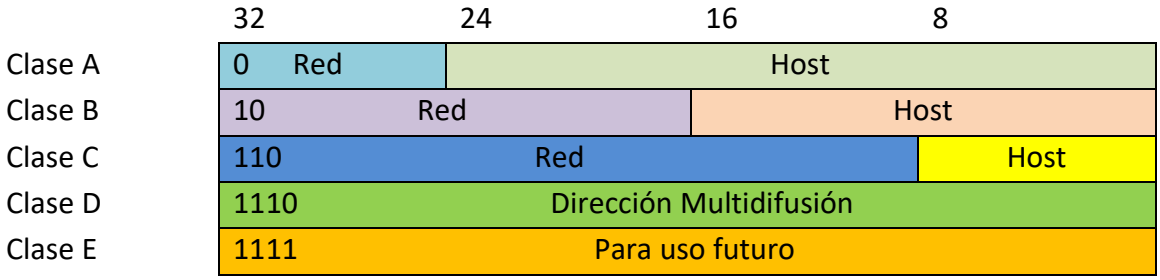


Figura 5.2.4. Clases de las direcciones IPv4.

Clase A. Un octeto para Id de red, tres octetos para identificador de host.

Las direcciones de red clase A
Desde 00000001 ⟶ 1
Hasta 01111110 ⟶ 126
Máscara de red: 255.0.0.0

Los 3 octetos restantes son utilizados para el identificador de host, los cuales son administrados y definidos por el administrador responsable de la red.

Clase B. Dos octetos para Id de red, dos octetos para identificador de host.

Las direcciones de red clase B
Desde 10000000.00000000 → 128.0
Hasta 10111111.11111111 → 191.255
Máscara de red: 255.255.0.0

Los dos octetos restantes son utilizados para el identificador del host, los cuales son administrados y definidos por el administrador de red responsable.

Clase C. Tres octetos para Id de red, un octeto para identificador de host.

Las direcciones de red clase C

Desde 11000000.100000000.00000000 → 192.0.0
Hasta 10111111.11111111.11111111 → 223.255.255
Máscara de red: 255.255.255.0

El octeto restante es utilizado para el identificador del host, el cual es administrado y definido por el administrador de red responsable. Todo lo anterior se ve simplificado en la tabla 5.2.1.

Tabla 5.2.1. Análisis numérico de las clases de redes.

Clase	Bits manejables en el prefijo	Rango del 1er octeto	No. de redes	Bits en el sufijo	No. de hosts por red
A	7	1 – 126	$2^7 - 2 = 126$	24	$2^{24} - 2 = 16{,}777{,}216$
B	14	128 – 191	$2^{14} = 16{,}384$	16	$2^{16} - 2 = 65{,}534$
C	21	192 – 223	$2^{21} = 2{,}097{,}152$	8	$2^8 - 2 = 254$
D	4	224 – 239	----------	------	----------
E	4	240 – 255	----------	------	----------

En una red IPv4 los hosts pueden comunicarse de tres formas:

- **Unidifusión (unicast)**
  Punto a punto Net Id + Host Id
- **Multidifusión (multicast)**
  De un punto a múltiples destinos simultáneamente (grupo)
  -Audio
  -Video
  -Software
  -Noticias
  Según el servicio, es una dirección particular en el rango 224.0.0.0 – 239.255.255.255
- **Difusión amplia (broadcast)**
  Es el envío a todos los nodos en una red Net Id + 111 … 111

Subredes

División de una red en varias partes para uso interno; pero con la capacidad de actuar como una sola red ante el mundo exterior.

Para implementar subredes el router principal de la empresa necesita una máscara de red que identifique la división entre:

Número de red	Número de subred	Host

Máscara de Red

Se trata de una sucesión de unos que abarca la porción de Id de red y adicionalmente la porción que será tomada del Id de host para utilizarse como Id de subred. Ésta se representa en la figura 5.2.5.

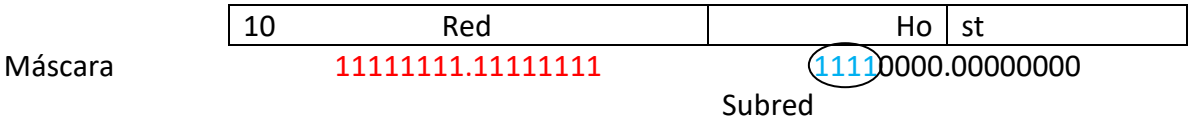


Figura 5.2.5. Formato de una máscara de red.

Se hace una suma lógica AND entre la dirección IP y la máscara para determinar la subred a la que se hace referencia y la máquina dentro de esa subred a la que se dirige el paquete (ver tabla 5.2.2 y tabla 5.2.3).

Tabla 5.2.2. Valores que pueden tomar los octetos de una sub-máscara de red.

Valor en binario que puede ser parte ser parte de una serie de unos seguida de una serie de ceros	Valor equivalente en decimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Ejemplo: Para una dirección IP 132.248.10.1 con máscara de red 255.255.0.0

132.248.10.1	=	10000100.11111000.00001010.00000100
255.255.255.0	=	11111111.11111111.11111111.00000000
Resultado 132.248.10.0	=	10000100.11111000.00001010.00000000

Tabla 5.2.3. Equivalencia por tamaño en redes entre CIDR y redes por clase.

Sub-máscara en notación decimal punteada	Sub-máscara en notación CIDR	Equivalencia en tamaño a redes por clase
255.0.0.0	/8	254 redes clase B o 1 red clase A
255.128.0.0	/9	128 redes clase B
255.192.0.0	/10	64 redes clase B
255.224.0.0	/11	32 redes clase B
255.240.0.0	/12	16 redes clase B
255.228.0.0	/13	8 redes clase B
255.252.0.0	/14	4 redes clase B

255.254.0.0	/15	2 redes clase B
255.255.0.0	/16	1 red clase B o 254 redes clase C
255.255.128.0	/17	128 redes clase C
255.255.192.0	/18	64 redes clase C
255.255.224.0	/19	32 redes clase C
255.255.240.0	/20	16 redes clase C
255.255.248.0	/21	8 redes clase C
255.255.252.0	/22	4 redes clase C
255.255.254.0	/23	2 redes clase C
255.255.255.0	/24	1 red clase C
255.255.255.128	/25	1/2 de red clase C
255.255.255.192	/26	1/4 de red clase C
255.255.255.224	/27	1/8 de red clase C
255.255.255.240	/28	1/16 de red clase C
255.255.255.248	/29	1/32 de red clase C
255.255.255.252	/30	1/64 de red clase C

Para redes que requieren acceso limitado a internet o mayor número de direcciones se utilizan direcciones privadas (ver tabla 5.2.4).

Tabla 5.2.4. Direcciones Privadas (RFC1918).

Clase	Direcciones	Máscara de red
A	10.0.0.0 – 10.255.255.255	255.0.0.0
B	172.16.0.0 – 172.31.255.255	255.240.0.0
C	192.168.0.0 – 192.168.255.255	255.255.0.0

Asignación de direcciones planificada y documentada para:

- No duplicar direcciones
- Proporcionar y controlar el acceso a la red
- Cuidar la seguridad y el rendimiento
- Decidir cuándo utilizar direcciones privadas y dónde se deben aplicar

Consideraciones

Si hay más dispositivos que direcciones públicas disponibles, sólo esos dispositivos que accederán directamente a Internet (servidores Web) requieren una dirección pública.

Un servicio NAT permitiría a los dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.

Direccionamiento lógico

Notación CIDR

Se introdujo en 1993 para brindar flexibilidad al dividir rangos de direcciones IP para crear subredes, de manera que no sea necesario asignar bloques de direcciones en los límites de los octetos, sino solo utilizar el número de bits necesarios para el número de subredes que se requieran.

La notación CIDR es de la siguiente manera: dirección IP / # bits de máscara

Donde:

$2^m - 2$ = cantidad de subredes, donde m = cantidad de bits que se tomarán prestados

$2^n - 2$ = cantidad de hosts por subred, donde n = cantidad de bits para cada host

A medida que la red TCP/IP se expandió en los 80's, el número de ordenadores con dirección IP pública creció exponencialmente forzando a los routers a incrementar la memoria necesaria para almacenar tablas de ruteo y administrar los recursos necesarios para su constante actualización.

Esto llevó al desarrollo de las subredes CIDR, sin embargo, este mismo crecimiento llevó a identificar que aún había un serio desperdicio de direcciones IP. Por lo que fue necesario desarrollar un nuevo esquema de direccionamiento, surgiendo entonces VLSM (Variable Length Subnet Mask)

Para realizar la tabla de ruteo por CIDR, se pueden tomar en cuenta dos datos: cantidad de subredes o cantidad de hosts.

La máscara de red se divide en dos partes:

Porción de red: Si la máscara es por defecto, en una dirección con clase, la cantidad de bits "1" en la porción de red, implica la dirección de red.

Porción de host: La cantidad de bits "0" en la porción de host en la máscara, indica que parte de la dirección de red se emplea para asignar direcciones de host.

Cabe mencionar que al realizar subneting se debe de tomar en cuenta que la primera y última subred no se toman en cuenta, es decir, no se pueden asignar aquellas direcciones de red cuya máscara de red sean todos 1 o 0, de ahí la fórmula $2^n - 2$ para calcular el número de subredes.

Ejemplo: Dada la red clase B 172.16.0.0/16, obtenga mediante el método de subneteo: 50 subredes con un mínimo de 1000 host por subred.

Nota: Este ejemplo está diseñado de manera tal que la cantidad de bits disponibles a usar sean justos a los requerimientos de la red.

Paso 1:

La máscara de red por defecto es:

Porción de Red		Porción de Host	
255	255	0	0
11111111	11111111	00000000	00000000 = /16

Empleando la fórmula $2^m - 2$ = cantidad de subredes, se obtiene:

$$2^m - 2 = 50 \Rightarrow m = \log_2(50 + 2) = 5.7 \Rightarrow m = 6 \text{ bits}$$

Por lo que se necesitan 6 bits para cubrir el requerimiento mínimo de 50 subredes, esto es:

$$2^6 - 2 = 62 \text{ subredes}$$

Como 6 son los bits que se tomaron prestados, la nueva máscara de red quedaría de la siguiente manera:

Porción de Red		Porción de Host	
11111111	11111111	**11111**00	00000000 = /22
255	255	252	0

Paso 2:

Una vez calculada la máscara de red, se obtendrá la cantidad de host por subred.

Se piden 1000 host por subred:

Empleando la fórmula $2^n - 2$ = cantidad de hosts por subred, obtenemos:

$$2^n - 2 = 1000 \Rightarrow n = \log_2(1000 + 2) = 9.9 \Rightarrow n = 10 \text{ bits}$$

$$2^{10} - 2 = 1022 \text{ hosts}$$

Porción de Red		**Porción de Host**	
172	16	0	0
10101100	00010000	00000**00**	**00000000**

Paso 3:

Ahora se obtendrá el rango por cada subred, para ello se trabajará con la porción de red de la dirección IP de la red, de manera específica, con la porción de red que se modificó en la máscara de red.

Porción de Red		**Porción de Host**	
172	16	0	0
10101100	00010000	00000**00**	**00000000**
		Subred	

Una manera sencilla para obtener el rango en cada subred es restando al número 256 el número de la máscara de subred adaptada, para este ejemplo, quedará de la siguiente manera:

$$256 - 252 = 4$$

Por lo tanto, 4 va a ser el rango entre cada subred:

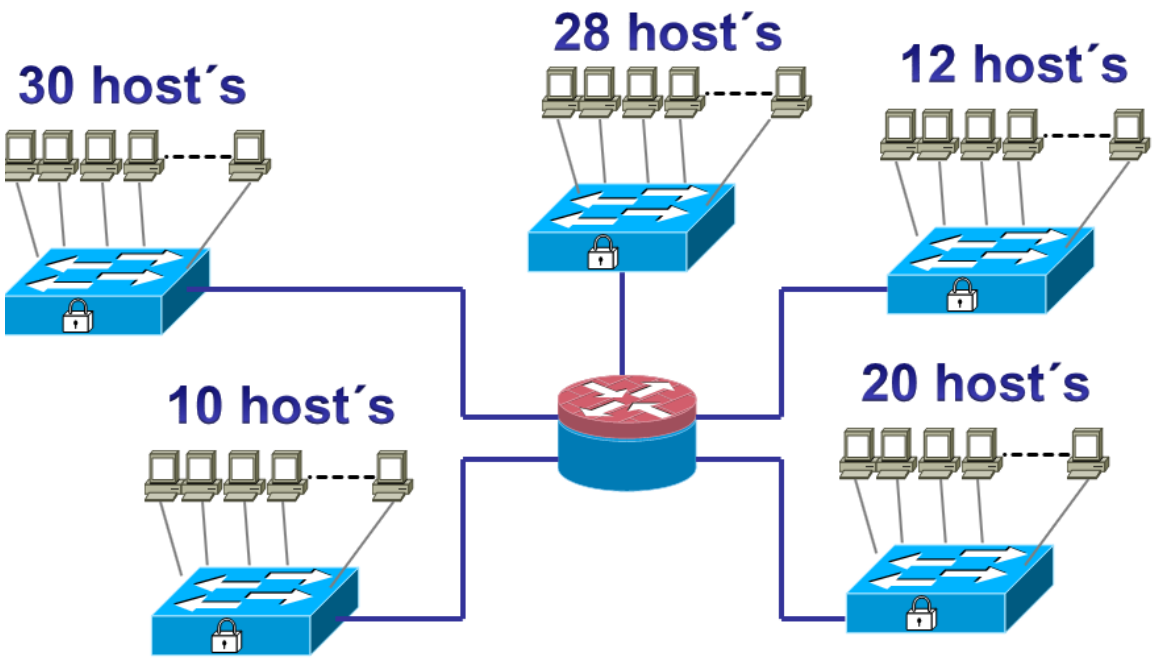
No. Subred	**Rango de IP's**		**Host asignados por subred**
	172.16.0.0	172.16.3.255	Esta subred no se utiliza
1	172.16.4.0	172.16.7.255	1022
2	172.16.8.0	172.16.11.255	1022
. . .	. . .	. . .	. . .
61	172.16.244.0	172.16.247.255	1022
62	172.16.248.0	172.16.251.255	1022
	172.16.252.0	172.16.255.255	Esta subred no se utiliza

La tabla de ruteo final quedará de la siguiente forma:

No. Subred	NetID	Rango de IP's asignables	Broadcast	Máscara de red	Cantidad de Hosts
1	172.16.4.0	172.16.4.1 172.16.7.254	172.16.7.255	255.255.252.0	1022
2	172.16.8.0	172.16.8.1 172.16.11.254	172.16.11.255	255.255.252.0	1022
. . .	. . .	. . .	. . .	. . .	. . .
61	172.16.244.0	172.16.244.1 172.16.247.254	172.16.247.255	255.255.252.0	1022
62	172.16.248.0	172.16.248.1 172.16.251.254	172.16.251.255	255.255.252.0	1022

Cuando se trabaja con CIDR, llega a haber ocasiones en las que son pocas las subredes o poco el número de host por subred las que hay que asignar, por lo tanto, la tabla de ruteo puede llegar a realizarse de dos formas: por cantidad de subredes o por cantidad de hosts.

Ejemplo: Realice el esquema de direccionamiento con notación CIDR para la red que se muestra. La dirección IP es 172.16.0.0



Por cantidad de subredes

Paso 1:

Máscara de red: $2^m - 2 = 5 \Rightarrow m = \log_2(5 + 2) = 2.8 \Rightarrow m = 3$ bits

$2^3 - 2 = 6$ subredes

172.16.0.0/19 => 255.255.224.0

Porción de Red		Porción de Host	
11111111	11111111	**111**00000	00000000 = /19
255	255	224	0

Paso 2:

El resto de bits se utilizarán para asignar los hosts, en este caso:

$2^{13} - 2 = 8190$ hosts utilizables por cada subred

172	.	16	.	0		.	0		
10101100	.	00010000	.	000	00000	.	00000000	Subred no asignable	
				0			1		
				000	00001		00000001		
				...			...		
				31			254		
				000	11111		11111110		
				31			255		
				000	11111		11111111		
				32			0	NetID	Subred 1
				001	00000		00000000		
				32			1	Rango Asignable	
				001	00001		00000001		
				...			...		
				63			254		
				001	11111		11111110		
				63			255	Broadcast	
				001	11111		11111111		

172	.	16	.	64	.	0	NetID	
				010 00000		00000000		
				64		1	Rango Asignable	Subred 2
				010 00000		00000001		
				...		...		
				95		254		
				010 11111		11111110		
				95		255	Broadcast	
				010 11111		11111111		
				96		0	NetID	Subred 3
				011 00000		00000000		
				96		1	Rango Asignable	
				011 00000		00000001		
				...		...		
				127		254		
				011 11111		11111110		
				127		255	Broadcast	
				011 11111		11111111		
10101100	.	00010000	.	128	.	0	NetID	Subred 4
				100 00000		00000000		
				128		1	Rango Asignable	
				100 00000		00000001		
				...		...		
				159		254		
				100 11111		11111110		
				159		255	Broadcast	
				100 11111		11111111		
				160		0	NetID	Subred 5
				101 00000		00000000		
				160		1	Rango Asignable	
				101 00000		00000001		
				...		...		
				191		254		
				101 11111		11111110		
				191		255	Broadcast	
				101 11111		11111111		

Tabla de ruteo

No. Subred	NetID	Rango de IP's asignables	Broadcast	Máscara de red	Cantidad de Hosts
1	172.16.32.0	172.16.32.1 172.16.63.254	172.16.63.255	255.255.224.0	8192
2	172.16.64.0	172.16.64.1 172.16.90.254	172.16.90.255	255.255.224.0	8192
3	172.16.91.0	172.16.91.1 172.16.127.254	172.16.127.255	255.255.224.0	8192
4	172.16.128.0	172.16.128.1 172.16.159.254	172.16.159.255	255.255.224.0	8192
5	172.16.160.0	172.16.160.1 172.16.191.254	172.16.191.255	255.255.224.0	8192

Por cantidad de hosts

Paso 1:

De acuerdo a la red, se asignará la cantidad de hosts a cada subred de acuerdo al número máximo que tenga una subred. En este caso, el mayor número de hosts de una subred es de 30, por lo tanto:

$$2^n - 2 = 30 \Rightarrow n = \log_2(30 + 2) = 5 \Rightarrow n = 5 \text{ bits}$$

$$2^5 - 2 = 30$$

Por lo tanto, se utilizarán 5 bits para realizar la asignación de IP's a cada subred.

Porción de Red			**Porción de Host**
172	16	0	0
10101100	00010000	00000000	000**00000**

Paso 2:

La cantidad de subredes será el resto de bits que no fueron utilizados por la porción de host.

$$2^{16-5} - 2 = 2^{11} - 2 = 2046 \text{ subredes}$$

Porción de Red		Porción de Host	
11111111	11111111	11111111	11100000 = /27
255	255	255	224

172	.	16	.	0	.	0		Subred no asignable	
10101100	.	00010000	.	00000000	.	000	00000		
						1			
						000	00001		
						...			
						30			
						000	11110		
						31			
						000	11111		
						32		NetID	Subred 1
						001	00000		
						33		Rango Asignable	
						001	00001		
						...			
						62			
						001	11110		
						63		Broadcast	
						001	11111		
						64		NetID	Subred 2
						010	00000		
						65		Rango Asignable	
						010	00001		
						...			
						94			
						010	11110		
						95		Broadcast	
						010	11111		
						96		NetID	Subred 3
						011	00000		
						97		Rango Asignable	
						011	00001		
						...			
						126			
						011	11110		
						127		Broadcast	
						011	11111		

172	.	16	.	0	.	128		NetID	
						100	00000		
						129		Rango Asignable	Subred 4
						100	00001		
						...			
						158			
						100	11110		
						159		Broadcast	
10101100	.	00010000	.	00000000	.	100	11111		
						160		NetID	
						101	00000		
						161		Rango Asignable	Subred 5
						101	00001		
						...			
						190			
						101	11110		
						191		Broadcast	
						101	11111		

Tabla de ruteo

No. Subred	NetID	Rango de IP's asignables	Broadcast	Máscara de red	Cantidad de Hosts
1	172.16.0.32	172.16.0.33 172.16.0.62	172.16.0.63	255.255.255.224	30
2	172.16.0.64	172.16.0.65 172.16.0.89	172.16.0.95	255.255.255.224	30
3	172.16.0.96	172.16.0.97 172.16.0.126	172.16.0.127	255.255.255.224	30
4	172.16.0.128	172.16.0.129 172.16.0.158	172.16.0.159	255.255.255.224	30
5	172.16.0.160	172.16.0.161 172.16.0.190	172.16.0.191	255.255.255.224	30

Como se puede observar, de acuerdo a cómo se decida realizar la tabla de subneteo, se tendrá un desperdicio de cantidad de hosts o de cantidad de subredes. Esta decisión de

cómo realizar el subneteo se hará con el administrador de la red para tomar las consideraciones necesarias.

Subneteo

Es la técnica que permite dividir una red para crear subredes de menor tamaño. Para crear subredes, se utiliza uno o más de los bits de la porción de host como bits de la porción de red. Mientras mayor es la cantidad de bits prestados:

- Se puede generar mayor cantidad de subredes
- Existen menos hosts en cada subred

Las fórmulas útiles para realizar subneting son:

$$\text{Número de subredes} = 2^m - 2$$

donde "m" es la cantidad de bits que se tomarán prestados de la porción de host.

$$\text{Número de hosts posibles} = 2^n - 2$$

donde "n" es la cantidad de bits que se tomarán prestados de la porción de host.

$$m = \text{número de bits de la porción de hosts} - n$$

VLSM

Se diseñó para maximizar la eficiencia del direccionamiento.

Entre sus características se encuentran:

- Se utilizan múltiples máscaras
- Las subredes que se crean no tienen el mismo número de equipos
- Se tiene una organización del espacio de direcciones más acorde con las necesidades reales
- El desaprovechamiento de direcciones IP es mínimo

Donde:

2^m = cantidad de subredes, donde m = cantidad de bits que se tomarán prestados

$2^n - 2$ = cantidad de hosts por subred, donde n = cantidad de bits para cada host

Por ejemplo:

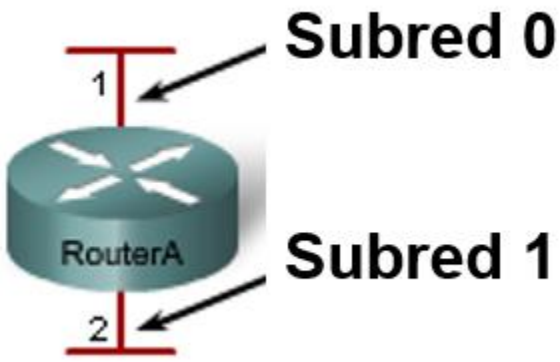
Red 197.224.119.0/25

11000101 . 11100000 . 01110111 . 00000000 Dirección IP

11111111 . 11111111 . 11111111 . 10000000 Máscara de Red

Se tienen 2 direcciones de subred:

Subred	Dirección de Red	Rango Asignable	Dirección de Broadcast	Máscara de red
0	197.224.119.0/25	197.224.119.1 197.224.119.126	197.224.119.127	255.255.255.128
1	197.224.119.128/25	197.224.119.129 197.224.119.254	197.224.119.255	255.255.255.128



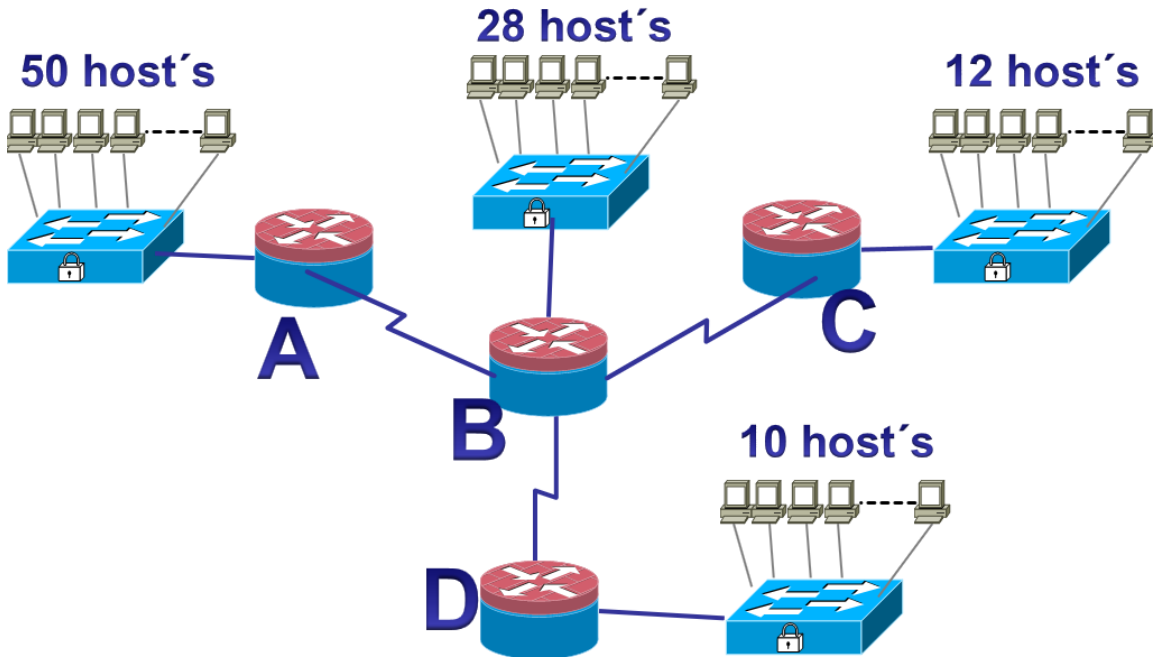
Para poder realizar la tabla de ruteo de una red, se debe de seguir una serie de pasos para realizar la asignación de IPs correctamente:

1. Hacer una lista de las subredes y ordenarlas por número de hosts de mayor a menor. Es decir, primero se asignarán IPs a las subredes que tengan más cantidad de hosts, y consecuentemente a los de menor cantidad.
2. Identificar la cantidad de bits requeridos por cada subred de acuerdo al número de host de cada subred más dos direcciones IP, correspondientes al netID y al broadcast. Por lo que la expresión final para obtener la cantidad de direcciones IP a usar para cada subred será: 2^n = cantidad de direcciones IP
3. Si dos routers están conectados entre sí, se considera que hay otra subred entre ambos, por lo que necesitaremos de 4 direcciones IP para esta subred, una del netID, dos para los nodos de los routers y una para el broadcast. Generalmente estos enlaces se realizan al final de la tabla de ruteo, ya que son como dos hosts en una subred, lo que las hace una subred de cantidad mínima en comparación con otras.

4. Una vez hecho el cálculo anterior, se asignará la primera dirección IP al netID de la subred, y la última dirección IP al broadcast. Todas las demás restantes, serán IPs asignables a cada host. De ahí el resultado de: $2^m - 2$ = cantidad de host por subred.

A continuación, se ejemplificará paso por paso la realización de la tabla de ruteo de una red.

Ejemplo: Dada la siguiente red con dirección IP 192.224.119.0, realizar el esquema de direccionamiento VLSM.



Paso 1:

Primeramente, se organizan las subredes de mayor a menor cantidad de hosts:

Subred	Cantidad de hosts
Router A	50
Router B	28
Router C	12
Router D	10
Enlace B-A	2
Enlace B-C	2
Enlace B-D	2

Paso 2:

Ahora que se tiene la lista ordenada de mayor a menor, se procede a calcular la cantidad de bits para cada subred, partiendo de la IP que se proporciona, en este caso, 192.224.119.0.

Router A

50 hosts + netId + broadcast = 52 direcciones IP

$2^n = 52 \Rightarrow n = \log_2(52) = 5.7 \Rightarrow n = 6$ bits

<table>
<tr><td>192</td><td>.</td><td>224</td><td>.</td><td>119</td><td>.</td><td colspan="2">0</td><td rowspan="2">NetID</td></tr>
<tr><td rowspan="9">11000000</td><td rowspan="9">.</td><td rowspan="9">11100000</td><td rowspan="9">.</td><td rowspan="9">01110111</td><td rowspan="9">.</td><td>00</td><td>000000</td></tr>
<tr><td colspan="2">1</td><td rowspan="6">Rango Asignable</td></tr>
<tr><td>00</td><td>000001</td></tr>
<tr><td colspan="2">...</td></tr>
<tr><td colspan="2">62</td></tr>
<tr><td>00</td><td>111110</td></tr>
<tr><td colspan="2">63</td><td rowspan="2">Broadcast</td></tr>
<tr><td>00</td><td>111111</td></tr>
<tr><td>255</td><td>.</td><td>255</td><td>.</td><td>255</td><td>.</td><td colspan="2">192</td><td rowspan="2">Máscara de Red</td></tr>
<tr><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>11</td><td>000000</td></tr>
</table>

Por lo tanto:

192.224.119.0 => NetID

192.224.119.1 - 192.224.119.62 => Rango de direcciones IP asignables

192.224.119.63 => Broadcast

255.255.255.192 => Máscara de Red

Se realizan los mismos pasos para las demás subredes.

Router B

28 hosts + netId + broadcast = 30 direcciones IP

$2^n = 30 \Rightarrow n = \log_2(30) = 4.9 \Rightarrow n = 5$ bits

<table>
<tr><td>192</td><td>.</td><td>224</td><td>.</td><td>119</td><td>.</td><td colspan="2">64</td><td rowspan="2">NetID</td></tr>
<tr><td rowspan="8">11000000</td><td rowspan="8">.</td><td rowspan="8">11100000</td><td rowspan="8">.</td><td rowspan="8">01110111</td><td rowspan="8">.</td><td>010</td><td>00000</td></tr>
<tr><td colspan="2">65</td><td rowspan="5">Rango Asignable</td></tr>
<tr><td>010</td><td>00001</td></tr>
<tr><td colspan="2">...</td></tr>
<tr><td colspan="2">94</td></tr>
<tr><td>010</td><td>11110</td></tr>
<tr><td colspan="2">95</td><td rowspan="2">Broadcast</td></tr>
<tr><td>010</td><td>11111</td></tr>
<tr><td>255</td><td>.</td><td>255</td><td>.</td><td>255</td><td>.</td><td colspan="2">224</td><td rowspan="2">Máscara de Red</td></tr>
<tr><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>111</td><td>00000</td></tr>
</table>

Por lo tanto:

192.224.119.64 => NetID

192.224.119.65 - 192.224.119.94 => Rango de direcciones IP asignables

192.224.119.95 => Broadcast

255.255.255.224 => Máscara de Red

Router C

12 hosts + netId + broadcast = 14 direcciones IP

$2^n = 14 \Rightarrow n = \log_2(14) = 3.8 \Rightarrow n = 4$ bits

192	.	224	.	119	.	96		NetID
11000000	.	11100000	.	01110111	.	0110	0000	
						97		Rango Asignable
						0110	0001	
						...		
						110		
						0110	1110	
						111		Broadcast
						0110	1111	
255	.	255	.	255	.	240		Máscara de Red
11111111	.	11111111	.	11111111	.	1111	0000	

Por lo tanto:

192.224.119.64 => NetID

192.224.119.65 - 192.224.119.94 => Rango de direcciones IP asignables

192.224.119.95 => Broadcast

255.255.255.240 => Máscara de Red

Router D

10 hosts + netId + broadcast = 12 direcciones IP

$2^n = 12 \Rightarrow n = \log_2(12) = 3.5 \Rightarrow n = 4$ bits

<table>
<tr><td>192</td><td>.</td><td>224</td><td>.</td><td>119</td><td>.</td><td colspan="2">112</td><td rowspan="2">NetID</td></tr>
<tr><td rowspan="8">11000000</td><td rowspan="8">.</td><td rowspan="8">11100000</td><td rowspan="8">.</td><td rowspan="8">01110111</td><td rowspan="8">.</td><td colspan="2">0111 0000</td></tr>
<tr><td colspan="2">113</td><td rowspan="5">Rango Asignable</td></tr>
<tr><td colspan="2">0111 0001</td></tr>
<tr><td colspan="2">...</td></tr>
<tr><td colspan="2">126</td></tr>
<tr><td colspan="2">0111 1110</td></tr>
<tr><td colspan="2">127</td><td rowspan="2">Broadcast</td></tr>
<tr><td colspan="2">0111 1111</td></tr>
<tr><td>255</td><td>.</td><td>255</td><td>.</td><td>255</td><td>.</td><td colspan="2">240</td><td rowspan="2">Máscara de Red</td></tr>
<tr><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>11111111</td><td>.</td><td>1111</td><td>0000</td></tr>
</table>

Por lo tanto:

192.224.119.112 => NetID

192.224.119.113 - 192.224.119.126 => Rango de direcciones IP asignables

192.224.119.127 => Broadcast

255.255.255.240 => Máscara de Red

Paso 3:

Se realiza el mismo procedimiento para los enlaces entre los routers:

Enlace B-A

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

192	.	224	.	119	.	128		NetID
11000000	.	11100000	.	01110111	.	100000	00	
						129		Rango Asignable
						100000	01	
						130		
						100000	10	
						131		Broadcast
						100000	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

192.224.119.128 => NetID

192.224.119.129 - 192.224.119.130 => Rango de direcciones IP asignables

192.224.119.131 => Broadcast

255.255.255.252 => Máscara de Red

Enlace B-C

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

192	.	224	.	119	.	132		NetID
11000000	.	11100000	.	01110111	.	100001	00	
						133		Rango Asignable
						100001	01	
						134		
						100001	10	
						135		Broadcast
						100001	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

192.224.119.132 => NetID

192.224.119.133 - 192.224.119.134 => Rango de direcciones IP asignables

192.224.119.135 => Broadcast

255.255.255.252 => Máscara de Red

Enlace B-D

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

192	.	224	.	119	.	136		NetID
11000000	.	11100000	.	01110111	.	100010	00	
						137		Rango Asignable
						100010	01	
						138		
						100010	10	
						139		Broadcast
						100010	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

192.224.119.136 => NetID

192.224.119.137 - 192.224.119.138 => Rango de direcciones IP asignables

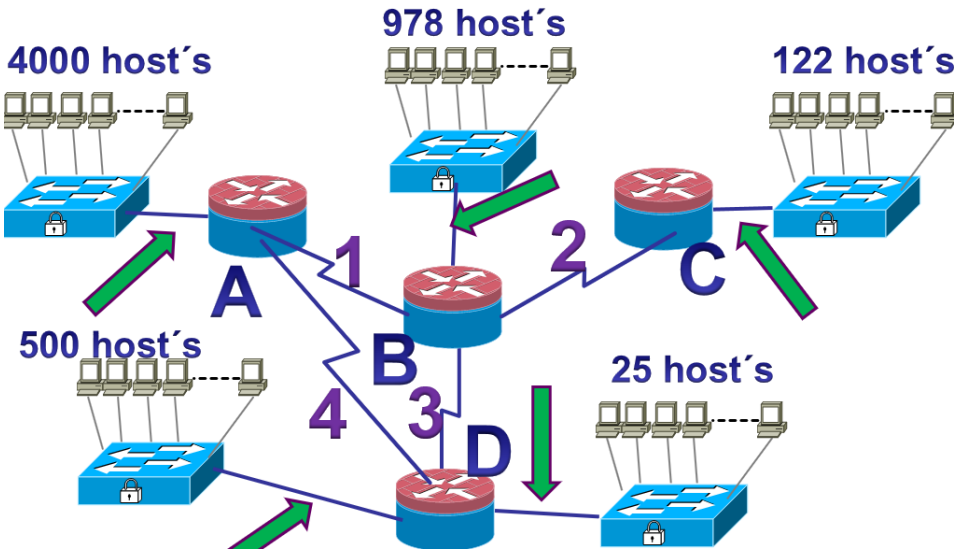
192.224.119.139 => Broadcast

255.255.255.252 => Máscara de Red

Una vez terminadas todas las subredes, se tiene la tabla de ruteo final:

Subred	NetID	Rango Asignable	Dirección de Broadcast	Máscara de Red
Router A 50 hosts	192.224.119.0/26	192.224.119.1 192.224.119.62	192.224.119.63	255.255.255.192
Router B 28 hosts	192.224.119.64/27	192.224.119.65 192.224.119.94	192.224.119.95	255.255.255.224
Router C 12 hosts	192.224.119.96/28	192.224.119.97 192.224.119.110	192.224.119.111	255.255.255.240
Router D 10 hosts	192.224.119.112/28	192.224.119.113 192.224.119.126	192.224.119.127	255.255.255.240
Enlace B-A 2 puntos	192.224.119.128/30	192.224.119.129 192.224.119.130	192.224.119.131	255.255.255.252
Enlace B-C 2 puntos	192.224.119.132/30	192.224.119.133 192.224.119.134	192.224.119.135	255.255.255.252
Enlace B-D 2 puntos	192.224.119.136/30	192.224.119.137 192.224.119.138	192.224.119.139	255.255.255.252

Ejemplo: Dada la siguiente red con dirección IP 142.24.0.0, realizar el esquema de direccionamiento VLSM.



Paso 1:

Subred	Cantidad de hosts
Router A	4000
Router B	978
Router C	122
Router D	500
Router D	25
Enlace B-A	2
Enlace B-C	2
Enlace B-D	2
Enlace A-D	2

=>

Subred	Cantidad de hosts
Router A	4000
Router B	978
Router D	500
Router C	122
Router D	25
Enlace B-A	2
Enlace B-C	2
Enlace B-D	2
Enlace A-D	2

Paso 2:

Router A

4000 hosts + netId + broadcast = 4002 direcciones IP

$2^n = 4002 \Rightarrow n = \log_2(4002) = 11.9 \Rightarrow n = 12$ bits

142	.	24	.	0		.	0	NetID
10001110	.	00011000	.	0000	0000	.	00000000	
				0			1	Rango Asignable
				0000	0000		0000001	
				...			...	
				15			254	
				0000	1111		11111110	
				15			255	Broadcast
				0000	1111		11111111	
255	.	255	.	240		.	0	Máscara de Red
11111111	.	11111111	.	1111	0000	.	00000000	

Por lo tanto:

142.24.0.0 => NetID

142.24.0.1 - 142.24.15.254 => Rango de direcciones IP asignables

142.24.15.255 => Broadcast

255.255.240.0 => Máscara de Red

Router B

978 hosts + netId + broadcast = 980 direcciones IP

$2^n = 980 \Rightarrow n = \log_2(980) = 9.9 \Rightarrow n = 10$ bits

142	.	24	.	16		.	0	NetID
10001110	.	00011000	.	000100	00	.	00000000	
				16			1	Rango Asignable
				000100	00		0000001	
				. . .			. . .	
				19			254	
				000100	11		11111110	
				19			255	Broadcast
				000100	11		11111111	
255	.	255	.	252		.	0	Máscara de Red
11111111	.	11111111	.	111111	00	.	00000000	

Por lo tanto:

142.24.16.0 => NetID

142.24.16.1 - 142.24.19.254 => Rango de direcciones IP asignables

142.24.19.255 => Broadcast

255.255.252.0 => Máscara de Red

Router D

500 hosts + netId + broadcast = 502 direcciones IP

$2^n = 502 \Rightarrow n = \log_2(502) = 8.9 \Rightarrow n = 9$ bits

142	.	24	.	20		.	0	NetID
10001110	.	00011000	.	0001010	0	.	00000000	
				20			1	Rango Asignable
				0001010	0		0000001	
				. . .			. . .	
				21			254	
				0001010	1		11111110	
				21			255	Broadcast
				0001010	1		11111111	
255	.	255	.	254		.	0	Máscara de Red
11111111	.	11111111	.	1111111	0	.	00000000	

Por lo tanto:

142.24.20.0 => NetID

142.24.20.1 - 142.24.21.254 => Rango de direcciones IP asignables

142.24.21.255 => Broadcast

255.255.254.0 => Máscara de Red

Router C

122 hosts + netId + broadcast = 124 direcciones IP

$2^n = 124 \Rightarrow n = \log_2(124) = 6.9 \Rightarrow n = 7$ bits

142	.	24	.	22	.	0		NetID
10001110	.	00011000	.	00010110	.	0	0000000	
						1		Rango Asignable
						0	0000001	
						.		
						.		
						.		
						126		
						0	1111110	
						127		Broadcast
						0	1111111	
255	.	255	.	255	.	128		Máscara de Red
11111111	.	11111111	.	11111111	.	1	0000000	

Por lo tanto:

142.24.22.0 => NetID

142.24.22.1 - 142.24.22.126 => Rango de direcciones IP asignables

142.24.22.127 => Broadcast

255.255.255.128 => Máscara de Red

Router D

25 hosts + netId + broadcast = 27 direcciones IP

$2^n = 27 \Rightarrow n = \log_2(27) = 4.7 \Rightarrow n = 5$ bits

142	.	24	.	22	.	128		NetID
10001110	.	00011000	.	00010110	.	100	00000	
						129		Rango Asignable
						100	00001	
						.		
						.		
						.		
						158		
						100	11110	
						159		Broadcast
						100	11111	
255	.	255	.	255	.	224		Máscara de Red
11111111	.	11111111	.	11111111	.	111	00000	

Por lo tanto:

142.24.22.128 => NetID

142.24.22.129 - 142.24.22.158 => Rango de direcciones IP asignables

142.24.22.159 => Broadcast

255.255.255.224 => Máscara de Red

Paso 3:

Enlace B-A

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

142	.	24	.	22	.	160		NetID
10001110	.	00011000	.	00010110	.	101000	00	
						161		Rango Asignable
						101000	01	
						162		
						101000	10	
						163		Broadcast
						101000	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

142.24.22.160 => NetID

142.24.22.161 - 142.24.22.162 => Rango de direcciones IP asignables

142.24.22.163 => Broadcast

255.255.255.252 => Máscara de Red

Enlace B-C

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

142	.	24	.	22	.	164		NetID
10001110	.	00011000	.	00010110	.	101001	00	
						165		Rango Asignable
						101001	01	
						166		
						101001	10	
						167		Broadcast
						101001	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

142.24.22.164 => NetID

142.24.22.165 - 142.24.22.166 => Rango de direcciones IP asignables

142.24.22.167 => Broadcast

255.255.255.252 => Máscara de Red

Enlace B-D

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

142	.	24	.	22	.	168		NetID
10001110	.	00011000	.	00010110	.	101010	00	
						169		Rango Asignable
						101010	01	
						170		
						101010	10	
						171		Broadcast
						101010	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

142.24.22.168 => NetID

142.24.22.169 - 142.24.22.170 => Rango de direcciones IP asignables

142.24.22.171 => Broadcast

255.255.255.252 => Máscara de Red

Enlace A-D

2 hosts + netId + broadcast = 4 direcciones IP

$2^n = 4 \Rightarrow n = \log_2(4) = 2 \Rightarrow n = 2$ bits

142	.	24	.	22	.	172		NetID
10001110	.	00011000	.	00010110	.	101011	00	
						173		Rango Asignable
						101011	01	
						174		
						101011	10	
						175		Broadcast
						101011	11	
255	.	255	.	255	.	252		Máscara de Red
11111111	.	11111111	.	11111111	.	111111	00	

Por lo tanto:

142.24.22.172 => NetID

142.24.22.173 - 142.24.22.174 => Rango de direcciones IP asignables

142.24.22.175 => Broadcast

255.255.255.252 => Máscara de Red

Tabla de ruteo

Subred	NetID	Rango Asignable	Dirección de Broadcast	Máscara de Red
Router A 4000 hosts	142.24.0.0/20	142.24.0.1 142.24.15.254	142.24.15.255	255.255.240.0
Router B 978 hosts	142.24.16.0/22	142.24.16.1 142.24.19.254	142.24.19.255	255.255.252.0
Router D 500 hosts	142.24.20.0/23	142.24.20.1 142.24.21.254	142.24.21.255	255.255.254.0
Router C 122 hosts	142.24.22.0/25	142.24.22.1 142.24.22.126	142.24.22.127	255.255.255.128
Router D 25 hosts	142.24.22.128/27	142.24.22.129 142.24.22.158	142.24.22.159	255.255.255.224
Enlace 1 2 puntos	142.24.22.160/30	142.24.22.161 142.24.22.162	142.24.22.163	255.255.255.252
Enlace 2 2 puntos	142.24.22.164/30	142.24.22.165 142.24.22.166	142.24.22.167	255.255.255.252
Enlace 3 2 puntos	142.24.22.168/30	142.24.22.169 142.24.22.170	142.24.22.171	255.255.255.252
Enlace 4 2 puntos	142.24.22.172/30	142.24.22.173 142.24.22.174	142.24.22.175	255.255.255.252

Para usar esta técnica se necesita un protocolo de enrutamiento que lo soporte, ya que ahora es necesario enviar tanto la dirección de la subred como la máscara de red correspondiente en las actualizaciones.

Entre los protocolos de enrutamiento internos que permiten el manejo de VLSM están RIPv2, EIGRP y OSPF.

Sumarización de rutas

Los routers pueden llegar a manejar tablas de enrutamiento tan grandes (a veces varios miles o cientos de miles de rutas) que la complejidad de la administración de las mismas sumado a la carga y el consumo de recursos sean elementos muy importantes con los cuales los ingenieros de redes deben lidiar para entregar un servicio eficiente, seguro y confiable en sus sistemas.

Una de las técnicas utilizadas para optimizar los recursos en este tipo de situaciones es la sumarización o creación de superredes, también denominado supernetting. La creación de

redes sumarizadas permite reducir considerablemente las entradas en la tabla de enrutamiento al resumir la información de direccionamiento de dos o más subredes en un solo bloque IP. La sumarización podría entenderse como el proceso inverso de creación de subredes, donde en ese caso se parte de una red inicial y se divide en bloques de igual tamaño para crear las subredes. En la sumarización lo que se busca es unir todas las subredes en un único bloque original.

Ejemplo: Las siguientes redes:

- 10.56.248.0/24
- 10.56.249.0/25
- 10.56.249.128/26
- 10.56.249.192/26
- 10.56.250.0/23

Pueden sumarizarse como: 10.56.248.0/22

Paso 1: Escribir las direcciones en binario.

10.56.248.0/24:
00001010.00111000.11111000.00000000

10.56.249.0/25
00001010.00111000.11111001.00000000

10.56.249.128/26
00001010.00111000.11111001.10000000

10.56.249.192/26
00001010.00111000.11111001.11000000

10.56.250.0/23
00001010.00111000.11111010.00000000

Paso 2: Ver cuantos bits coinciden de izquierda a derecha en todas las redes a la vez. Con esto se obtiene el prefijo en bits:

00001010.00111000.11111000.00000000
00001010.00111000.11111001.00000000
00001010.00111000.11111001.10000000
00001010.00111000.11111001.11000000
00001010.00111000.11111010.00000000

22 bits coinciden perfectamente de izquierda a derecha, por lo que el resultado va a ser /22.

Paso 3: Se pone en cero todos los bits que no coinciden y se escribe un número único:

00001010.00111000.1111100.00000000

Paso 4: Se pasa ese número a decimal:

00001010 = 10
00111000 = 56
11111000 = 248
00000000 = 0

= 10.56.248.0

Paso 5: Se junta el resultado anterior con el prefijo del paso 2:

10.56.248.0/22

Paso 6: Opcionalmente se escribe el prefijo de la máscara en decimal:

22 bits = 11111111.11111111.11111100.00000000 = 255.255.252.0

Otro ejemplo más visual para la sumarización de redes puede ser lo siguiente:

172	.	30	.	4	.	0
10101100		**00011110**		**000001**	00	00000000
172	.	30	.	5	.	0
10101100		**00011110**		**000001**	01	00000000
172	.	30	.	6	.	0
10101100		**00011110**		**000001**	10	00000000
172	.	30	.	7	.	0
10101100		**00011110**		**000001**	11	00000000

El resultado de la sumarización es:

172	.	30	.	4	.	0
10101100		**00011110**		**000001**	00	00000000

Con prefijo de red /22.

IPv6

Es la versión 6 del Protocolo de Internet (IP). Está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet. IPv4 soporta 4,294,967,296 (232) direcciones de red diferentes, mientras que IPv6 soporta 340,282,366,920,938,463,463,374,607,431,768,211,456 (2128 o 340 sextillones) direcciones, cerca de 4,3 x 1020 (430 trillones) direcciones por cada pulgada^2 *6.7 x 1017 (670 mil billones) direcciones/mm^2. Si se hace una comparación de direcciones IPv4 vs IPv6, se observa:

Dirección IPv4 en binario: 10000100.11111000.00111111.10111111
Dirección IPv4 en decimal: 132.248.63.191
Dirección IPv6 en binario:
0011 1111 1111 1110 : 0011 0011 0010 1000 : 0000 0000 0000 0100 : 0000 0000 0000 0010 : 0000 0010 0101 0000 : 0000 0100 1111 1111 : 1111 1110 0101 1100 : 1011 0011 1111 0100
Dirección IPv6 en hexadecimal IPv6: 3FFE:3328:4:3:250:4FF:FE5C:B3F4

Características principales

- Mayor espacio de direcciones, de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Simplifcación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad con el protocolo (IPsec).
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular que requieren manejo especial por los routers IPv6, tal como calidad de servicio o servicios de tiempo real.
- Capacidades de autenticación y privacidad.

La trama de ipv6 se puede observar en la figura 5.2.6:

<table>
<tr><td>0 – 3</td><td>4 – 11</td><td>12 – 15</td><td>16 – 23</td><td>24 – 31</td></tr>
<tr><td>Versión</td><td>Clase de tráfico</td><td colspan="3">Etiqueta de flujo</td></tr>
<tr><td colspan="3">Longitud del paquete</td><td>Siguiente cabecera</td><td>Límite de saltos</td></tr>
<tr><td colspan="5">Dirección origen</td></tr>
<tr><td colspan="5">Dirección destino</td></tr>
</table>

Figura 5.2.6. Trama IPv6.

Esta cabecera tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

- **Versión:** Es el número de versión IP, es decir, 6.
- **Clase de tráfico:** El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de video y audio sin control de congestión.
- **Etiqueta de flujo:** El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino específico. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20 bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo. La utilización de esta etiqueta, que identifica un camino a lo largo de la red, posibilita conmutar en vez de encaminar. Su uso viene descrito en el RFC 1809.
- **Longitud del paquete:** Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes.
- **Siguiente cabecera:** Indica el tipo de cabecera que sigue a la cabecera fija de IPv6.
- **Límite de datos:** Es el número de saltos máximo que le quedan al paquete. Este número es establecido a un valor máximo por el origen y decrementado en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es decrementado y toma el valor de 0, el paquete es descartado.
- **Dirección origen:** Es la dirección del origen del paquete.
- **Dirección destino:** Es la dirección del destino del paquete.

Otros protocolos importantes de la capa de red son los siguientes:

NAT (Network Address Translation)

Traduce direcciones IP “locales” también conocidas como “direcciones privadas” dentro de una empresa en una dirección “real” o “pública” para dirigirse al exterior, de manera que esta condición, que es contar con direcciones privadas que toda organización puede utilizar para sus comunicaciones internas permite que exista un mayor número de direcciones IP para las comunicaciones en el mundo.

Los tres rangos de direcciones locales o privadas son:

- 10.0.0.0 – 10.255.255.255/8 ⟶ 16,777,216 hosts
- 172.16.0.0 – 172.31.255.255/12 ⟶ 1,048,576 hosts
- 192.268.0.0.- 192.168.255.255/16 ⟶ 65,536 hosts

Así, cuando un equipo de una red que está configurado con una IP privada desea comunicación al exterior, debe pasar por el servidor NAT quien le asignará en carácter de préstamo una dirección IP pública que será liberada cuando el equipo en cuestión

concluya su comunicación al exterior y dicha dirección podrá ser asignada a otro equipo que lo requiera como se muestra en la figura 5.2.7.

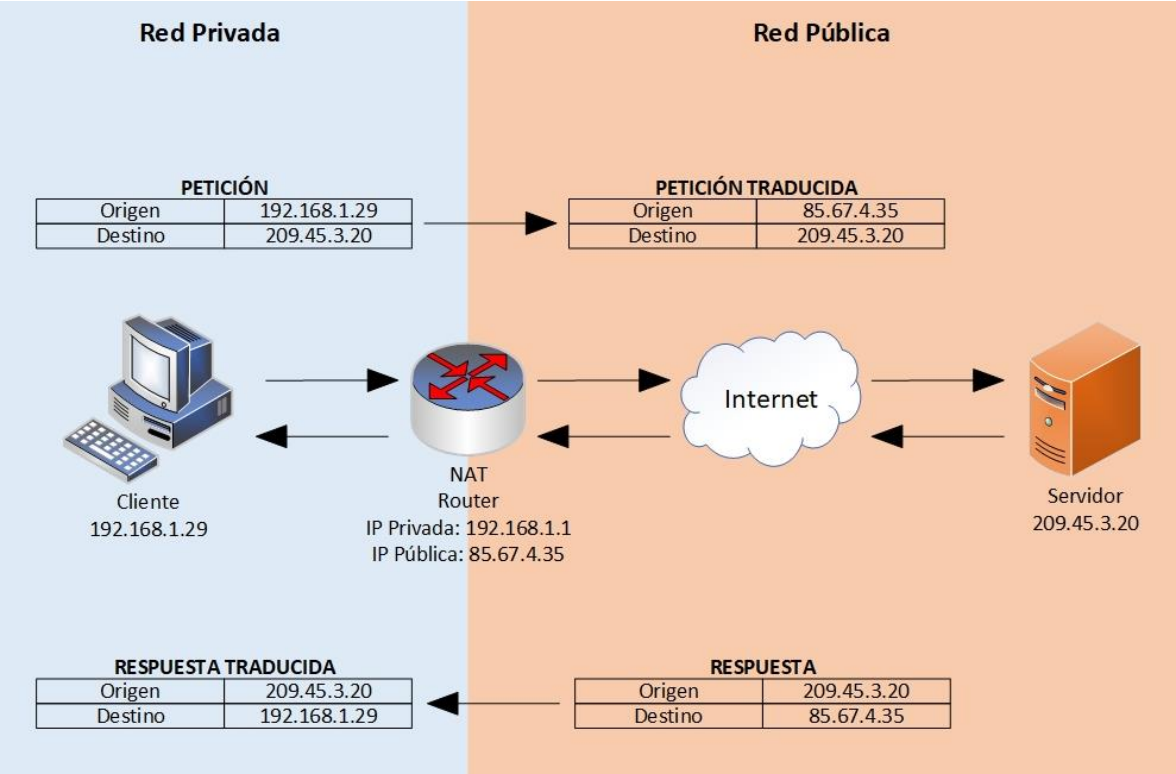


Figura 5.2.7. Asignación de dirección IP por medio de NAT.

Nodo que envía.

- Toma datos de TCP
- Pone los datos en un paquete (datagrama)
- Decide si es necesaria la fragmentación
- Determina ruta de acceso
- Envía el datagrama
- Local: Consigue la dirección física y envía
- Remoto: envía a un ruteador

Nodo que recibe

- Toma el paquete del nivel de enlace
- Determina si el paquete ha sido fragmentado
- Si está fragmentado lo re ensambla
- Pasa el datagrama a TCP

ARP (Address Resolution Protocol - Protocolo de resolución de direcciones)

En la red virtual de Internet, cada host tiene una dirección lógica IP. En las subredes físicas, cada host tiene una dirección de hardware. Para transmitir un datagrama al destino (host o enrutador) que se encuentre en la misma subred física, el datagrama debe encapsularse en un paquete que contenga la dirección hardware del destino.

ARP permite a una fuente encontrar la dirección de hardware de un destino que se encuentre en la misma subred física. Recibe como entrada la dirección IP del destino y regresa su dirección física (ver figura 5.2.8). Funciona en subredes que tienen la capacidad de difusión.

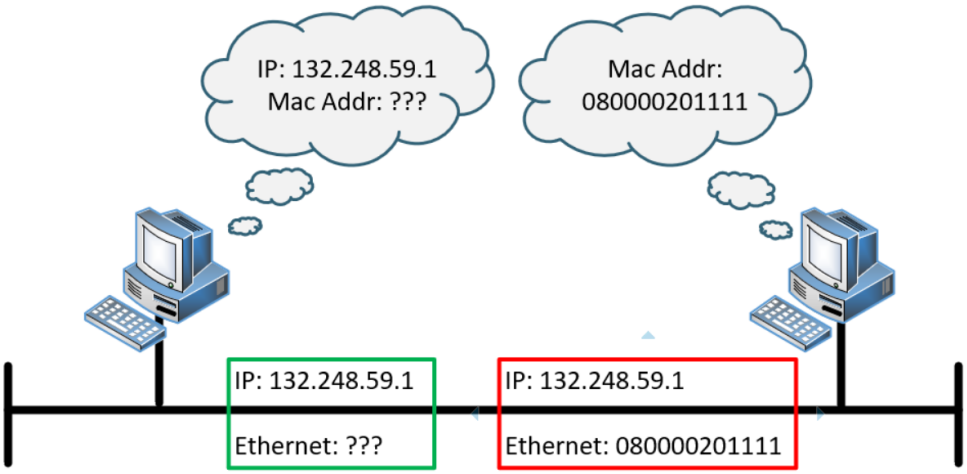


Figura 5.2.8. Protocolo de resolución de direcciones.

El Address Resolution Protocol (ARP) permite "mapear" de una dirección IP a una dirección física del equipo (MAC address para Ethernet) que está en una red local.

Por ejemplo, en IPv4, la dirección es de 32 bits. En una red de área local, sin embargo, las direcciones de la MAC son de 48 bits. Usualmente se utiliza una tabla llamada "cache ARP", que se usa para mantener la correlación entre la dirección MAC y la correspondiente IP address. ARP provee reglas para hacer dicha correlación y proveer las direcciones en conversión en ambos sentidos (ver figura 5.2.9).

0	8	16	24	31
Tipo de Hardware		Tipo de Protocolo		
HLen	PLen	Operación		
Sender HA (octeto 0 – 3)				
Sender HA (octeto 4 – 5)		Sender IP (octeto 0 – 1)		
Sender IP (octeto 2 – 3)		Target HA (octeto 0 – 1)		
Target HA (octeto 2 – 5)				
Target IP (octeto 0 – 3)				

Figura 5.2.9. Cabecera ARP.

Tipo de Hardware. Especifica un tipo de interfaz de hardware por el cual el envío requiere una respuesta. Ejemplo: Ethernet 1.

El tipo de Protocolo. Especifica el tipo del protocolo de dirección del alto-nivel donde el remitente lo ha provisto. Ejemplo: 0x800 IP

HLen. La longitud de la dirección de hardware.

PLen. La longitud de la dirección del protocolo.

Operación. Las operaciones son las siguientes:

1. ARP request
2. ARP response
3. RARP request
4. RARP response
5. Dynamic RARP request
6. Dynamic RARP reply
7. Dynamic RAR error
8. InARP request
9. InARP reply

Dirección del Hardware del origen. Longitud en bytes de la longitud del hardware.

Dirección del Protocolo del origen. Longitud en bytes de la longitud del protocolo.

El mensaje ARP se encapsula en un paquete de la subred física que se difunde por todas las máquinas de la subred. La difusión es muy costosa ya que todos los receptores deben procesar el paquete.

Cada fuente mantiene en caché una tabla con la pareja de direcciones (IP, hardware) que ha adquirido recientemente.

El mensaje ARP incluye la pareja de dirección de emisor para que los receptores puedan guardarla en su propia tabla.

Cuando se configura la interfaz de red de un equipo se emite un ARP (gratuito) para actualizar las tablas de las máquinas de la subred y asegurar la unicidad de una dirección IP.

ICMP (Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet)

Es un protocolo que permite administrar información relacionada con errores de los equipos en red. ICMP no permite corregir los errores, sino que los notifica a los protocolos de capas cercanas (ver figura 5.2.10).

Las funciones clave de ICMP son:

- **Anunciar errores en la red.** Tal como el host o una porción de la red (o completa) sean "inalcanzables", esto solamente muestra algún tipo de falla. Un paquete TCP o UDP directos a un número de puerto.
- **Anunciar congestión de la red.** Cuando un "router" empieza a tener "buffering" (cortes en su transmisión, es decir, no de manera fluida) de muchos paquetes, debido a la no disponibilidad de transmitir estos tan rápido como se están recibiendo, se genera un mensaje ICMP de apagar el origen. Con esto ocasiona que la fuente mande "más despacio" los paquetes a transmitir.
- **Asistencia a Fallas.** ICMP soporta una función "echo", el cual envía justamente un paquete round-trip entre dos hosts. El comando "ping" (Packet InterNet Groper) es una utilería muy común en la administración de redes, que está basado en la siguiente característica. Ping transmitirá una serie de paquetes, calculando el valor promedio de la vía round-trip en tiempo y porcentaje de paquetes perdidos.
- **Anuncia tiempos fuera (timeout).** Si unos paquetes IP tienen el campo "TTL" borrado (tienen el valor en cero), el router descarta los paquetes que fueron generados con esta configuración. Traceroute es una utilería capaz de mapear rutas de red que envían paquetes con valores pequeños de TTL y se pueden observar los "timeouts" de los ICMP anunciados.

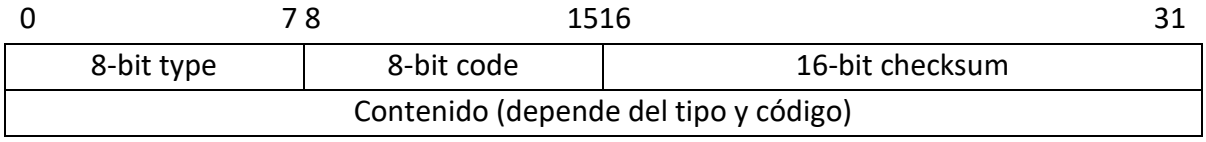


Figura 5.2.10. Cabecera ICMP.

Tipo. Los mensajes pueden ser un error o de información. Los errores de mensaje pueden ser:

0/8. Solicitud/respuesta Eco
3. Destino inalcanzable
5. Redirección (enrutamiento)
11. Tiempo excedido.
9/10. Anuncio/Solicitud de enrutador
17/18. Solicitud/Respuesta de máscara

Código. Para cada tipo de mensaje diferentes códigos están definidos. Donde los mensajes son:

- No routing hacia el destino
- Comunicación con destino administrativamente prohibido
- No es un vecino
- Dirección inalcanzable
- Puerto inalcanzable

Checksum. Los 16 bits en complemento a 1 de la suma de los mensajes ICMP iniciando con el tipo ICMP. Al calcular el valor del checksum debe ser cero.

Identificador. Un identificador para ayudar a encontrar peticiones respuestas; debe ser cero.

Número de secuencia. Número de secuencia para ayudar a encontrar peticiones respuestas; debe ser cero.

Dirección de la máscara. Una dirección de 32 bits.

Redirección

Cuando un enrutador recibe un host un datagrama cuya mejor "ruta" hacia el destino pasa por otro enrutador de la misma subred física, envía un mensaje de "redirección" al host fuente para pedirle que los siguientes datagramas que envíe al mismo destino los dirija directamente al otro enrutador.

0 para una red	2 para una red con un tipo de servicio
1 para un host	3 para un host con un tipo de servicio

Tiempo excedido

Cuando se descarta un datagrama debido a que su TTL llega a cero, se envía un mensaje "tiempo excedido" hacia la fuente.

El código del mensaje indica si el datagrama se descartó en un salto (0) o durante el reensamblado (1).

El mensaje "tiempo excedido" se utiliza para implementar el comando "traceroute".

Este comando imprime que enrutadores se encuentran en la ruta hasta cierto destino.

IGMP (Internet Group Management Protocol)

Se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

Los mensajes ICMP se envían en datagramas IP (ver figura 5.2.11). La cabecera IP tendrá siempre un número de protocolo de 2, indicando IGMP y un tipo de servicio de cero (rutina). El campo de datos IP contendrá mensaje IGMP de 8 bytes con el formato mostrado en la figura que se muestra a continuación:

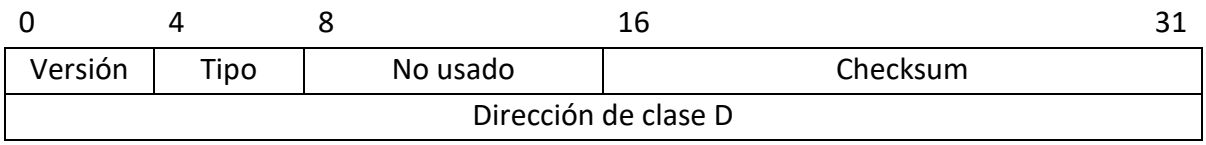


Figura 5.2.11. Cabecera IGMP.

Versión. Versión IP de 4 bits. Siempre 1.

Tipo. Especifica una recuperación o un informe.

1 – Especifica una recuperación que envía un router multicast.
2 – Especifica un informe que envía un host

Checksum. Una suma de comprobación de 16 bits calculada como para ICMP.

Dirección de clase D. Esta es cero para una petición y es una dirección de grupo multicast válida para un informe.

IGP (Interior Gateway Protocol)

Se utilizan dentro de un sistema autónomo (SA). Los IGP son responsables de construir y mantener la información de ruteo dentro del dominio administrativo (SS) y por este motivo se los considera "internos". Estos protocolos forman la estructura del SA, y considerando su aplicación en redes extensas, las características primordiales con las que deben contar son robustez, rápida convergencia y optimización del tráfico generado por los mismos. Es de vital importancia que la red interna del proveedor ISP sea eficiente, robusta y segura; y es por esto que los protocolos IGP se diseñan para cumplir con estos parámetros. En una implementación correcta, el IGP no debería tener que mantener muchos prefijos (esto afecta su performance), y no debería contar con prefijos externos al SA, salvo algunas excepciones.

Los protocolos IGP pueden ser divididos en dos categorías:

Vector – distancia

Tienen en cuenta la cantidad de saltos al tomar la decisión del camino que debe atravesar un datagrama para llegar a destino, sin tener en cuenta las características del salto.

Estado – Enlace

Tienen en cuenta parámetros de los links, como ancho de banda de los links que se atraviesan, para tomar la decisión.

Los protocolos IGP que han sido estandarizados y se utilizan hoy en día son: RIP (vector – distancia), OSPF (estado – enlace) e IS-IS (estado – enlace); siendo los dos últimos los más populares y eficientes.

EGP (External Gateway Protocol)

Un protocolo de tipo EGP se utiliza para intercambiar información de ruteo entre diferentes SA. El único protocolo utilizado hoy en día como EGP es BGP (Border Gateway Protocol). Todos los esfuerzos de desarrollo de diferentes ingenieros, grupos y empresas se centran en mejorar y ampliar las prestaciones de este protocolo, y no en desarrollar nuevos estándares. Esto se debe a que BGP es el protocolo de Internet utilizado por todas las organizaciones que deseen interconectarse. Por ser utilizado entre diferentes dominios administrativos, y por transportar mucha información (todos los prefijos de Internet) debe ser un protocolo granular a nivel de políticas de interconexión, aplicando mecanismos para asegurar el transporte de información. Estas son las premisas con las que se diseñó BGP.

BGP (Border Gateway Protocol)

Utiliza los números de SA como vector, para evitar “loops” en el enrutamiento. Este protocolo forma un vector que contiene todos los números de SA que ha atravesado dicho anuncio, y por ende indica el camino que toma el paquete en la red (Saltos de SA). BGP intercambia rutas entre diferentes SA, y esto hace que BGP utilice a los SA como sus "saltos", indicando los trayectos a nivel de sistemas autónomos y no routers. BGP utiliza la información que recibe para armar una base de datos que contiene toda la información de alcance de la red, que a su vez intercambia con otros vecinos BGP.

BGP se ha extendido para poder transportar otros tipos de familias de direccionamiento. De esta forma, puede transportar rutas IPv6, VPN-IPv4, VPN-IPv6 y etiquetas MPLS, entre otras. Cuando se configura al protocolo BGP para transportar otra familia de direccionamiento, al mismo se lo llama "Multi-Protocol BGP (MP-BGP)".

RIP (Routing Information Protocol)

Es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

Cuando un usuario se conecta al servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.

Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

Características

- Es un protocolo de enrutamiento por vector – distancia
- Utiliza el conteo de saltos como su única métrica para la selección de rutas
- Las rutas publicadas con conteo de saltos mayores que 15 son inalcanzables
- Se transmiten mensajes cada 30 segundos

Versiones

RIPv1. No soporta subredes ni CIDR (Encaminamiento Inter-Dominios sin Clases, estándar para la interpretación de direcciones IP). Tampoco incluye ningún mecanismo de autenticación de los mensajes. Actualmente en desuso. Se rige por la RFC 1058.

RIP v2. Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Se rige por la RFC 1723-2453.

RIPng. RIP para IPv6. Se rige por la RFC 2080.

Tabla 5.2.5. Ventajas y desventajas del protocolo RIP.

Ventajas	Desventajas
• Es más fácil de configurar a comparación de otros protocolos • Es un protocolo abierto, es decir, admite versiones derivadas, aunque no necesariamente compatibles • Es soportado por la mayoría de los fabricantes	• Para determinar la mejor métrica, únicamente toma en el número de saltos, descartando otros criterios • No está diseñado para resolver cualquier posible problema de encaminamiento

DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host)

Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento

quién ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.

Provee los parámetros de configuración a las computadoras conectadas a la red informática que lo requieran (Mascara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

Asignación dinámica

El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

5.3 Algoritmos y protocolos de enrutamiento

Los algoritmos y protocolos de enrutamiento son una parte de software de la capa de red encargada de decidir la línea de salida por la que será transmitido un bloque de datos de entrada. Un ejemplo de enrutamiento de un mensaje entre personas se representa en la figura 5.3.1.

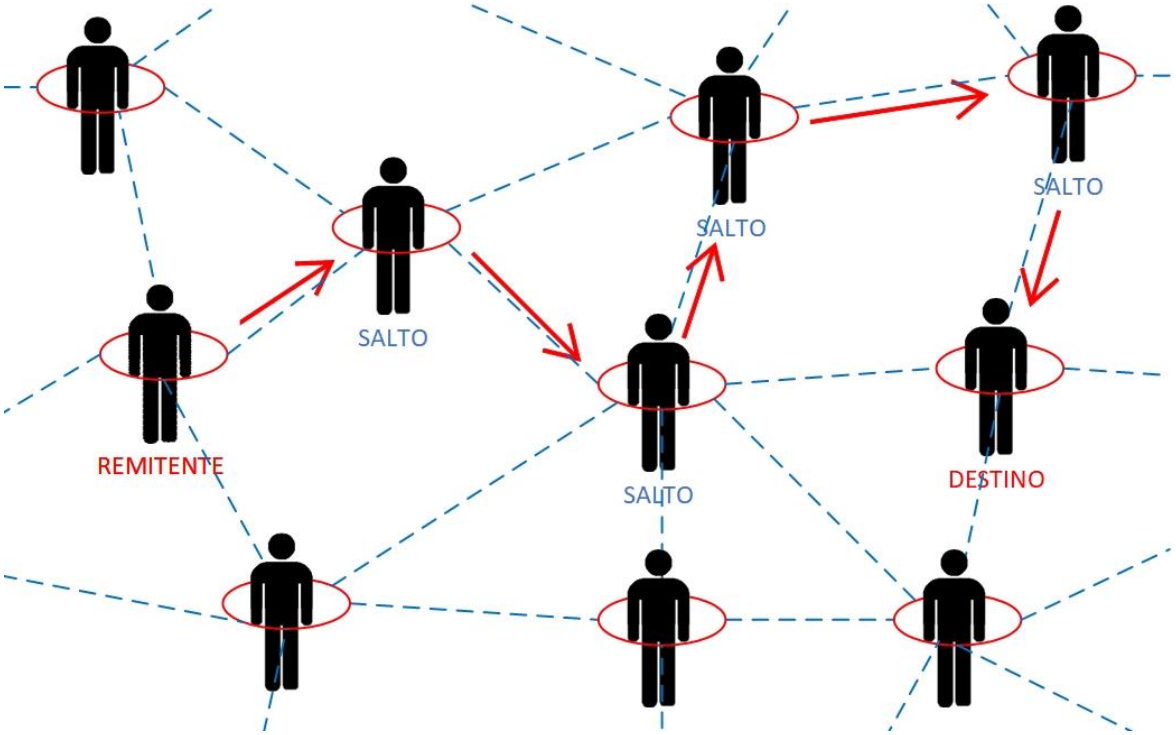


Figura 5.3.1. Ejemplo de enrutamiento de un mensaje.

Estáticos

La decisión de qué ruta se seguirá es calculada anticipadamente y se carga en los routers al inicializar la red.

OSPF (Open Shortest Path First - Enrutamiento por la trayectoria más corta)

Desarrollado por Dijkstra en 1959. La idea es armar un grafo de la subred, donde cada nodo representa un router y cada arco una línea de comunicación (o enlace). El algoritmo encuentra la trayectoria más corta para escoger una ruta entre 2 routers.

1. Cada nodo se etiqueta con su distancia al nodo de origen a través de la mejor trayectoria conocida.
2. Inicialmente no se conocen trayectorias.
3. A medida que avanza algoritmo, y se encuentran trayectorias, pueden cambiar etiquetas de tentativa a permanente.

Métricas para longitud de trayectoria:

- Cantidad de escalas
- Distancia geográfica en km
- Retardo medio de encolamiento
- Tráfico medio

Las etiquetas en los arcos del grafo se calculan previamente (ver figura 5.3.2).

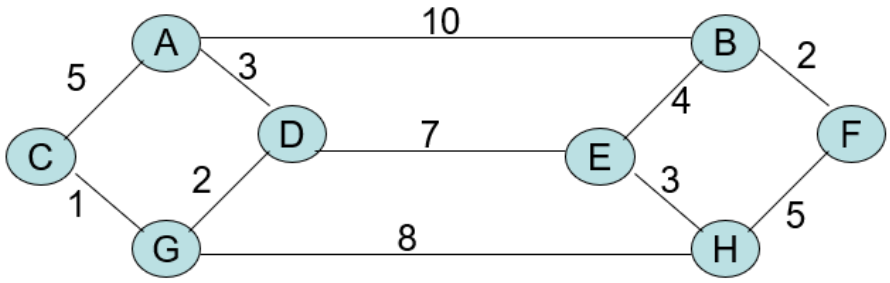


Figura 5.3.2. Ejemplo de grafo.

Las ventajas principales de OSPF son las siguientes:

- En comparación con los protocolos de direccionamiento vector de distancia como el protocolo de información de direccionamiento (RIP), OSPF es más adecuado para servir entre redes heterogéneas de gran tamaño. OSPF puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.
- Con OSPF, se puede dividir un sistema autónomo (AS) en áreas y mantenerlas separadas para disminuir el tráfico de direccionamiento de OSPF y el tamaño de la base de datos de estado de enlace de cada área.
- OSPF proporciona un direccionamiento multivía de coste equivalente. Se pueden añadir rutas duplicadas a la pila TCP utilizando saltos siguientes distintos.

Inundación

Características

- Si un nodo recibe un paquete, lo envía a todos sus vecinos (menos a aquel que se lo ha enviado)
- Simple
- Eventualmente múltiples copias llegarán al destino
- No requiere información de la red para funcionar
- Necesitamos identificar cada paquete para distinguir si un paquete lo hemos recibido ya o no

Propiedades

- Todos los posibles caminos se prueban (ver figura 5.3.3)
- Al menos un paquete viaja por el camino más rápido
- Todos los nodos son visitados
- Desventaja: mucho tráfico generado

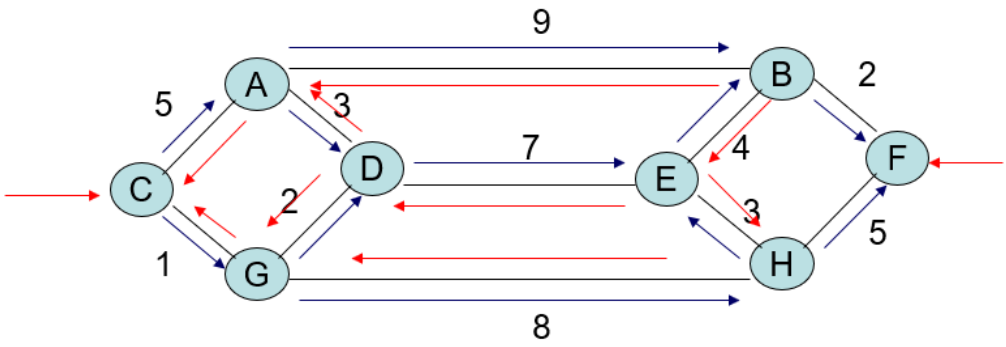


Figura 5.3.3. Inundación.

Inundación selectiva

Es una variante donde enrutadores envían paquetes no por todas, sino por las líneas que van aproximadamente en la dirección correcta. Su uso es en aplicaciones militares, en caso de falla de muchos routers, o para actualizar todas las bases de datos distribuidas (ver figura 5.3.4).

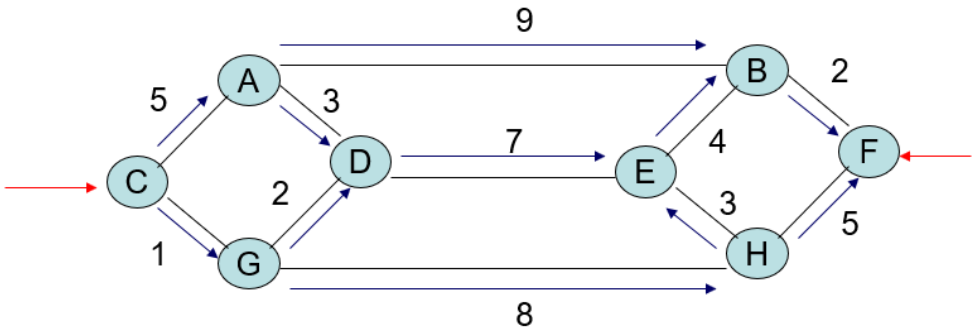


Figura 5.3.4. Inundación selectiva.

Dinámicos

La decisión de qué ruta se usará varía dependiendo de diferentes factores: tráfico, distancia, número de escalas, tiempo estimado de tránsito, entre otros.

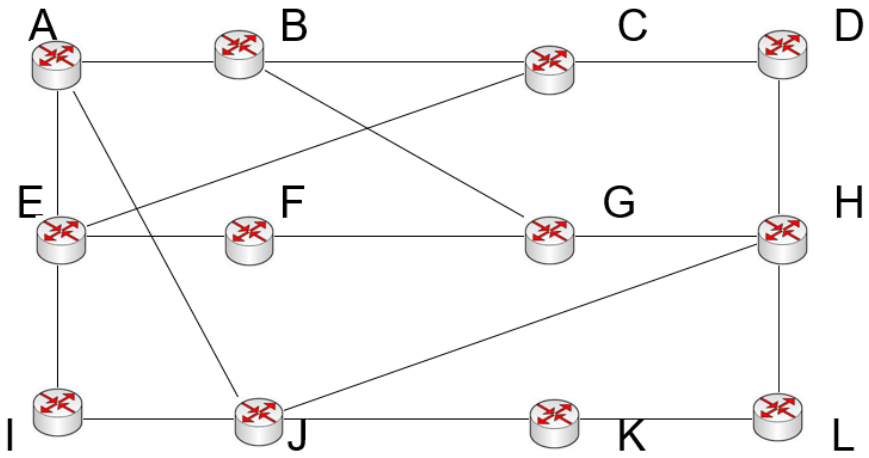
Enrutamiento por vector de distancia

Basado en tablas que se actualizan cada cierto intervalo de tiempo intercambiando información con sus vecinos. Su base es el algoritmo Ford-Fulkerson en 1962, el algoritmo original de ARPANET y utilizado hasta 1979.

- Conocimiento de toda la red
- Distribución de información sólo con vecinos
- El intercambio de tablas es a intervalos regulares

Utilizado en Internet bajo el nombre de RIP que después fue reemplazado por el algoritmo de enrutamiento por estado de enlace.

Ejemplo:



Esta es red de 12 nodos, nos enfocaremos al nodo J el cual tiene 4 vecinos, A, I, H y K. Periódicamente recibirá un vector de distancia de cada uno de sus vecinos. Cada vector tendrá 12 posiciones, uno por cada nodo destino.

	A	I	H	K	J
A	0	24	20	21	
B	12	36	31	28	
C	25	18	19	36	
D	40	27	8	24	
E	14	7	30	22	
F	23	20	19	40	¿?
G	18	31	6	31	
H	17	20	0	19	
I	21	0	14	22	
J	9	11	7	10	
K	24	22	22	0	
L	29	33	9	9	
	JA	**JI**	**JH**	**JK**	
	8	**10**	**12**	**6**	

El nodo J conoce el coste de los enlaces con sus vecinos, y con base en esta información más los vectores de distancia debe de calcular y actualizar la tabla de encaminamiento.

Se conocen ya la distancia a 4 nodos:

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28		
C	25	18	19	36		
D	40	27	8	24		
E	14	7	30	22		
F	23	20	19	40		
G	18	31	6	31		
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10		
K	24	22	22	0	6	K
L	29	33	9	9		
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

Para el nodo B:

JA + AB = 8 + 12 = 20 JI + IB = 10 + 36 = 46 JH + HB = 12 + 31 = 43 JK + KB = 6 + 28 = 34

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28	¿?	¿?
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

El valor más chico es de 20, el cual implica el nodo A. Por lo tanto, el vector distancia del nodo J al nodo B será de 20, teniendo como nodo de salida al nodo A.

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36		
D	40	27	8	24		
E	14	7	30	22		
F	23	20	19	40		
G	18	31	6	31		
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10		
K	24	22	22	0	6	K
L	29	33	9	9		
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

Para el nodo C:

JA + AC = 8 + 25 = 33 JI + IC = 10 + 18 = 28 JH + HC = 12 + 19 = 31 JK + KC = 6 + 36 = 42

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	¿?	¿?
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

El valor más chico es de 28, el cual implica el nodo I. Por lo tanto, el vector distancia del nodo J al nodo I será de 28, teniendo como nodo de salida al nodo I.

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24		
E	14	7	30	22		
F	23	20	19	40		
G	18	31	6	31		
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10		
K	24	22	22	0	6	K
L	29	33	9	9		
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

Realizamos los mismos pasos para cada nodo hasta obtener la tabla final.

	A	I	H	K	J	
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	J
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA	**JI**	**JH**	**JK**		
	8	**10**	**12**	**6**		

Tabla 5.3.1. Ventajas y desventajas del enrutamiento por vector de distancia.

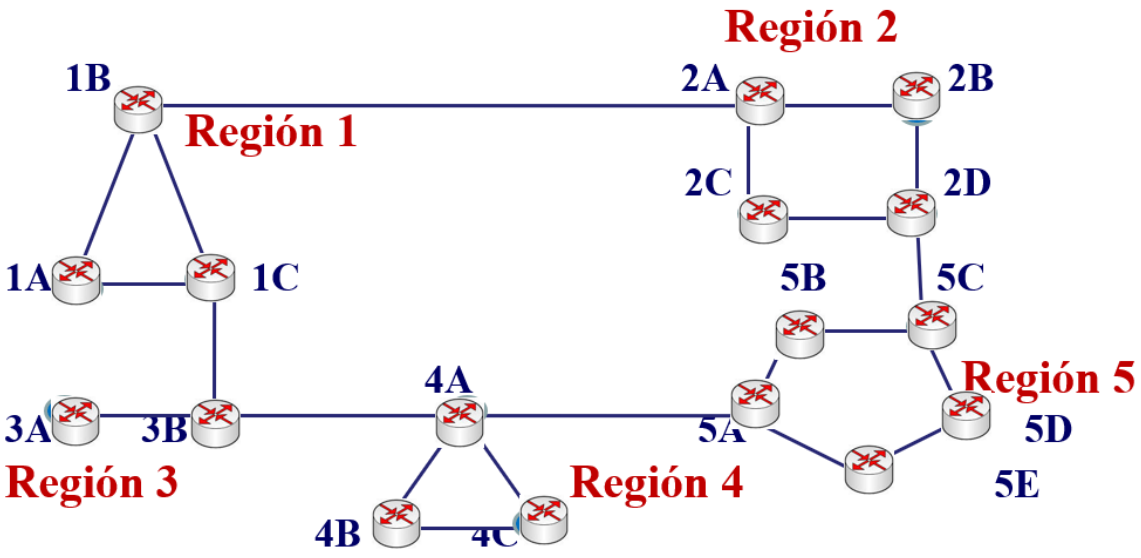
Ventajas	Desventajas
• Muy sencillo • Muy robusto (debido al envío periódico de la información) • Consumo de memoria bajo: cada nodo sólo ha de almacenar distancias con el resto de los nodos	• Convergencia lenta • Pueden aparecer bucles (ciclos infinitos) • Adaptabilidad a los cambios, ya que sólo sabe a quién tiene que enviar un paquete (no se cuenta con la topología de la red) • Consumo alto de capacidad: se transmiten vectores cuyo tamaño es del orden del número de nodos de la red pues cada nodo comunica a su vecino todas las distancias que conoce.

Enrutamiento Jerárquico

El enrutamiento jerárquico divide por regiones, todos los routers se conocen dentro de su región, pero no la estructura interna de otras regiones. Conforme crecen las redes, crecen sus tablas de ruteo.

- Consumen más memoria para su almacenamiento
- Utilizan más tiempo de CPU para examinarlas y actualizarlas
- Requieren más ancho de banda para enviar sus informes de estado

Ejemplo:



Desde el Router 1B se desea llegar a todos los demás, por lo que para ello se usa la siguiente tabla:

Destino	Cantidad de saltos	Router de salida
1A	1	1A
1B	-	-
1C	1	1C
2A	1	2A
2B	2	2A
2C	2	2A
2D	3	2A
3A	3	1C
3B	2	1C
4A	3	1C
4B	4	1C
4C	4	1C
5A	4	1C
5B	5	1C
5C	4	2A
5D	5	2A
5E	5	1C

O bien, esta taba puede reducirse a describir únicamente el camino a cada región:

Destino	Cantidad de saltos	Router de salida
1A	1	1A
1B	-	-
1C	1	1C
Región 2	1	1A
Región 3	2	1C
Región 4	3	1C
Región 5	4	1C

Enrutamiento por estado de enlace

Cada router:

- Construye un LSP (Paquete de Estado de Enlace)
- Tiene información solamente de sus vecinos
- Comparte información con todos los routers por medio del algoritmo de inundación selectiva
- Comparte su información sólo cuando hay algún cambio y se dice que “va a publicar”

Cada router calcula las rutas óptimas para alcanzar todos los destinos de la red con base en los LSP que tiene de sus vecinos (ver tabla 5.3.3).

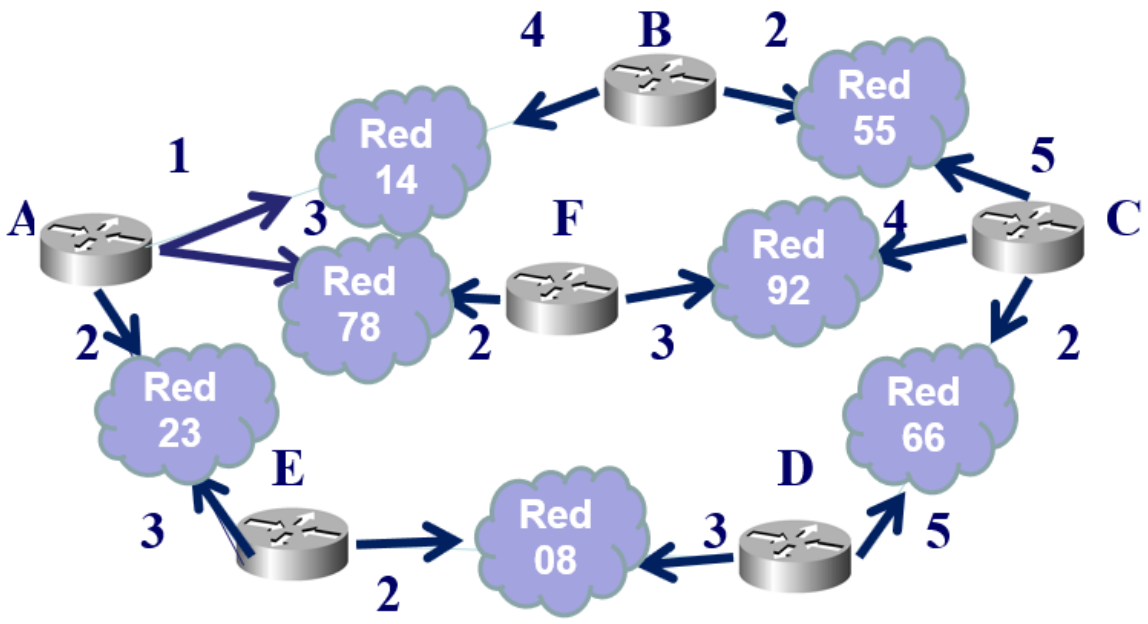
Tabla 5.3.3. LSP (Paquete de Estado de Enlace).

Anunciante	Red	Coste	Vecino

- **Anunciante.** Id del router que hace la publicación.
- **Red.** Id de la red destino a la que puede comunicarse.
- **Coste.** Atributo que se haya considerado.
- **Vecino.** Id del router vecino.

Con la información que "todos" comparten, "todos" elaboran su Base de Datos de los Estados de Enlace, que es exactamente igual para todos.

Ejemplo:



Anunciante	Red	Coste	Vecino
A	14	1	B
	78	3	F
	23	2	E
B	14	4	A
	55	2	C
C	55	5	B
	92	4	F
	66	2	D
D	66	5	C
	08	3	E
E	08	2	D
	23	3	A
F	78	2	A
	92	3	C

5.4 Servicios orientados a conexión y no orientados a conexión

Servicios orientados a conexión

En el esquema orientado a la conexión, se establecen circuitos virtuales, es decir, sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo. En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los routers que haya por el camino elegido reservarán recursos para ese circuito virtual específico.

Como cada sistema es capaz de establecer una conexión, se pueden presentar inconvenientes cuando se establecen conexiones al mismo tiempo en los dos extremos que se desean comunicar. Cada proceso debe indicar cuando ha terminado de usar un circuito virtual, de modo que la dirección pueda purgarse de la tabla de los enrutadores

Servicios no orientados a conexión

Es un servicio que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas. Cuando una entidad tiene información para transmitir, sencillamente la envía, (tramas, paquetes, bloques, etc.).

El proveedor trata cada objeto de información de forma independiente y autónoma, incluso aunque se trate de un conjunto de objetos pertenecientes al mismo mensaje. El usuario confía simplemente en que cada objeto ha de llegar a su destino.

En el esquema no orientado a conexión, los paquetes enviados se conocen como datagramas, cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

5.5 Control de la congestión

Las redes basadas en routers consiste en enlazar operacionalmente a diferentes velocidades de transmisión. Esto puede conducir a problemas de congestionamiento de tráfico. Los problemas de congestionamiento pueden ser más comúnmente cuando las redes operan a diferentes tasas de datos y con esto provocando exceso de tráfico en uno o más de estos enlaces.

Un método más aceptado para manejar las congestiones es usar una técnica llamada “Source Quench”. En esta técnica, el router monitorea la utilización del ancho de banda de las redes adjuntas.

Cuando el promedio de los datos que se están transmitiendo supera un umbral de alcance preestablecido, el router enviará un paquete de congestión para que los dispositivos que envían reduzcan o paren la salida. Cuando la congestión ha sido liberada, el dispositivo origen “amortiguado” restablece su transmisión de manera normal.

5.6 Seguridad a nivel de capa de red

IPsec (Internet Protocol security)

Es un protocolo que está sobre la capa del protocolo de Internet (IP). Este, permite a dos o más equipos comunicarse de forma segura (de ahí viene el nombre). La “pila de red” IPsec incluye soporte para las dos familias de protocolos, IPv4 e IPv6 (ver figura 5.6.1).

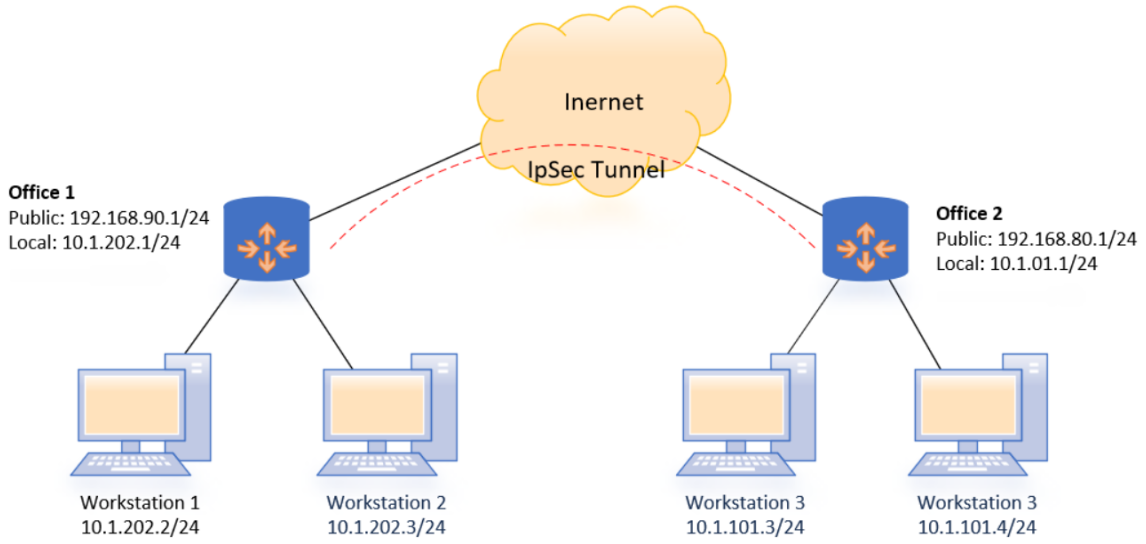


Figura 5.6.1. Ejemplo de Ipsec.

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. También incluye protocolos para el establecimiento de claves de cifrado.

IPsec emplea dos protocolos diferentes - AH y ESP - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores.

IPsec autentica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores.

El objetivo principal de IPsec es proporcionar protección a los paquetes IP. IPsec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPsec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec.

Características

- **ESP (Encapsulating Security Payload – Protocolo Carga de Seguridad de Encapsulación).** ESP proporciona privacidad a los datos mediante el cifrado de los paquetes IP.

- **Claves basadas en criptografía.** Las claves cifradas, que se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito. Se utiliza material de claves diferente para cada segmento del esquema de protección global y se puede generar nuevo material de claves con la frecuencia especificada en la directiva de IPsec.
- **Administración automática de claves.** Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques. IPsec usa el protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar dinámicamente claves cifradas entre los equipos que se comunican.
- **Seguridad a nivel de red.** IPsec existe en el nivel de red, proporcionando seguridad automática a todas las aplicaciones.
- **Autenticación mutua.** IPsec permite el intercambio y la comprobación de identidades sin exponer la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicar con la protección de IPsec. Pueden estar en cualquier dominio de confianza de la empresa. La comunicación se cifra, lo que dificulta la identificación e interpretación de la información.
- **Filtrado de paquetes IP.** Este proceso de filtrado habilita, permite o bloquea las comunicaciones según sea necesario mediante la especificación de intervalos de direcciones, protocolos o, incluso, puertos de protocolo específicos.

Tipos de ataque en la capa de red

La seguridad entre redes es implementada en un dispositivo intermediario (router o firewall) en el perímetro de la red. La función del firewall realizada por este dispositivo permite que datos conocidos y confiables accedan a la red.

La activación de las variadas características de seguridad que se encuentran embebidas en los routers resulta importante para impedir el control no autorizado del mismo. La utilización de contraseñas fuertes y la configuración correcta de los protocolos de administración a través de conexiones cifradas son algunas de las medidas que pueden tomarse para proteger estos equipos.

Además, se debe tener en cuenta las vulnerabilidades que puedan existir en los protocolos de encaminamiento, como RIP u OSPF, ya que pueden terminar en la inyección de routers falsos. La comprensión de estos protocolos facilitará la gestión segura de la red.

Adicionalmente existe una serie de otras problemáticas que atañen a esta capa. En particular, la posibilidad de que un atacante pretenda enviar datos desde un equipo con una determinada dirección IP cuando en realidad lo hace desde otro, es lo que se denomina como IP spoofing. Una manera de mermar estos ataques es la inclusión de procesos de autenticación en la capa de la aplicación, acompañados de mecanismos de cifrado de los datos.

Otro de los elementos clave para la seguridad informática dentro de la capa de red es la Lista de Control de Acceso (ACL - Access Control List). Estas listas permiten o deniegan conexiones entre equipos pertenecientes a redes diferentes, según el protocolo, los puertos, o las direcciones IP involucradas en la comunicación.

El control del acceso se compone de recursos de información protegidos que especifican a quién puede otorgarse acceso para tales recursos.

El sistema operativo proporciona una seguridad discrecional y de conocimiento necesario. El propietario de un recurso de información puede otorgar a otros usuarios derechos de lectura o de grabación para dicho recurso. Un usuario al que se le conceden derechos de acceso sobre un recurso puede transferir dichos derechos a otros usuarios. Esta seguridad permite un flujo de información controlada por el usuario en el sistema; el propietario de un recurso de información define los permisos de acceso sobre el objeto.

Los usuarios disponen de acceso basado en el usuario sólo para los objetos que poseen. Normalmente, los usuarios reciben los permisos de grupo o los permisos por omisión sobre un recurso. La tarea principal de la administración del control del acceso es la definición de la calidad de miembro de un grupo de los usuarios, pues ello determina los derechos de acceso de los usuarios a los archivos de los que no son propietarios.

Los objetos del sistema de archivos por lo general están asociados a una Lista de control de accesos (ACL), la cual normalmente consta de una serie de Entradas de control de accesos (ACE). Cada ACE define la identidad y sus derechos de acceso relacionados.

El propietario del recurso de información es el responsable de la gestión de los derechos de acceso. Los recursos están protegidos por bits de permiso, que se incluyen en la modalidad del objeto.

Cuando un usuario inicia la sesión en una cuenta, los ID de usuario y los ID de grupo asignados a esa cuenta se asocian a los procesos de usuario. Estos ID determinan los derechos de acceso del proceso.

La activación de firewalls de capa de red puede menguar estos ataques, ya que estos dispositivos pueden delinear el interior de la red del exterior haciendo corresponder sus puertos internos/externos con el espacio de direcciones asignado. Esto es, un firewall puede detectar un paquete que dice provenir del interior, pero que ha ingresado a través del puerto de conexión al exterior, para descartarlo o generar la correspondiente alerta.

Algunos fabricantes de cortafuegos añaden características como:

- Accesos
- Proporcionar enlace VPN a otra red
- Autenticación
- Filtrado de contenido

Existen tres principales tecnologías de firewall:

- **Filtrado de Paquetes (Packet Filter).** Se basa en permitir o denegar el tráfico de red basado en el encabezado de cada paquete. No guarda los estados de una conexión, es decir, no tiene el concepto de sesión.
- **Filtrado por Estado (Stateful Application Inspection).** Permite abrir "puertas" a cierto tipo de tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina. Mantiene un registro de las conexiones, las sesiones y su contexto.
- **Filtrado por Aplicación (Full Application Inspection).** Es capaz de inspeccionar hasta el nivel de aplicación. No sólo la validez de la conexión sino todo el contenido de la trama. Es considerado como el más seguro. Soporta autenticación a nivel de usuario.

Un ejemplo de reglas que puede tener un firewall son los mostrados en la figura 5.6.2:

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.3	tcp	cualquiera	80
3	Aceptar	192.168.10.0	cualquiera	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Figura 5.6.2. Ejemplo de reglas de firewall.

ARP Spoofing

Para que capa 2 pueda dar servicios a capa 3 existen dos protocolos llamado ARP y RARP, cada dirección MAC (de capa 2) está asociada a una dirección IP. Estas relaciones son almacenadas en una tabla de direcciones MAC contra direcciones IP, tanto en los switches como en los dispositivos que estén conectados en una red.

Ejemplo de tabla de MAC vs IP:

Interface: 10.10.10.100 — 0xb

Internet Address	Physical Address	Type
10.10.10.1	00-1f-b3-d2-c1-c1	dynamic
10.10.10.255	ff-ff-ff-ff-ff-ff	static

Mediante peticiones falsas de ARP es posible falsificar cualquier dirección MAC en una red de cómputo; por lo tanto, cualquier tráfico puede ser re direccionado a un equipo falso y esto permite:

- Robo de sesiones de aplicaciones.
- Sniffing de tráfico de la red interna (incluso en un switch).
- Ataques de denegación de servicio.
- Ataques de “hombre en medio”.

Tema 6

Capa de transporte

Objetivo: El alumno distinguirá los diferentes tipos de protocolos, métodos y estándares utilizados en la capa de transporte del modelo OSI mediante el análisis del funcionamiento de los protocolos TCP y UDP.

El objetivo de la capa de la capa 4 del modelo OSI es brindar un transporte confiable asegurando que los datos lleguen a su destino sin errores y en la secuencia correcta, coordina múltiples aplicaciones para que interactúen en la red simultáneamente de tal forma que los datos enviados por una aplicación sean recibidos por la aplicación correspondiente.

6.1 Servicios de la capa de transporte

- **Seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino**
  Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de transporte mantener los diversos streams (flujos de información) de comunicación entre estas aplicaciones.
- **Protocolos de transporte**
  Los protocolos de la capa de transporte son dos, TCP y UDP.
  - *UDP*: es un servicio sin conexión, no se establece una sesión entre los hosts, no garantiza ni confirma la entrega de las unidades de datos y no las secuencia.
  - *TCP*: es un servicio orientado a la conexión, se establece una sesión entre los hosts. TCP garantiza la entrega de los bloques de datos mediante el uso de confirmaciones y la entrega secuenciada de datos.
- **Provee comunicación lógica entre aplicaciones corriendo en diferentes máquinas**
- **Los protocolos de transporte sólo corren en los sistemas finales**
  - *Lado emisor*: divide el mensaje de la aplicación en segmentos y los pasa a la capa de red.
  - *Lado receptor*: reensambla los segmentos en forma de mensajes y los pasa a la capa de aplicación.
- **La capa de transporte se apoya en y enriquece los servicios de la capa de red**

6.2 Manejo de Paquetes

La capa de transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

Fragmentación de paquetes

Así como cada aplicación crea datos de stream para enviarse a una aplicación remota, estos datos se pueden preparar para enviarse a través de los medios en partes manejables. Los protocolos de la capa de transporte describen los servicios que segmentan estos datos de la capa de aplicación. Esto incluye la encapsulación necesaria en cada sección de datos, y cada una de estas secciones requiere que se agreguen encabezados en la capa de transporte para indicar la comunicación a la cual está asociada.

Secuenciamiento

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

Reensamblaje de paquetes

En el host de recepción, cada sección de datos se puede direccionar a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de aplicación. Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de la capa para reensamblar las partes de los datos en streams para pasarlos a la capa de aplicación.

Las aplicaciones no necesitan conocer los detalles de operación de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, la ruta o camino tomado por los datos, la congestión en un enlace o el tamaño de la red. Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado. Posteriormente la capa de transporte ordena estas secciones antes de entregarlas a la aplicación adecuada.

6.3 Control de flujo

El objetivo es que el emisor no sature al buffer del receptor. La aplicación puede ser lenta para leer el buffer. El servicio de acoplado de velocidades consiste en acoplar la velocidad del emisor con la tasa de consumo de la aplicación (ver figura 6.3.1).

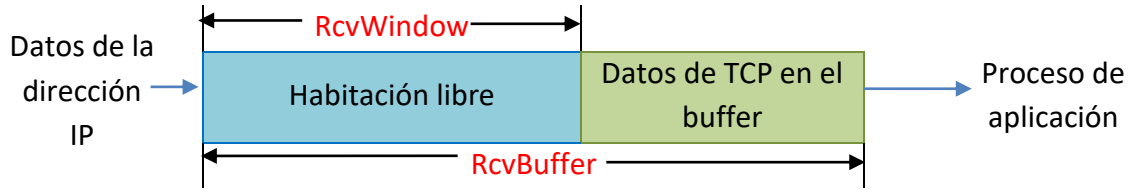


Figura 6.3.1. Representación del control de flujo.

El receptor comunica su espacio disponible incluyendo el valor de RcvWindow en los segmentos. El emisor limita los nuevos datos a RcvWindow, esto garantiza que el buffer del receptor no se sature (ver figura 6.3.1).

Solicitud de respuesta automática (ARQ)

Para el control de errores en la transmisión de datos se utilizan protocolos que garantizan la integridad de los mismos, además de que suelen utilizarse en sistemas que no actúan en tiempo real, ya que el tiempo que se pierde en el reenvío puede ser considerable y suele ser más útil emitir mal en el momento, que hacerlo correctamente un tiempo después.

Esta técnica de control de errores se basa en el reenvío de los paquetes de información que se detecten como erróneos.

Otro método que se emplea es el método de código polinómico, donde el transmisor y el receptor deben acordar un polinomio generador, G(x), por adelantado. Tanto los bits mayor como menor del generador deben ser 1. Para calcular la suma de comprobación para un marco con m bits correspondiente al polinomio M(x), el marco debe ser más largo que el polinomio generador. La idea es anexar una suma de comprobación al final del marco de tal manera que el polinomio representado por el marco más la suma de comprobación sea divisible entre G(x). Cuando el receptor recibe el marco con suma de comprobación, intenta dividirlo entre G(x). Si hay un residuo, ha habido un error de transmisión.

Ejemplo 1:

Datos: 11100110101 G(x)=10011

Polinomio de datos:

1	1	1	0	0	1	1	0	1	0	1
X^{10}	X^9	X^8			X^5	X^4		X^2		X^0

Polinomio del generador:

1	0	0	1	1
X^4			X^1	X^0

Se multiplica el elemento de mayor exponente del generador por el polinomio completo del dato:

$X^4 * (X^{10}+X^9+X^8+ X^5+X^4+X^2+X^0) = X^{14}+X^{13}+X^{12}+X^9+X^8+X^6+X^4$

Se divide el resultado anterior entre el generador de la siguiente forma:

$X^{10}+X^9+X^8+X^7+X^5+X^4+X^3+X^0$

$X^4+X^1+X^0 \mid X^{14}+X^{13}+X^{12}+X^9+X^8+X^6+X^4$

$X^{14}+X^{11}+X^{10}$

$X^{13}+X^{12}+X^{11}+X^{10}+X^9+X^8+X^6+X^4$

$X^{13}+X^{10}+X^9$

$X^{12}+X^{11}+X^8+X^6+X^4$

$X^{12}+X^9+X^8$

$X^{11}+X^9+X^6+X^4$

$X^{11}+X^8+X^7$

$X^9+X^8+X^7+X^6+X^4$

$X^9+X^6+X^5$

$X^8+X^7+X^5+X^4$

$X^8+X^5+X^4$

X^7

$X^7+X^4+X^3$

X^4+X^3

$X^4+X^1+X^0$

$X^3+X^1+X^0$

$X^3+X^1+X^0$ <= CRC será igual al residuo de la división realizada

Por lo tanto:

Datos: 11100110101 CRC: 1011

Bloque a enviar: 111001101011011

Ejemplo 2:

Datos: 1101011011 G(x)=10011

Polinomio de datos:

1	1	0	1	0	1	1	0	1	1
X^9	X^8		X^6		X^4	X^3		X^1	X^0

Polinomio del generador:

1	0	0	1	1
X^4			X^1	X^0

Se multiplica el elemento de mayor exponente del generador por el polinomio completo del dato:

$X^4 * (X^9+X^8+X^6+X^4+X^3+X^1+X^0) = X^{13}+X^{12}+X^{10}+X^8+X^7+X^5+X^4$

Se divide el resultado anterior entre el generador de la siguiente forma:

$$
\begin{array}{rl}
 & X^9+X^8+\quad\quad X^3+\quad X^1 \\
X^4+X^1+X^0 & \overline{\left|\begin{array}{l} X^{13}+X^{12}+\quad X^{10}+\quad X^8+X^7+\quad X^5+X^4 \end{array}\right.} \\
 & \underline{X^{13}+\quad\quad X^{10}+X^9} \\
 & \quad X^{12}+\quad\quad X^9+X^8+X^7+\quad X^5+X^4 \\
 & \quad \underline{X^{12}+\quad\quad X^9+X^8} \\
 & \quad\quad\quad\quad\quad X^7+\quad X^5+X^4 \\
 & \quad\quad\quad\quad\quad \underline{X^7+\quad\quad\quad X^4+X^3} \\
 & \quad\quad\quad\quad\quad\quad\quad X^5+\quad X^3 \\
 & \quad\quad\quad\quad\quad\quad\quad \underline{X^5+\quad\quad\quad X^2+X^1} \\
 & \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad X^3+X^2+X^1
\end{array}
$$

$X^3+X^2+X^1$ <= CRC será igual al residuo de la división realizada
Por lo tanto:

Datos: 1101011011 CRC: 1110
Bloque a enviar: 11010110111110

Parada y espera (Stop-wait)

Este protocolo asegura que la información no se pierda y que las tramas o paquetes se reciban en el orden correcto. El emisor, después de enviar una sola trama, no envía las demás hasta que recibe una señal ACK; el receptor, cuando recibe una trama válida (sin errores), envía al emisor la señal ACK.

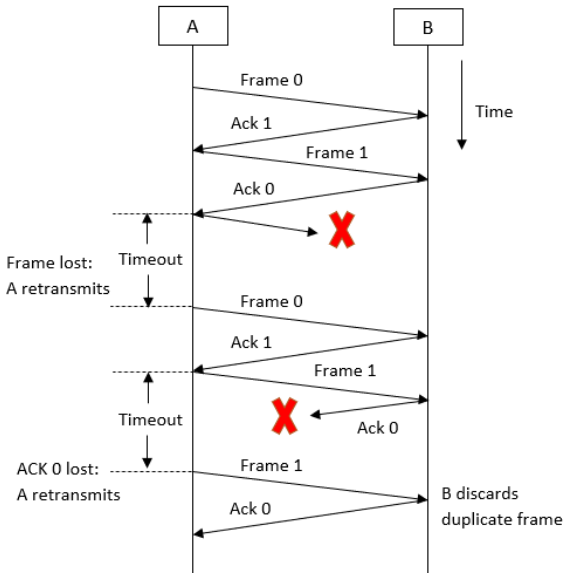


Figura 6.3.2 Ejemplo de stop-wait.

Así, hasta no recibir un ACK, el emisor no envía el siguiente dato (ver figura 6.3.3).

Reglas del protocolo:

1. El emisor envía un paquete y espera a que el receptor confirme positiva o negativamente su recepción.
2. El receptor envía un reconocimiento positivo ACK (ACKnowledgement) cuando el paquete ha llegado sin errores.
3. El receptor envía un reconocimiento negativo o NAK (Negative Acknowledgement) cuando el paquete ha llegado con errores, aunque esto es opcional. Si este es el caso, el emisor vuelve a enviar el paquete.
4. El emisor lanza un temporizador para cada paquete enviado con el objetivo de saber cuánto tiempo debe esperar una confirmación.

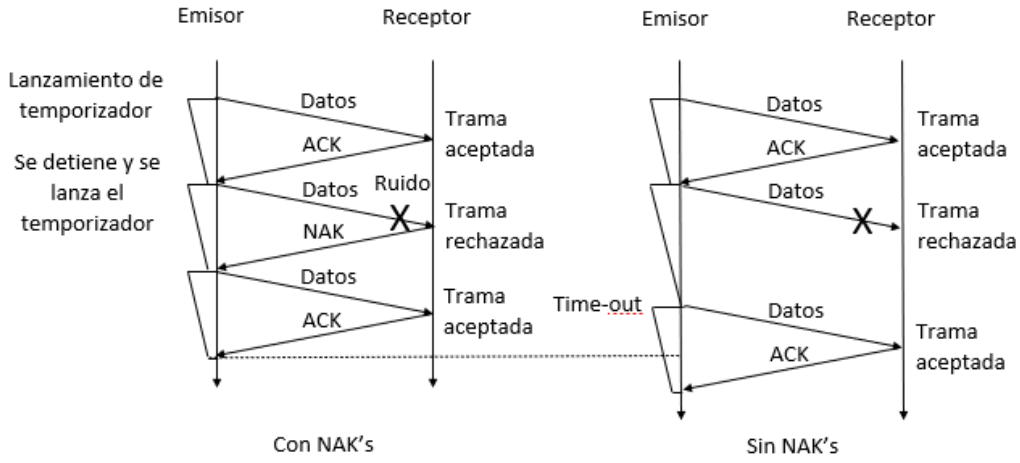


Figura 6.3.3. Representación del procedimiento stop-wait.

Los paquetes duplicados deben confirmarse positivamente para evitar interbloqueos. Un ejemplo de esto se representa en la figura 6.3.4.

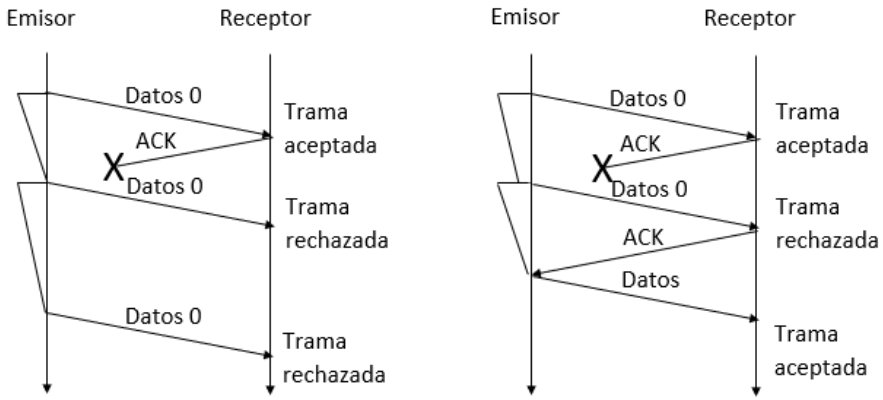


Figura 6.3.4. Representación del caso de paquetes duplicados.

Los paquetes de confirmación deben enumerarse también para evitar la pérdida de datos. Un ejemplo de la pérdida de datos se representa en la figura 6.3.5.

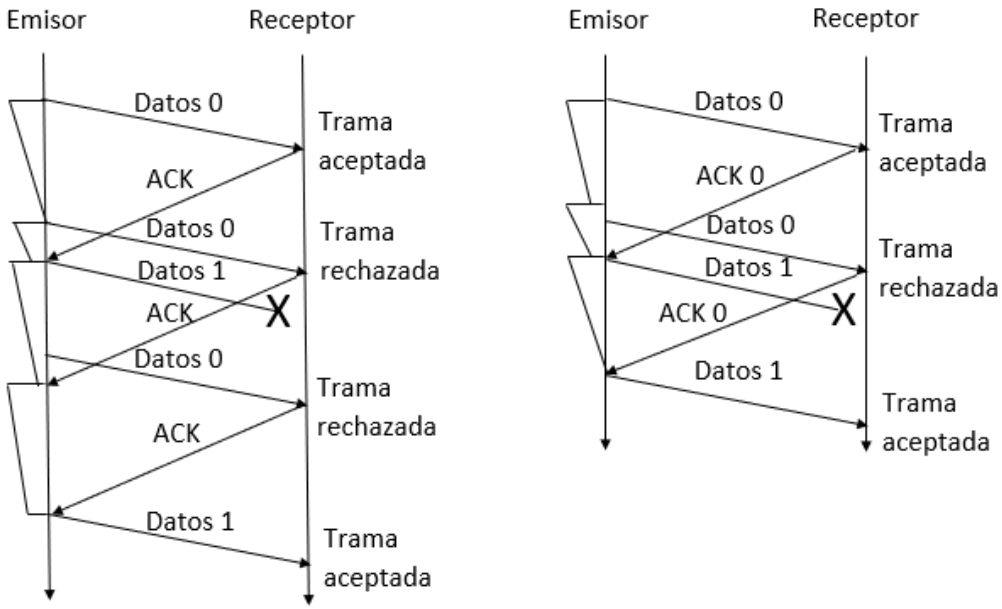


Figura 6.3.5. Representación de la pérdida de datos.

Cálculo del grado o nivel de utilización

Cuando se trabaja con redes es de suma importancia conocer la manera en cómo se están comunicando los datos, para de esta manera realizar un análisis que permita determinar la calidad del enlace de comunicaciones. Para esto es necesario analizar el comportamiento de la red y de esta manera estimar su rendimiento, debido a que una red mal configurada o con un pobre rendimiento puede ocasionar grandes pérdidas de tiempo, bajas en la productividad, entre otras cosas en sistemas de comunicaciones de gran tamaño.

La utilización mide el uso de un recurso particular en un cierto periodo de tiempo. La medida se expresa generalmente bajo la forma de porcentaje en el cual el uso de un recurso se compare con su capacidad máxima operacional. Con las medidas de la utilización, se puede identificar la congestión (o la congestión potencial) en la red.

La utilización es la medida del principio para determinar en qué medida se están utilizando los enlaces de la red. La utilización baja puede indicar los flujos de tráfico en lugares inesperados. Mientras que las líneas se utilizan excesivamente, los efectos pueden llegar a ser significativos. Los saltos repentinos en la utilización de recursos pueden indicar una condición de falla.

Así, Se define a la utilización o eficiencia como el tiempo en el cual los paquetes son transmitidos sin que existan colisiones en el canal cuando hay una cantidad suficientemente grande de nodos transmitiendo, esto debido a que cuando hay muchas estaciones que requieren transmitir, la transmisión disminuye frecuentemente hasta un 50% del valor de diseño de la red.

Como rango deseable de la utilización de la red, si este valor es equivalente o mayor al 75%, se recomienda una reinstalación o rediseño de la red, pues esto indica que los recursos actuales en breve no serán suficientes para el tráfico de red que se genera.

$$U = \frac{L}{L + V2R}$$

Donde:
L -> Longitud de la trama
V -> Velocidad de transmisión
R -> Retardo de propagación

Ejemplo: Considere una LAN instalada bajo el estándar EIA/TIA 568 que opera a una velocidad de 100 Mb/s y tiene una longitud de 10 kilómetros en la cual se transmiten tramas de 5000 bits. ¿Cuál es el nivel de utilización del canal de transmisión?

$$U = \frac{L}{L + V2R} = \frac{5000}{5000 + (100x10^6) * 2 * R}$$

La velocidad de la luz es aproximadamente $C = 2.98x10^8 \approx 3x10^8$. Como el tiempo de propagación de la señal en el cobre es 2/3 la velocidad de la luz:

$$t_{prop} = \frac{2}{3} * 3x10^8 = 2x10^8$$

$$R = \frac{10\ km}{2x10^8} = \frac{10\ 000\ m}{2x10^8\ {}^{m}/_{s}} = 50x10^{-6}\ seg$$

Por lo tanto:

$$U = \frac{L}{L + V2R} = \frac{5000}{5000 + (100x10^6) * 2 * (50x10^{-6})} * 100 => \boldsymbol{U = 33.3\%}$$

Ventana deslizante

La ventana deslizante es un mecanismo dirigido al control de flujo de datos de tipo software, es decir, el control del flujo se lleva a cabo mediante el intercambio específico de caracteres o tramas de control, con lo que el receptor indica al emisor cuál es su estado de disponibilidad para recibir datos. Este dispositivo es necesario para no inundar al receptor con envíos de tramas de datos. El receptor, al recibir datos debe procesarlo, si no lo realiza a la misma velocidad que el transmisor los envía se verá saturado de datos, y parte de ellos se pueden perder. Para evitar tal situación la ventana deslizante controla este ritmo de envíos del emisor al receptor. Con este dispositivo se resuelven dos grandes problemas: el control de flujo de datos y la eficiencia en la transmisión.

El protocolo de ventana deslizante permite al emisor transmitir múltiples segmentos de información antes de comenzar la espera para que el receptor le confirme la recepción de los segmentos, tal confirmación se llama validación, y consiste en el envío de mensajes denominados ACK del receptor al emisor.

Transmisión

Permite al emisor transmitir múltiples paquetes de información en una sola ráfaga, la cual corresponde a tantas unidades de datos como lo permita al tamaño de la ventana. Al término de ésta, el receptor envía la confirmación de recepción y la ventana se desliza para enviar la siguiente ráfaga (ver figura 6.3.6).

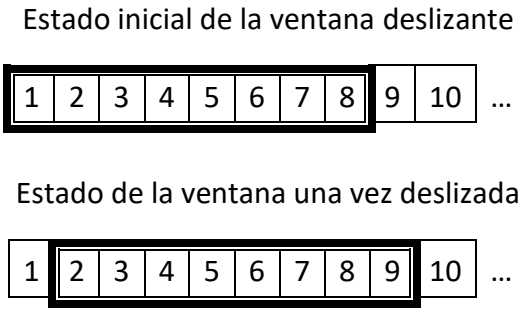


Figura 6.3.6. Representación del funcionamiento de la ventana deslizante.

Validación

La validación se realiza desde el receptor al emisor y contiene el número del siguiente bloque de datos que espera recibir el receptor, o el de la última trama recibida con éxito, ACK n (siendo n el número de la trama indicada). Con esta indicación el emisor es capaz de distinguir el número de los envíos realizados con éxito, los envíos perdidos y los envíos que se esperan recibir.

Cuando llega un paquete al receptor, este envía un ACK al emisor. El ACK puede ser el del último paquete recibido o indicando cuál es el paquete recibido con su número.

Se lleva a cabo mediante los siguientes pasos:

1. *Piggybacking.* Técnica de retardar temporalmente los ACK para que puedan viajar en el siguiente paquete de datos.
2. Los paquetes que han sido enviados pero no han sido validados se denominan Unacknowledge.
3. El número de paquetes que pueden ser Unacknowledge en un momento dado está limitado por el tamaño de la ventana.

Desempeño

La transmisión es continua con base en el número de bloques de datos que contiene la ventana (ver figura 6.3.7).

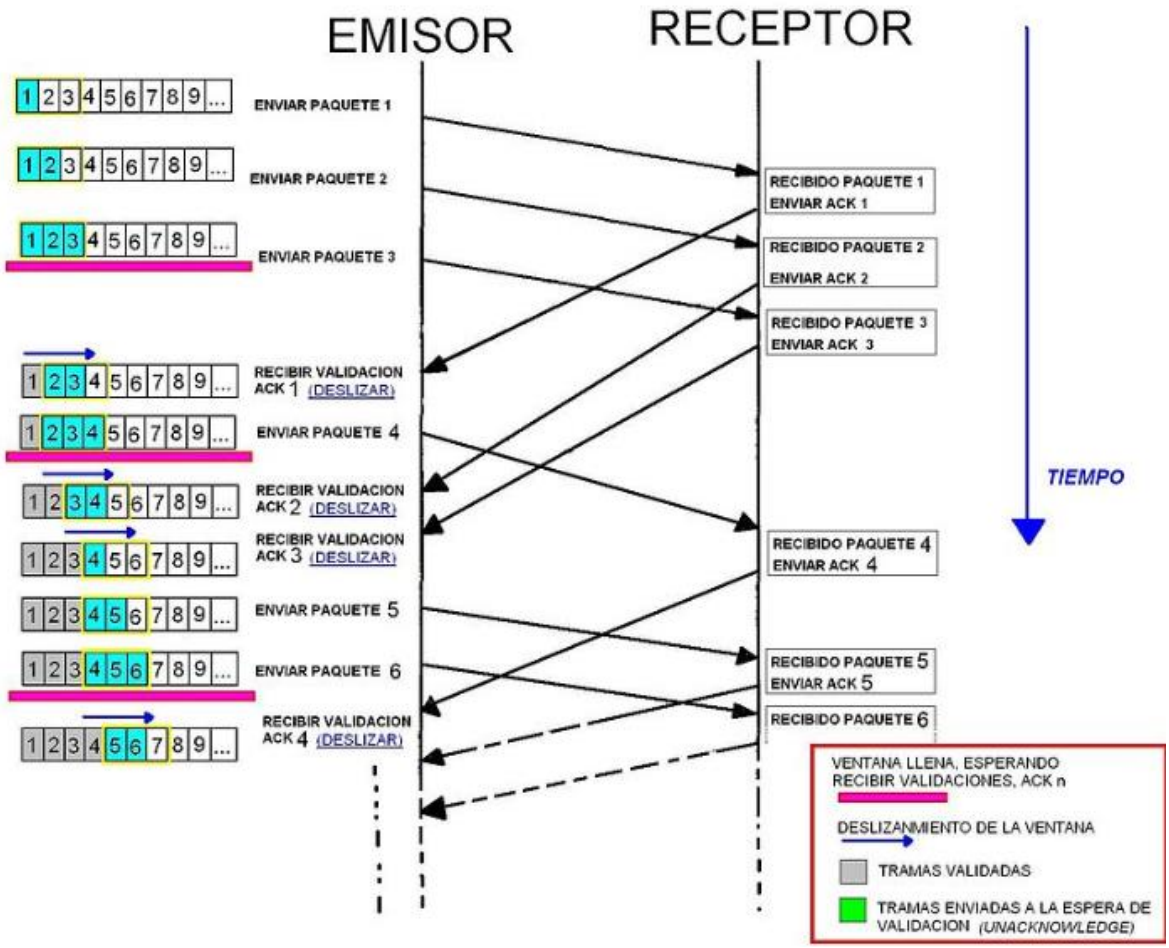


Figura 6.3.7. Desempeño de la ventana deslizante.

Buffer

Guarda en un buffer todos los paquetes enviados y no validados por si necesitase retransmitirlos. El tamaño del buffer debe ser igual o mayor al tamaño de la ventana. Sólo se borran si llega un ACK y así se puede deslizar la ventana una posición más.

Temporizador

El buffer asigna un temporizador a cada uno de los paquetes transmitidos. El temporizador limita el tiempo de esperar para recibir la validación de cada paquete. En caso de finalizar el tiempo sin éxito, se reenviará el paquete (ver figura 6.3.8).

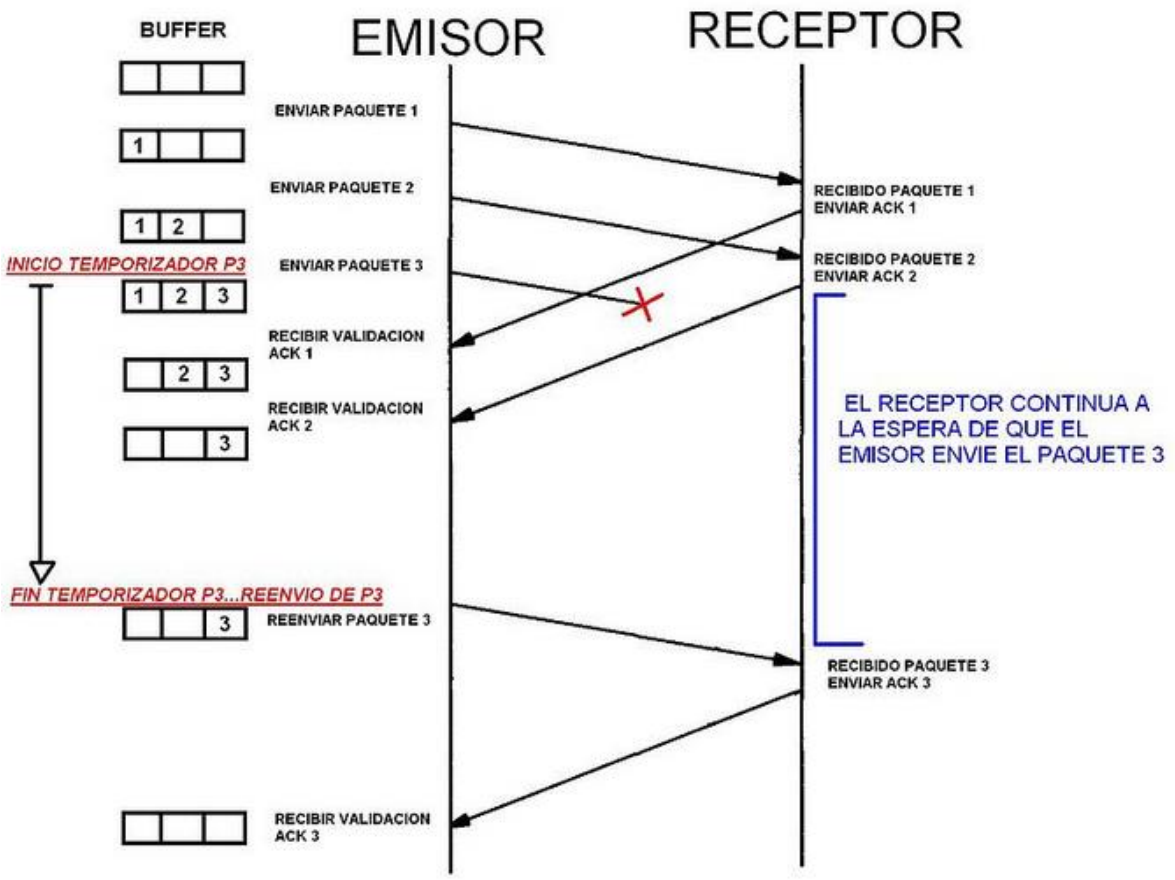


Figura 6.3.8. Representación del temporizador en ventana deslizante.

Ventana de recepción

Permite al receptor recibir paquetes desordenados. El receptor los ordena siguiendo una lista secuencial consecutiva. Almacena los paquetes temporalmente en un buffer hasta que se termine la transmisión y este en posesión de todos.

Recuperación de errores

Cuando el receptor detecta un paquete no válido lo descarta siempre. Para ello realiza una de las siguientes estrategias:

- *Estrategia de retransmisión no selectiva:* El receptor rechaza todos los paquetes recibidos a partir de detectar uno con error y envía una señal (NACK n). Luego el emisor comienza la retransmisión de los paquetes descartados por el receptor. Este método no es demasiado efectivo ya que se pierde mucho tiempo de transmisión.
- *Estrategia de retransmisión selectiva:* El receptor solo descarta el paquete erróneo y acepta los posteriores almacenándolos en el buffer de recepción. También envía una señal NACK n al detectar uno con error. Posteriormente el emisor comienza la retransmisión del paquete fallido y lo conectará con los paquetes almacenados en el buffer. Este método es efectivo y optimiza la retransmisión.

Cálculo del grado o nivel de utilización

$$U = \frac{N}{2a+1} \qquad a = \frac{R}{ttt} \qquad ttt = \frac{L}{V}$$

Donde:
N -> capacidad del buffer
L -> longitud de la trama
V -> velocidad de transmisión
R -> retardo de propagación
ttt -> tiempo total de transmisión de la trama

Ejemplo: Si el nivel de utilización es equivalente a 1 (100%) y se tienen los siguientes datos, ¿cuál es la capacidad del buffer?

V= 400 KBps
L = 5000 bits
R = 250 mseg

$$ttt = \frac{L}{V} = \frac{5000}{8 * (400x10^3)} = 1.5625x10^{-3}$$

$$a = \frac{R}{ttt} = \frac{250x10^{-3}}{1.5625x10^{-3}} = 160$$

$$U = \frac{N}{2a+1} => 1 = \frac{N}{2 * 160 + 1} => N = 2 * 160 + 1 => \mathbf{N = 321}$$

6.4 Protocolos del nivel de transporte

Debido a que las distintas aplicaciones poseen distintos requerimientos, existen varios protocolos de la capa de transporte. Para algunas aplicaciones, los segmentos deben llegar en una secuencia específica de manera que puedan ser procesados en forma exitosa. En algunos casos, todos los datos deben recibirse para ser utilizados por cualquiera de las mismas. En otros casos, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red. En las redes convergentes actuales, las aplicaciones con distintas necesidades de transporte pueden comunicarse en la misma red. Los distintos protocolos de la capa de transporte poseen distintas reglas que permiten que los dispositivos gestionen los diversos requerimientos de datos.

Algunos protocolos proporcionan sólo las funciones básicas para la entrega eficiente de las secciones de datos entre las aplicaciones adecuadas. Estos tipos de protocolos son útiles para aquellas aplicaciones cuyos datos son sensibles a las demoras.

Otros protocolos de la capa de transporte describen procesos que brindan funciones adicionales, como asegurar la entrega confiable entre las aplicaciones. Si bien estas funciones adicionales proveen una comunicación más sólida entre aplicaciones de la capa de transporte, representan la necesidad de utilizar recursos adicionales y generan un mayor número de demandas en la red (ver figura 6.4.1).

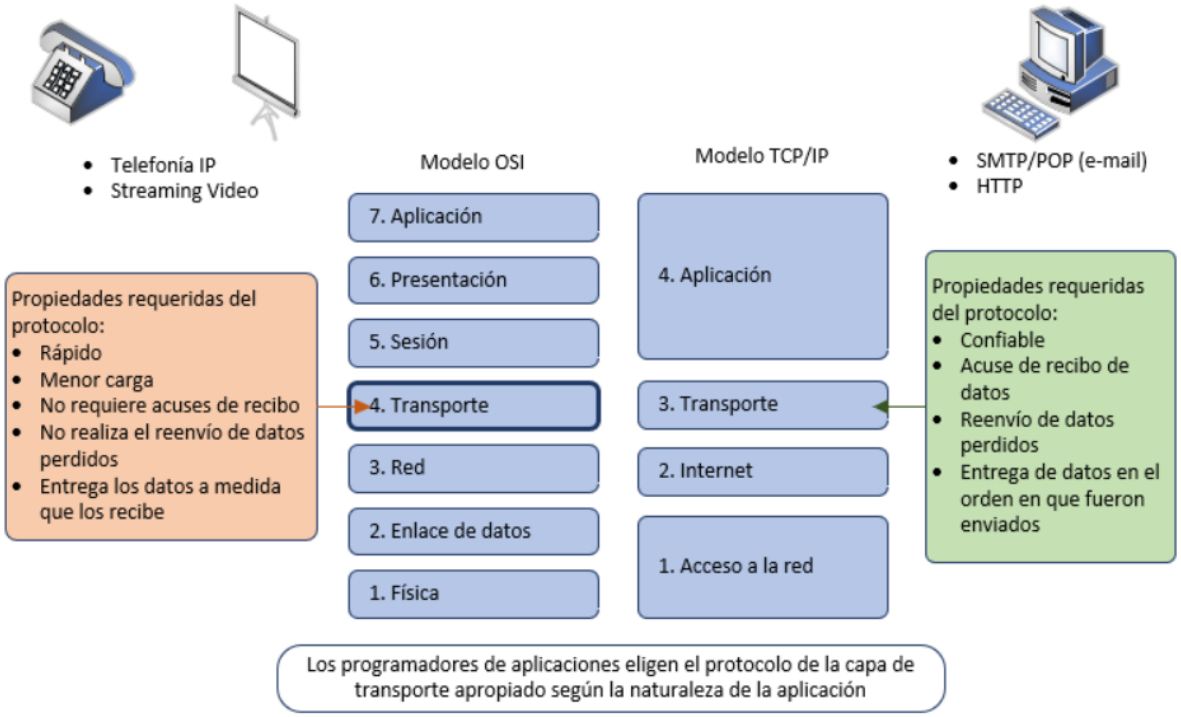


Figura 6.4.1. Características de la capa de transporte.

Los dos protocolos más comunes de la capa de Transporte del conjunto de protocolos TCP/IP son el Protocolo de control de transmisión (TCP) y el Protocolos de datagramas de usuario (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

Protocolo TCP (Transmission Control Protocol – Protocolo de Control de Transmisión)

TCP es un protocolo orientado a la conexión, descrito en la RFC 793. TCP incurre en el uso adicional de recursos para agregar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga.

Algunas de las aplicaciones que utilizan TCP son:

- Exploradores Web
- E-mail
- Transferencia de archivos

TCP utiliza el Protocolo Internet, el protocolo subyacente para transportar datagramas, y soportar la transmisión de bloques de una corriente continua de datagramas entre puertos de proceso. TCP asegura que los datos no se dañen, se pierdan, se dupliquen o se entregan desordenados a un proceso receptor. Esta seguridad de fiabilidad de transporte evita que los programadores de aplicaciones tengan que crear protecciones de comunicaciones en el software. La cabecera TCP está conformada por los campos que se presentan en la figura 6.4.2

<table>
<tr><td>0 – 3</td><td>4 – 6</td><td>7 – 15</td><td>16 – 31</td></tr>
<tr><td colspan="3">Puerto TCP origen</td><td>Puerto TCP destino</td></tr>
<tr><td colspan="4">Número de secuencia</td></tr>
<tr><td colspan="4">Número de acuse de recibo</td></tr>
<tr><td>HELN</td><td>Reservado</td><td>Banderas</td><td>Ventana</td></tr>
<tr><td colspan="3">Checksum</td><td>Puntero de urgencia</td></tr>
<tr><td colspan="4">Opciones</td></tr>
</table>

Figura 6.4.2. Cabecera TCP.

Puerto origen. Identifica el número de puerto de un programa de aplicación de origen.

Puerto destino. Identifica el número de puerto de un programa de aplicación de destino.

Un puerto lógico es una salida de bits, que pueden ser 1 o 0, o sea, es el valor que se usa en el modelo de la capa de transporte para distinguir entre las múltiples aplicaciones que

se pueden conectar al mismo host, o puesto. Entonces un puerto lógico de Internet es una interfaz de software que permitirá el ingreso y salida de data por aplicaciones que usan Internet.

Los puertos se identifican por números desde 1 hasta 65.000 pudiendo llegar a más, siendo conocidos los puertos de 1 a 1024. Entre los más conocidos de TCP se encuentran:

- **Puerto 80**: Este puerto es el que se usa para la navegación web de forma no segura HTTP.
- **Puerto 443**: Este puerto es también para la navegación web, pero en este caso usa el protocolo HTTPS que es seguro.
- **Puerto 21**: El puerto 21 por norma general se usa para las conexiones a servidores FTP en su canal de control.
- **Puerto 990**: Si se utiliza FTPS se hace uso del puerto por defecto 990, aunque se puede cambiar.
- **Puerto 22**: Por normal genera este puerto se usa para conexiones seguras SSH y SFTP, siempre que no se haya cambiado el puerto de escucha del servidor SSH.
- **Puerto 23**: Telnet, sirve para establecer conexión remotamente con otro equipo por la línea de comandos y controlarlo. Es un protocolo no seguro ya que la autenticación y todo el tráfico de datos se envía sin cifrar.

Más adelante se tratará con mayor profundidad este tema.

Número de secuencia. Especifica el número de secuencia del primer byte de datos de este segmento.

Número de acuse de recibo. Identifica la posición del byte más alto recibido.

HLEN. Especifica el tamaño de la cabecera en palabras de 32 bits.

Reservado. Reservado para uso futuro.

Banderas:

- **NS.** ECN-nonce concealment protection. Para proteger frente a paquetes accidentales o maliciosos que se aprovechan del control de congestión para ganar ancho de banda de la red.
- **CWR.** Congestion Window Reduced. La bandera se activa por el host emisor para indicar que ha recibido un segmento TCP con la bandera ECE activado y ha respondido con el mecanismo de control de congestión.
- **ECE.** Para dar indicaciones sobre congestión.
- **URG.** El campo de puntero urgente es válido.
- **ACK.** El campo de reconocimiento es válido.
- **PSH.** El segmento solicita un PUSH.

- **RTS.** Restablece la conexión.
- **SYN.** Sincroniza los números de secuencia.
- **FIN.** El remitente ha alcanzado el final de la corriente de bytes.

Ventana. Especifica la cantidad de datos que el destino está dispuesto a aceptar.

Checksum. Verifica la integridad de la cabecera y los datos de segmento.

Puntero de urgencia. Indica datos que se deben entregar lo más rápidamente posible. Este puntero especifica la posición donde finalizan los datos urgentes.

Opciones. Para poder añadir características no cubiertas por la cabecera fija.

Protocolo UDP (User Datagram Protocol – Protocolo de Datagramas de Usuario)

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como "mejor intento" (ver figura 6.4.3).

Entre las aplicaciones que utilizan UDP se incluyen:

- Sistema de nombres de dominios (DNS)
- Streaming de vídeo
- Voz sobre IP (VoIP)

Dado que los remitentes no saben qué procesos están activos en un momento determinado, UDP utiliza los puertos de protocolo de destino (o puntos de destino abstractos en una máquina), identificados por enteros positivos, para enviar mensaje a uno de los múltiples destinos de un sistema principal. Los puertos de protocolo reciben y conservan los mensajes en las colas hasta que las aplicaciones de la red de recepción pueden recuperarlos.

0 — 15	16 — 31
Puerto origen	Puerto destino
Longitud del mensaje	Checksum

Figura 6.4.3. Cabecera UDP.

Puerto origen. Dirección del puerto de protocolo que envía la información.

Puerto destino. Dirección del puerto de protocolo que recibe la información.

Los puertos más usados de UDP son:

- **Puerto 23:** Este puerto es usado en dispositivos Apple para su servicio de Facetime.

- **Puerto 53:** Es utilizado para servicios DNS, este protocolo permite utilizar tanto TCP como UDP para la comunicación con los servidores DNS.
- **Puerto 514:** Es usado por Syslog, el log del sistema operativo.
- **Puerto 1701**: Es usado por el protocolo de VPN L2TP.

Longitud del mensaje. Longitud en octetos del datagrama UDP.

Checksum. Proporciona una comprobación en el datagrama UDP utilizando el mismo algoritmo que IP.

Seguridad en capa de transporte

Se podría decir que la meta de la capa de transporte es ofrecer un servicio, económico y confiable a sus usuarios. Para lograr este tipo de calidad en el servicio la capa se basa en dos tipos de servicios: el orientado a la conexión (establecimiento, transferencia de datos y liberación) y el no orientado (donde se manejan los paquetes).

Mientras que las partes o elementos clave que hacen funcionar esta capa o protocolo, son los siguientes:

- Direccionamiento
- Establecimiento de conexión
- Liberación de una conexión
- Control de flujo y almacenamiento en buffer
- Multiplexación
- Recuperación de caídas

Las preocupaciones de seguridad a este nivel se ciernen sobre:

- **El cifrado de los datos que se transfieren**
  El cifrado es un método para evitar que alguien pueda tener acceso a información que se desea preservar. Este método consiste en alterar un mensaje antes de transmitirlo, generalmente mediante la utilización de una clave, de modo que su contenido no sea legible para los que no posean dicha clave. De esta forma, cualquier persona que tenga acceso al mensaje no podrá entender su contenido a menos que cuente con la clave para descifrarlo.
- **La autenticación de las partes intervinientes**
  Actualmente se emplea una gama de mecanismos de autenticación que se clasifican en cinco grupos:
  - Algo que el usuario conoce
  - Algo que el usuario tiene

- Algo que caracteriza al usuario (algo que es)
- Algo que el usuario sabe hacer
- Algo que determina su posición

Lo más adecuado es emplear dos mecanismos de autenticación que pertenezcan a grupos distintos.

- **La prevención de manipulaciones que atenten contra la integridad de los datos**
  No solo es necesario cifrar, sino hacerlo de manera que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, el cifrado no tendría valor. Esto implica que el sistema de cifrado a emplear no esté comprometido, es decir, que no se conozca forma de romperlo. En otras palabras, utilizar mecanismos de cifrado robustos.
- **Ataques de reinyección**
  Es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

Ataques en TCP

- *SYN Flood.* Este aprovecha algunas de las debilidades del esquema de tres vías para el establecimiento de la conexión. En él, un equipo malicioso puede enviar múltiples peticiones SYN a otro terminal, y luego dejar de responder. El host de destino quedará a la espera de una confirmación, manteniendo la conexión tentativa en espera. Si se satura el número máximo de hilos de conexiones no confirmadas que el host puede soportar, éste quedará inhabilitado para aceptar nuevas comunicaciones, produciendo una denegación del servicio (ver figura 6.4.4).

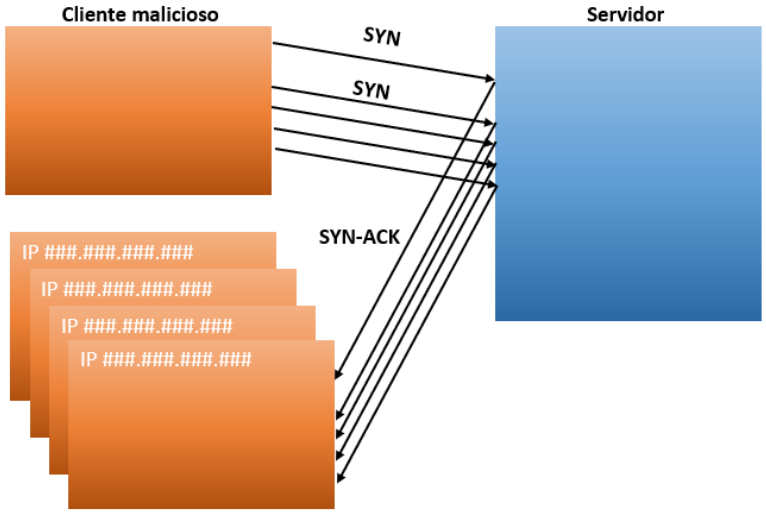


Figura 6.4.4. Ataque SYN Flood.

- *SYN+ACK.* Consiste en enviar directamente falsos paquetes SYN+ACK a un elevado ritmo. El servidor deberá usar gran parte de su capacidad de procesamiento para atender estas peticiones que están fuera de orden normal de 3-way handshake. Esta inundación puede agotar los recursos del sistema (memoria y CPU principalmente) utilizados para procesar esta irregularidad, lo que podría resultar en una degradación del rendimiento (ver figura 6.4.5).

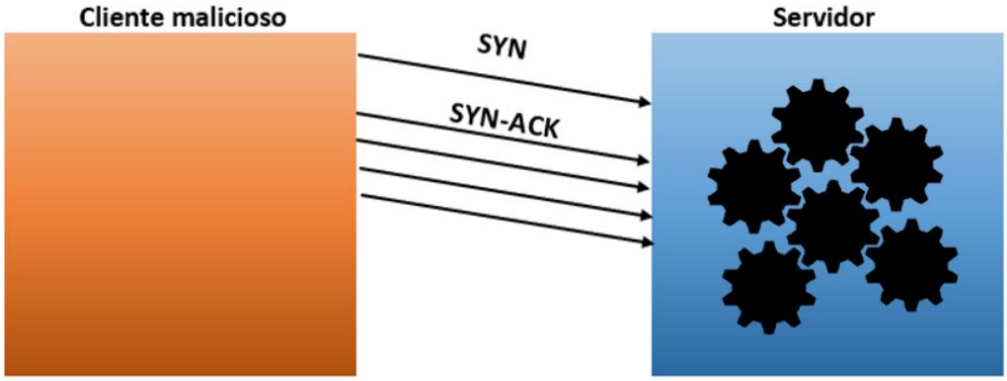


Figura 6.4.5. Ataque SYN+ACK.

- *ACK Flood.* Los paquetes ACK y PUSH-ACK tienen como finalidad confirmar la correcta recepción de los paquetes enviados en ambos sentidos. Durante un ataque ACK Flood el sistema objetivo recibe falsos paquetes ACK a un elevado ritmo. Estos paquetes, que no pertenecen a ninguna de las sesiones de la lista de conexiones, tienen como objetivo agotar los recursos del sistema (memoria y CPU principalmente) al tener que procesarlos, generando una degradación de servicio o incluso una interrupción del mismo (ver figura 6.5.6).

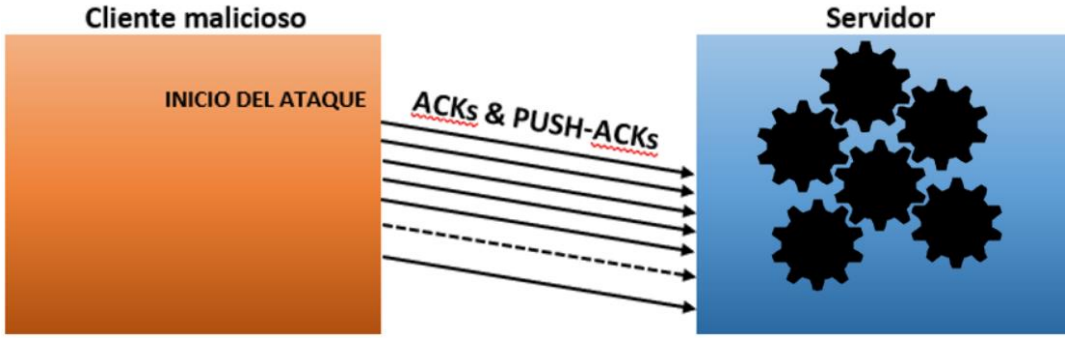


Figura 6.4.6. Ataque ACK Flood.

Una solución a estos problemas consiste en incrementar el número de conexiones no confirmadas en el servidor, o bien, decrecer la cantidad de tiempo en que este último esperará por una confirmación (75 segundos por defecto).

Además de esto, es relativamente sencillo conocer qué aplicaciones están escuchando en qué puertos en un end system o en un conjunto de end systems. A esto se le conoce como escaneo de puertos, y puede ser realizado con programas como Nmap (ver figura 6.4.7).

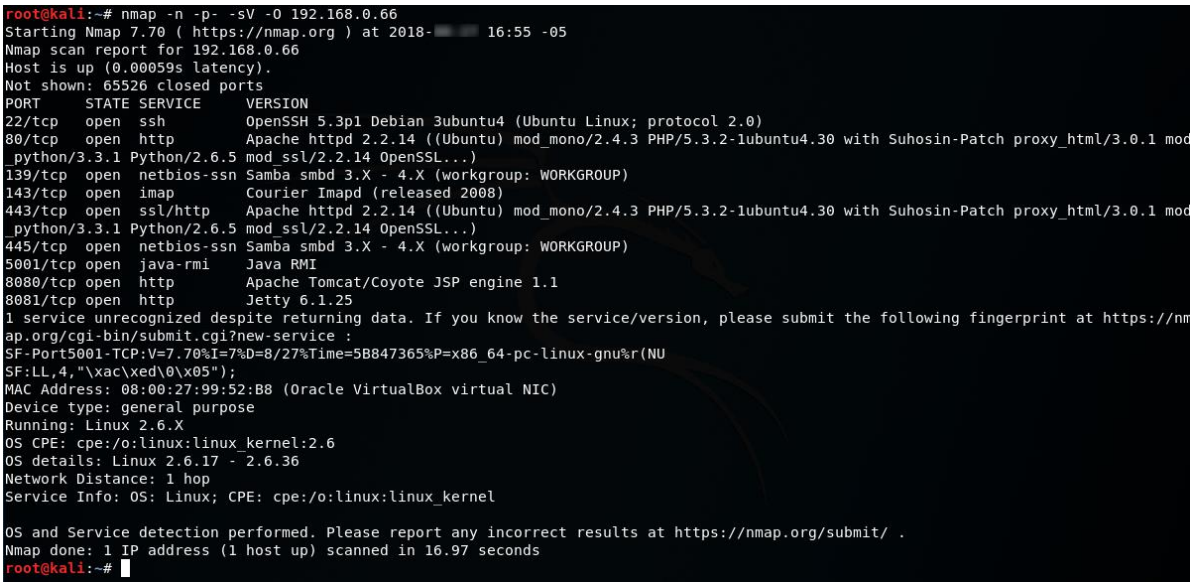


Figura 6.4.7. Ejemplo de mapeo de una dirección IP con Nmap.

Si un intruso detecta algún host corriendo determinada aplicación de la que conocemos alguna vulnerabilidad, esto puede ser el punto de partida de un ataque.

Las conexiones TCP no descritas pueden representar una importante amenaza a la seguridad. Esto se debe a que pueden indicar que algo o alguien está conectado al host local. Además, las conexiones TCP innecesarias pueden consumir recursos valiosos del sistema y por lo tanto disminuir el rendimiento del host.

Incremento en la Seguridad

Se puede añadir seguridad a la red de datos de la siguiente manera:

- Denegar el establecimiento de sesiones TCP.
- Sólo permitir sesiones para ser establecidas por servicios específicos.
- Sólo permitir tráfico como parte de sesiones ya establecidas.

Esta seguridad puede implementarse para todas las sesiones o sólo para las sesiones seleccionadas.

Los números de puerto de origen seleccionados al azar colaboran con la seguridad. Si existe un patrón predecible para la selección del puerto de destino, un intruso puede

simular el acceso a un cliente de manera más sencilla intentando conectarse al número de puerto que tenga mayor posibilidad de estar abierto.

La utilización de protocolos de capa 4 de comunicación segura, como SSL, TLS o SSH, permiten la protección de los datos mediante el cifrado de los mismos, y deben ser considerados al momento de establecer conexiones para la administración remota de dispositivos.

Finalmente, ya que en la capa de transporte la conexión es extremo a extremo, aumentar la protección en los terminales resulta el primer paso para impedir conexiones fraudulentas. La actualización de aplicaciones para salvaguardar la red de las vulnerabilidades y errores que puedan presentar constituye una medida inicial de fortalecimiento del equipo.

6.5 Puertos lógicos

Los puertos lógicos de red suelen estar numerados para de esta forma poder identificar la aplicación que lo usa. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes. Originalmente estos números de puertos fueron usados solo por TCP y UDP, pero ahora también los utilizan SCTP (Stream Control Transmision Protocol – Protocolo de Transmisión de Control de Corriente) y DCCP (Data Congestion Control Protocol – Protocolo de Control de Congestión de Datagramas). Estos protocolos pertenecen al cuarto nivel del modelo OSI, encargados de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red.

Un puerto puede estar en cualquiera de los siguientes estados:

- Abierto
- Cerrado
- Bloqueado (sigiloso)

Existen 65535 puertos lógicos de red. Aunque podemos usar cualquiera de ellos para cualquier protocolo, existe una entidad, la IANA, encargada de su asignación, la cual creó tres categorías:

Puertos bien conocidos

Puertos del 0 al 1023 son puertos reservados para el sistema operativo y usados por "Protocolos Bien Conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de e-mail), Telnet y FTP.

Puertos registrados

Comprendidos entre 1024 y 49151 son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista publicada en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.

Puertos dinámicos

Comprendidos entre los números 49152 y 65535 son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Su uso es poco común, son usados en conexiones peer to peer (P2P). Los puertos más utilizados o comunes están descritos en la tabla 6.5.1.

Tabla 6.5.1. Lista de Números de Puertos más usados o comunes.

Puerto	Nombre	Información
20	FTP Data	Puerto utilizado en modo activo para el proceso de transferencia de datos FTP.
21	FTP	Servicio para compartir archivos FTP.
22	SSH	Secure SHell, utilizado principalmente para conexión por línea de comandos entre otras muchas funciones. Uso casi exclusivo para Linux, en Windows algunas aplicaciones pueden abrirlo.
23	Telnet	TELecommunication NETwork permite controlar un equipo remotamente. Puerto potencialmente peligroso.
25	SMTP	TELecommunication NETwork, usado para envío de correo electrónico. Un puerto muy escaneado para aprovechar vulnerabilidades para el envío de SPAM. Asegúrate de validar usuarios para el envío de correo.
53	DNS	Sistema de nombre de dominio, utilizado para resolver la dirección IP de un dominio.
59	DCC	Direct Client-to-Client, usado de forma predeterminada para el envío de ficheros en algunos programas como IRC.
79	Finger	Informa al cliente datos sobre los usuarios conectados a un determinado servicio del servidor. Puede revelar información no deseada.
80	HTTP	Servidor Web. Utilizado para navegación web. Este servicio por si solo ya supone un riesgo, suele ser escaneado y se las ingenian para encontrar nuevas entradas por él.

110	POP3	Una de las formas de acceder a los correos de tu cuenta de correo electrónico personal.
113	IDENT	Un antiguo sistema de identificación de usuarios. Puerto potencialmente peligroso.
119	NNTP	Servidor de noticias.
135	NetBIOS	Remote Procedure Calls. Usado para compartir tus archivos en red, usar únicamente en red local y no hacia Internet, ya que cualquiera podría acceder al contenido que compartas de tu ordenador. Es habitual encontrarlo abierto en Windows.
139	NetBIOS	Usado para compartir servicios compartidos de impresoras y/o archivos. Potencialmente peligroso si se encuentra abierto ya que se puede acceder a un gran contenido del equipo.
143	IMAP	Otra forma de acceder a los correos electrónicos de tu cuenta de correo electrónico personal. Más moderna que el POP3 y con una funcionalidad similar.
389	LDAP	Lightweight Directory Access Protocol. Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
443	HTTPS	Usado para navegación Web en modo seguro. Se usa junto con un certificado de seguridad. Los comercios electrónicos por ejemplo aseguran sus ventas gracias a este servicio.
445	MSFT DS	Server Message Block. Puede considerarse un puerto peligroso.
563	POP3 SSL	Conexión POP3 pero con cifrado SSL. Una forma más segura de acceder a los correos electrónicos de tu cuenta personal ya que el intercambio de datos se realiza cifrado por medio de Secure Socket Layer (SSL).
993	IMAP4 SSL	Una forma más segura de acceder a los correos de tu cuenta personal por medio cifrado Secure Socket Layer (SSL), cifrando los datos de la comunicación.
995	POP3 SSL	Conexión POP3 pero con cifrado SSL. Una forma más segura de acceder a los correos electrónicos de tu cuenta personal ya que el intercambio de datos se realiza cifrado por medio de Secure Socket Layer (SSL).
1080	Proxy	Servicio de proxy. Garantiza a los clientes del servicio mas seguridad en las conexiones en Internet, ya que tu IP no aparece en las conexiones, apareciendo la IP del servidor proxy.
1723	PPTP	Virtual private network (VPN). Puerto usado para conectar equipos por medio de Red Privada Virtual.
3306	MySQL	Base de datos MySQL. La base de datos usada de forma más frecuente como complemento a las páginas web dinámicas.
5000	UPnP	Universal Plug'n'Play, facilita el reconocimiento de periféricos pero innecesario para Internet.

8080	Proxy Web	Una forma de navegar de forma más privada por Internet, ya que el servidor oculta tu IP al navegar por Internet.

Tema 7

Capa de sesión

Objetivo: El alumno analizará los diferentes tipos de protocolos, métodos y estándares revisando los mismos en la capa se sesión del modelo OSI.

La capa de sesión usa las funciones de la capa de transporte para efectuar las suyas y ofrecérselas a la capa de presentación. Si se definieran entidades de presentación de datos, como procesos que ofrecen información para ser transmitida a un par remoto, la capa de sesión administra la forma en que los datos de cada una de estas entidades transmiten colaborativamente con su par remoto.

La capa de sesión se encarga entonces de decidir si la transmisión de una entidad de presentación a otra va a ser alternada, lo que en programación se suele llamar sincronizada o bloqueante, es decir, que mientras una entidad transmite la otra escucha y no realiza otra actividad hasta que la transmisión termine y sólo en ese momento podría transmitir si fuera necesario. La otra modalidad de sesión es no bloqueante o asíncrona, que obviamente consiste en que las entidades transmiten sin esperar a que el otro lado reciba la información.

A la capa de sesión usualmente se le responsabiliza de iniciar y gestionar la conexión de alto nivel, es decir, entre entidades de presentación dentro de un servicio particular. Allí se decide cuándo y cómo iniciar una conexión, qué requisitos debe cumplir y en qué modalidad se llevará a cabo.

Otra responsabilidad de la capa de sesión es establecer puntos de chequeo, de tal manera que, si la operación es interrumpida, la transacción pueda mantener su integridad, es decir, deshacer todo o recuperar lo que se había hecho.

7.1 Servicios de nivel sesión

La capa de sesión se ocupa del control de la concurrencia. Cuando un servicio está en escucha y varias comunicaciones intentan abrir una sesión con éste, la capa de sesión administra cuándo y cómo se van a establecer las comunicaciones concurrentes con el servidor en cuestión (ver figura 7.1.1).

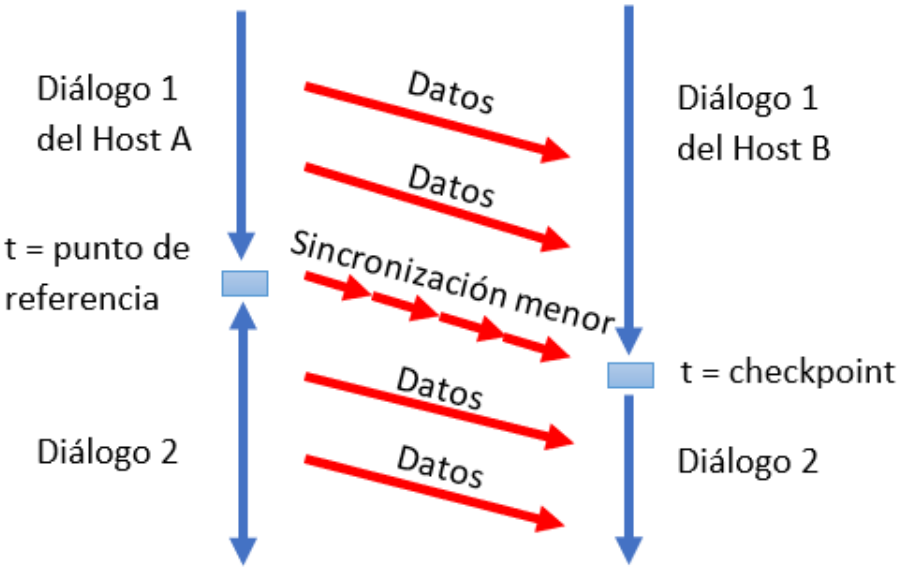


Figura 7.1.1. Servicios de la capa de sesión.

Sincronización

Los usuarios pueden insertar puntos de sincronización en el flujo del mensaje. Cada uno de estos puntos lleva un número de sede. Cuando un usuario invoca una primitiva para solicitar un punto de sincronización, el otro obtiene una indicación. De la misma manera si uno de ellos invoca una primitiva para resincronización, el otro también obtiene una indicación de esto.

El almacenamiento de los mensajes y la subsiguiente retransmisión posterior se lleva a cabo en la capa de presentación que es justo la que está arriba de la capa de sesión; lo que la capa de sesión proporciona es una forma de transportar señales de sincronización y resincronización numeradas a través de la red.

En la capa de sesión, se le conoce como testigos o tokens a derechos que permiten invocar distintos servicios y que se asignan dinámicamente entre los interlocutores. El servicio asociado a un testigo sólo puede ser invocado por su poseedor. Los tipos de testigos son: de datos, de liberación de conexión, de sincronización menor y de sincronización mayor.

Los elementos a tener en cuenta en la sincronización son:

- ***Puntos de sincronización mayores.*** Son utilizados para que ciertas actividades, definidas por los participantes de la sincronización, se hagan completamente o no se hagan. Son necesarios para poder tener el testigo de sincronización mayor o actividad. Delimitan las unidades de diálogo. Son siempre confirmados.
- ***Puntos de sincronización menores.*** Son puntos que sincronizan tareas menos críticas. Es necesario tener el testigo de sincronización menor. Se insertan dentro de las unidades de diálogo. Pueden ser no confirmados.
- ***Unidades de diálogo.*** Las delimitadas por los puntos de sincronización mayor (ver figura 7.1.2).

Figura 7.1.2. Unidades de diálogo.

Intercambio de datos

La característica más importante de la capa de sesión es el intercambio de datos. Una sesión sigue un proceso de tres fases:

1. **Establecimiento**

   En el establecimiento de una sesión un usuario de sesión invoca una primitiva S-CONNECT.request con el objeto de establecer una sesión, el proveedor de sesión solo ejecuta un T-CONNECT.request para establecer una conexión de transporte. De la misma manera, el establecimiento de una sesión, al igual que el establecimiento de una conexión de transporte, implica una negociación entre los corresponsales (usuarios) para fijar los valores de varios parámetros como pueden ser la calidad de servicio, y la bandera indicando si los datos acelerados están o no permitidos. Estos se pasan a la conexión de transporte sin que se les haga modificación alguna (ver figura 7.1.3).

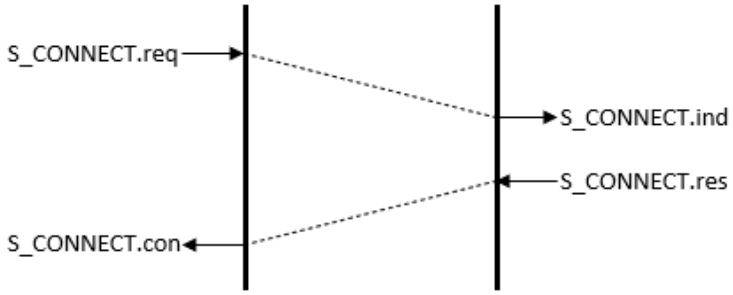


Figura 7.1.3. Establecimiento de la conexión para el intercambio de datos.

2. Utilización

En esta fase, se realiza el intercambio de datos entre los participantes de la sesión activa (ver figura 7.1.4).

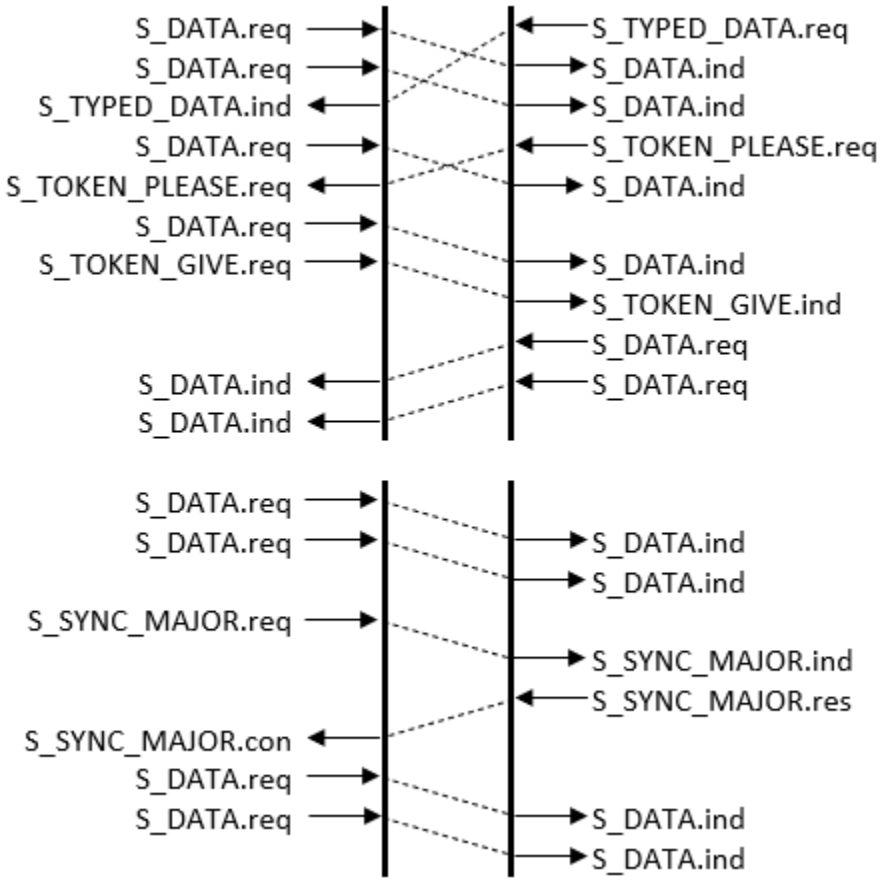


Figura 7.1.4. Utilización de la conexión para el intercambio de datos.

3. Liberación

En la liberación existen importantes diferencias entre una sesión y una conexión de transporte. La principal entre estas es la forma de cómo se liberan las sesiones y las conexiones de transporte.

Las conexiones de transporte terminan con la primitiva T-DISCONNECT.request, que produce una liberación abrupta y puede traer como resultado la pérdida de los datos en tráfico que haya en el momento de la liberación (ver figura 7.1.5).

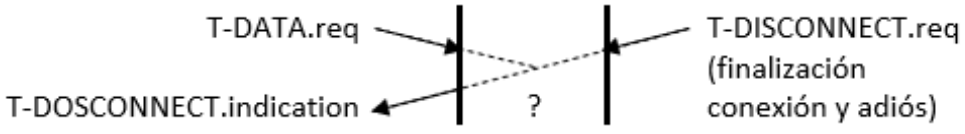


Figura 7.1.5. Caso de primitiva T-DISCONNECT.request.

Las sesiones en cambio, se terminan con la primitiva S-RELEASE.request que resulta en una liberación ordenada en la cual los datos no se llegan a perder (ver figura 7.1.6).

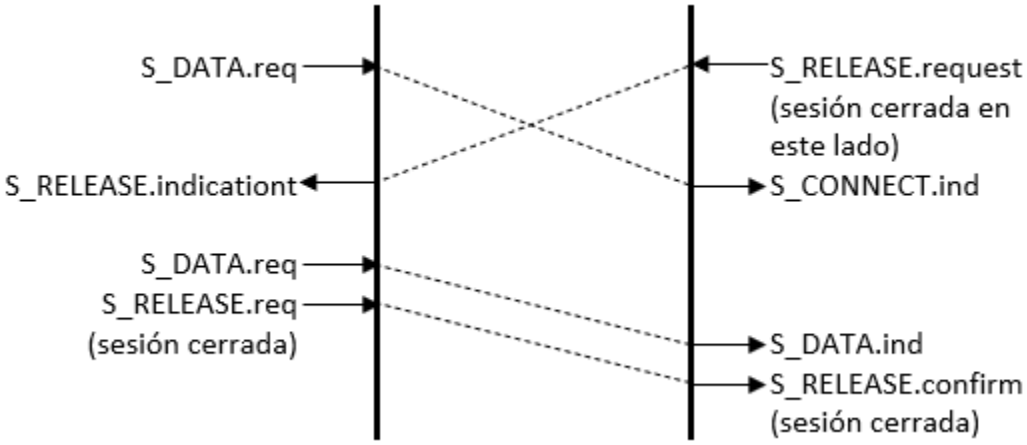


Figura 7.1.6. Caso de primitiva S-RELEASE.request.

Administración del Diálogo

El hecho de mantener un seguimiento de a quién le corresponde el turno de hablar (y hacerlo cumplir), se denomina administración del diálogo. Y es uno de los servicios que puede ofrecer la capa de sesión en el momento que se le solicite.

Todas las conexiones del modelo OSI son full-dúplex, es decir, las PDU (Unidad de Datos Particular) se pueden mover en ambas direcciones sobre la misma conexión. Hay varias situaciones en las que el software de capas superiores está estructurado de tal forma que espera que los usuarios tomen su turno. El modo de operación más natural para el usuario es el de enviar una solicitud al sistema de base de datos y después esperar la respuesta. El hecho de permitir que los usuarios envíen una segunda o tercera solicitud antes de que la primera haya sido contestada, trae como consecuencia una complicación innecesaria al sistema. Lógicamente resulta deseable que el sistema funcione en modo full-dúplex, o bien que le toque el turno de transmitir al usuario o al sistema de base de datos.

La realización de la administración del diálogo se hace mediante el empleo de un testigo de datos. En el momento en que se establece una sesión, el funcionamiento full-dúplex es una de las opciones elegibles. Si se selecciona el funcionamiento half-duplex la negociación inicial también determina qué extremo poseerá primeramente el testigo. Solamente el usuario que tiene el testigo puede transmitir datos, el otro deberá permanecer en silencio. Una vez que el extremo que posee el testigo haya terminado de hacer su transmisión, se lo pasará a su corresponsal por medio de la primitiva S-TOKEN-GIVE.request.

7.2 Llamadas a procedimientos remotos (RPC)

El protocolo RPC (Remote Procedure Call) es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. RPC es la transferencia sincrónica de datos y control entre dos partes de un programa distribuido a través de espacios de direcciones disjuntas.

Los objetivos de RPC son:

- Proporcionar un middleware que simplifique el desarrollo de aplicaciones distribuidas
- Evitar que el programador tenga que interactuar directamente con el interfaz de Sockets
- Abstraer (ocultar) los detalles relativos a la red
- El Servidor ofrece procedimientos que el cliente llama como si fueran procedimientos locales
- Se busca ofrecer un entorno de programación lo más similar posible a un entorno no distribuido.
- El sistema RPC oculta los detalles de implementación de esas llamadas remotas Implementa la llamada remota mediante un dialogo petición respuesta.
  - *Mensaje de petición:* identifica procedimiento llamado, contiene parámetros de la llamada.
  - *Mensaje de respuesta:* contiene valores devueltos. Se encarga de enviar o recibir mensajes para comunicar ambas partes. Se encarga de gestionar los contenidos de esos mensajes (empaquetado y formateado de datos).

Otros protocolos importantes de la capa de sesión son los siguientes:

- **SCP (Protocolo de comunicación simple).** Es básicamente idéntico al protocolo RCP. A diferencia de éste, los datos son cifrados durante su transferencia para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos.
- **ASP (Protocolo de sesión Apple Talk).** Fue desarrollado por Apple Computers, ofrece establecimiento de la sesión, mantenimiento y desmontaje, así como la secuencia petición. ASP es un protocolo intermedio que se basa en la parte superior de Apple Talk Protocolo de transacción (ATP) que es el original fiable de nivel de sesión.

Todas estas capacidades se podrían incorporar en las aplicaciones de la capa 7. Sin embargo, ya que todas estas herramientas para el control del diálogo son ampliamente aplicables, parece lógico organizarlas en una capa separada, denominada capa de sesión, la cual surgió como una necesidad de organizar y sincronizar el diálogo y controlar el intercambio de datos.

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

Tema 8

Capa de presentación

Objetivo: El alumno analizará los diferentes tipos de protocolos, representación de datos, técnicas de compresión y cifrado de datos a través de los estándares utilizados en la capa de presentación del modelo OSI para mantener la seguridad de la información.

La capa de presentación del modelo OSI se encarga de traducir el formato y asigna una sintaxis a los datos para su transmisión en la red.

Entre sus principales funciones se encuentran (ver figura 8.1.1):

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
- Cifrado de los datos para transmisión y descifrado de los datos cuando se reciben en el destino.

8.1 Representaciones comunes de los datos

Se han diseñado diferentes secuencias de patrones de bits para representar símbolos de texto. A cada secuencia se le conoce como código y al proceso de representar los símbolos se le llama codificación.

ASCII 7 bits

El Instituto Nacional Norteamericano de Estándares (ANSI: American Nacional Standards Institute) desarrolló un código llamado Código norteamericano de estándares para intercambio de información (ASCII: American Standard Code for Information Interchange). Este código utiliza siete bits para cada símbolo. Esto significa que 128 (27) símbolos distintos pueden definirse mediante este código. La figura 8.1.1 muestra la representación de la palabra “BYTE” en código ASCII de 7 bits.

Figura 8.1.1. Representación de la palabra “BYTE” en ASCII de 7 bits.

Características:

- ASCII utiliza un patrón de siete bits que varía de 0000000 a 1111111.
- El primer patrón (0000000) representa el carácter nulo (la ausencia de carácter).
- El último patrón (1111111) representa el carácter de eliminación.

- Hay 31 caracteres de control (no imprimibles).
- Los caracteres numéricos (0 a 9) se codifican antes que las letras.
- Hay varios caracteres de impresión especiales.
- Las letras mayúsculas (A ... Z) están antes que las letras minúsculas (a ... z).
- Los caracteres en mayúsculas y en minúsculas se distinguen sólo por un bit. Por ejemplo, el patrón para A es 1000001; el patrón para a es 1100001. La única diferencia es el sexto bit a partir de la derecha.
- Hay seis caracteres especiales entre las letras mayúsculas y minúsculas.

ASCII 8 bits

Para hacer que el tamaño de cada patrón sea de 1 byte (8 bits), a los patrones de bits ASCII se les aumenta un 0 más a la izquierda. Ahora cada patrón puede caber fácilmente en un byte de memoria. En otras palabras, en ASCII extendido el primer patrón es 00000000 y el último es 01111111.

Algunos fabricantes han decidido usar el bit de más para crear un sistema de 128 símbolos adicional. Sin embargo, este intento no ha tenido éxito debido a la secuencia no estándar creada por cada fabricante.

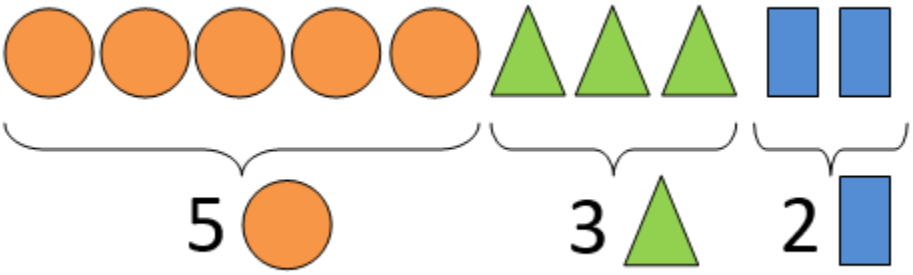
Unicode

Ninguno de los códigos anteriores representa símbolos que pertenecen a idiomas distintos al inglés. Por eso, se requiere un código con mucha más capacidad. Una coalición de fabricantes de hardware y software ha diseñado un código llamado Unicode que utiliza 16 bits y puede representar hasta 65536 (216) símbolos. Diferentes secciones del código se asignan a los símbolos de distintos idiomas en el mundo. Algunas partes del código se usan para símbolos gráficos y especiales. El lenguaje Java utiliza este código para representar caracteres. Microsoft Windows usa una variación de los primeros 256 caracteres.

8.2 Compresión de datos

Otra de las funciones de la capa de presentación es la compresión de los archivos. La compresión funciona mediante el uso de algoritmos (fórmulas matemáticas complejas) para reducir el tamaño de los archivos. El algoritmo busca patrones de bits repetidos en el archivo y entonces los reemplaza con un token. Un token es un patrón de bit mucho más corto que representa el patrón largo. Un ejemplo que representa la compresión de datos se puede observar en la figura 8.2.1.

Archivo sin comprimir



Archivo comprimido

Figura 8.2.1. Representación de la compresión de datos.

Formatos de compresión con pérdidas

Este tipo de compresión elimina datos para disminuir aún más el tamaño, con lo que reduce la calidad. En la compresión con pérdida el bit rate (tasa de bits define el número de bits que se transmiten por unidad de tiempo) puede ser constante (CBR) o variable (VBR). Una vez realizada la compresión, no se puede obtener la señal original, aunque sí una aproximación cuya semejanza con la original dependerá del tipo de compresión. Este tipo de compresión se da principalmente en imágenes, vídeos y sonidos. Además de estas funciones la compresión permite que los algoritmos usados para reducir las cadenas del código desechen información redundante de la imagen. Uno de los formatos que permite compensar esta pérdida es el JPG, que emplea técnicas que suavizan los bordes y áreas que tienen un color similar permitiendo que la falta de información sea invisible a simple vista. Este método permite un alto grado de compresión con pérdidas en la imagen que, muchas veces, sólo es visible mediante un acercamiento zoom.

Formatos de compresión sin pérdidas

Los datos antes y después de comprimirlos son exactos en la compresión sin pérdida. Una mayor compresión solo implica más tiempo de proceso. El bit rate siempre es variable en este tipo de compresión, dado que se depende del formato de compresión o el tipo de archivo a comprimir. Se utiliza principalmente en la compresión de texto, distribución de software o envío de archivos por correo.

8.3 Cifrado de datos

El cifrado de los datos protege la información durante la transmisión. Las transacciones financieras utilizan el cifrado para proteger la información confidencial que se envía a través de Internet. Se utiliza una clave de cifrado para cifrar los datos en el lugar origen y luego descifrarlos en el lugar destino. La criptología ha ido evolucionando con el paso del tiempo, en la figura 8.3.1 se muestra una clasificación general.

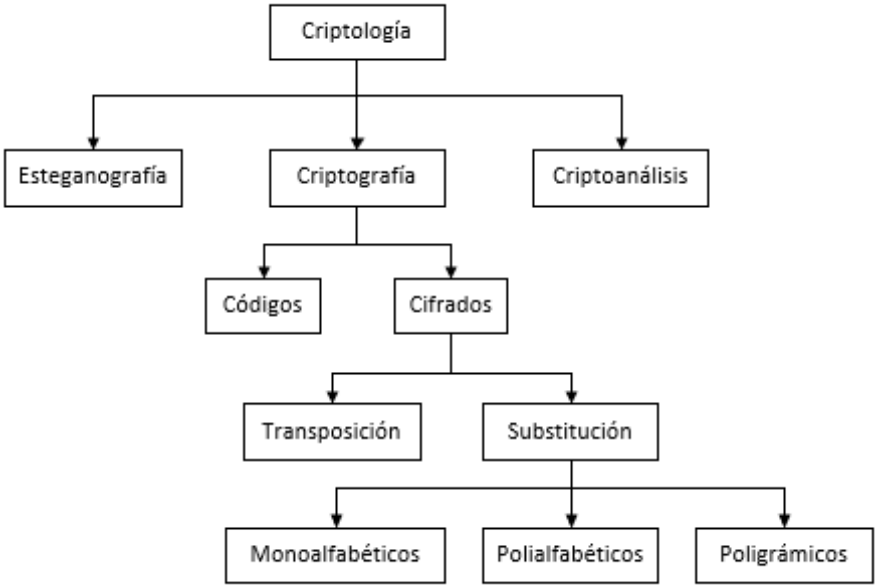


Figura 8.3.1. Clasificación general de la criptografía.

Algoritmos simétricos

El cifrado mediante clave simétrica significa que dos o más usuarios, tiene una única clave secreta, esta clave será la que cifrará y descifrará la información transmitida a través del canal inseguro. Es decir, la clave secreta la deben tener los dos usuarios, y con dicha clave, el usuario A cifrará la información, la mandará a través del canal inseguro, y a continuación el usuario B descifrará esa información con la misma clave que ha usado el usuario A (ver figura 8.3.2).

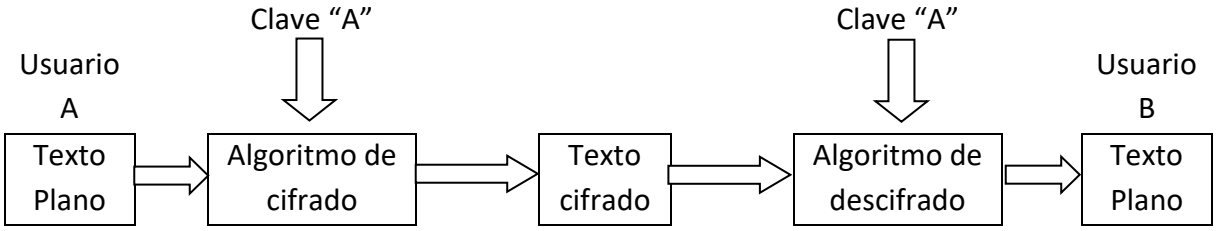


Figura 8.3.2. Funcionamiento de los algoritmos simétricos.

Para que un algoritmo de clave simétrica sea fiable debe cumplir:

- Una vez que el mensaje es cifrado, no se puede obtener la clave de cifrado/descifrado ni tampoco el texto en claro.
- Si conocemos el texto en claro y el cifrado, se debe tardar más y gastar más dinero en obtener la clave, que el posible valor derivado de la información sustraída (texto en claro).

Se debe de tener en cuenta que los algoritmos criptográficos son públicos, por lo que su fortaleza debe depender de su complejidad interna, y de la longitud de la clave empleada para evitar los ataques de fuerza bruta.

La seguridad en clave simétrica reside en la propia clave secreta, y por tanto el principal problema es la distribución de esta clave a los distintos usuarios para cifrar y descifrar la información. La misión del emisor y receptor es mantener la clave en secreto. Si cae en manos equivocadas ya no se podría considerar que la comunicación es segura y se debería generar una nueva clave.

Otro problema reside en que la cantidad de las claves secretas a guardar, es proporcional al número de canales seguros que se desean mantener. Esto no es un problema en sí, pero se deben administrar bien las llaves para que no existan equivocaciones. Este problema no se va a presentar en los algoritmos asimétricos porque cada usuario tiene una pareja de claves, una pública y la otra privada, independientemente del número de canales seguros que se establezcan.

La principal ventaja de los algoritmos simétricos es la velocidad de los algoritmos, y son muy usados para el cifrado de grandes cantidades de datos.

Los algoritmos simétricos más conocidos son:

- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- RC2
- RC4
- RC5
- IDEA (International Data Encryption Algorithm)
- AES (Advanced Encryption Standard)
- SAFER (Secure and Fast Encription Routine)
- Blowfish

Algoritmos asimétricos

Este tipo de algoritmos se basan en dos claves distintas (de ahí el nombre de criptografía asimétrica). Una de las claves se denomina pública y la otra privada. La clave pública (como su nombre lo indica) puede hacerse pública, por el contrario, la clave privada sólo es conocida por el propietario de la misma (ver figura 8.3.3).

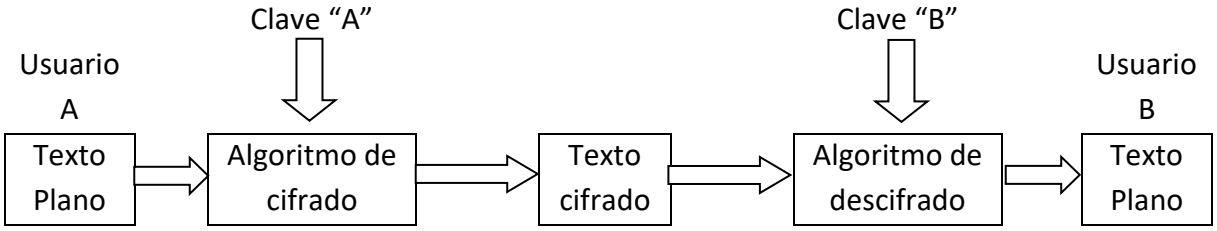


Figura 8.3.3. Funcionamiento de los algoritmos asimétricos.

Cuando una persona quiere firmar digitalmente un mensaje usa su clave privada, de esta forma cualquier persona que posea la clave pública del remitente podrá comprobar que el mensaje ha sido firmado correctamente. Un caso de ejemplo del uso del cifrado asimétrico se representa en la figura 8.3.4.

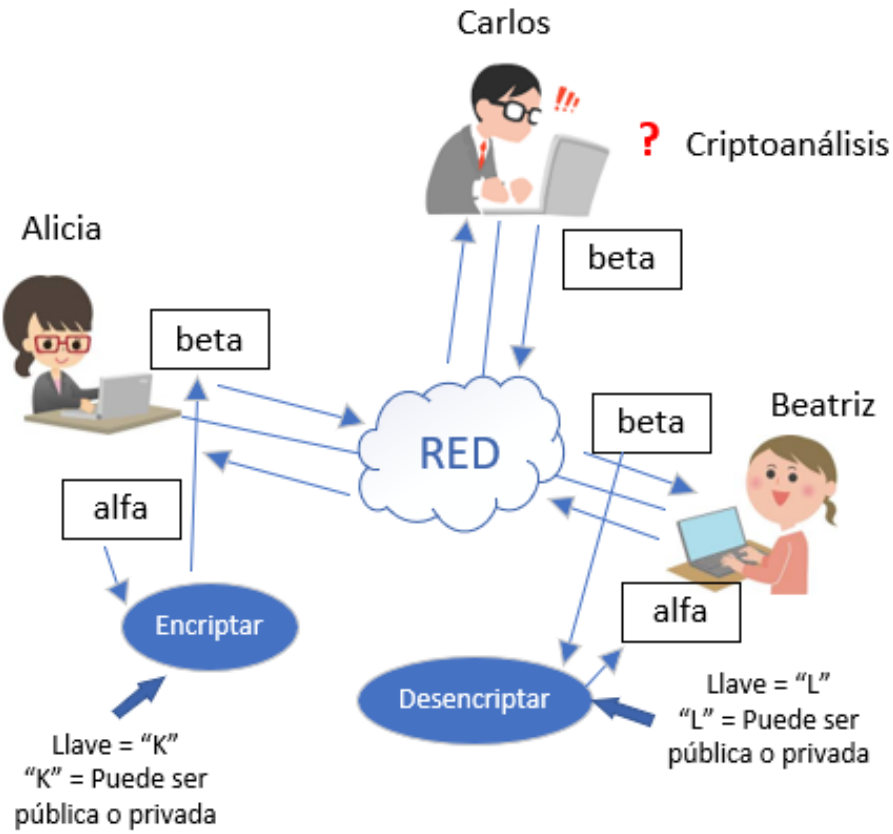


Figura 8.3.4. Ejemplo del uso de cifrado asimétrico.

Para cifrar un mensaje se usa la clave pública del destinatario, así cuando éste reciba el mensaje sólo él podrá usar su clave privada para descifrarlo y por tanto sólo él puede ver el contenido del mensaje.

Los algoritmos asimétricos ofrecen autenticidad, que consiste en:

- **Confidencialidad.** Cifrando las comunicaciones.
- **No repudio.** Mediante firma electrónica.
- **Integridad.** El mensaje que se recibe es de quien dice ser y contiene lo que el remitente escribió.

Algunos usos de este tipo de algoritmos pueden ser:

- Cifrado y descifrado de mensajes
- Firmado y verificación de mensajes
- Acceso seguro a servicios remotos
- Firmado de código

Los algoritmos de cifrado asimétrico más conocidos son:

- RSA (Rivest, Shamir, Adleman)
- Diffie-Hellman
- ECC (Elliptical Curve Cryptography)

Seguridad por medio de la criptografía

El surgimiento de redes de comunicación, en particular de Internet, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario entonces, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de una tecnología denominada criptografía.

Hoy en día la criptografía está muy presente como sistema de seguridad. A la hora de usar un correo electrónico, de introducir claves, de realizar firmas electrónicas o incluso llamar a través de un teléfono móvil, la secuencia de datos que se utiliza está cifrada para así evitar que alguien intercepte las comunicaciones.

La protección de datos ante la curiosidad de ciertos usuarios no es el único aspecto relacionado con la seguridad en la conexión entre redes. Se deben de tener en cuenta como mínimo los siguientes servicios de seguridad:

1. Proteger los datos para que no puedan ser leídos por personas sin autorización.
2. Impedir que las personas sin autorización inserten, borren o modifiquen mensajes.
3. Verificar al emisor de cada uno de los mensajes.
4. Hacer posible que los usuarios transmitan electrónicamente documentos firmados.

Los procedimientos criptográficos son inherentes a la protección de la identidad de alguna persona, de ahí que tengan que estar presentes en todos los aspectos del día con día.

Algunos ejemplos de los usos que se le da a la criptografía en la vida cotidiana de toda sociedad pueden ser:

- Comercio electrónico
  - Compras en línea
  - Con dispositivos móviles
  - Pagos con tarjetas de crédito o débito
  - Pago de impuestos
- Cifrado de almacenamiento
  - Bases de datos
  - Dispositivos de almacenamiento
  - Almacenamiento distribuido
- Cifrado de comunicaciones
  - Correo electrónico
  - Redes inalámbricas
  - Redes sociales
  - Mensajería instantánea
  - Intercambio de documentos
  - Radio/TV
- Cifrado de investigaciones
- Cifrado en sector financiero
  - Cajeros automáticos

En sistemas orientados a conexión, la autenticación puede realizarse en el momento en que se establece una sesión.

Las redes públicas que realizan la capa de sesión, también incluyen la capa de presentación, después de todo, la mayor parte del trabajo que hace ésta es precisamente ofrecer los servicios de sesión disponibles a los usuarios de la capa de aplicación.

Funciones Hash (MD4, MD5, SHA-1, SHA-2)

Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

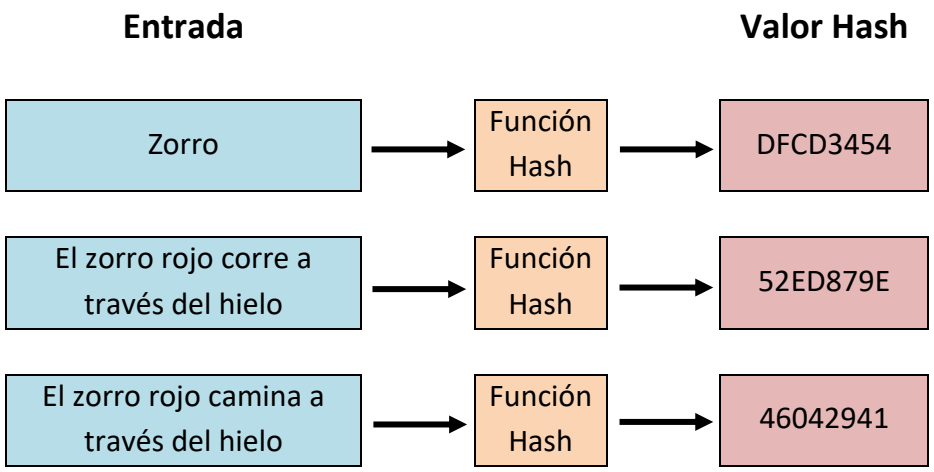


Figura 8.3.5. Funcionamiento de las funciones hash.

Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varios cometidos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.

Este sistema de criptografía usa algoritmos que aseguran que con la respuesta (o hash) nunca se podrá saber cuáles han sido los datos insertados, lo que indica que es una función unidireccional. Sabiendo que se puede generar cualquier resumen a partir de cualquier dato, se debe de tomar en cuenta que existe la posibilidad de que se pueden repetir estos resúmenes (hash), podría haber colisiones, ya que no es fácil tener una función hash perfecta (que consiga que no se repita la respuesta), pero esto no supone un problema, ya que si se consiguieran (con un buen algoritmo) dos hash iguales los contenidos serían totalmente distintos.

Las funciones hash son ampliamente usadas, una de las utilidades que tiene es proteger la confidencialidad de una contraseña, ya que podría estar en texto plano y ser accesible por cualquiera y aun así no poder ser capaces de deducirla.

Otro uso que tiene esta función es la de garantizar la integridad de los datos y es algo que se ha visto muchas veces, por ejemplo, en algunas webs que proporcionan descargas de archivos grandes, por ejemplo: software, dando junto a su vez el resumen del archivo y la función empleada.

Firmar un documento digitalmente ayuda a verificar la identidad del emisor de un mensaje. El método más simple de firma digital consiste en crear un hash de la información enviada y cifrarlo con una clave privada (de un par de claves de la criptografía asimétrica) para que cualquiera con la clave pública pueda ver el hash real y verificar que el contenido del archivo es el que ha sido mandado.

Ciclo de vida de claves o contraseñas

Existen distintos mecanismos de gestión de identidades y controles de acceso. Algunos están implementados en los sistemas operativos habituales, otros están disponibles a través de servicios en línea, como pueden ser el social login, la federación de identidades, los servicios de intermediarios de seguridad de acceso a la nube, entre otros. En cualquier caso, se debe establecer un procedimiento claro para habilitar y revocar las credenciales y permisos de acceso a los distintos servicios y aplicaciones. Como la contraseña es el más utilizado de estos factores, la gestión de las contraseñas es uno de los aspectos más importantes para asegurar los sistemas de información.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir unas buenas prácticas, para lo cual, se implementa el ciclo de vida de las claves o contraseñas (ver figura 8.3.7), la cual consta de seis etapas:

Figura 8.3.6. Representación gráfica del ciclo de vida de claves o contraseñas.

Generación de contraseñas

Da inicio al ciclo de vida de tus claves o contraseña. Lo ideal es establecer protocolos para generar claves y contraseñas seguras y para lograrlo es necesario:

- Emplear una mezcla de símbolos y caracteres sin coherencia lógica
- Ayudarse de mnemotecnias e imágenes mentales conocidas únicamente por quien establece la contraseña segura
- Evitar utilizar información personal tal como fecha de nacimiento propia y similares

Distribución

Comprende la forma en cómo llega y se autentica la clave o contraseña en el banco o Base de Datos (DB) que autoriza el acceso a la plataforma para la que se creó tal clave o contraseña. Esta puede ser de:

- **Distribución manual.** La clave se envía mediante canales distintos a la línea de comunicación mediante la cual se mandan mensajes cifrados, por ejemplo: Carta certificada + vía telefónica + fax; Inyección de claves.
- **Distribución central.** Las partes interesadas en el intercambio seguro de datos establecen una conexión cifrada por un tercero. Este elemento se encarga de entregar las claves cifradas seguras de comunicación a ambos extremos.
- **Distribución certificada por:**
  - *Transferencia de clave.* El emisor genera una clave asimétrica con la llave pública del receptor (criptografía asimétrica)
  - *Intercambio o acuerdo de clave.* El emisor y el receptor conocen de antemano la clave (criptografía simétrica)

Protocolo de recuperación de contraseña

Se refiere a los mecanismos que se activan cuando al usuario se le olvida la clave o contraseña que generó. En principio se manejan dos opciones para activar este protocolo:

- Recuperación de clave o contraseña
- Restablecimiento de clave o contraseña

Ambas opciones están supeditadas a las políticas y condiciones de gestión de claves y contraseñas establecidas por el propietario de la aplicación o servicio. Las mismas se encargan de verificar la autenticidad de la data proporcionada al momento de establecer la clave o contraseña.

Políticas de uso

Maneja todas las consideraciones para generar, emplear, recuperar, reemplazar y disponer de las claves y contraseñas. Determina los límites de uso, y esto incluye:

- Tipo de caracteres
- Longitud de la contraseña
- Políticas de almacenamiento en la DB
- Políticas de recuperación de clave o contraseña olvidada
- Caducidad u obsolescencia de las claves.

Almacenamiento en DB

Con el propósito de autenticar usuarios y proteger sus datos con sus claves o contraseñas, el propietario del sistema debe almacenar o alojar toda esta información en una base de datos y restringir el acceso a ella. Tal restricción se basa en los siguientes controles de seguridad:

- Cifrado de los archivos que contienen las calves y contraseñas.
- Activación del control de acceso al sistema operativo de la DB.
- Almacenamiento de hashes criptográficos para claves y contraseñas unidireccionales en lugar de guardar las claves y contraseñas como tal.
- Verificación de los elementos del host (capacidades de seguridad del host, las amenazas en su contra, requerimientos de autenticación).

Caducidad u Obsolescencia

Es la etapa final del ciclo de vida de claves y contraseñas. Comprende las políticas de disposición final de las claves o contraseñas cuando ya concluyó el tiempo de vida estimado para su renovación o si es que caen en desuso, ya que una de las principales premisas para evitar su descubrimiento, robo o revelado es que las claves y contraseñas no deben usarse por tiempo indefinido.

La criptografía y el ciclo de vida de claves y contraseñas son parte de la seguridad informática de toda empresa. Esto, porque la seguridad informática vela por la protección de la data sensible ante amenazas y vulnerabilidades de los sistemas; y su razón fundamental es blindarlos contra cualquier intromisión a lo largo del ciclo.

Tema 9

Capa de aplicación

Objetivo: El alumno identificará y pondrá en práctica diferentes tipos de aplicaciones con base en las necesidades funcionales y requerimientos de seguridad de los usuarios en una red de datos.

La capa de aplicación provee un significado para los procesos relacionados a las aplicaciones para el intercambio de información. Incluidos servicios usados para establecer y terminar conexiones entre dispositivos, y servicios para monitorear y administrar los sistemas, siendo interconectados también como los varios recursos que se empleen (ver figura 9.1.1).

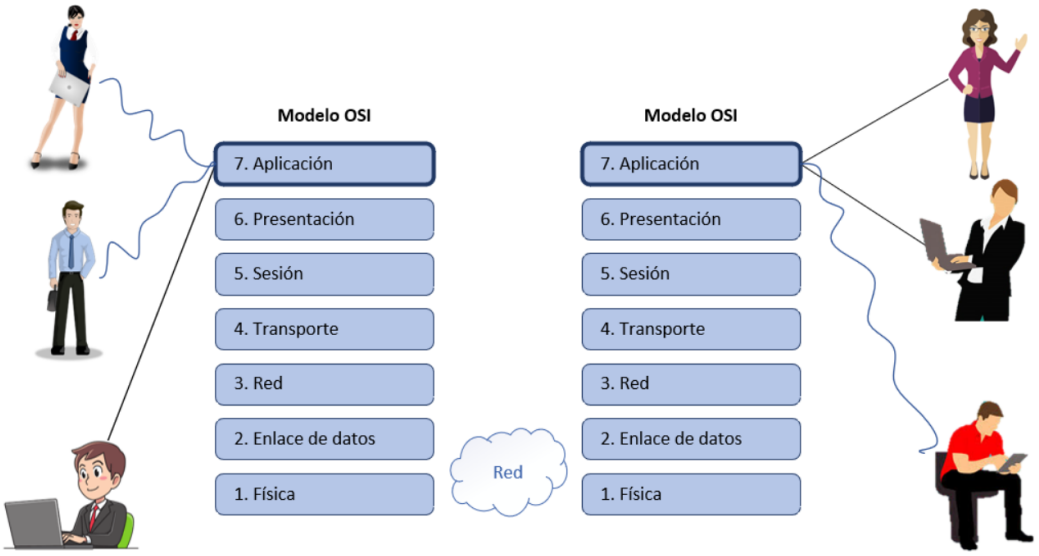


Figura 9.1.1. Representación del modelo OSI con énfasis en la capa de aplicación.

La capa de aplicación maneja los paquetes de datos de las aplicaciones cliente-servidor, servicios de nombre de dominio y aplicaciones de red. Entre los servicios y protocolos están los siguientes:

- **HTTP:** Protocolo para la distribución y colaboración de sistemas de información de hipermedia.
- **Cliente – servidor:** Servicio en el cual diversos dispositivos se conectan a un servidor central.
- **Correo electrónico:** Servicio utilizado para la transferencia de mensajes y archivos adjuntos.
- **Telnet:** Protocolo utilizado para conectar con un equipo remoto a través de la red.
- **FTP:** Protocolo que permite la transferencia de datos entre un cliente y un servidor.

La capa de aplicación es encargada de:

- Identificar y establecer la disponibilidad de los socios de la comunicación deseada.
- Sincronizar las aplicaciones participantes.
- Establecer acuerdos con respecto a los procedimientos para la recuperación de errores.
- Controlar la integridad de los datos.

9.1 Servicios web

Un servicio web realiza una tarea específica o un conjunto de tareas. La descripción de servicio proporciona todos los detalles necesarios para interactuar con el servicio, incluidos los formatos de mensaje (que detallan las operaciones), los protocolos de transporte y la ubicación.

HTTP (HyperText Transfer Protocol – Protocolo de Transferencia de Hipertexto)

HTTP es un protocolo de nivel de aplicación para la distribución y colaboración de sistemas de información de hipermedia. Este protocolo fue creado en el CERN en 1989, esta aplicación surgió por la necesidad de poder lograr la comunicación de grandes grupos de científicos para intercambiar: archivos, planos, dibujos, fotos y otros documentos, mediante el concepto "ligando documentos". Este servicio se encuentra por defecto en el puerto 80.

Actualmente su su estructura contiene varias secciones como son:

- Mensajes HTTP
- Respuestas
- Conexiones
- Peticiones
- Métodos de definición
  - *GET.* Este método solicita solicita al servidor que envíe la página html, además de codificar adecuadamente el MIME.
  - *HEAD.* Este método solamente solicita la cabecera del mensaje, sin página.
  - *PUT.* Es el método inverso de GET.
  - Otros métodos: POST, OPTIONS, DELETE, CONNECT, TRACE.
- Definición de código de estado
- Entidades

Este protocolo puede ser utilizado para muchas tareas más allá de su uso para el hipertexto, tal como servidores de nombres y sistemas de administración de objetos distribuidos, a través de la extensión de su solicitud de métodos, códigos de errores y cabeceras.

Una característica de HTTP es el "tipificar" y negociar la representación de datos, permitiendo a los sistemas construir independientemente los datos para que sean transferidos.

HTTP ha sido usado en la WWW (World Wide web) iniciada desde 1990. Esta especificación define el protocolo designado "HTTP/1.1", y existe una actualización al RFC 2068.

HTTPS (HyperText Transfer Protocol Secure – Protocolo de Transferencia de Hipertexto Seguro)

HTTPS es la versión segura del protocolo HTTP, utiliza un cifrado basado en SSL (Secure Socket Layers) para crear un canal seguro entre servidor y cliente. El puerto estándar para este protocolo es el 443.

Para conocer si la página web que se está visitando utiliza un protocolo seguro, en cuanto a la trasmisión de los datos que se está transcribiendo, se debe observar si en la barra de direcciones del navegador, aparece https al comienzo de la url.

Si se necesita enviar o acceder a información sensible en un sitio web es mucho más seguro que se realice a través de HTTPS, debido a su mayor nivel de cifrado. Por ejemplo, el acceso a una cuenta o plataforma de banca en línea implica el intercambio de información confidencial, que requiere acceso seguro.

Los datos que se envían mediante HTTPS están protegidos con tres capas clave de seguridad:

1. **Cifrado:** Se cifran los datos intercambiados para mantenerlos a salvo de miradas indiscretas. Eso significa que cuando un usuario está navegando por un sitio web, nadie puede "escuchar" sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas ni robarle información.
2. **Integridad de los datos:** los datos no pueden modificarse ni dañarse durante las transferencias, ni de forma intencionada ni de otros modos, sin que esto se detecte.
3. **Autenticación:** demuestra que los usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques “man-in-the-middle” y contribuye a la confianza de los usuarios.

HTTPS sirve como subcapa bajo capas regulares de una aplicación HTTP, la cual cifra y descifra las solicitudes de una página de Internet, así como las páginas que son devueltas por el servidor web, protegiendo los datos a medida que viaja entre el servidor y el cliente. El nivel de cifrado depende del navegador usado y del servidor remoto. Es utilizado especialmente por sistemas que manejan dinero, transacciones comerciales, datos personales o contraseñas.

Al navegar por una página web el navegador busca automáticamente en la URL para determinar si la página está utilizando HTTP o HTTPS. Si la página está utilizando HTTPS del navegador intercambia algunos parámetros SSL con el servidor web, y entonces se abre una conexión segura. El navegador web busca automáticamente el certificado, que no requiere ninguna acción por parte del usuario en la mayoría de las situaciones.

Las páginas web tienden a ser más lentas cuando se utiliza HTTPS debido al tiempo requerido para cifrar la información. Dado que las páginas son más lentas pueden proporcionar una experiencia de usuario más pobre, HTTPS es a menudo reservada para las páginas en el que se transfiere la información sensible.

Una práctica recomendada para implementar el protocolo HTTPS es la utilización de certificados de seguridad potentes. Para poder habilitar el protocolo HTTPS en un sitio web, se debe obtener un certificado de seguridad. El certificado lo emite una autoridad de certificación (CA, Certification Authority), que toma las medidas necesarias para verificar que la dirección web pertenezca realmente a la organización. De este modo, se protege a los usuarios de cualquier ataque “man-in-the-middle”. Al configurar el certificado, se debe de asegurar de obtener un nivel de seguridad alto escogiendo una clave de 2048 bits. Cuando se escoge el certificado del sitio, se debe hacer lo siguiente:

- Escoger el certificado de una CA de confianza que ofrezca asistencia técnica
- Decidir qué tipo de certificado se necesita:
  - Un certificado único para un origen seguro único (por ejemplo: www.ejemplo.com)
  - Un certificado para varios dominios para varios orígenes seguros conocidos (por ejemplo: www.ejemplo.com, cdn.ejemplo.com, ejemplo.co.uk)
  - Un certificado comodín para un origen seguro con muchos subdominios dinámicos (por ejemplo: a.ejemplo.com, b.ejemplo.com)

Otros protocolos de la capa de aplicación son los siguientes:

- **DNS (Domain Name Service - Servicio de Nombres de Dominios).**
  Se utiliza para resolver nombres de Internet en direcciones IP. El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Contienen el nombre, la dirección y el tipo de registro (ver figura 9.1.2). Los tipos de registro son los siguientes:
  - **A:** Una dirección de dispositivo final.
  - **NS:** Un servidor de nombre autoritativo.
  - **CNAME:** El nombre canónico para un alias; se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.

- **MX:** Registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correo.

Si no puede resolver el nombre con sus registros almacenados, se comunica con otros servidores. El servidor almacena de forma temporal la dirección numérica que coincide con el nombre en la memoria caché.

Algunos ejemplos de dominios de nivel superior:

- **.au:** Australia
- **.co:** Colombia
- **.com:** Empresa o industria
- **.jp:** Japón
- **.org:** Organización sin fines de lucro

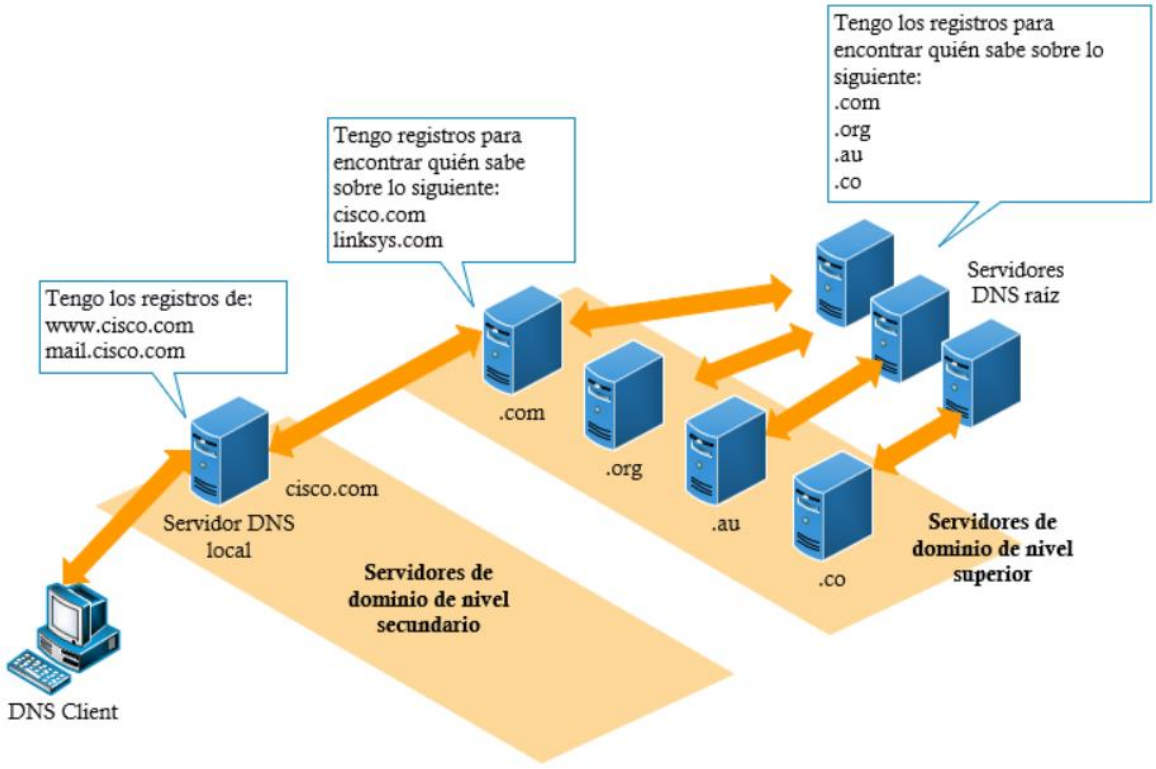


Figura 9.1.2. Funcionalidad del protocolo DNS.

- **DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuración Dinámica de Host).**

  Se utiliza para asignar una dirección IP, una máscara de subred, un gateway predeterminado y un servidor DNS a un host. DHCP permite que un host obtenga una dirección IP de forma dinámica. Se establece contacto con el servidor de DHCP y se le solicita la dirección; este elige la dirección de un rango de direcciones configurado

llamado “pool” y se la concede al host por un período establecido (ver figura 9.1.3). DHCP se utiliza para hosts de uso general, como los dispositivos para usuarios finales; el direccionamiento estático se utiliza para dispositivos de red como gateways, switches, servidores e impresoras.

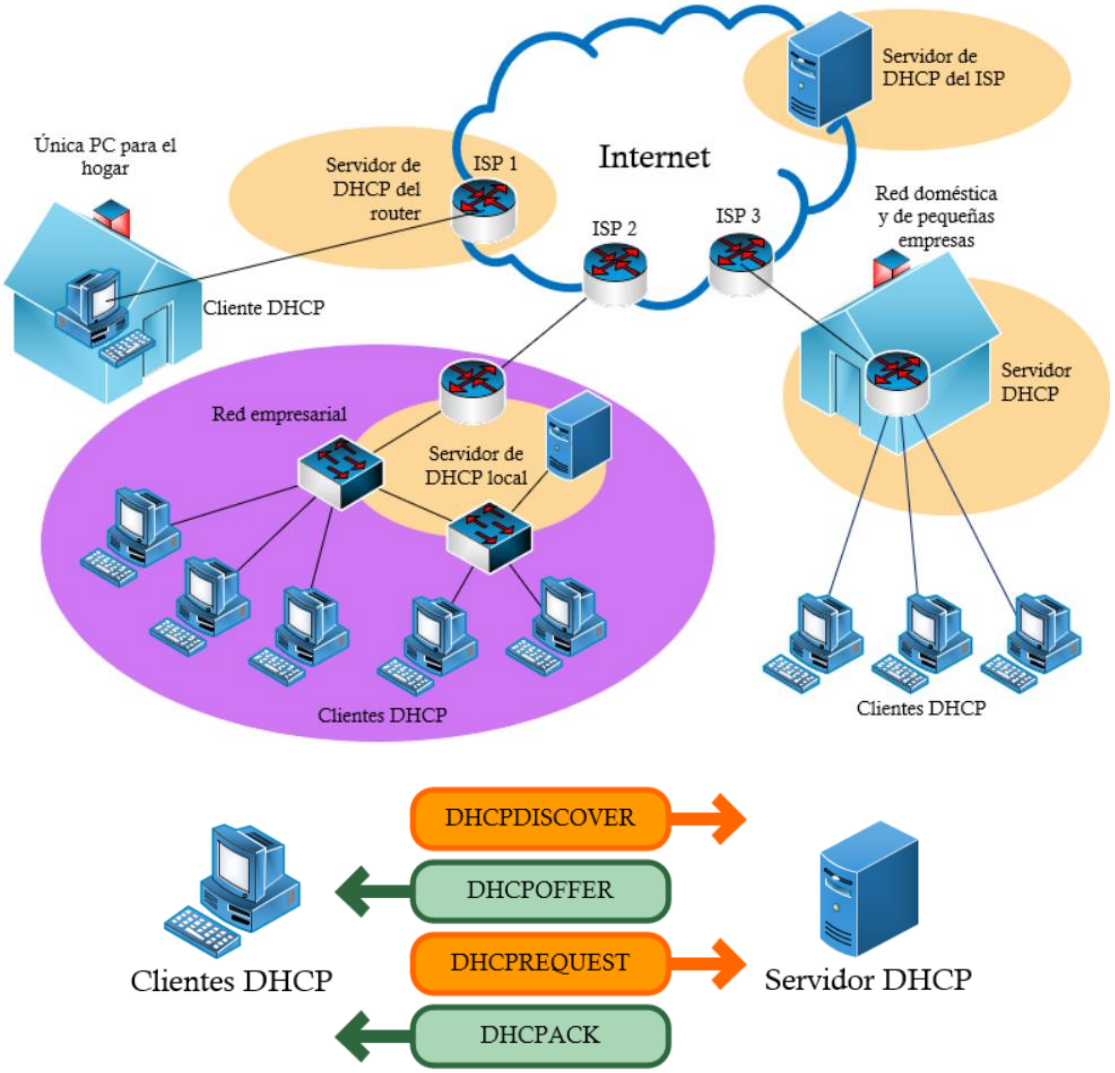


Figura 9.1.3. Funcionalidad del protocolo DHCP.

- **SMTP (Simple Mail Transport Protocol - Protocolo Simple de Transferencia de Correo).**

Se utiliza para la transferencia de mensajes y archivos adjuntos de correo electrónico.

En redes punto a punto, la interacción entre los protocolos de aplicación con las aplicaciones de usuario final funciona mediante el establecimiento por solicitud entre cliente y servidor (ver figura 9.1.4).

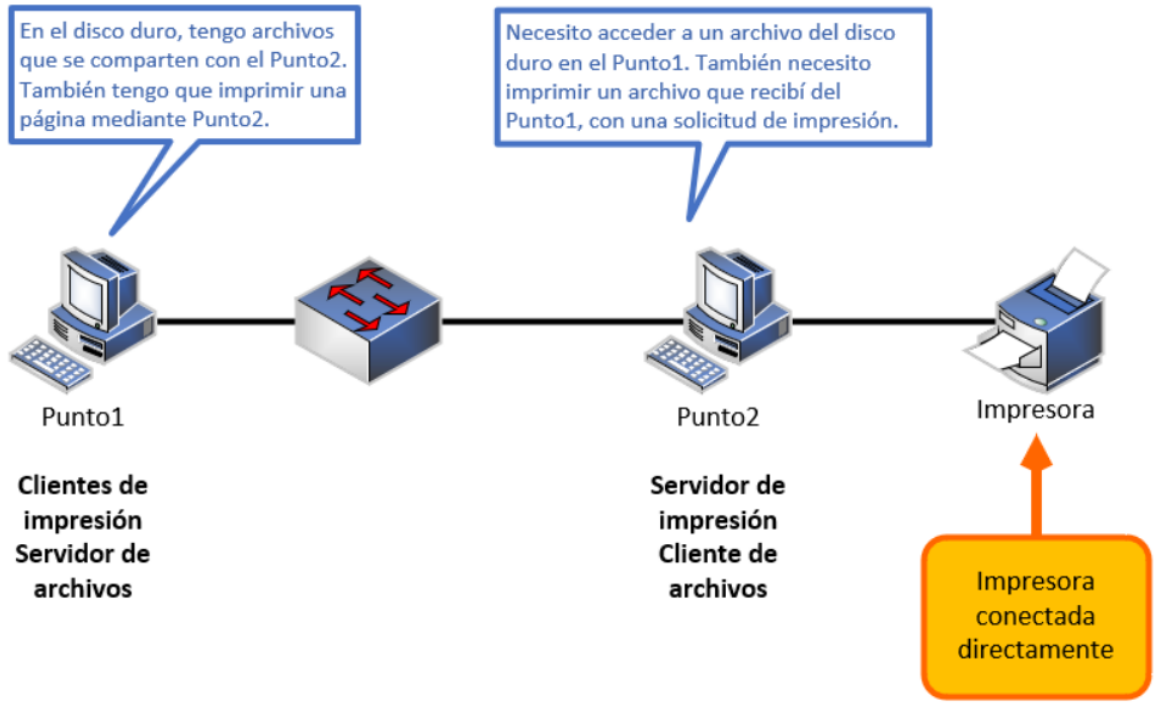


Figura 9.1.4. Representación de la comunicación por SMTP.

Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación (ver figura 9.1.5).

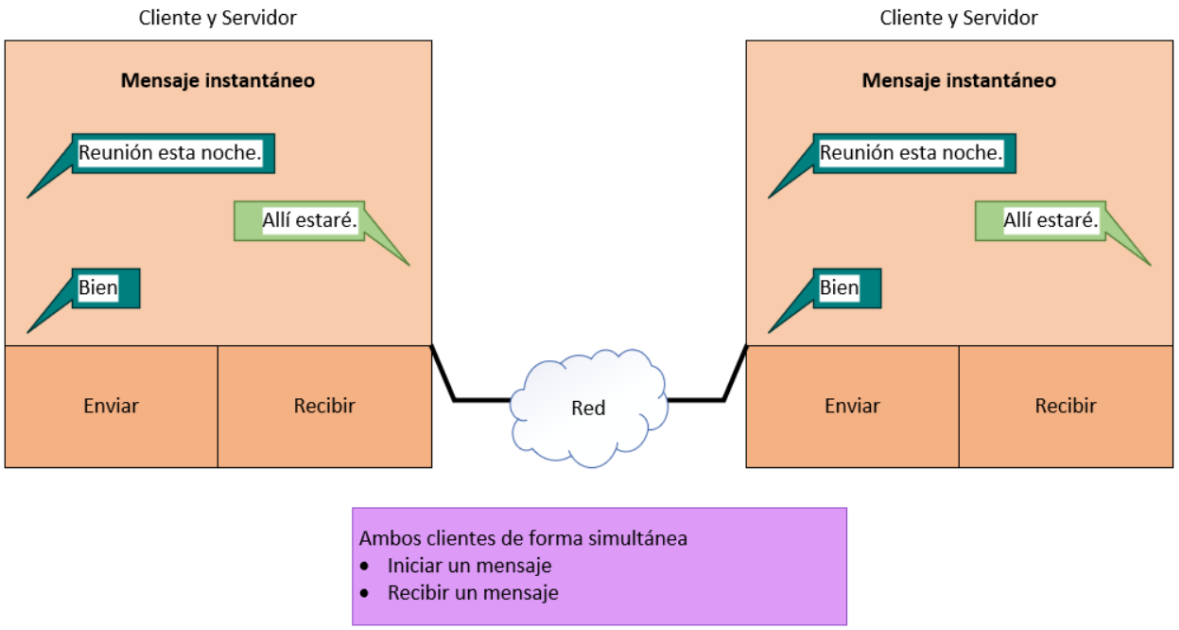


Figura 9.1.5. Ejemplo de comunicación por DHCP.

9.2 Compartir archivos

SMB (Server Message Block – Bloque de Mensajes de Servidor)

SMB es un protocolo de solicitud-respuesta y de cliente-servidor. Los servidores pueden poner sus recursos a disposición de los clientes en la red (ver figura 9.1.6).

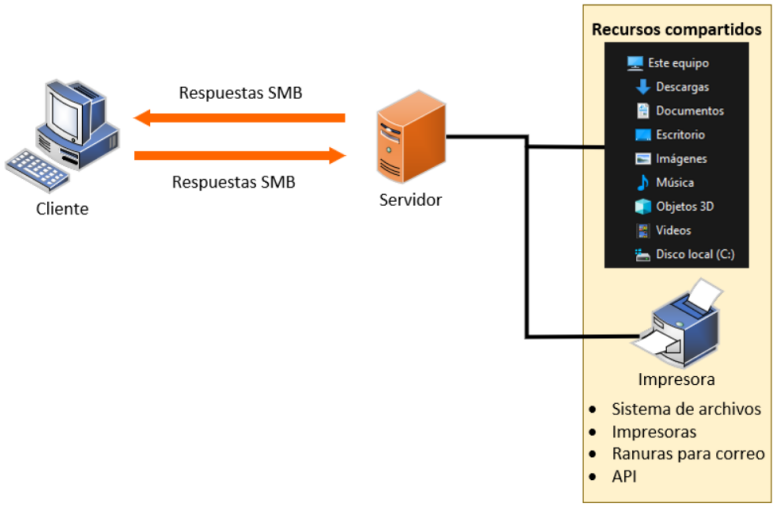


Figura 9.2.1. Protocolo SMB.

Los clientes establecen una conexión a largo plazo a los servidores. Una vez establecida la conexión, el usuario puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

Con el protocolo SMB, se puede copiar un archivo de una PC a otra con Windows Explorer (ver figura 9.1.7).

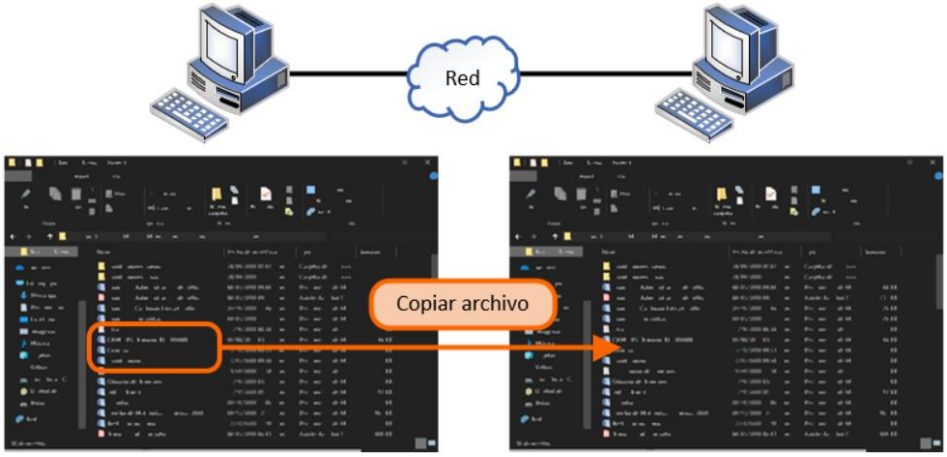


Figura 9.2.2. Copiado de un archivo de una PC a otra PC.

Este protocolo tiene la desventaja de servir solamente para redes LAN. Su configuración se basa en la asignación de permisos a los archivos o carpetas que se desean compartir.

NFS (Network File System – Sistema de Archivos de Red)

Es un protocolo que permite acceso remoto a un sistema de archivos a través de la red. Todos los sistemas Unix pueden trabajar con este protocolo; cuando se involucran sistemas Windows, se debe utilizar Samba en su lugar.

Si no se utilizan las características de seguridad basadas en Kerberos (protocolo de seguridad que usa una criptografía de claves simétricas para validar usuarios con los servicios de red), debería asegurarse de que sólo los equipos autorizados a utilizar NFS puedan conectarse a los varios servidores RPC necesarios, porque el protocolo básico confía en la información recibida a través de la red. El firewall debería por tanto prohibir la usurpación de IPs (IP spoofing o suplantación de direcciones IP) para prevenir que una máquina externa se haga pasar por una interna y el acceso a los puertos apropiados debería estar restringido únicamente a los equipos que deban acceder a espacios compartidos por NFS.

Características:

- Tiene fama de rápido
- En las pruebas ha dado un pésimo resultado
- Sirve tanto a través de internet como LAN
- Su configuración, con autenticación no es trivial
- A partir de Windows 8 sólo se soporta este protocolo en la versión Enterprise y los clientes no nativos como Nekodrive tampoco soportan Windows 8
- Tiene una gran estabilidad superior a SMB para ficheros grandes

9.3 Sesión remota

Telnet (Telecommunication Network)

Telnet es uno de los protocolos más antiguos de Internet y se utiliza para conectar con un equipo remoto a través de la red, de forma que el ordenar cliente se comporta como una terminal conectada con el ordenador remoto. Todo lo que se necesita es un cliente Telnet.

El propósito de Telnet es proporcionar comunicación bastante general, bidireccional. Su meta fundamental es permitir un método estándar de interconectar la terminal de dispositivos y procesos centralizados de terminal de extremo a extremo. Es previsto que el protocolo se puede también utilizar para comunicación de terminal-terminal (linking) y comunicación de proceso-proceso (cómputo distribuido).

Cuando una conexión Telnet se establece, cada terminal asume un origen y fin realizando una “Terminal de Red Virtual” o NVT (siglas en ingles).

Este servicio se encuentra por defecto en el puerto 23.

Hay tres razones principales por las que telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los dominios de uso general de telnet tienen varias vulnerabilidades descubiertas sobre los años, y varias más que podrían aún existir.
- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión, así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.
- Telnet carece de un esquema de autenticación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

SSH (Secure Shell)

SSH es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si se tiene un servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura, gestionar claves RSA (cifrado asimétrico utilizado para cifrar y autenticar) para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizando mediante SSH.

SSH trabaja de forma similar a como se hace con telnet La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

SSH permite autenticar a un usuario utilizando su password Unix ordinario. La única diferencia es que el password no viaja nunca en claro por la red. Si se utiliza SSH para sustituir a Telnet o FTP se evita el peligro de que un password sea capturado por posibles sniffers en la red.

Por otra parte, se sigue siendo vulnerable a los llamados "ataques de diccionario" contra el password: si un atacante tiene acceso al fichero */etc/passwd*, no resulta difícil averiguar passwords formados a partir de palabras susceptibles de figurar en un diccionario. Esto significa que sigue siendo extremadamente importante que el administrador proteja debidamente el fichero */etc/passwd* y que los usuarios utilicen passwords "seguros" (lo más aleatorios posible, combinando mayúsculas, minúsculas, dígitos y puntuación).

9.4 Transferencia de archivos

FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos)

FTP permite la transferencia de datos entre un cliente y un servidor. El protocolo FTP tiene varios objetivos:

- Promover la distribución de archivos (computadora programas y/o datos)
- Animar indirecto o implícito (vía uso de los programas) de computadoras remotas
- Proteger a un usuario de variaciones en sistemas de almacenamiento de archivo entre los hosts
- Transferir datos confiablemente y eficientemente

Un cliente FTP es una aplicación que se ejecuta en una PC y que se utiliza para insertar y extraer datos en un servidor que ejecuta un demonio FTP. Para transferir datos correctamente, FTP requiere dos conexiones entre el cliente y el servidor: una para los comandos y las respuestas y otra para la transferencia de archivos propiamente dicha (ver figura 9.4.1).

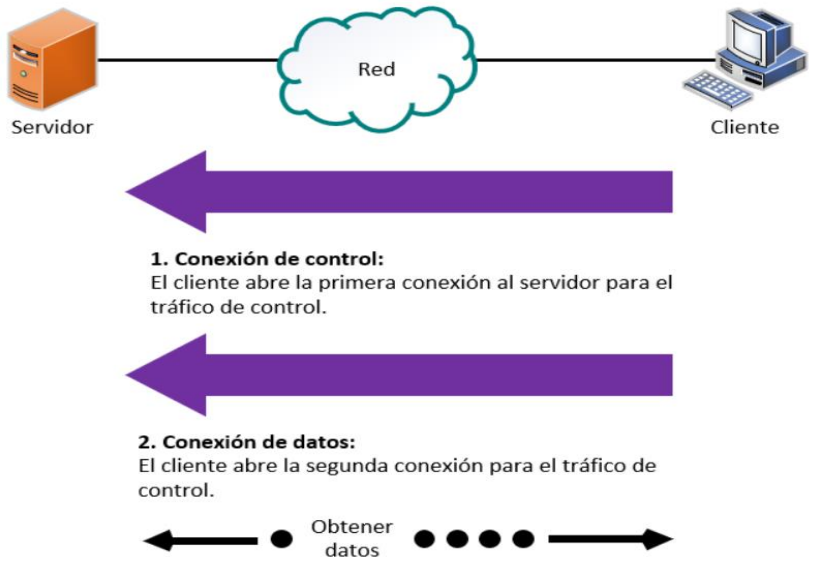


Figura 9.4.1. Conexión de cliente a servidor FTP.

De acuerdo con los comandos enviados a través de la conexión de control, los datos pueden descargarse desde el servidor o cargarse desde el cliente.

FTP, aunque usado directamente por un usuario en una terminal, se diseña principalmente para uso de programas. Este servidor se basa en dos maneras de transferencia (activo y pasivo), por esto utiliza dos puertos para dichas transferencias: 20 y 21.

FTP queda descartado como sistema de transferencia de ficheros, ya que para LAN existen soluciones mejores y para internet FTP es inseguro, pese a su extendido uso. Sin embargo, es el que mejor rendimiento y velocidad ofrece si el servidor tiene pocos recursos, ya que no deberá cifrar y descifrar la conexión

SFTP (Secure File Transfer Protocol – Protocolo Seguro de Transferencia de Archivos)

Es un protocolo del nivel de aplicación que permite la transferencia y manipulación de archivos sobre un flujo de datos fiable. Es utilizado con SSH para proporcionar la seguridad a los datos y permite ser usado con otros protocolos de seguridad.

Descripción y características

- Permite la realización de diferentes operaciones sobre archivos remotos.
- Se aplica con más frecuencia en plataformas Unix, aunque existen servidores SFTP en la mayoría de las plataformas.
- Está diseñado para ser un protocolo independiente.
- No es aún un estándar de internet.
- La versión más utilizada es la versión 3, ejecutada por el servidor OpenSSH de SFTP.
- En su versión 4, redujo sus vínculos con la plataforma Unix, por lo que muchos Windows basan sus implementaciones en servidores SFTP.
- SFTP utiliza el puerto 22 de TCP.
- La seguridad en la transferencia no la provee directamente el protocolo SFTP, sino SSH o el protocolo que sea utilizado en su caso para este cometido.
- Para subir archivos, los archivos transferidos pueden estar asociados con sus atributos básicos, como el de tiempo, esta última es una ventaja sobre el protocolo FTP común, ya que no dispone de ningún crédito para incluir archivos en la fecha original.
- Los programas de SFTP ofrecen para los clientes que los utilizan una interfaz interactiva similar a la de los tradicionales programas de FTP.

Uso del comando SFTP

- Puede ser usada para abrir una sesión segura interactiva de FTP. Es similar a FTP excepto que utiliza una conexión cifrada segura.

- Una vez autenticado, podrá utilizar un conjunto de comandos similar al conjunto utilizado por el comando FTP.
- Ejecutando el comando *man sftp* en el intérprete de comandos, se puede obtener un listado de todos los comandos.

VSFTPD (Very Secure FTP Daemon)

Es un equipamiento lógico utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente porque sus valores predeterminados son muy seguros, por lo que dejar esos valores no representaría ningún problema, además de la sencillez para su configuración personalizada cuando es requerido. En la actualidad se estima que VSFTPD podría ser quizá el servidor FTP más seguro del mundo.

Es un servidor FTP seguro y rápido distribuido bajo la licencia GPL para sistemas Unix incluido GNU/Linux. Fue diseñado e implementado enfocándose en la seguridad. Emplea técnicas de codificación segura para resolver los buffers overflows.

Características

- Soporte para direcciones IP virtuales
- Soporte para usuarios virtuales
- Se ejecuta de manera independiente o a través de inetd (Super Servidor de Internet)
- Poderosa configuración para cada usuario
- Soporte para el control de ancho de banda
- Límites para direcciones IP
- Soporte para IPv6
- Soporte de encriptación a través de SSL

TFTP (Trivial File Transfer Protocol – Protocolo de Transferencia de Archivos Trivial)

Es un protocolo de transferencia de archivos asociado al puerto 69 y basado en UDP que no proporciona ninguna seguridad (ver figura 9.4.2). Por lo tanto, en la mayoría de sistemas es obligatorio que este servicio esté desactivado; su uso principal es el arranque de estaciones diskless o de routers a través de la red, ya que la simpleza del protocolo permite implementarlo en un chip, y sólo en ese caso se ofrece el servicio.

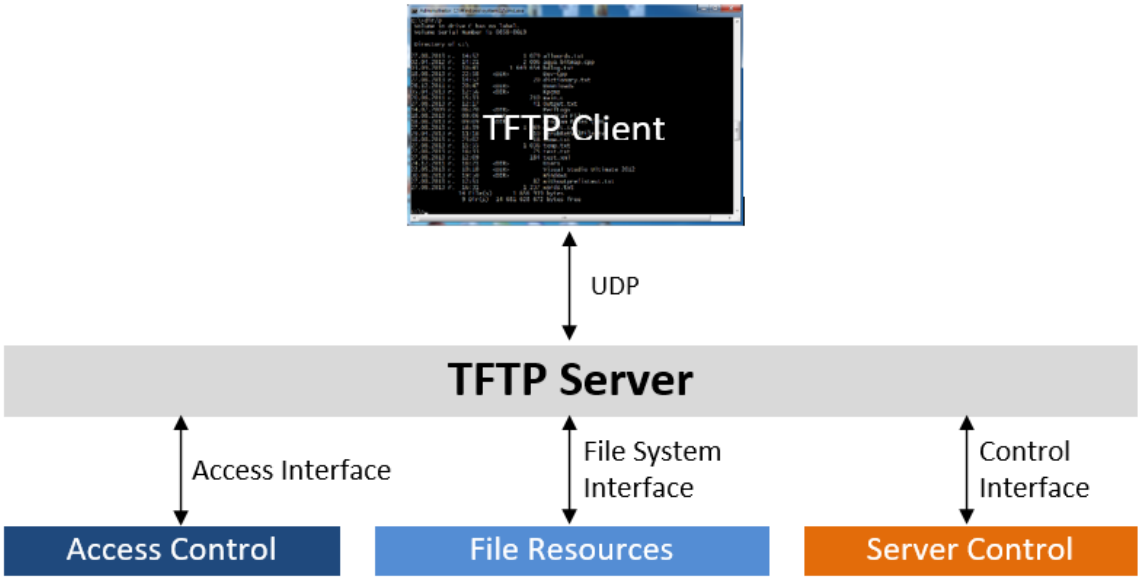


Figura 9.4.2. Conexión TFTP.

Características

- Utiliza UDP (en el puerto 69) como protocolo de transporte
- No puede listar el contenido de los directorios
- No existen mecanismos de autenticación o cifrado
- Se utiliza para leer o escribir archivos de un servidor remoto
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos “ascii" e "imagen" (binario) del protocolo FTP

Existen cinco tipos de paquetes:

1. Petición de lectura (RRQ)
2. Petición de escritura (WRQ)
3. Datos (DATA)
4. Reconocimiento (ACK)
5. Error (ERROR)

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.
- B responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.
- La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.
- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

9.5 Correo electrónico

IMAP (Internet Message Acces Protocol – Protocolo de Acceso a Mensajes de Internet)

IMAP ofrece la posibilidad de administrar e-mails directamente en el servidor de e-mail, es decir, si se elige el protocolo IMAP para establecer una cuenta de correo en el programa de e-mail, los correos que se reciban no se descargarán en el ordenador, sino que simplemente se recibirá una lista de los mensajes y sus correspondientes asuntos. Generalmente sólo aparecerán los encabezamientos de los e-mails (esta opción también podrá modificarse en los respectivos programas de e-mail). Además, se puede crear una carpeta en el servidor de e-mail y desplazar ahí mensajes.

Ventajas al utilizar IMAP:

- Poder acceder a los e-mails desde cualquier ordenador
- Poder compartir un buzón de correo con otros usuarios
- IMAP permite crear carpetas y subcarpetas en el servidor de forma rápida y sencilla. Las carpetas creadas con los programas de e-mail se encontrarán en realidad en el servidor
- Se pueden llevar a cabo tareas como buscar o clasificar con ordenadores que no tengan mucha potencia, ya que la acción tiene lugar en el servidor y no en el PC local
- Además, el servidor IMAP soporta extensiones IDLE, es decir, los nuevos e-mails recibidos se mostrarán como no leídos en la bandeja de entrada y se recibirá un aviso.

POP

POP se pone en contacto con el servicio de correo electrónico y descarga todos los mensajes nuevos de él. Una vez que se descargan en su equipo PC, se eliminan del servicio de correo electrónico. Esto significa que después de descargar el correo electrónico, solo se puede obtener acceso a él desde el mismo equipo. Si se intenta obtener acceso al correo electrónico desde otro dispositivo, los mensajes que haya descargado anteriormente no estarán disponibles.

SMTP (Simple Mail Transport Protocol - Protocolo Simple de Transferencia de Correo)

Es un protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras (ver figura 9.5.1). Está definido en el RFC 821 y 2821. Este servicio se encuentra por defecto en el puerto 25.

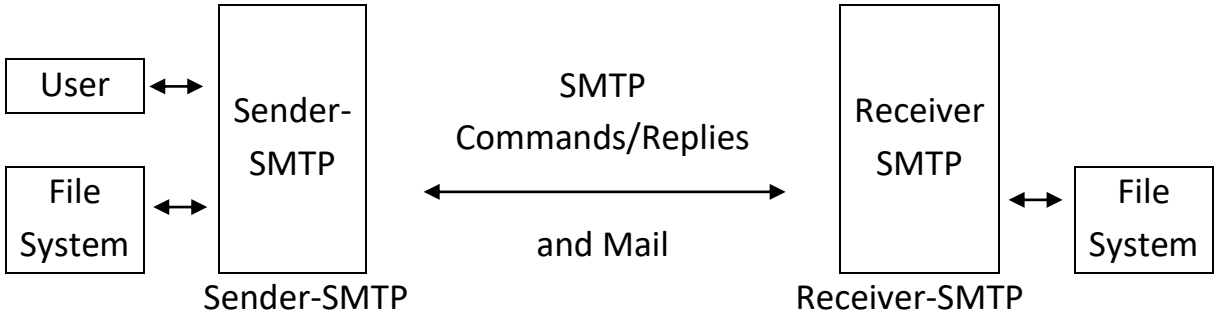


Figura 9.5.1. Representación de la conexión SMTP.

Códigos de estado SMTP

- **2XX.** La operación solicitada mediante el comando anterior ha sido concluida con éxito.
- **3XX.** La orden ha sido aceptada, pero el servidor está pendiente de que el cliente le envíe nuevos datos para terminar la operación.
- **4XX.** Para una respuesta de error, pero se espera a que se repita la instrucción.
- **5XX.** Para indicar una condición de error permanente, por lo que no debe repetirse la orden.

Los servidores y clientes más comunes y conocidos están representados en la tabla 9.5.1.

Tabla 9.5.1. Ejemplo de servidores y clientes SMTP.

Servidores	Clientes
Sendmail Qmail PostFix Exchange	Pine Mailx Outlook Eudora Elm Incredimail Lotus Notes Thunderbird Windows Mail Gmial SquirrelMail

9.6 Protocolo de autenticación

NIS (Network Information Service – Sistema de Información de Red)

Originalmente NIS se llamaba Páginas Amarillas (Yellow Pages), o YP, que todavía se utiliza para referirse a él. Desafortunadamente, ese nombre es una marca registrada de Orange Spain, que exigió a Sun abandonar ese nombre. Sin embargo, YP permanece como prefijo en los nombres de la mayoría de las órdenes relacionadas con NIS, como ypserv e ypbind.

NIS (Network Information Service – Sistema de Información de Red) es el nombre del protocolo de servicios de directorios cliente-servidor. Su función principal es el envío de datos de configuración en sistemas distribuidos tales como nombre de usuarios y host entre computadoras en una red. Consta de un servidor, varias herramientas de administración y una biblioteca de la parte cliente. Este protocolo fue desarrollado por Sun Microsystems.

Sun Microsystems llega a la concusión de realizar este protocolo, ya que permitiría mayor distribución de información a todos los nodos de su red, observando la carencia existente bajo DNS la cual brinda una información limitada solo prestándole importancia a la correspondencia entre el nombre del nodo y la dirección IP siendo casi incoherente configurar el DNS cuando no existiese conectividad a internet en una determinada administración de una LAN. El sistema de Información de Red brinda prestaciones de acceso a base de datos genéricas pudiendo distribuir la información contenida en los diferentes ficheros a todos los nodos de su red, pareciendo así una red individual con las mismas cuentas en todos sus nodos.

La expansión de este protocolo ha estado disponible en todas las distribuciones de Unix, ha estado referenciada a su vez bajo dominio público gracias a implementaciones libres existentes en su mayoría donadas por Sun Microsystems.

Una de las ventajas de NIS frente a otros sistemas de validación de usuarios, es que utiliza la base de usuarios */etc/passwd*, estándar en estos sistemas. Puede ser visto entonces como una forma de exponer los usuarios/clave de un host para que puedan validar en máquinas remotas.

LDAP (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorios)

Es un conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de la red. Está basado en el estándar X.500 para compartir directorios, pero es menos complejo e intensivo en el uso de recursos. Por esta razón, a veces se habla de LDAP como "X.500 Lite." El estándar X.500 es un directorio que contiene información de forma jerárquica y categorizada, que puede incluir nombres, directorios y números telefónicos.

LDAP organiza la información en un modo jerárquico usando directorios. Estos directorios pueden almacenar una gran variedad de información y se pueden incluso usar de forma similar al Servicio de información de red (NIS), permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina en la red acreditada con LDAP.

Sin embargo, en la mayoría de los casos, LDAP se usa simplemente como un directorio telefónico virtual, permitiendo a los usuarios acceder fácilmente la información de contacto de otros usuarios. Pero LDAP va mucho más lejos que un directorio telefónico tradicional, ya que es capaz de propagar su consulta a otros servidores LDAP por todo el mundo, proporcionando un repositorio de información ad-hoc global. Sin embargo, en este momento LDAP se usa más dentro de organizaciones individuales, como universidades, departamentos del gobierno y compañías privadas.

LDAP es un sistema cliente/servidor. El servidor puede usar una variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápidas y en gran volumen. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede, o bien consultar un directorio, o intentar modificarlo. En el evento de una consulta, el servidor, puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta. Si la aplicación cliente está intentando modificar información en un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información.

En LDAP, las entradas están organizadas en una estructura jerárquica en árbol. Tradicionalmente, esta estructura reflejaba los límites geográficos y organizacionales. Las

entradas que representan países aparecen en la parte superior del árbol. Debajo de ellos, están las entradas que representan los estados y las organizaciones nacionales. Debajo de estás, pueden estar las entradas que representan las unidades organizacionales, empleados, impresoras, documentos o todo aquello que pueda imaginarse (ver figura 9.6.1).

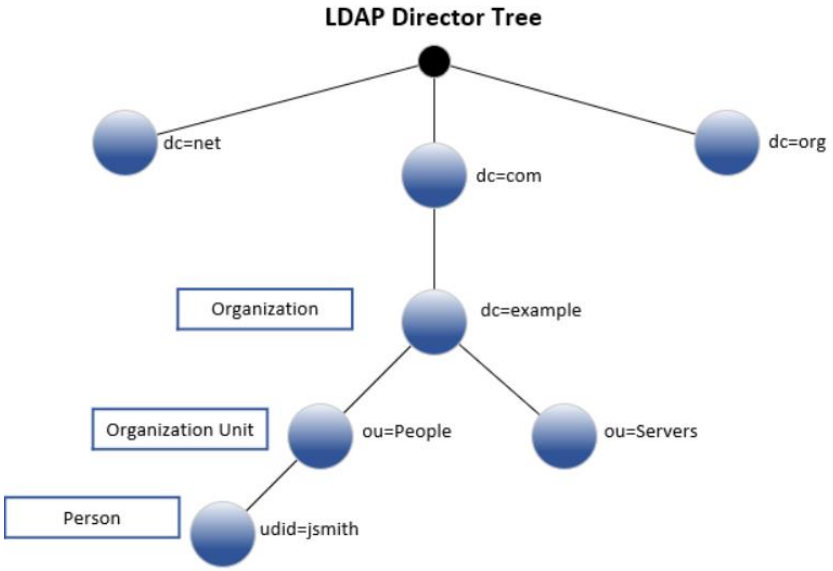


Figura 9.6.1. Estructura en árbol de directorios por LDAP.

Kerberos

La seguridad e integridad de sistemas dentro de una red puede ser complicada. Puede ocupar el tiempo de varios administradores de sistemas sólo para mantener la pista de cuáles servicios se están ejecutando en una red y la manera en que estos servicios son usados. Más aún, la autenticación de los usuarios a los servicios de red puede mostrarse peligrosa cuando el método utilizado por el protocolo es inherentemente inseguro, como se evidencia por la transferencia de contraseñas sin encriptar sobre la red bajo los protocolos FTP y Telnet. Kerberos es una forma eliminar la necesidad de aquellos protocolos que permiten métodos de autenticación inseguros, y de esta forma mejorar la seguridad general de la red. Su logo se muestra en la figura 9.6.2.

Figura 9.6.2. Kerberos.

Kerberos es un protocolo de seguridad creado por MIT que usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

Los servicios de redes más convencionales usan esquemas de autenticación basados en contraseñas. Tales esquemas requieren que cuando un usuario necesita una autenticación en un servidor de red, debe proporcionar un nombre de usuario y una contraseña. Lamentablemente, la información de autenticación para muchos servicios se transmite sin estar cifrada. Para que un esquema de este tipo sea seguro, la red tiene que estar inaccesible a usuarios externos, y todos los usuarios de la red deben ser de confianza.

Aún en este caso, una vez que la red se conecte a la Internet, ya no puede asumir que la red es segura. Cualquier intruso del sistema con acceso a la red y un analizador de paquetes puede interceptar cualquier contraseña enviada de este modo, comprometiendo las cuentas de usuarios y la integridad de toda la infraestructura de seguridad.

El primer objetivo de Kerberos es el de eliminar la transmisión a través de la red de información de autenticación. Un uso correcto de Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en la red.

Un servidor Kerberos se denomina KDC (Kerberos Distribution Center), y provee dos servicios fundamentales: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). El primero tiene como función autenticar inicialmente a los clientes y proporcionarles un ticket para comunicarse con el segundo, el servidor de tickets, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece un servicio. Además, el servidor posee una base de datos de sus clientes (usuarios o programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el cliente al que pertenece. La arquitectura de Kerberos está basada en tres objetos de seguridad: clave de sesión, ticket y autenticador (ver figura 9.6.3).

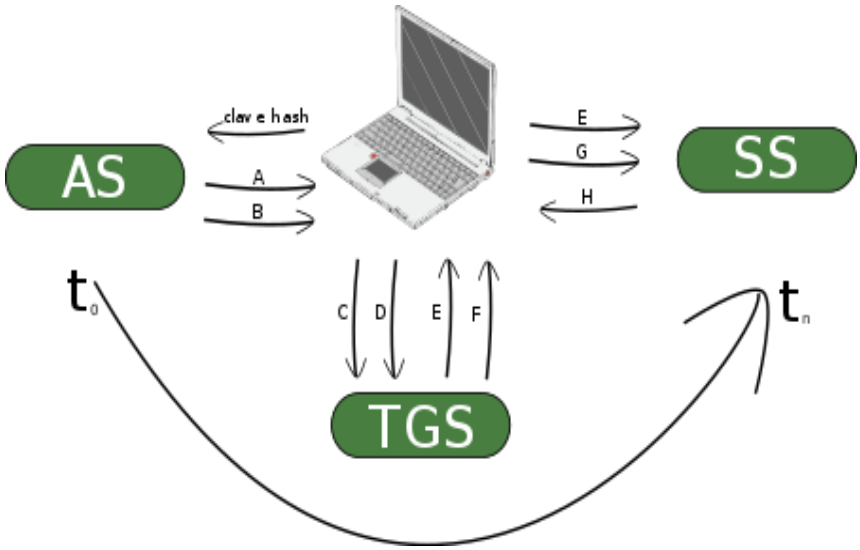


Figura 9.6.3. Servicios del servidor Kerberos.

- La clave de sesión es una clave secreta generada por Kerberos y expedida a un cliente para uso con un servidor durante una sesión de trabajo.
- El ticket es un testigo expedido a un cliente del servicio de tickets de Kerberos para solicitar los servicios de un servidor. El ticket garantiza que el cliente ha sido autenticado recientemente.
- El autenticador es un testigo construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación. Sólo puede ser utilizado una vez.

RADIUS (Remote Access Dial In User Service – Protocolo de Servicio de Usuario de Acceso Telefónico)

Es un protocolo que destaca sobre todo por ofrecer un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red.

La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Generalmente, el protocolo RADIUS se considera un servicio sin conexión. Los problemas relacionados con la disponibilidad de los servidores, la retransmisión y los tiempos de espera son tratados por los dispositivos activados por RADIUS en lugar del protocolo de transmisión.

El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso de daemon que se ejecuta en UNIX o una máquina del Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados y a los actos en la respuesta. Los servidores de RADIUS reciben las

peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación (ver figura 9.6.4).

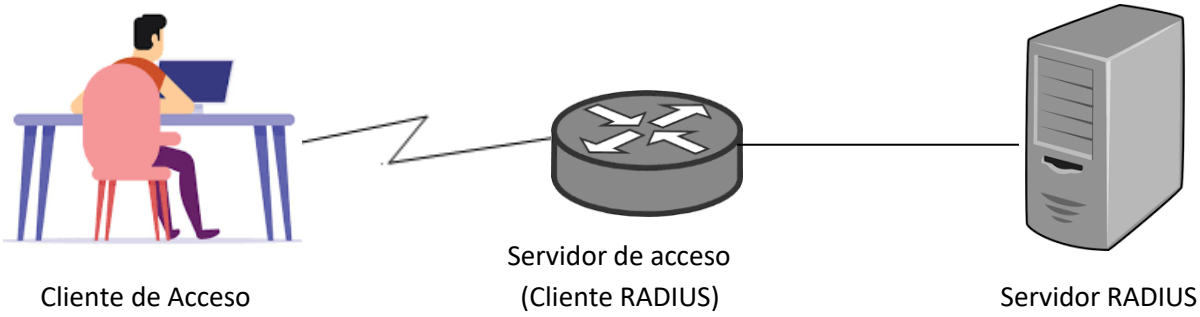


Figura 9.6.4. Funcionamiento de RADIUS.

1. El usuario inicia la autenticación PPP al NAS.
2. NAS le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña [PAP]) o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña [CHAP]).
3. Contestaciones del usuario.
4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.
5. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar.
6. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar.

El servidor RADIUS puede soportar varios métodos para autenticar un usuario. Cuando se proporciona el nombre de usuario y la contraseña original dados por el usuario, puede soportar el login PPP, PAP o de la GRIETA, de UNIX, y otros mecanismos de autenticación.

Comúnmente, el ingreso de un usuario al sistema consiste en un pedido (Solicitud de acceso) desde el NAS hacia el servidor RADIUS y de una correspondiente respuesta (Aceptación de acceso o Rechazo de acceso) desde el servidor. El paquete access-request contiene el nombre de usuario, la contraseña encriptada, la dirección IP NAS, y el puerto. El Early Deployment del RADIUS fue hecho usando el número del puerto 1645 UDP, que está en conflicto con el servicio del “datametrics”. Debido a este conflicto, el RFC 2865 asignó oficialmente el número del puerto1812 para el RADIUS. El formato del pedido proporciona asimismo información sobre el tipo de sesión que el usuario desea iniciar. Por ejemplo, si la interrogación se presenta en el modo de carácter, la inferencia es “tipo de

servicio = EXEC-usuario," pero si la petición se presenta en el PPP en modo de paquete, la inferencia es "tipo deservicio = Usuario entramado" y el "tipo de Framed =PPP".

Cuando el servidor de RADIUS recibe el pedido de acceso del NAS, busca una base de datos para el nombre de usuario enumerado. Si el nombre de usuario no existe en la base de datos, se carga un perfil predeterminado o el servidor RADIUS inmediatamente envía un mensaje Access-Reject (acceso denegado). Este mensaje de acceso rechazado puede estar acompañado de un mensaje de texto que indique el motivo del rechazo.

En RADIUS, la autenticación y la autorización están unidas. Si se encuentra el nombre de usuario y la contraseña es correcta, el servidor RADIUS devuelve una respuesta de Acceso-Aceptar e incluye una lista de pares de atributo-valor que describe los parámetros que deben usarse en esta sesión (ver figura 9.6.5). Los parámetros comunes incluyen el tipo de servicio (shell o entramado), el tipo de protocolo, la dirección IP para asignar el usuario (estática o dinámica), la lista de acceso a aplicar o una ruta estática para instalar en la tabla de ruteo de NAS. La información de configuración en el servidor RADIUS define qué se instalará en el NAS.

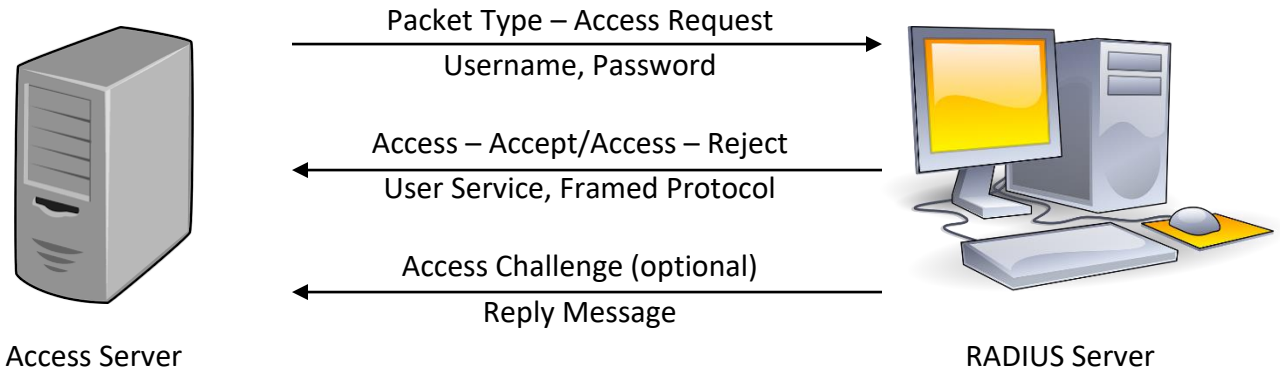


Figura 9.6.5. Proceso de autenticación de RADIUS.

Portal captivo o cautivo

Es una página de inicio de sesión personalizado en redes empresariales que los usuarios invitados deben pasar antes de poder conectarse a la red Wi-Fi. Aeropuertos, bares y hoteles son los lugares más comunes donde se utiliza esta función, pero realmente cualquier negocio puede beneficiarse de las ventajas que un portal cautivo proporciona. Es una solución dual para una seguridad y marketing avanzados.

Normalmente un portal cautivo presenta al usuario los términos de servicio y este debe aceptarlos expresamente antes de poder acceder al hotspot Wi-Fi. En algunos casos el portal cautivo puede requerir de una contraseña. Medidas como esta garantizan una seguridad jurídica en caso de que se cometa cualquier delito digital en internet. Otras

funciones de seguridad protegen a los recursos de la empresa presentes en la red. El uso de un portal cautivo brinda además un mayor control sobre el ancho de banda, ofreciendo la posibilidad de limitar de forma personalizada los tiempos de conexión a la red de cada usuario.

En el aspecto comercial los portales cautivos suponen una oportunidad para llevar a cabo un marketing natural y apropiado; facilitan una captación más profunda del cliente en un punto crítico de su experiencia en la red y es un medio muy poderoso que puede utilizarse para una gran variedad de necesidades comerciales. Un ejemplo de un portal cautivo está representado en la figura 9.6.6.

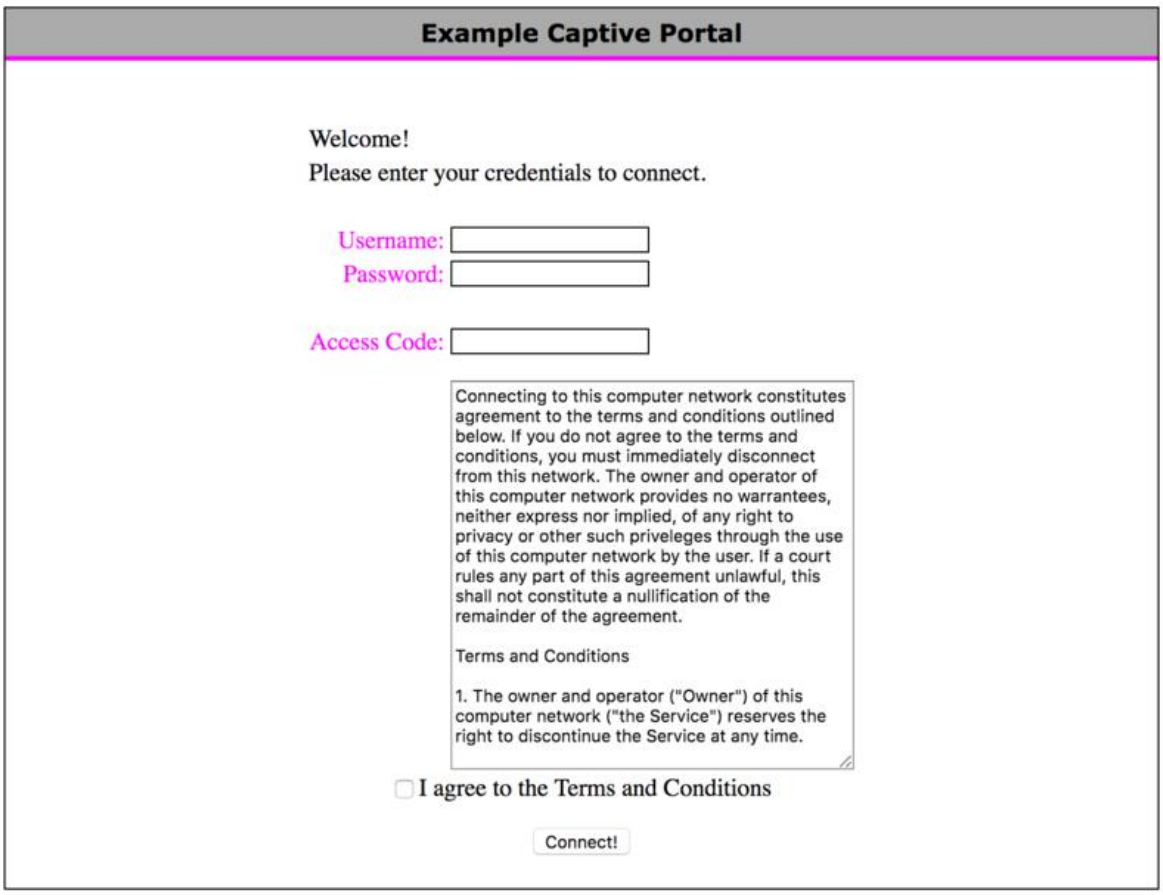


Figura 9.6.6. Ejemplo de portal cautivo.

9.7 Mecanismos de seguridad

Firma digital

La firma digital es el tipo de firma electrónica más avanzado y seguro, que permite cumplir con los requisitos legales y normativos más exigentes al ofrecer los más altos niveles de

seguridad sobre la identidad de cada firmante y la autenticidad de los documentos que firman.

Las firmas digitales utilizan un ID digital basado en certificado que emite una autoridad de certificación (CA) acreditada o un proveedor de servicios de confianza (TSP). De este modo, cuando se firma un documento de forma digital, la identidad acaba vinculada al individuo de forma exclusiva, la firma se asocia al documento mediante cifrado y todo puede verificarse con la tecnología subyacente que se conoce como "infraestructura de clave pública" (PKI).

La firma digital se ha concebido para evitar falsificaciones. Se crea con los mayores niveles de seguridad, que, además, la protegen y la amparan, desde el momento en que se emite el certificado hasta el momento en que se archivan los documentos firmados, y mucho más.

Certificado digital

El certificado digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. Además, permite la firma electrónica de documentos. El receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma.

El certificado digital permite cifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de la misma.

En definitiva, la principal ventaja es que disponer de un certificado ahorrará tiempo y dinero al realizar trámites administrativos en Internet, a cualquier hora y desde cualquier lugar.

Un certificado digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja.

El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

9.8 Seguridad a nivel de capa de aplicación

La capa de aplicación en la pila TCP/IP, y sus capas equivalentes en el modelo OSI, se ocupan del manejo de la sesión y las aplicaciones que se ejecutan en el equipo.

Aquí encontramos una variada combinación de protocolos que permiten a los terminales acceder a numerosos servicios. Entre ellos, SMTP, POP, IMAP, DNS, HTTP, HTTPS, DHCP, FTP, TFTP. LA configuración de estos servicios está sujeta a la experiencia del administrador, y se debe ser cuidadoso para prevenir que malas configuraciones se vuelvan una puerta de acceso a la red.

La implantación de un firewall de alto nivel permite un mayor control del tráfico de red. A diferencia de los firewalls de capa de red o de capa de transporte, aquellos que trabajan sobre la capa de aplicación permiten filtrar paquetes con base a un gran abanico de opciones, incluyendo una vasta diversidad de protocolos.

Además, en esta capa encontramos Sistemas de Detección de Intrusiones IDS (Intrusion Detection System), Sistemas de Prevención de Intrusiones IPS (Intrusion Prevention System), y demás soluciones integrales de seguridad. Estas aplicaciones actúan sobre la pila TCP/IP completa, pudiendo detectar comportamientos peligrosos según múltiples criterios, emitiendo las alertas pertinentes.

De esta manera, con un firewall vamos a poder detectar que de forma externa algún atacante está tratando de realizar acciones maliciosas, y será posible evitarlo. Además, de forma complementaria, una solución antivirus brinda las herramientas para evitar que un archivo recibido por correo electrónico, a través de un dispositivo USB o descargado directamente de Internet ejecute alguna acción maliciosa que ponga en riesgo la información.

IDS (Intrusion Detection System)

Cuando hablamos de IDS nos referimos a un sistema que se va a encargar de monitorear el comportamiento de una red para detectar e informar sobre posibles intrusiones no autorizadas, con lo cual se puede prevenir que se vea afectada la integridad de la red.

Un IDS está monitoreando la red para detectar cuando un sistema está realizando una actividad sospechosa a través de examinar el tráfico de red y las llamadas al sistema. Por su parte, el firewall va a establecer cuando una conexión entre dos equipos a través de Internet no está de acuerdo con las políticas de seguridad establecidas para ese entorno de red. Y con un antivirus se puede determinar cuando en un equipo o servidor un archivo en particular puede realizar actividades maliciosas que puedan afectar la seguridad de la información.

IPS (Intrusion Prevention System)

IPS es una herramienta muy similar a IDS, pero que además de alertar sobre las detecciones también puede bloquearlas o prevenirlas en el momento de su detección.

Otro aspecto relevante una vez alcanzado este nivel de abstracción es la educación de los usuarios, y la definición de políticas de seguridad para el departamento de IT. La seguridad de los equipos informáticos resulta un binomio entre el correcto despliegue de las barreras técnicas de defensa, y la instrucción del usuario del equipo, y los usuarios administrativos que sobre él poder tienen. No podemos considerar sólo una de estas artistas.

Por otra parte, las soluciones antivirus van a permitir detectar cuándo algún archivo, correo electrónico, página web o cualquier otro recurso utilizado en la computadora está relacionado con algún tipo de código malicioso. Una buena solución antivirus debe detectar cuándo un archivo que se va a ejecutar en el dispositivo, sea móvil o de escritorio, tiene algún tipo de comportamiento malicioso para no permitir su ejecución, y por lo tanto prevenir el daño o robo de la información.

Conclusión

Ahora que se conocen los conceptos necesarios que definen lo que es una red de datos, la importancia de ésta y su estructura, se puede concluir que el diseño e implementación de una, es una actividad que requiere de muchas consideraciones, no sólo para que ésta sea funcional, sino también para que sea una red segura en todos los ámbitos posibles, como por ejemplo la implementación de protocolos de autenticación mediante contraseñas, autenticación biométrica o seguridad física.

Sin embargo, como se mencionó a lo largo del desarrollo de estos materiales, las redes de datos se integran de componentes tanto de hardware como de software, y es justo en este segundo grupo donde el trato, configuración, y gestión de los recursos recae principalmente en aspectos digitales, por lo que el énfasis en seguridad informática es resaltante para los administradores de la red.

Las redes de datos en la actualidad se encuentran prácticamente en todas las actividades de la sociedad, empresas, instituciones, organismos y gobiernos que entre otros, hacen uso de las redes y sus servicios día con día y para que las actividades se realicen de manera correcta es necesario que los responsables de ellas desde su instalación cuando son nuevas, o cuando se está en un proceso de actualización de la red deben considerar además de su correcta instalación y configuración, los aspectos importantes de la seguridad de la información en todas y cada una de las capas que integran a las redes.

Así, un buen administrador de redes debe de ser capaz de hacer notar los aspectos que pudieran estar haciendo falta en las redes ya instaladas para que además de llevar a cabo la gestión adecuada para su buen uso, también esté en condiciones de realizar una mejora y actualización a través de un mantenimiento perfectivo para que, al final de la implementación, ésta sea una red funcional y protegida en todo momento de cualquier

persona, sistema o proceso que intentara dañar o mal utilizar de alguna forma la red instalada.

Seguro de que este material será de gran apoyo a las siguientes generaciones que cursen o impartan la asignatura Redes de Datos Seguras, y para que esté a disposición de todos aquellos que deseen utilizarlo, estará publicado en la página del laboratorio de redes y seguridad.

TRABAJO FUTURO

Uno de los compromisos de la carrera de Ingeniería en Computación es revisar y actualizar periódicamente su plan de estudios a fin de que éste siempre esté vigente y los contenidos de las asignaturas estén orientados a brindar una formación integral con temas de actualidad, de manera que los temarios de las asignaturas se modifican con cierta regularidad y por ello, se tiene el compromiso de llevar un seguimiento a los cambios que en su momento presente el temario de Redes de Datos Seguras, a fin de hacer las modificaciones necesarias y actualizar el contenido del presente trabajo, además de siempre considerar los comentarios de los estudiantes que hagan uso de este material de apoyo.

Referencias

Tema 1:

Arango, A. A. Armando. (2016, 12 julio). funciones de las redes de datos. Recuperado 26 marzo, 2020, de https://prezi.com/jnhh-1uwqb-a/funciones-de-las-redes-de-datos/

Colaboradores de Wikipedia. (2020, 10 marzo). Seguridad de redes. Recuperado 26 marzo, 2020, de https://es.wikipedia.org/wiki/Seguridad_de_redes

EcuRed. (s.f.). Redes de datos - EcuRed. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Redes_de_datos

redes de datos [Publicación en un blog]. (2014, 4 diciembre). Recuperado 26 marzo, 2020, de http://hellynsemartinez.blogspot.com/

Upelmaturintv, U. (2010, 19 julio). redes de informatica y comunicacion de datos [Archivo de vídeo]. Recuperado 26 marzo, 2020, de https://www.youtube.com/watch?v=9RB4pTOBK8Q

Wikiversidad. (2019, 11 noviembre). Redes de datos. Recuperado 26 marzo, 2020, de https://es.wikiversity.org/wiki/Redes_de_datos

¿Qué es una red informática? - RedUSERS. (2013, 15 febrero). Recuperado 26 marzo, 2020, de http://www.redusers.com/noticias/que-es-una-red-informatica/

Tema 2:

1&1 IONOS Inc. (2019, 6 septiembre). Los tipos de redes más conocidos. Recuperado 26 marzo, 2020, de https://www.ionos.mx/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/

Carlos Villagómez, C. V. (2018, 20 febrero). TCP/IP. Recuperado 26 marzo, 2020, de https://es.ccm.net/contents/282-tcp-ip

EcuRed. (s.f.). NetBios. Recuperado 26 marzo, 2020, de https://www.ecured.cu/NetBios

IBM. (s.f.). Protocolos TCP/IP. Recuperado 26 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_protocols.htm

IEEE Sección México | Home. (s.f.). Recuperado 26 marzo, 2020, de http://ieee.org.mx/IEEE/IEEE_Seccion_Mexico.html

ITU. (s.f.-b). UIT: Comprometida para conectar el mundo. Recuperado 26 marzo, 2020, de https://www.itu.int/es/Pages/default.aspx

James Tiberius Kirk, J. T. K. (2016, 12 noviembre). ISO 7498-2. Recuperado 26 marzo, 2020, de https://prezi.com/mjji1z0_lqch/iso-7498-2/

Matilde Amescua, M. A. (2015). NORMAS Y ESTANDARES DEL CABLEADO ESTRUCTURADO. Recuperado 26 marzo, 2020, de https://slideplayer.es/slide/1094384/

Netware. (s.f.). Recuperado 26 marzo, 2020, de http://redespagina.tripod.com/netware.htm

Normas EIA/TIA [Publicación en un blog]. (2012, 22 octubre). Recuperado 26 marzo, 2020, de http://lilwatne.blogspot.com/

Redesbasico150. (2002). Estándares TIA EIA. Recuperado 26 marzo, 2020, de https://sites.google.com/site/redesbasico150/introduccion-a-los-estandares-de-cableado/estandares-tia-eia

SNA. (s.f.). Recuperado 26 marzo, 2020, de http://redespagina.tripod.com/sna.htm

AppleTalk and the OSI Model(IM:N). (s. f.). Recuperado 6 de junio de 2020, de http://mirror.informatimago.com/next/developer.apple.com/documentation/mac/Networking/Networking-21.html

Tema 3:

ANSI/TIA/EIA 607 - Diseño de Data Centers - UNFV. (s.f.). Recuperado 26 marzo, 2020, de http://bracamontedatacenters.weebly.com/ansitiaeia-607.html

Asis Rodríguez, A. R. (2012, 10 junio). Fibra Óptica, qué es y cómo funciona. Recuperado 26 marzo, 2020, de https://www.fibraopticahoy.com/fibra-optica-que-es-y-como-funciona/

Cable de datos de par trenzado STP Cat5e de Gotham Audio. (2014, 15 abril). Recuperado 26 marzo, 2020, de http://telcoavi.es/blog/cable-de-datos-de-par-trenzado-stp-cat5e-de-gotham-audio/

CABLEADO ESTRUCTURADO-: NORMA EIA/TIA 568. (s.f.). Recuperado 26 marzo, 2020, de http://www.cgtic.unacar.mx/normatividad/norma568.pdf

Carlos Villagómez, C. V. (2017a, 22 septiembre). Transmisión de datos - Cableado. Recuperado 26 marzo, 2020, de https://es.ccm.net/contents/685-transmision-de-datos-cableado

Carlos Villagómez, C. V. (2017b, 12 diciembre). Equipos de red - Repetidor. Recuperado 26 marzo, 2020, de https://es.ccm.net/contents/298-equipos-de-red-repetidor

Cervi. (s.f.). Sistema de cableado UTP Cat.6A. Recuperado 26 marzo, 2020, de https://www.cervi.es/ES/3-productos/36--sistemas-de-cableado-y-racks/270-sistema-de-cableado-utp-cat6a.html

Colaboradores de Wikipedia. (2012, 22 mayo). Radiocomunicación por microondas. Recuperado 26 marzo, 2020, de https://es.wikipedia.org/wiki/Radiocomunicaci%C3%B3n_por_microondas

dispositivos activos y pasivos [Publicación en un blog]. (2013, 27 mayo). Recuperado 26 marzo, 2020, de http://activos-pasivos.blogspot.com/

DISPOSITIVOS DE INTERCONEXION DE REDES. (2011, 8 junio). Recuperado 26 marzo, 2020, de https://cecy09.wordpress.com/dispositivos-de-interconexion-de-redes/

Dominic Francis, D. F. (s.f.). Tipos de cables UTP. Recuperado 26 marzo, 2020, de https://techlandia.com/tipos-cables-utp-lista_85429/

EcuRed. (s.f.-a). Red inalámbrica. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Red_inal%C3%A1mbrica

EcuRed. (s.f.-b). Frame relay. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Frame_relay

EcuRed. (s.f.-c). Cable coaxial. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Cable_coaxial

EcuRed. (s.f.-d). Fibra óptica. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Fibra_%C3%B3ptica

EIA-569. (2012, 19 enero). Recuperado 26 marzo, 2020, de https://es.slideshare.net/neyneyney/eia569

Estándares de comunicaciones RS232, RS422, RS485. (s.f.). Recuperado 26 marzo, 2020, de http://www.puntoflotante.net/RS485.htm

Grupo PowerData. (s.f.). Seguridad de datos: En qué consiste y qué es importante en tu empresa. Recuperado 26 marzo, 2020, de https://www.powerdata.es/seguridad-de-datos

IBM. (s.f.). Descubrimiento de conectividad entre dispositivos ATM. Recuperado 26 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/SSSHRK_4.2.0/disco/reference/dsc_agents_for_atm_devs.html

Información UTP Cat.8. (2017, 6 junio). Recuperado 26 marzo, 2020, de https://www.openup.es/informacion-utp-cat-8/

INFRARROJO(IRDA). (s.f.). Recuperado 26 marzo, 2020, de http://tsusistemas.tripod.com/julia1.html

La instalación física de una red. (s.f.). Recuperado 26 marzo, 2020, de http://spain-s3-mhe-prod.s3-website-eu-west-1.amazonaws.com/bcv/guide/capitulo/8448180828.pdf

Las Microondas como Medio de Transmisión [Publicación en un blog]. (s.f.). Recuperado 26 marzo, 2020, de https://telematicaupoliyolanda.wordpress.com/las-microondas-como-medio-de-transmision/

Martínez Lugo Alfonso, M. L. A. (2009, 13 marzo). Medios De Enlace [Publicación en un blog]. Recuperado 26 marzo, 2020, de http://martinezlugoalfonso.blogspot.com/2009/03/medios-de-enlace.html

Ms. González, G. (2013, 8 noviembre). El switch: cómo funciona y sus principales características | Redes Telemáticas. Recuperado 26 marzo, 2020, de http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

Paula Torres, P. T. (2015, 11 septiembre). ANSI/TIA/EIA - 606 - A. Recuperado 26 marzo, 2020, de https://prezi.com/_nrrnyiuknlb/ansitiaeia-606-a/

Ramón Jesús Millán Tejedor, R. J. M. T. (2009). ATM (Asyncronous Transfer Mode). Recuperado 26 marzo, 2020, de https://www.ramonmillan.com/tutoriales/atm.php

Redes de computadoras. (s.f.). 1.3 Medios de transmisión. Recuperado 26 marzo, 2020, de https://sites.google.com/site/sabyrodriguezgamez/unidad1/1-3-medios-de-transmision

RS-449. (s.f.). Recuperado 26 marzo, 2020, de https://esacademic.com/dic.nsf/eswiki/980118

Seguridad física. (s.f.). Recuperado 26 marzo, 2020, de https://www.uv.es/sto/cursos/icssu/html/ar01s04.html

Tecnar - Cartagena, T. C. (2014, 24 agosto). Dispositivos Activos y Pasivos - Cableado Estructurado. Recuperado 26 marzo, 2020, de https://es.slideshare.net/fernandobogallodelassalas/taller-1-38294348

Tecnonología Fácil. (2016, 18 noviembre). Cable UTP o cable de red. Recuperado 26 marzo, 2020, de https://tecnologia-facil.com/que-es/cable-utp-cable-de-red/

Textos Científicos. (2005, 19 noviembre). Fibra óptica. Recuperado 26 marzo, 2020, de https://www.textoscientificos.com/redes/fibraoptica

Vinicio Monge, V. M. (2015). Medios de Transmisión Redes de Computadoras. Recuperado 26 marzo, 2020, de https://slideplayer.es/slide/1094146/

¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? (2017, 6 julio). Recuperado 26 marzo, 2020, de https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

Tema 4:

1&1 IONOS Inc. (2018a, 2 julio). CSMA/CA: protocolo de acceso al medio para redes inalámbricas. Recuperado 26 marzo, 2020, de https://www.ionos.mx/digitalguide/servidores/know-how/csmaca-protocolo-de-acceso-al-medio-para-redes-inalambricas/

1&1 IONOS Inc. (2018b, 15 agosto). Ethernet (IEEE 802.3). Recuperado 27 marzo, 2020, de https://www.ionos.mx/digitalguide/servidores/know-how/ethernet-ieee-8023/

DSL - ADSL. (2010, 30 agosto). Recuperado 27 marzo, 2020, de https://es.slideshare.net/tucho235/dsl-adsl

3.6.1 Sincrona y Asincrona. (s.f.). Recuperado 27 marzo, 2020, de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/361_sincrona_y_asincrona.html

4. LAS ESPECIFICACIONES IEEE 802 - REDES LOCALES. (s.f.). Recuperado 27 marzo, 2020, de https://sites.google.com/site/milagrosysandraredeslocales/home/4-las-especificaciones-ieee-802

[Seguridad en SDLC]. (s.f.). Recuperado 27 marzo, 2020, de https://www.audea.com/seguridad-en-sdlc/

Black, U. D. (1987). *Redes de transmisión de datos y proceso distribuido* (Ed. rev.). Madrid, España: Díaz de Santos.

Capa 2 OSI | Enlace de Datos. (s.f.). Recuperado 27 marzo, 2020, de https://eltallerdelbit.com/capa-2-osi

CAPA ENLACE DE DATOS: “CONTROL DE ACCESO AL MEDIO”. (2012, 21 septiembre). Recuperado 27 marzo, 2020, de https://solucionesinfomatica.wordpress.com/2012/09/21/capa-enlace-de-datos-control-de-acceso-al-medio/

Capitulo 2. La Capa de Enlace de Datos. (s.f.). Recuperado 26 marzo, 2020, de https://sites.google.com/site/comdatosgrupo4/contenidos/cap2_capa-enlace-datos

Carlos Villagómez, C. V. (2017, 20 octubre). El protocolo ARP. Recuperado 26 marzo, 2020, de https://es.ccm.net/contents/260-el-protocolo-arp

Certsuperior. (2012, 28 mayo). Handshake: el proceso de intercambio de información privada. Recuperado 27 marzo, 2020, de https://www.certsuperior.com/handshake-el-proceso-de-intercambio-de-informacian-privada/

Colaboradores de Wikipedia. (2020, 10 febrero). IEEE 802.15 [Publicación en un blog]. Recuperado 26 marzo, 2020, de https://es.wikipedia.org/wiki/IEEE_802.15

Control de Enlace de Datos de Alto Nivel (HDLC). (s.f.). Recuperado 27 marzo, 2020, de http://www.comunidad.escom.ipn.mx/ncortez/rc/HDLC.pdf

EcuRed. (s.f.-a). Estándares Inalámbricos [Publicación en un blog]. Recuperado 26 marzo, 2020, de https://www.ecured.cu/Est%C3%A1ndares_Inal%C3%A1mbricos

EcuRed. (s.f.-b). Wired Equivalent Privacy (WPE). Recuperado 26 marzo, 2020, de https://www.ecured.cu/Wired_Equivalent_Privacy_(WPE)

EcuRed. (s.f.-c). WPA2 - EcuRed. Recuperado 26 marzo, 2020, de https://www.ecured.cu/WPA2

EcuRed. (s.f.-d). Control de acceso al medio. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Control_de_acceso_al_medio

EcuRed. (s.f.-e). Conmutación (Redes de comunicación). Recuperado 27 marzo, 2020, de https://www.ecured.cu/Conmutaci%C3%B3n_(Redes_de_comunicaci%C3%B3n)

EcuRed. (s.f.-f). Control de acceso al medio. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Control_de_acceso_al_medio

Eduardo Patricio Sánchez, E. P. S. (2010, 4 junio). Reflexiones de seguridad en capa 2 (Modelo OSI). Recuperado 27 marzo, 2020, de http://www.magazcitum.com.mx/?p=442

El ciclo SDLC en 7 fases. (2014, 14 junio). Recuperado 27 marzo, 2020, de https://www.viewnext.com/el-ciclo-sdlc-en-7-fases/

El ciclo SDLC en 7 fases. (2018, 14 junio). Recuperado 27 marzo, 2020, de https://www.viewnext.com/el-ciclo-sdlc-en-7-fases/

El control de la congestión. (s.f.). Recuperado 27 marzo, 2020, de http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/congest.html

Evelio Martinez, E. M. (2007, 11 julio). Transmisión Sincrona y Asincrona. Recuperado 27 marzo, 2020, de http://eveliux.com/mx/curso/transmisiincrona-y-asincrona.html

FDDI: FIBER DISTRIBUTED DATA INTERFACE. (s.f.). Recuperado 27 marzo, 2020, de http://www.lcc.uma.es/%7Eeat/services/fddi/fddi.htm

Fernando Saavedra, F. S. (s.f.). Seguridad en SDLC. Recuperado 27 marzo, 2020, de https://www.audea.com/es/seguridad-en-sdlc/

Formato de la Trama Ethernet. (s.f.). Recuperado 27 marzo, 2020, de http://redesdecomputadores.umh.es/enlace/ethernet/Formato_Trama_ethernet.html

IBM. (s.f.). Redes de control síncrono de enlace de datos. Recuperado 26 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzajt/rzajtsdlccon.htm

Jorge Colemanres, J. C. (2018, 3 febrero). Estándares IEEE 802 [Publicación en un blog]. Recuperado 26 marzo, 2020, de http://estandaresieee802redes.blogspot.com/

Metodo de Acceso al Medio EDIO" [Publicación en un blog]. (2009, 5 febrero). Recuperado 27 marzo, 2020, de http://accedealmedio.blogspot.com/

MODOS DE TRANSMISIÓN. (s.f.). Recuperado 27 marzo, 2020, de http://joan004.tripod.com/modtra.htm

Netspotapp software. (s.f.). Protocolos de seguridad inalámbrica: WEP, WPA, WPA2, y WPA3. Recuperado 26 marzo, 2020, de https://www.netspotapp.com/es/wifi-encryption-and-security.html

PROTOCOLO HDLC. (s.f.). Recuperado 27 marzo, 2020, de http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/28691/Redes_Cap06.pdf?sequence=6

Solucionesinfomatica. (2012, 22 septiembre). CAPA ENLACE DE DATOS: "CONTROL DE ACCESO AL MEDIO". Recuperado 27 marzo, 2020, de https://solucionesinfomatica.wordpress.com/2012/09/21/capa-enlace-de-datos-control-de-acceso-al-medio/

Tema 3: Subnivel de Control de acceso al medio (MAC). (s.f.). Recuperado 27 marzo, 2020, de http://www4.ujaen.es/~mdmolina/rrcc/Tema3MAC.pdf

WPA. (s.f.). Recuperado 26 marzo, 2020, de http://www.bdat.net/seguridad_en_redes_inalambricas/x59.html

Tema 5:

Millán Tejedor, R. (2001). El protocolo IPv6 (I). Recuperado 7 de junio de 2020, de https://www.ramonmillan.com/tutoriales/ipv6_parte1.php

Sumarización de direcciones IP [Publicación en un blog]. (s.f.). Recuperado 27 marzo, 2020, de http://blog.capaocho.net/2009/03/sumarizacion-de-direcciones-ip_10.html

¿Qué es Sumarizar y como se realiza y calcular [Publicación en un blog]. (2016, 4 marzo). Recuperado 27 marzo, 2020, de https://bloggspace.wordpress.com/2016/03/04/que-es-sumarizar-y-como-realiza-y-calcular/

2.3. Rutas estaticas predeterminadas y sumarizadas - CCNA 2. (s.f.). Recuperado 27 marzo, 2020, de https://sites.google.com/site/cursoccna22015/enrutamiento-estatico/2-3-rutas-estaticas-predeterminadas-y-sumarizadas

Denise Giusto Bilić, D. G. B. (2015, 1 julio). Cómo fortalecer las distintas capas de las redes informáticas | WeLiveSecurity. Recuperado 27 marzo, 2020, de https://www.welivesecurity.com/la-es/2015/06/01/como-fortalecer-capas-redes-informaticas/

3.1 Capa de red. (s.f.). Recuperado 27 marzo, 2020, de https://sites.google.com/site/sabyrodriguezgamez/unidad-iii/3-1-capa-de-red

Colaboradores de Wikipedia. (2013, 18 marzo). Categoría:Protocolos de nivel de red. Recuperado 27 marzo, 2020, de https://es.wikipedia.org/wiki/Categor%C3%ADa:Protocolos_de_nivel_de_red

Colaboradores de Wikipedia. (2019, 7 noviembre). Capa de red. Recuperado 27 marzo, 2020, de https://es.wikipedia.org/wiki/Capa_de_red

DHCP. (s.f.). Recuperado 27 marzo, 2020, de https://camber1redes.wordpress.com/dhcp/

DSL - ADSL. (2010, 30 agosto). Recuperado 27 marzo, 2020, de https://es.slideshare.net/tucho235/dsl-adsl

EcuRed. (s.f.-a). IPX. Recuperado 27 marzo, 2020, de https://www.ecured.cu/IPX

EcuRed. (s.f.-b). Capa de red. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Capa_de_red

EcuRed. (s.f.-c). Protocolos de red. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Protocolos_de_red

EcuRed. (s.f.-d). Protocolo RIP. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Protocolo_RIP

IBM. (s.f.-a). Autorización de acceso de lista de control de acceso. Recuperado 27 marzo, 2020, de

https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.osdevice/acl_access_auth.htm

IBM. (s.f.-b). Listas de control de accesos. Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.osdevice/acl.htm

IBM. (s.f.-c). Protocolos a nivel de red Internet. Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/protocols_internet_netlevel.htm

IBM. (s.f.-d). OSPF (Open Shortest Path First). Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_71/rzajw/rzajwospf.htm

IGMP - Protocolos de la familia Internet. (s.f.). Recuperado 27 marzo, 2020, de http://personales.upv.es/rmartin/tcpip/cap02s07.html

Luis Müller, L. M. Ing.. (2011). Seguridad en la capa de Red. – IPSec. Recuperado 27 marzo, 2020, de http://www.laminfo.com/blog/archivos/__5_unidad_V_IP_sec.pdf

Protocolos BGP, IGP y EGP [Publicación en un blog]. (s.f.). Recuperado 27 marzo, 2020, de https://grd1503687jjfdog.blogspot.com/p/protocolos-bgp-igp-y-egp.html

Tablas y tipos de enrutamiento. (s.f.). Recuperado 27 marzo, 2020, de https://docs.oracle.com/cd/E19957-01/820-2981/gdyen/index.html

Tema 6:

Capitulo 5. Análisis de Rendimiento en Redes. (s.f.). Recuperado 27 marzo, 2020, de https://sites.google.com/site/comdatosgrupo4/contenidos/cap5_arendredes

Ataques de REPLAY. (s.f.). Recuperado 27 marzo, 2020, de https://sites.google.com/site/ignaciomatillairaola/informatica/diccionario/ataques-de-replay

Capa de Transporte. (s.f.). Recuperado 27 marzo, 2020, de https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/Cap3_Transporte.pdf

CAPITULO 4 Capa de Transporte del modelo OSI. (s.f.). Recuperado 27 marzo, 2020, de https://pabloyela.files.wordpress.com/2014/02/ccna-exploration-04.pdf

Capítulo 3Capa de Transporte. (s.f.). Recuperado 27 marzo, 2020, de https://www.fing.edu.uy/tecnoinf/maldonado/cursos/redes/material/redes-transporte.pdf

Cisco. (2017, 16 enero). Administración de rendimiento: Informe oficial de Mejores Prácticas. Recuperado 27 marzo, 2020, de https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15115-perfmgmt.html

David Cantón, D. C. (2015, 9 abril). DoS: Capa de Infraestructura. Recuperado 27 marzo, 2020, de https://www.incibe-cert.es/blog/dos-capa-infraestructura

Especial Modelo OSI: Capa de Transporte - CulturaciÃ³n. (s.f.). Recuperado 27 marzo, 2020, de http://culturacion.com/especial-modelo-osi-capa-de-transporte/

IBM. (s.f.-a). Definiciones de campo de cabecera de TCP. Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_71/com.ibm.aix.networkcomm/protocols_tcp_headerfields.htm

IBM. (s.f.-b). User Datagram Protocol. Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_71/com.ibm.aix.networkcomm/protocols_userdatagram.htm

IBM. (s.f.-c). Protocolo de control de transmisiones (Transmission Control Protocol). Recuperado 27 marzo, 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_71/com.ibm.aix.networkcomm/protocols_userdatagram.htm

Javier Ríos, J. R. (2014, 15 marzo). Protocolo Stop and Wait. Recuperado 27 marzo, 2020, de https://prezi.com/wjmqv1ecslxz/protocolo-stop-and-wait/

Maria Fernanda Hurtado, M. F. H. (2015, 24 junio). CAPA DE TRANSPORTE DEL MODELO OSI. Recuperado 27 marzo, 2020, de https://es.slideshare.net/mafercita98/capa-de-transporte-del-modelo-osi-49793665

Protocolo ventana deslizante. (2014, 13 abril). Recuperado 27 marzo, 2020, de https://es.slideshare.net/asanterom/protocolo-ventana-deslizante

Espinosa, O. (2019, 27 octubre). Principales puertos TCP y UDP y para qué sirven cada uno de ellos. Recuperado 19 de junio de 2020, de https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

Puertos Lógicos - GESTION DE REDES DE DATOS «SMT». (s. f.). Recuperado 19 de junio de 2020, de https://sites.google.com/site/gestionderedesdedatossmt/puertos-y-servicios/puertos-fisicos/puertos-fisicos

Tema 7:

Capa de Sesión. (s.f.). Recuperado 27 marzo, 2020, de http://itcelenes.mx.tripod.com/Unidad8CapadeSesion.html

Clasificación de Puertos de Red [Publicación en un blog]. (2012, 5 octubre). Recuperado 27 marzo, 2020, de http://cocolibre.blogspot.com/2012/10/clasificacion-de-puertos-de-red.html

César, C. (2009, 21 septiembre). ¿En qué consiste la capa 5 del modelo OSI? Capa de sesión. Recuperado 27 marzo, 2020, de https://cesarcabrera.info/en-que-consiste-la-capa-5-del-modelo-osi-capa-de-sesion/

EcuRed. (s.f.-a). Capa de Sesión. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Capa_de_Sesi%C3%B3n

EcuRed. (s.f.-b). Llamada a procedimiento remoto. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Llamada_a_procedimiento_remoto

Selene Hernandez Ramirez, S. H. R. (2016, 17 mayo). Capa 5 del modelo OSI (Sesion) [Publicación en un blog]. Recuperado 27 marzo, 2020, de https://prezi.com/1-qd0unlms6y/capa-5-del-modelo-osi-sesion/

Universidad Tecnológica de la región norte de Guerrero. (2009, 11 noviembre). Capa De Sesion. Recuperado 27 marzo, 2020, de https://es.slideshare.net/jhonatan281289/capa-de-sesion-2480524

Victor, V. (2009, 3 junio). Capa Sesion. Recuperado 27 marzo, 2020, de https://es.slideshare.net/boreasH/redes-modelo-osicapa-de-sesion-victor-mamani-catachuraboreash

Tema 8:

3.1 Algoritmos de cifrado simétrico. (s.f.). Recuperado 27 marzo, 2020, de https://www.uv.es/~sto/cursos/seguridad.java/html/sjava-12.html

Alexander Guedez, A. G. (2018, 23 abril). Criptografía y seguridad informática: El ciclo de vida de claves y contraseñas y su relación con tus entornos digitales. Recuperado 27 marzo, 2020, de https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

ALGORITMOS DE ENCRIPTACIÓN SIMÉTRICA Y ASIMÉTRICA. (2012, 14 noviembre). Recuperado 27 marzo, 2020, de https://mariiss15.wordpress.com/2012/11/14/algoritmos-de-encriptacion-simetrica-y-asimetrica/

Antonio Y áñez Izquierdo, A. Y. I. (2011, octubre). Formatos de compresión. Recuperado 27 marzo, 2020, de http://www.edu.xunta.gal/centros/cfrcoruna/aulavirtual2/file.php/110/FormacionBasica4-Compresion.pdf

Brian Donohue, B. D. (2014, 10 abril). ¿Qué Es Un Hash Y Cómo Funciona? Recuperado 27 marzo, 2020, de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Capa 6 OSI | Capa de Presentación. (2012, 21 febrero). Recuperado 27 marzo, 2020, de https://eltallerdelbit.com/capa-6-osi-capa-de-presentacion

CAPA DE PRESENTACION MODELO OSI [Publicación en un blog]. (2012, 23 mayo). Recuperado 27 marzo, 2020, de http://computecsena.blogspot.com/2012/05/capa-de-presentacion-modelo-osi.html+

Capa de Presentación. (s.f.). Recuperado 27 marzo, 2020, de http://itcelenes.mx.tripod.com/unidad9Capadepresentacion.html

Compresión con pérdida y sin pérdida. (s.f.). Recuperado 27 marzo, 2020, de https://comprimeme.wordpress.com/compresion-con-perdida-y-sin-perdida/

Criptografía en la actualidad.. (2016, 8 enero). Recuperado 27 marzo, 2020, de https://nietosanchez.wordpress.com/2016/01/08/criptografia-en-la-actualidad/

Gabriel Pantoja, G. P. (2013, 2 mayo). Criptografía y su importancia en nuestra vida diaria. Recuperado 27 marzo, 2020, de https://es.slideshare.net/econtinua/criptografa-y-su-importancia-en-nuestra-vida-diaria

Yran Marrero Travieso, Y. M. T. Ing. (2003, 18 septiembre). La Criptografía como elemento de la seguridad informática. Recuperado 27 marzo, 2020, de http://scielo.sld.cu/scielo.php?script=sci_arttext

Pedro Gutiérrez, P. G. (2013, 15 enero). ¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales. Recuperado 27 marzo, 2020, de https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Sergio De Luz, S. D. L. (2010, 4 noviembre). Criptografía : Algoritmos de cifrado de clave simétrica. Recuperado 27 marzo, 2020, de https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Tema 2. Representación de Datos. (s.f.). Recuperado 27 marzo, 2020, de http://www.tel.uva.es/personales/josdie/fprog/Material/FP06_Tema02_RepresentacionDatos.pdf

Tema 9:

1.3. ¿Qué es LDAP? (s.f.). Recuperado 28 marzo, 2020, de https://www.sergio-gonzalez.com/doc/10-ldap-samba-cups-pykota/html/openldap-que-es.html

11.4. Servidor de archivos NFS. (s.f.). Recuperado 27 marzo, 2020, de https://debian-handbook.info/browse/es-ES/stable/sect.nfs-file-server.html

Adobe Sign. (s.f.). Qué es la firma digital y cómo funciona. Recuperado 28 marzo, 2020, de https://acrobat.adobe.com/mx/es/sign/capabilities/digital-signatures-faq.html

Adrián Crespo, A. C. (2017, 2 junio). Qué es un servidor RADIUS y cómo funciona. Recuperado 28 marzo, 2020, de https://www.redeszone.net/2017/06/02/servidor-radius-funciona/

Ayuda de Search Console. (s.f.). Proteger sitios web con el protocolo HTTPS. Recuperado 27 marzo, 2020, de https://support.google.com/webmasters/answer/6073543?hl=es

Camilo Gutiérrez Amaya, C. G. A. (2015, 24 abril). IDS, Firewall y Antivirus: ¿qué debes tener instalado? | WeLiveSecurity. Recuperado 27 marzo, 2020, de https://www.welivesecurity.com/la-es/2015/04/24/ids-firewall-antivirus-debes-instalar/

Capa 7 OSI | Capa de Aplicación. (2012, 21 marzo). Recuperado 27 marzo, 2020, de https://eltallerdelbit.com/capa-7-osi-capa-de-aplicacion

Denise Giusto Bilić, D. G. B. (2015, 1 julio). Cómo fortalecer las distintas capas de las redes informáticas | WeLiveSecurity. Recuperado 27 marzo, 2020, de https://www.welivesecurity.com/la-es/2015/06/01/como-fortalecer-capas-redes-informaticas/

EcuRed. (s.f.-a). SSH. Recuperado 27 marzo, 2020, de https://www.ecured.cu/SSH

EcuRed. (s.f.-b). Telnet. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Telnet

EcuRed. (s.f.-c). SFTP. Recuperado 27 marzo, 2020, de https://www.ecured.cu/SFTP

EcuRed. (s.f.-d). Vsftpd. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Vsftpd

EcuRed. (s.f.-e). Tftp. Recuperado 27 marzo, 2020, de https://www.ecured.cu/Tftp

EcuRed. (s.f.-f). NIS. Recuperado 28 marzo, 2020, de https://www.ecured.cu/NIS

EcuRed. (s.f.-g). Kerberos. Recuperado 28 marzo, 2020, de https://www.ecured.cu/Kerberos

Aníbal Coto Cortés, A. C. C. Ing. (s.f.). Capítulo 10:Capa de aplicación. Recuperado 27 marzo, 2020, de http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter10_Capa%20de%20aplicacion.pdf

Joel Barrios Dueñas, J. B. D. (2016, 21 septiembre). Instalación y configuración de vsftpd. Recuperado 28 marzo, 2020, de http://www.alcancelibre.org/staticpages/index.php/09-como-vsftpd

Kerberos. (s.f.). Recuperado 28 marzo, 2020, de https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html

Microsoft. (s.f.). ¿Qué son IMAP y POP? Recuperado 28 marzo, 2020, de https://support.office.com/es-es/article/%C2%BFqu%C3%A9-son-imap-y-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9

Protocolo ligero de acceso a directorios (LDAP). (s.f.). Recuperado 28 marzo, 2020, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html

Rubén Infante Docio, R. I. D. (2013, 3 diciembre). Protocolos de transferencia de archivos (FTP, NFS, SMB, UPnP, DLNA) Parte 1. Recuperado 27 marzo, 2020, de https://www.rubeninfante.com/2013/12/03/protocolos-de-transferencia-de-archivos-ftp-nfs-smb-upnpdlna-parte-1/

STRATO AG, Customer-Care IT. (s.f.). ¿Qué es IMAP y cómo se utiliza? Recuperado 28 marzo, 2020, de https://www.strato.es/faq/correo/que-es-imap-y-como-se-utiliza/

Universitat Politècnica de València. (2012). ¿Qué es un Certificado Digital? : Certificados Digitales : UPV. Recuperado 28 marzo, 2020, de https://www.upv.es/contenidos/CD/info/711545normalc.html

Wikilibros. (2015, 23 enero). NIS servicio para validar usuarios. Recuperado 28 marzo, 2020, de https://es.wikibooks.org/wiki/NIS_servicio_para_validar_usuarios

¿Cómo el RADIUS trabaja? (s.f.). Recuperado 28 marzo, 2020, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf

¿Qué es HTTPS? (s.f.). Recuperado 27 marzo, 2020, de http://www.cavsi.com/preguntasrespuestas/que-es-https/

¿Qué es un portal cautivo? (s.f.). Recuperado 28 marzo, 2020, de https://www.linksys.com/es/r/resource-center/portal-cautivo/

Anexo B

Martínez Rioja Rubén. (s. f.). El cableado estructurado de una red de área local. Recuperado 28 de marzo de 2020, de https://www.adrformacion.com/knowledge/administracion-de-sistemas/el_cableado_estructurado_de_una_red_de_area_local.html

Barrera, A. (2017, 13 octubre). CABLEADO ESTRUCTURADO: ¿QUÉ ES Y CUÁLES SON SUS ELEMENTOS? Recuperado 28 de marzo de 2020, de https://www.nextu.com/blog/cableado-estructurado-que-es-y-cuales-son-sus-elementos/

Club de Integradores Viakon. (2017, 19 junio). ¿Qué es el Cableado Estructurado? Recuperado 28 de marzo de 2020, de http://clubdeintegradoresviakon.com/que-es-el-cableado-estructurado/

Joskowicz, Dr. Ing., J. (2013, octubre). Cableado Estructurado. Recuperado 28 de marzo de 2020, de https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf

Anexo A
Administración de redes

Para la implementación de una red de datos, primero se deben de evaluar ciertos parámetros importantes que tendrá la red, este será el proceso administrativo, el cual tiene como propósito garantizar un adecuado nivel de servicio, de acuerdo a un costo determinado.

La administración de redes consiste en las siguientes etapas:

1. **Planeación.** Se considera desde el inicio, la infraestructura del sistema, del que depende la vida futura de la red. Políticas y ética que rigen el cómputo.
2. **Organización.** Se implementarán modelos de la administración de redes para su óptimo desempeño. Se utilizarán modelos para la administración de los protocolos utilizados en las redes de datos.
3. **Integración.** Implementación de tecnologías actuales e integración de éstas para el adecuado funcionamiento de las redes.
4. **Dirección.** El administrador debe contar con las habilidades directivas que le permitan interactuar con el equipo de trabajo, teniendo la capacidad de conjuntar esfuerzos en beneficio de la red.
5. **Control.** Optimizar las representaciones de los elementos que componen la red, a través de la monitorización continua del sistema, manejando estándares para la medición y ejecución de acciones preventivas y correctivas.

Los administradores de red deben asegurar la planificación de la seguridad de la red para que proporcione servicio continuo.

Planeación

Objetivos del diseño en las redes. Su objetivo es determinar la estructura física y lógica de la red. Es fundamental para evitar problemas de:

- Pérdidas de datos
- Caídas continuas de la red
- Problemas de lentitud en el procesamiento de la información
- Problemas de seguridad de la información

Cuando se diseña una red o se amplía, es fundamental la realización de un diseño detallado siguiendo una planificación. Los beneficios que puede traer es la reducción de costos y mejorar el rendimiento diario.

Características y fases involucradas en el desarrollo de una red.

- *Multiservicio.* Soporte de datos, audio y video.
- *Calidad de servicio. Priorización por tipo de aplicación.*
- *Administración y monitoreo.* Soporte de protocolos como SNMP.
- *Escalable.* La red debe estar preparada para crecer.
- *Alta disponibilidad.* Redundancia en enlaces y componentes.
- *Buena relación beneficio-costo.*

Construcción e implementación de una red.

1. **Especificación de Requerimientos.** Se especifican los requerimientos y variables que van a estar presentes en el diseño de una red.
2. **Fase de Diseño de la red.** Toma los elementos de la especificación para diseñar la red en base a las necesidades de la organización.
3. **Fase de Instalación.** Se toman "los planos" de la fase de diseño y se empiezan a instalar físicamente los dispositivos y elementos de la red.
4. **Fase de pruebas.** Consiste en realizar toda clase de pruebas a la red ya instalada para comprobar o constatar que cumple con las especificaciones de requerimientos.

Metas del diseño.

Es el cuestionamiento que debe realizar un diseñador de redes antes de comenzar la fase de diseño:

- ¿Quién va a usar la red?
- ¿Qué tareas van a desempeñar los usuarios en la red?
- ¿Quién va a administrar la red?
- ¿Quién va a pagar por ella?
- ¿Quién va a pagar por mantenerla?

Metas claves.

- **Desempeño.** Los tipos de datos procesados pueden determinar el grado de desempeño requerido.
- **Volumen proyectado de tráfico.** Algunos equipos de interconexión pueden ocasionar cuellos de botella en las redes con tráfico pesado.
- **Expansión futura.** Planear el crecimiento de la red para que las necesidades de la compañía no se saturen en un futuro inmediato.
- **Seguridad.** Cifrado de datos, nivel de seguridad que se tiene en el manejo de las contraseñas, el tipo de sistemas respaldos.
- **Redundancia.** Las redes robustas requieren redundancia si algún elemento falla, la red deberá por sí misma seguir operando.
- **Compatibilidad de hardware y software.** Los sistemas deben ser compatibles para que puedan funcionar y comunicarse entre sí.
- **Compatibilidad entre organización y gente.** Capacitación del personal de la compañía.
- **Costo.** Costo que implica diseñar, operar y mantener una red.

Análisis de requerimientos de hardware.

Es conveniente analizar la existencia y las necesidades de hardware que se requieren para una red de datos.

1. **Identificación de la red.** Consiste en conocer y cuantificar cada uno de los elementos que lo componen, la topología e identificar posibles puntos de falla. Existen dos tipos:
   - *Automático.* Se realiza a través de un software.
   - *Manual.* Se basa en la observación.
2. **Análisis del tráfico de la red.** Permite identificar los dispositivos dedicados al tráfico, tecnologías empleadas, ubicación de dispositivos en cada segmento y el uso de segmentos con base en el tipo de tráfico.
3. **Niveles de confianza.** Comportamiento que guarda cierto dispositivo con relación al estado ideal de éste (funcionalidad y seguridad). Existen tres tipos:
   - *Alto.* Nivel ideal. Se refiere a que el dispositivo funcione sin ningún problema.
   - *Medio.* El dispositivo funciona medianamente, requiere soporte técnico.
   - *Bajo.* El dispositivo no funciona como debería aún con soporte técnico.
4. **Capacidades del dispositivo.** Características de los dispositivos que pueden llegar a tener un impacto sobre el rendimiento eficiente de la red:
   - Tecnologías que emplean grandes recursos.
   - Servicios que requieren gran ancho de banda.
   - Comunicación sofisticada de paquetes.

5. **Consideraciones en la elección de dispositivos.**
   - Incompatibilidad
   - Costos
   - Marcas
   - Funcionalidad
   - Capacidad
   - Tiempo de vida
   - Protocolo que implementan
   - Servicios
   - Seguridad
   - Mejoramiento
6. **Análisis de requerimiento de usuario.**
   - Identificar servicios
   - Identificar costos
   - Identificar perfil de usuario (sus necesidades)
   - Especificar requerimientos en niveles
   - Clasificar necesidades en niveles
   - Identificar niveles de jerarquía en el sistema
7. **Requerimientos.**
   - Necesidades del cliente
   - Organización
   - Comunicación constante
   - Identificar necesidades que satisface el software.

Análisis de requerimientos de software

Se deben tomar en cuenta los mismos aspectos que en los requerimientos de hardware. Se deben considerar a nivel lógico (instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red).

Antes de realizar la instalación se debe considerar:

- Memoria y almacenamiento
- Asegurar que no exista conflicto alguno entre las versiones actuales y las que se pretenden instalar.
- Satisfacer la necesidad de respaldo frecuente de las configuraciones de los equipos de red.
- Recolectar y analizar el tráfico que circula por la red.

Diseño de políticas de cómputo

El diseño de políticas de seguridad es necesario para proteger sus activos físicos y lógicos. Los administradores de red no implementan las medidas correctivas disponibles y los agresores explotan el descuido.

Una política es un conjunto de reglas que guían una identidad, cada regla define una acción.

Una política de seguridad en cómputo es un documento que define reglas y principios para lograr la seguridad, tener un orden y hacer buen uso de variables de red. En ellas se

especifican las condiciones, los derechos y las obligaciones de cada persona que colabore en dicha organización (ver figura A.1.1).

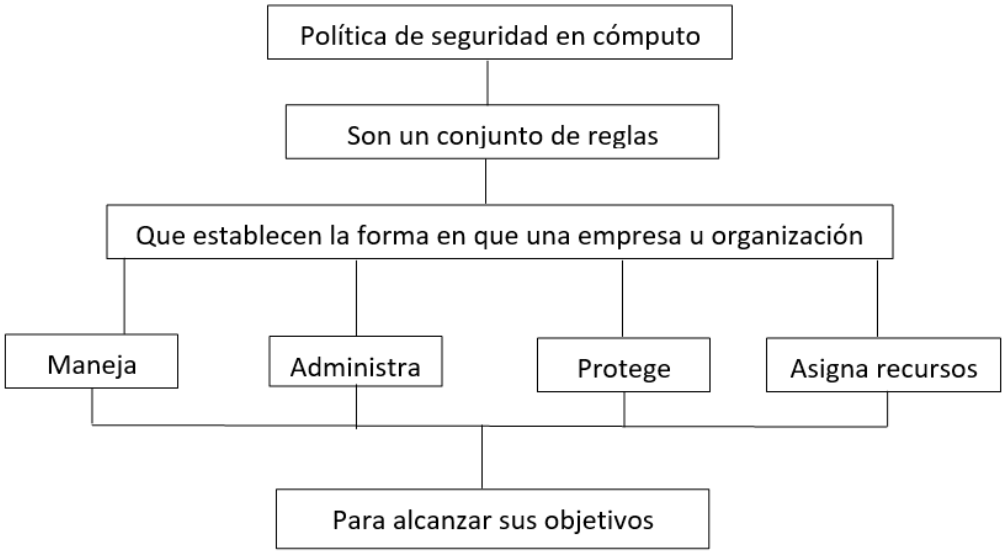


Figura A.1.1. Diagrama de políticas de seguridad.

Objetivos

- Informar a los usuarios y al personal acerca de os requisitos obligatorios para proteger los bienes de TI.
- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos.
- Prevenir la pérdida de información.
- Uso adecuado y eficiente de los sistemas de cómputo y telecomunicaciones.
- Estandarizar la seguridad tanto en el ámbito humano y tecnológico.

Para poder realizar una política de seguridad se debe dar respuesta a las siguientes preguntas:

1. ¿Cuál es la problemática?
2. ¿Qué se debe proteger?
3. ¿De qué se debe proteger?
4. ¿Qué tipo de usuarios son?

Una vez contestadas estas preguntas, hay que tomar en cuenta los siguientes aspectos:

1. **¿Quién debe poder usar los recursos?**
   A cada empleado se le asignan recursos, ya que no todos necesitan los mismos para realizar su trabajo.
2. **¿Qué constituye un uso adecuado de los recursos?**
   Se deberán establecer los lineamientos del uso aceptable de dichos recursos. La política debe establecer qué tipo de uso es aceptable y cuál inaceptable de manera clara.

3. **¿Quién debe proporcionar acceso al sistema?**
   Los directivos, junto con los expertos en TI definen los requisitos de seguridad, identifican y dan prioridad, proporcionando acceso al sistema al personal calificado.
   Para que esto sea posible, es necesario crear políticas por secciones:
   - *Usuarios.* Existen distintos tipos de usuarios (estudiantes, profesores, entre otros). Es necesario establecer derecho y obligaciones.
   - *Cuentas.* Creación, seguimiento y características de las cuentas (altas y bajas).
   - *Administradores.* Necesitan recabar información de directorios y archivos de los usuarios para diagnosticar problemas o investigar violaciones a la seguridad.
   - *Seguridad Física.* Acceso físico, estructura del edificio, entre otras cosas. Se establecen controles para permitir o denegar el acceso a las instalaciones.
   - *Red.* Configuración de los sistemas operativos, accesos lógicos, remotos, autenticaciones, internet, entre otros.
   - *Seguridad Lógica.* Son medidas electrónicas tales como permisos dentro del sistema operativo reglas de acceso a las capas de red (firewalls, routers, switches, entre otros).
4. **¿Quién debe tener privilegios de administración?**
5. **¿Cuáles son los derechos y responsabilidades de los usuarios?**
   Son responsables de hacer respaldos de sus datos. Se pueden implementar acciones legales contra los usuarios que divulguen información que pueda estar patentado. Cumplir con los lineamientos.

Organización

Las habilidades que debe de tener al administrador de redes son:

- Supervisar
- Comprobar
- Sondear
- Configurar y controlar componentes (hardware y software)

¿Qué aspectos debe dominar?

- *Escalable.* Crecimiento a futuro.
- *Transparente.* Protocolos y configuraciones de manera clara.
- *Eficiente.* Cumple los requerimientos del cliente.
- *Confiable.* Siempre funcionando, que los paquetes lleguen a su destino.

Principales tareas del administrador de redes

- *Monitoreo.* Revisar el tráfico de red, las comunicaciones que se establecen, vigilar el tiempo de respuesta y detectar posibles fallas.

- *Mejorar los procesos.* Si se detecta alguna problemática en el funcionamiento de una parte de la red, deberá de poder arreglar y mejorar dicho aspecto de manera automática.
- *Seguridad.* Que el sistema y le red estén libres de riesgo.
- *Redireccionar el tráfico de la red.* Si las comunicaciones establecidas son insuficientes para que la transmisión de datos e información sea de manera fluida, el administrador debe de ver las posibles soluciones para establecer más canales de comunicaciones en la red para mantener un buen flujo de transmisión y recepción de datos.
- *Capacidad de restablecimiento.* Si la red o uno de sus servicios llega a fallar, se debe de tener un plan para reestablecer los servicios requeridos que tuvieron falla.
- *Altas, bajas de cuentas de acceso.* Controlar las cuentas de acuerdo a sus privilegios y teniendo control de las cuentas que siguen activas para que no haya riesgo de actividades ilícitas por parte de una cuenta que ya no debería de seguir en operación, sobre todo si tiene altos privilegios.

Entidad de Administración de Redes

- Entidad Administradora
- Base de información de administración (MIB)
- Agente administrador de red
- Protocolo de administrador de red

La OSI (Organization International for Standardzation) creó un comité para generar un modelo para a administración de una red (ver figura 1.3).

- **Organización.** Descripción de los componentes de la administración de la red (administrador-agente).
- **Información.** Estructura y almacenamiento de la información de administración de los objetos de la red (MIB).
- **Comunicación.** Verificación de comunicación agente y proceso.
- **Funcionalismo.** Direcciona las aplicaciones que se encuentra en el NMS (Network Management System).

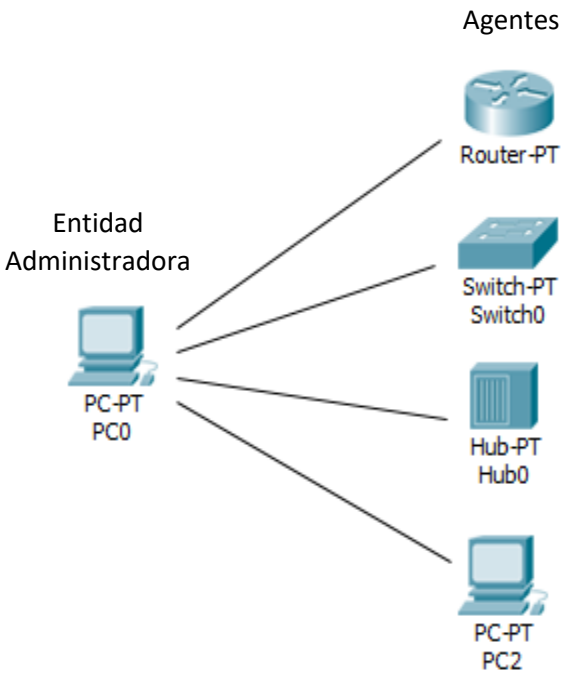


Figura A.1.2. Diagrama estructural de la administración de redes.

Anexo B
Cableado Estructurado

Ya se han mencionado los elementos y características más importantes del cableado estructurado en el tema 3 correspondiente a la capa física. Como complemento, en este apartado se mencionan características más detalladas, así como recomendaciones para realizar instalaciones del cableado estructurado.

Retomando lo visto en el tema 3, el cableado estructurado es la infraestructura de cable destinada a transportar a lo largo y ancho de una red LAN los datos que requieran compartir los usuarios.

Éste puede basarse en distintos estándares, como por ejemplo EIA/TIA 568, 569, 598, 606 o 607, los cuales ayudan a la clasificación y organización de los cables que se utilizarán en la infraestructura dependiendo de las necesidades. Sin embargo, no se ha hablado sobre recomendaciones de seguridad o formas de implementación de cables y equipos, por lo que a continuación se mencionan las recomendaciones más importantes que se deben considerar cuando se vaya a implementar la infraestructura.

El cableado estructurado no debe ser dependiente de un dispositivo específico, comienza a partir del punto de demarcación de la compañía o el proveedor de internet. Cada sistema de cableado estructurado es diferente debido a variaciones en la estructura arquitectónica de la construcción donde se va a llevar a cabo la instalación.

- Si es una instalación de un edificio de varios pisos o es una instalación de un solo nivel con varios edificios, el sistema de cableado es distinto. El cableado en condiciones hostiles de temperatura o ruido electromagnético depende de la zona en que se encuentre la infraestructura.
- El tipo de cable y conectores varía dependiendo de los requerimientos, sin embargo, se debe de tomar en cuenta lo que indique el estándar ya que cuando se usa fibra óptica es distinto a cuando se usa solamente UTP
- El cableado puede tener un objetivo de video vigilancia para seguridad o de voz digital para un call center y tendrá requerimientos distintos de tasa de transmisión y confiabilidad, por ejemplo, un centro de atención a clientes o un casino que implementa cámaras de video para vigilar que los clientes no hagan trampa.
- El tipo de dispositivos que se conectarán con los cables como pantallas inteligentes, videocámaras, sensores o computadoras, los cuales representan requisitos de conexión diferentes y cableado con características específicas.
- Cuando existe infraestructura previa de cableado, el diseño debe considerar qué parte conservar y qué parte renovar conforme a lo que dictan los estándares sobre tipo de cable, categoría, capacidad y distancias de los equipos.
- Los requerimientos del cliente, los cuales son las restricciones naturales de presupuesto, confiabilidad, vida útil, capacidad, distancia y calidad de servicio.
- Otro de los datos no menos importantes a considerar son las garantías de los productos influyen en el cálculo de la vida útil de la instalación y las conexiones de redundancia para proporcionar robustez al sistema.

Entrada al Edificio

Estas instalaciones pueden contener dispositivos de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, así como sus equipos. Se recomienda que se encuentren ubicados en un lugar seco, cerca de las canalizaciones del backbone.

Cuarto de Equipos

Los equipos de este cuarto pueden incluir centrales telefónicas, equipos informáticos, centrales de video, por decir algunos ejemplos. Es importante que únicamente existan equipos directamente relacionados con los sistemas de telecomunicaciones.

En el diseño y ubicación de la sala de equipos, se deben considerar:

- Posibilidades de expansión, es decir, prever el crecimiento en los equipos que irán ubicados en la sala de equipos, y prever la posibilidad de expansión de la sala.
- Evitar que la sala de equipos sea ubicada en áreas con riesgo o posibilidad de filtraciones de agua, ya sea por el techo o por las paredes.
- Facilidades de acceso para equipos de gran tamaño.
- La estimación de espacio para esta sala es de 0.07 m^2 por cada 10 m^2 de área utilizable del edificio. Si no se dispone de mejores datos, se puede estimar el área utilizable como el 75% del área total. En edificios de propósitos específicos (hoteles, hospitales, entre otros) el área utilizable es generalmente mucho más grande que el área efectiva de trabajo. En estos casos, el cálculo puede hacerse en función del área efectiva de trabajo. En todos los casos, el tamaño mínimo recomendado de 13.5 m^2.
- Es recomendable que esté ubicada cerca del backbone, ya que al cuarto de equipos llegan generalmente una cantidad considerable de cables correspondiente a este subsistema.

Cableado Vertical (Backbone)

Este sistema proporciona interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones.

En el cableado vertical, a diferencia del horizontal, resulta más ventajoso realizar instalaciones independientes para la telefonía y datos. De este modo, si fuera necesario sustituir el backbone, se realizaría con un coste relativamente bajo, y causando menos molestias a los ocupantes del edificio que si estuviesen unidos telefonía y datos.

Existen dos tipos de cableado en cuanto se refiere al backbone, éstos son cableado externo entre edificios y cableado interno al edifico.

El cableado externo entre edificios es necesario para interconectar las entradas al edifico de cada uno de éstos en una sola instalación. La recomendación ANSI/TIA/EIA-569 admite, para estos casos, cuatro tipos de canalizaciones: Subterráneas, directamente enterradas, aéreas, y en túneles.

El cableado interno conecta el cuarto de equipos con el cuarto de telecomunicaciones. Estas conexiones pueden ser a través de ductos, bandejas o escalerillas portacables, por mencionar algunos ejemplos.

El cableado vertical se puede realizar con cables UTP o con fibra óptica. Cuando se emplea cable UTP, como lo indica la norma, en la actualidad se debe instalar categoría 6 o superior

y se colocará un cable desde el cuarto de equipo por cada cuarto de telecomunicaciones a conectar con la red.

Armario o Cuarto de Telecomunicaciones

En este cuarto se encuentran conmutadores y todos los elementos centralizados que corren a través de tramos horizontales hasta el área de trabajo.

El diseño o selección de los armarios o cuartos de telecomunicaciones debe considerar, además de voz y datos, como se ha mencionado, la incorporación de otros sistemas de información del lugar tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones internos (como los denominados edificios inteligentes).

Entre las consideraciones más representativas del cuarto de telecomunicaciones se destacan:

- Deben estar propiamente iluminadas
- Precauciones en el manejo del cable.
- Evitar tensiones en el cable.
- Los cables no deben enrutarse en grupos muy apretados.
- Utilizar rutas de cable y accesorios apropiados 100 ohms UTP y STP.
- Se deben tener en cuenta los requerimientos eléctricos de los equipos de telecomunicaciones que se instalarán en estas salas. En algunos casos, es recomendable disponer de paneles eléctricos propios para las salas de telecomunicaciones.
- Debe contener un mínimo de dos tomas corrientes AC de 110 V y 15 A con circuitos independientes.
- No puede compartir espacio con instalaciones eléctricas que no estén relacionadas con las telecomunicaciones.
- No hacer trazados con giros un ángulo mayor de 90 grados y el cable debe hacer una curva lo más suave posible.
- El área a servir es mayor a 1.000 m^2. En estos casos, se recomienda una sala de telecomunicaciones por cada 1.000 m^2 de área utilizable.
- Evitar hacer empalmes, y, en caso necesario, de máxima calidad y blindados con termo retráctil o doble aislante no perecedero (no usar cinta adhesiva de electricista).
- Una altura mínima recomendada es de 2.6 metros.

- Si posee equipos activos, su temperatura ambiente debe encontrarse entre 18 y 24 °C y la humedad entre 30% y 50%. De lo contrario, la temperatura debe estar entre 10 y 35 °C y la humedad inferior a 85%.
- Debe encontrarse en un lugar sin riesgo de inundación o en contacto con agua. En caso de haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso. En dichos lugares no pueden encontrarse tuberías de agua ni sobre el cableado ni alrededor.
- Dependiendo de las circunstancias puede ser necesario emplear materiales aislantes de humedad o repelentes de insectos o roedores.
- Los tamaños recomendados para las salas de telecomunicaciones, asumiendo un área de trabajo por cada 10 m^2, son las mostradas en la figura B.1.1.

Área utilizable	Tamaño recomendado de la sala de telecomunicaciones
500 m^2	3 m x 2.2 m
800 m^2	3m x 2.8 m
1.000 m^2	3m x 3.4 m

Figura B.1.1. Tamaños recomendado para salas de telecomunicaciones.

Cableado Horizontal

Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado horizontal y deben tenerse en cuenta las siguientes consideraciones:

- Se recomienda la utilización de canaletas, ductos bajo piso elevado, bandejas (rejillas) o canaletas perimetrales para transportar los cables horizontales desde el backbone hasta el área de trabajo.
- Una tubería de ¾ pulgada (unos 2 centímetros) por cada dos cables UTP.
- Una tubería de 1 pulgada (2,54cm) por cada cable de dos fibras ópticas.
- Los radios mínimos de curvatura deben ser bien implementados.
- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo deben estar ubicados en lugares accesibles.
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empalme (patch panels) y cables de empalme utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Se deben hacer ciertas consideraciones a la hora de seleccionar el cableado horizontal, ya que contiene la mayor cantidad de cables individuales en el edificio.

Los costes en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal, pueden ser muy altos. Para evitar estos costes, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario.

La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la relocalización de áreas de trabajo. El diseñador también debe considerar incorporar otros sistemas de información del edificio, por ejemplo, televisión por cable, control ambiental, seguridad, audio, alarmas y sonido, al seleccionar y diseñar el cableado horizontal.

Área de Trabajo

Se recomienda asumir un área de trabajo por cada 10 m^2 de área utilizable del edificio. Esto presupone áreas de trabajo de aproximadamente 3 x 3 m. En algunos casos, las áreas de trabajo pueden ser más pequeñas, generando por tanto mayor densidad de áreas de trabajo por área utilizable del edificio.

Se recomienda prever como mínimo tres dispositivos de conexión por cada área de trabajo. Con base a esto y la capacidad de ampliación prevista se deben prever las dimensiones de las canalizaciones.

Instalación del cableado estructurado

Para realizar la instalación de la infraestructura, se deben contemplar 5 etapas a desarrollar:

1. **Preventa/venta.** Comprende tareas como clasificación de solicitudes de propuestas, cálculos de costos, elaboración de oferta, redacción de contrato.
2. **Obra gruesa.** En este aspecto se hace la instalación de todos los cables mediante techos, paredes, conductos de piso verticales y horizontales. Esta fase es la que pudiera generar mayor molestia al cliente por ruidos o cantidad de escombros. Es importante hacer un trabajo limpio, cerrando cualquier abertura y cuidando las instalaciones involucradas.
3. **Terminación.** Entre las acciones se encuentra administración de cables y conexión de alambres. Es posible que se muevan algunos muebles o mesas, por lo que se deben procurar orden y silencio.
4. **Finalización.** Incluye pruebas de cables, diagnóstico de fallas y certificación.
5. **Asistencia al cliente.** Se monitorea la instalación realizada y los resultados finales del proyecto. Posterior al trabajo, se debe ofrecer asistencia continua en caso de anomalías o dudas.

Protección del cableado estructurado

Como medida de seguridad adicional, se aconsejan las siguientes protecciones hacia la infraestructura:

- Es importante incorporar un plan de mantenimiento preventivo para el sistema de cableado estructurado. Esto es vital para evitar su deterioro y posible avería.
- Delegar a una persona responsable del mantenimiento de la organización de cableado. Será la única autorizada para realizar o supervisar movimientos, adiciones o cambios a los cables de parcheo, etiquetado y bastidores.
- Previo a la instalación, es importante hacer un buen diseño de dicho cableado. Lo cual implica planificar sus parches, problemas de flujo de aire y de refrigeración. Así como la elección del cableado adecuado.
- Retirar todos los cables viejos y sin usar antes de ejecutar la instalación.
- Es importante ejecutar un método de etiquetado de cables en ambos extremos. Esto mantendrá los cables estructurados organizados y fácil de ubicar en caso de solventar problemas.
- Para evitar polvo y electricidad estática, se aconseja utilizar piso de concreto, terrazo o loza. Pudiera considerarse tratar paredes y pisos para minimizar dichos elementos.
- Es importante cuidar de no doblar los cables más allá de su radio de curvatura especificado. Este parámetro incidirá en lo fuerte de la señal de datos.
- Para fines de la protección eléctrica, se requiere de una infraestructura eléctrica. Esto permitirá cambiar o realizar la acometida eléctrica respectiva y distribución de circuitos eléctricos y puesta a tierra.
- Debe preverse un modo de actuación del sistema de cableado estructurado en caso de incendio. De igual forma, habrá que colocar sistemas de detección y prevención de los mismos.

Anexo C
Evaluación del material

Este material de apoyo será utilizado por alumnos y profesores, pudiendo acceder a éste desde una plataforma en línea, dicho material contará con retroalimentación para tomar en cuenta la opinión de quienes hagan uso de él, así como dar un mantenimiento y actualización a los temas de ser necesario.

Como primera evaluación del material, se solicitó el apoyo de alumnos que estuvieran inscritos en las asignaturas de Redes de Datos Seguras, los cuales, al momento de hacer la evaluación, ya tenían conocimientos hasta el tema 4, por lo que fueron los encargados de evaluar los temas 1-4. Además, también se solicitó apoyo de alumnos de la asignatura de Administración de Redes, quienes al momento ya habían cursado Redes de Datos Seguras, éstos pudieron realizar la evaluación de los temas 5-9.

A continuación, se presenta la información recabada de manera estadística a través de un conjunto de gráficas y que se acompañan al final con los cuestionarios respondidos.

Se les preguntó a los encuestados sobre el desarrollo y contenido de los temas, si consideran a éstos apropiados o si tienen comentarios al respecto. Se consideró como “excelente” a aquellos que argumentaron que el material se presenta de una buena forma, así como dando detalles sobre qué es lo que más les agradó de este. Del mismo modo, se consideró como “bueno” a quienes simplemente comentaron que el material es adecuado como apoyo, sin dar detalles sobre el por qué su opinión. Estos resultados pueden observarse en la figura C.1.1.

Figura C.1.1. Contenido de los temas: desarrollo e imágenes.

Adicionalmente a esto, algunas personas comentaron ciertos detalles que pudieran ser mejorados, por ejemplo, algunas imágenes que pudieran ser reemplazadas por unas de mejor calidad, lo cual posteriormente se realizó.

En cuanto a los ejemplos presentados, se tomó el criterio de la gráfica anterior para representar los resultados. Sin embargo, hubo comentarios los cuales decían que sería conveniente agregar ejercicios referentes a las prácticas de laboratorio o al software dedicado a la simulación del cableado entre dispositivos, lo cual será considerado posteriormente. Estos resultados pueden observarse en la figura C.1.2.

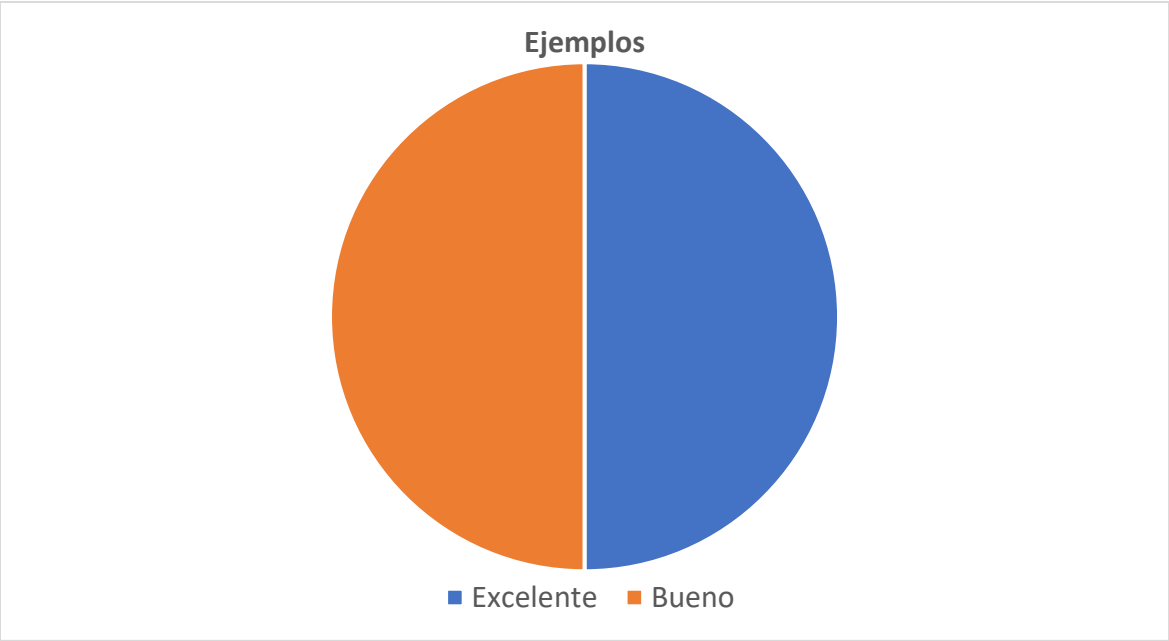


Figura C.1.2. Contenido de los temas: desarrollo e imágenes.

Se preguntó sobre si se tenía algún comentario sobre falta de contenido, estos resultados pueden verse en la figura C.1.3.

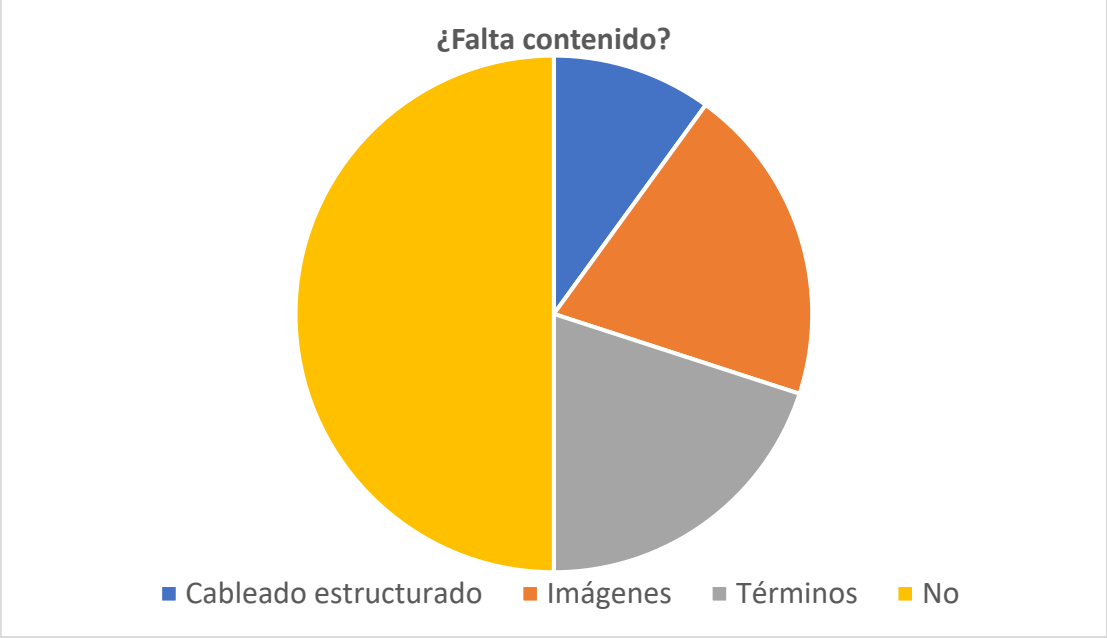


Figura C.1.3. Contenido de los temas: desarrollo e imágenes.

Los comentarios incluyen el agregar más información sobre el cableado estructurado, y es por esta razón que se decidió crear el Anexo B, el cual hace recomendaciones sobre la implementación de éste.

También se retomó lo anteriormente dicho sobre las imágenes, además de también la inclusión de más imágenes detalladas sobre ciertos temas para una mejor comprensión.

Finalmente, también se recalcó sobre las palabras o términos usados que fueran presentados tanto en español como en inglés, de modo que se eviten confusiones en temas posteriores en los que son usados.

A continuación, se presentan las respuestas de diez alumnos, de los cuales cinco estaban cursando la asignatura de Redes de Datos Seguras al momento de la encuesta, y el resto de ellos ya la habían cursado en algún semestre anterior.

Encuesta 1

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Sí, me parece que se da de manera clara la información, las imágenes son de mucha utilidad para entender algunos conceptos.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Creo que en algunos temas falta detallar un poco más, por ejemplo, en la parte de cableado estructurado, falta información ya que, a, mi parecer es uno de los temas más importantes.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Sí, son de bastante ayuda, sobre todo en la parte de las topologías. Las tablas comparativas de los estándares también me parecen de utilidad para ver de manera más clara las diferencias entre ellos.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Creo que faltarían más ejemplos en algunos temas, también para el cableado estructurado me parece que son importantes.

- ¿Consideras que le hace falta mejorar en algo a este material?

En la parte de "Beneficios de las redes locales. Usos y aplicaciones" me parece que falta información, sólo habla de la parte de beneficios.

La parte de cableado estructurado podría estar más detallada, la explicación de los subsistemas es muy resumida y también se podrían agregar algunas imágenes en esa parte.

En los dispositivos de interconexión, podría tener mayor detalle del funcionamiento y utilización de los dispositivos.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Sí, creo que es muy útil porque rescata lo más importante de los temas y podría ser una buena guía para estudiar para los exámenes.

Encuesta 2

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Si, la mayoría de las definiciones y conceptos están explicados con un lenguaje muy accesible y conciso, evitando en su mayoría terminologías demasiado complejas, sustituyéndolas por ejemplos y ayudándose de diagramas para facilitar su comprensión.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Los temas abarcados en estos cuatro módulos contienen todos los temas que hemos visto en clase, he incluso hay algunos conceptos y términos que no fueron mencionados en clase y que desconocía, en especial en el Tema 1, como el Exploit y el Payload y en el Tema 3, con los protocolos RS-X, y también profundizaron mucho en varios temas que solamente se mencionaron, por lo que considero que está demasiado completa esta guía.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Estoy de acuerdo en que el uso de estos diagramas, imágenes y hasta tablas son de mucha ayuda para ver de forma gráfica procesos, sistemas, componentes, etc., que de otra forma sería más complicado de imaginar o visualizar.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Hay pocos ejemplos, pero me parece que son muy útiles en especial en el Tema 4, en donde se debe describir el funcionamiento de los protocolos y el contenido de las tramas, que información contienen, como se leen, etc. Si no los tuviera, sería complicado entender o recordar todo el proceso que se lleva a cabo.

- ¿Consideras que le hace falta mejorar en algo a este material?

Una cosa que noté es que algunos de los términos sólo se escribieron en español, como en el caso de las subestaciones del cableado estructurado y algunos componentes de la red, siendo que generalmente se manejan con sus nombres en inglés, por lo que se debería añadir esa parte porque no siempre se encuentran estos conceptos con estos nombres en la bibliografía.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Si, la información está demasiado detallada y profundiza mucho en algunos puntos, además de que se explica de forma muy sencilla los conceptos más básicos para evitar redundar demasiado en su descripción, los temas están muy completos y están apegados al temario.

Encuesta 3

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Si, la estructura es muy buena, y no se presenta una saturación de contenido, lo que podría resultar algo contraproducente.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Si, se abarcan los temas de tal manera que, si uno desea profundizar más en el tema, tiene los fundamentos para saber que buscar.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Si, sin embargo, podría mejorar puntualizando cada aspecto mostrado en las mismas.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Si, resultan muy amigables en la comprensión del tema, y de ser necesario permite puntualizar lo recién estudiado.

- ¿Consideras que le hace falta mejorar en algo a este material?

Únicamente el puntualizar cada aspecto mostrado en las imágenes y quizá remarcar los ejemplos con otra tonalidad o agregar índices dinámicos con la finalidad de agilizar la búsqueda de información.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Pero por supuesto que sí, es un muy buen material para una materia con un temario muy extenso.

Encuesta 4

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Sí, ya que cuenta con ejemplos variados sobre todo en el tema 5, que es de los temas que más se complican en la asignatura.

Para los demás temas la información presentada es buena, ya que se presenta un concepto, características y ventajas, algún ejemplo práctico también ayudaría.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Pienso que para la teoría es suficiente ya que contiene todos los temas que se hablan en el curso, o al menos en la forma en que yo los vi. De la misma manera pasa con los ejemplos que hay, ya que soy muy parecidos a las clases de teoría. En cuanto a la parte del laboratorio no creo que aporte lo suficiente en cuanto a los ejemplos.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Sí, sobre todo las relacionadas a la forma de comunicación y paso de mensajes, así como las cabeceras, otras imágenes no pienso que sean necesarias pero ayudan a ilustrar y no abrumarse con tanto texto.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Al menos en el tema 5 sí, ya que se presenta más de uno con diferentes casos y que se resuelven un poco diferente, considero que algún ejemplo en packet tracer estará bien.

- ¿Consideras que le hace falta mejorar en algo a este material?

Considero que algunas imágenes contienen ciertos conceptos o términos que no se explican del todo, como las que se encuentran en el tema 7.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Sí, ya que en ocasiones las clases están llenas de diapositivas u otro material que solo queda en manos del profesor o en apuntes que muchas veces no son bien tomados por la cantidad de información que se da. Al tener estos apuntes siempre se puede recurrir a conceptos que no quedaron claros, o bien para preparar temas antes de que los del profesor.

Considero que los apuntes en esta materia son necesarios, ya que como mencioné antes la información que se da es bastante, sobre todo en las últimas capas. En mi caso estás no se

vieron bien por falta de tiempo o las daban otros compañeros en exposiciones, donde muchas veces no se presta la suficiente atención.

Encuesta 5

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Si, porque la información presentada en los documentos es necesaria para el entendimiento de los conceptos visto en cada una de las practicas.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Si, como lo mencione anteriormente me parece una información, clara concisa y necesaria.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Si, las imágenes son claras para la comprensión del contenido.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Si, ya que se resuelven con detalle además de contar con más de un ejemplo.

- ¿Consideras que le hace falta mejorar en algo a este material?

Si, existen algunas abreviaciones (como net id) que no define en el documento, sería bueno agregar una nota a pie de página (aunque quizás está definido en prácticas anteriores). Sin embargo, lo que alcancé a leer, dejaría así tal cual las practicas.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Sí, podría ser una buena guía para comprender los temas vistos en la materia.

Encuesta 6

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Si, considero que se presenta de forma clara.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Si, de hecho, lo veo con bastante información complementaria que a veces no se logra abarcar dentro del aula por falta de tiempo.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Si, creo que todas las imágenes presentadas apoyan a reforzar los conceptos mostrados, así como reforzar estos mismos.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Si, los ejemplos apoyados de las imágenes ayudan bastante en la comprensión general del desarrollo de los problemas prácticos.

- ¿Consideras que le hace falta mejorar en algo a este material?

Al menos yo ubique que dentro de la topología GAN faltó cerrar el paréntesis, aparte de eso considero que la redacción y ortografía de los textos son buenas.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Si, de hecho, en el momento que estoy realizando esta encuesta es un día antes de mi examen parcial y considero que este material es un buen apoyo complementario, y que hubiera sido bueno tenerlo como material del cual estudiar.

Encuesta 7

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Si, en lo personal considero que el contenido esta explicado de una manera clara y concisa, donde se presentan ejemplos que permiten entender paso a paso, como se lleva a cabo el proceso del protocolo o el subneteo, además, las imágenes y las explicaciones son lo suficientemente claras, para su fácil entendimiento por la forma en como fueron planteados.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Si, la verdad para los temas revisados, la información es suficiente y se presenta de manera resumida su contenido, resaltando lo más importante de cada uno y que como consecuencia, permite que el individuo que haga uso del material, entienda de la mejor manera posible y con ejemplos sencillos y explicados los conceptos, sin necesidad de un profesor que le explique la totalidad de los temas.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Pese a que los apuntes contienen mucho texto, en lo personal las imágenes que logré observar son sencillas y permiten anclar el concepto teórico a un esquema o ejemplo físico, que facilita su compresión y permite entender lo que sucede gráficamente en los procesos.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Si, para el caso de VLSM y CIDR, donde regularmente los alumnos presentan problemas al comprender el tema, o no encuentran ejercicios o ejemplos explicados con detalle, me agradó la forma en cómo se redactan los ejemplos en el material, ya que, con base en tablas, imágenes y formulas, explica paso a paso, el proceso matemático que se realiza, y permite que sea más fácil comprender lo que sucede al momento de realizar ese tipo de subneteo.

- ¿Consideras que le hace falta mejorar en algo a este material?

No, la verdad considero que los ejemplos para el caso del tema 5, están muy completos y explicados con mucha claridad, lo que permite que sea posible entender mejor como realizar los ejercicios y el proceso que se sigue para que podamos resolver cualquier problema similar. Para el resto de los temas son muy teóricos y que pueden extenderse aún más, sin embargo, considero, que la información proporcionada es suficiente para entender los conceptos.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Si, dado que, en un principio, se me complico el funcionamiento de VLSM y CIDR, este material hubiese sido de gran ayuda, para entender mejor como resolver esos ejercicios con más rapidez, además, debo agregar que la información teórica planteada, de igual manera es importante ya que permite reforzar o en caso de no entender en clase al cien por ciento los temas, su información, permitiendo que los alumnos acrediten y refuercen lo visto en clase.

Encuesta 8

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

De acuerdo, ya que te da de forma clara y concisa los diferentes subtemas que se abordan en el temario, te explica desde lo más sencillo como puede ser la definición de algunos conceptos básicos, así como su funcionamiento con sus respectivos ejemplos, es muy digerible a la hora de estudiarlo y no es tan pesado a la hora de leerlo.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Tomando en cuenta lo que se ve en el curso con esto bastaría ya que si se le meten más temas extra ya no resultaría factible porque se convertiría en algo repetitivo.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Si, ya que te ilustran la forma adecuada lo que se quiere dar a entender incluso en algunos casos sin haber leído el texto, los ejemplos son muy claros.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Claro que sí, de hecho, es lo que me llamo la atención ya que son muy bien explicados de forma clara y concisa, esto nos ayuda a la hora de llevarlo a lo practico tener más fundamentos para así poder entender más rápidamente los temas.

- ¿Consideras que le hace falta mejorar en algo a este material?

No, está muy completo el material.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Claro que sí, y me hubiera ayudado bastante.

Encuesta 9

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Sí, porque da definiciones concisas sobre cada uno de los puntos y aborda los puntos fundamentales de cada tema.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Sí, porque cada uno de los capítulos brinda información detallada.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Sí, porque tienen buena resolución y son alusivas a los temas en cuestión.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Sí, aunque se podrían agregar algunos ejemplos sobre qué dispositivos o protocolos son parte de las diferentes partes del modelo OSI para que sea más sencillo entender para qué sirve cada capa.

- ¿Consideras que le hace falta mejorar en algo a este material?

En general el material es muy bueno y lo único que podría agregarse en dado caso podrían ser uno o dos ejercicios prácticos para el lector, en el cual se tengan que relacionar conceptos, completar enunciados o cosas así.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Sí, en especial del tema 4 que contiene las especificaciones de diversos protocolos de capa 2, los cuales suelen ser difíciles de entender al principio.

Encuesta 10

Cuestionario de retroalimentación de Material para Apoyo a la Docencia

*** en cada pregunta, favor de escribir las razones que justifiquen su respuesta.**

- ¿Consideras que el contenido de los temas tratados se presenta de forma clara?

Sí ya que se mantiene una trazabilidad con los temas y cada uno lleva un encaminamiento con el siguiente tema, no son aislados totalmente.

- ¿Te parece que el contenido de los temas es suficiente para su estudio?

Sí, nos da esa oportunidad de poder profundizar en cada tema y expandir nuestro conocimiento con buenos ejemplos.

- ¿Piensas que las imágenes ilustrativas son adecuadas para representar el tema al que pertenecen?

Sí, en las topologías, diagramas de seguridad (triada) y los modelos (OSI, TCP/IP, etc.) se comprende mejor el concepto.

- ¿Los ejemplos desarrollados ayudan a una mejor comprensión del desarrollo de los problemas prácticos?

Sí y como cada uno de estos viene con un recuadro de ventajas y desventajas es mucho más fácil saber en qué lugar podemos aplicar cada caso.

- ¿Consideras que le hace falta mejorar en algo a este material?

No, considero que cada elemento contenido en el material es bastante amplio y es bastante robusto para poder dedicarle un semestre completo.

- De haber tenido la oportunidad, ¿hubieras utilizado este material como complemento a tus clases de la asignatura de Redes de Datos Seguras?

Claro que sí, el modelo OSI no se explica tan a fondo y desconocía la cantidad de modelos existentes por lo que ampliar mis conocimientos con este material hubiera sido de mucha utilidad.

Glosario de Términos

Activo de información: Es todo aquello con valor para una organización y que necesita protección, tales como información, aplicaciones, procesos, servicios, infraestructura y personal.

Amenazas: Todo aquello que puede causar daño, modificación o pérdida en los activos de una organización.

ARP: Protocolo que permite a una fuente encontrar la dirección de hardware de un destino que se encuentre en la misma subred física.

ARP spoofing: Tipo de ataque que consiste en falsificar cualquier dirección MAC en una red de cómputo.

ASCII: Secuencia de 7 u 8 bits que representan símbolos.

Atacantes: Individuo o elementos que atentan contra la seguridad de un activo o un sistema.

Ataque: Acciones organizadas e intencionadas causadas por una o más entidades para ocasionar daño o problemas a un sistema o red.

Autenticación. Confirma que la identidad de una o más entidades conectadas a una o más entidades sea verdadera.

Bit rate: Tasa de bits define el número de bits que se transmiten por unidad de tiempo.

Cableado estructurado: Infraestructura de cable destinada a transportar a lo largo y ancho de una red LAN los datos que requieran compartir los usuarios.

Certificado digital: Medio que permite garantizar técnica y legalmente la identidad de una persona en Internet, así como cifrar las comunicaciones.

Cifrado: Garantizar que la información no es inteligible para individuos, entidades o procesos no autorizados a través de lo cual proporciona confidencialidad a la información.

Confidencialidad. Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.

Control de acceso: Servicio que provee protección contra uso no autorizado de los activos de un sistema, permitiendo que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.

Control de encaminamiento. Permite enviar determinada información por determinadas zonas consideradas clasificadas, así como habilitar la posibilidad de solicitar otras rutas en caso de que se detecten persistentes violaciones de integridad en una ruta determinada.

DHCP: Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Disponibilidad. Asegura que la información sea accedida cuando se requiera por la gente, sistema o proceso con acceso a ella.

DNS: Protocolo utilizado para resolver nombres de Internet en direcciones IP.

EGP: Protocolo utilizado para intercambiar información de ruteo entre diferentes sistemas autónomos.

Estándares: Normas que permiten implementar, brindar o apoyar en un objetivo particular; y deben seguirse para que se cumpla de la mejor forma posible el objetivo.

Exploit: Es el medio que un atacante utiliza para aprovechar una vulnerabilidad con la finalidad de atacar un activo. Puede ser una secuencia de comandos o un fragmento de datos.

Firewall: Sistema que protege a un ordenador o red de ordenadores contra intrusiones.

Firma digital. Este implica el cifrado, por medio de una clave secreta del emisor, de una cadena comprimida de datos que se va a transferir.

FTP: Protocolo que permite la transferencia de datos entre un cliente y un servidor.

Hash: Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

HTTP: Protocolo para la distribución y colaboración de sistemas de información de hipermedia.

ICMP: Protocolo que permite administrar información relacionada con errores de los equipos en red. No permite corregir los errores, sino que los notifica a los protocolos de capas cercanas.

IDS: Sistema encargado de monitorear el comportamiento de una red para detectar e informar sobre posibles intrusiones no autorizadas, con lo cual se puede prevenir que se vea afectada la integridad de la red.

IGMP: Protocolo que se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten la multidifusión y miembros de grupos de multidifusión.

IGP: Protocolo responsable responsables de construir y mantener la información de ruteo dentro del dominio administrativo.

IMAP: Protocolo que ofrece la posibilidad de administrar e-mails directamente en el servidor de e-mail, estableciendo una cuenta de correo en el programa de e-mail.

Impacto: Consecuencias o efecto producido por un ataque.

Incidente: Es cualquier evento que afecte la continuidad del negocio y atente contra la confidencialidad, integridad o disponibilidad de la información.

Información: Comprende todo elemento intercambiado entre dispositivos.

Integridad. Asegura que los datos almacenados en los equipos y/o transferidos en una conexión no sean modificados.

IP: Protocolo que tiene información de direccionamiento para el encaminamiento de paquetes y cuyas responsabilidades son entregar datagramas a través de la red basado en el mejor esfuerzo y ofrecer la fragmentación y el re ensamblado de datagramas para soportar los enlaces de datos con tamaños diferentes de las Unidades de Transmisión Máxima (MTU).

IPS: Herramienta muy similar a IDS, pero que además de alertar sobre las detecciones también puede bloquearlas o prevenirlas en el momento de su detección.

IPsec: Protocolo IP que permite a dos o más equipos comunicarse de forma segura.

Kerberos: Protocolo de seguridad creado por MIT que usa una criptografía de claves simétricas para validar usuarios con los servicios de red.

LDAP: Conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de la red.

Máscara de red: Sucesión de unos que abarca la porción de Id de red y adicionalmente la porción que será tomada del Id de host para utilizarse como Id de subred.

Mecanismos de seguridad: Dispositivos o elementos para resguardar la información entre la red privada y la red externa.

Medio: Es la conexión que hace posible que los dispositivos se relacionen entre sí.

Modelo OSI: Modelo de referencia que describe cómo se transmite la información de una aplicación de software en un dispositivo a través del medio de transmisión hasta una aplicación de software en otro dispositivo.

NAT: Protocolo que traduce direcciones IP privadas en una dirección pública.

NFS: Protocolo que permite acceso remoto a un sistema de archivos a través de la red.

NIC: Dispositivo que permite la conexión en red de varios ordenadores.

NIS: Protocolo de servicios de directorios cliente-servidor cuya función principal es el envío de datos de configuración en sistemas distribuidos tales como nombre de usuarios y host entre computadoras en una red.

No repudio. Este servicio protege contra usuarios que quieran negar falsamente haber enviado o recibido un mensaje.

Normas de facto (del hecho): Son normas que aparecieron y se desarrollaron sin ningún plan formal.

Normas de jure (por ley): Estándares formales y legales adaptados por algún organismo de estandarización autorizado.

Payload: Son las acciones posteriores a explotar una vulnerabilidad. Generalmente son tareas automatizadas para un determinado objetivo.

Proxy: Es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos.

Recursos: Es todo aquel elemento que forma parte de la red, y que puede ser identificado y accedido directamente.

Red de datos: Conjunto de dispositivos y software conectados entre sí mediante vías o medios de transmisión que comparten recursos, datos e información entre ellos de manera segura, eficiente y confiable.

Redes inalámbricas: Término que se utiliza para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas.

Riesgo: Posibilidad de la ocurrencia de un evento no deseado. En seguridad informática, es la probabilidad de que una amenaza logre explotar una vulnerabilidad, representando un impacto a la organización.

RIP: Protocolo usado en sistemas de conexión a internet en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

RPC: Protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

Seguridad: Conjunto de protecciones que permiten resguardar un bien.

Seguridad perimetral: Abarca equipos que van desde el último punto de administración hasta las estaciones finales.

Shellcode: Es una secuencia de bytes (opcodes) que representan instrucciones en ensamblador. Son parte esencial de muchos exploits, puesto que representan el payload. Se usa para ejecutar un código arbitrario, aunque históricamente se emplea para abrir un Shell en el sistema vulnerado.

Sistema: Conjunto de elementos que trabajan en conjunto para lograr uno o varios objetivos.

SMB: Protocolo de solicitud-respuesta y de cliente-servidor para compartir recursos.

SMTP: Protocolo utilizado para la transferencia de mensajes y archivos adjuntos de correo electrónico.

SSH: Protocolo que sirve para acceder a máquinas remotas a través de una red.

Streams: Flujo de información que se transmite entre dispositivos.

TCP: Servicio orientado a la conexión, se establece una sesión entre los hosts. Garantiza la entrega de los bloques de datos mediante el uso de confirmaciones y la entrega secuenciada de datos.

Telnet: Protocolo utilizado para conectar con un equipo remoto a través de la red.

Topología: Es la forma en que los dispositivos que forman parte de la red están conectados entre sí.

Tráfico de relleno. Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

Trama: Segmento de información enviada o recibida entre dispositivos.

UDP: Servicio sin conexión, no se establece una sesión entre los hosts, no garantiza ni confirma la entrega de las unidades de datos y no las secuencia

Unicidad. Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos.

Vulnerabilidad: Es un defecto o falla de seguridad en los sistemas que una o varias amenazas podrían aprovechar para causar un posible daño a ciertos activos o a toda la organización.

Vulnerabilidad de día cero: Son desconocidas por el fabricante (de una aplicación o sistema) y sus usuarios, hasta el día que se presentan los ataques dirigidos.