Universidad Nacional de Catamarca
Facultad de Ciencias Exactas y Naturales

REDES DE INFORMACIÓN Y COMUNICACIÓN I

Mgst. Diego Emanuel Peralta

Lic. Luis Emilio Martin

AÑO 2021

Redes de información y comunicación I

Peralta, Diego Emanuel
Martin, Luis Emilio

Peralta, Diego Emanuel
Redes de información y comunicación I / Diego Emanuel Peralta ; Luis Emilio Martin. - 1a ed. - Catamarca : Editorial Científica Universitaria de la Universidad Nacional de Catamarca, 2021.
Libro digital, HTML

Archivo Digital: descarga y online
ISBN 978-987-661-383-5

1. Almacenamiento de la Información. 2. Comunicación. I. Martin, Luis Emilio. II. Título.
CDD 302.231

Queda hecho el depósito que marca la ley 11.723.
E.C.U. 2018
Avda. Belgrano 300 - Pab. Variante I - Planta Alta - Predio Universitario - San Fernando del Valle de Catamarca - 4700 - Catamarca - República Argentina

Prohibida la reproducción, por cualquier medio mecánico y/o electrónico, total o parcial de este material, sin autorización del autor.
Todos los derechos de autoría quedan reservados por el autor.

Prologo:

El presente libro está basado en la introducción a la redes de información y comunicación de datos, donde se busco poder volcar toda la información recolectada por diferentes fuentes bibliográficas, para poder crear un ejemplar que sirva de guía y material educativo, para los alumnos pertenecientes a la Facultad De Ciencias Exactas Y Naturales De Catamarca.

Este trabajo ha sido escrito en base a los contenidos dictados en la materia redes de información 1 , pertenecientes a la tecnicatura informática con orientación en redes, el cual servirá de soporte educativo principal a la cátedra, permitiendo tener una bibliografía de cabecera como referencia.

Por último se trabajo de forma interdisciplinar con la cátedra redes de información 2 perteneciente a la misma carrera e institución, buscando articular los contenidos de forma horizontal y verticalmente de modo que permita construir puentes curriculares entre las dos asignaturas.

DEDICATORIA

El presente libro está dedicado a mi madre y a mi abuelo que me iluminan desde el cielo.
A mi abuela que fue un pilar fundamental en todo proceso de mi vida.
A mis hijas, padre, hermanas, familiares y amigos que me brindan un apoyo constante

Mgst. Diego Emanuel Peralta

El presente libro está dedicado a mi familiares padres, esposas hijos y hermanas por su constante apoyo incondicional de vida
A mi gran amigo Diego Emanuel Peralta

Lic. Luis Emilio Martin

AGRADECIMIENTOS

Se agradece por el constante apoyo en la formación docente y profesional a la Vicerrectora ***Dra. Elina Azucena Silvera de Buenader.***

Al ***Dr. Raúl Ortega*** *por el apoyo a la publicación de este libro.*

ÍNDICE

INTRODUCCIÓN A LAS REDES DE COMUNICACIÓN 4
CAPÍTULO I: MEDIOS DE COMUNICACIÓN 6
MEDIOS GUIADOS: EL CABLE COAXIAL 8
TIPOS DE CABLE COAXIAL 8
CABLE DE PAR TRENZADO TP (UTP, STP, FTP) 9
CABLE DE FIBRA ÓPTICA 11
Componentes de la fibra óptica 12
SISTEMA DE CABLEADO ESTRUCTURADO 16
Organismos 18
Normas 19
Cableado Horizontal o De Planta 20
Cableado vertical o troncal 21
PUNTO DE DEMARCACIÓN 25
TIPOS DE CONEXIONES EN CABLES HORIZONTALES 26
Estándares De Prueba De Cables 27
MODELO DE REFERENCIA OSI Y PROTOCOLO TCP/IP 29
Funciones y Capa 29
COMUNICACIONES DE PAR A PAR 31
TCP/IP 32
TCP/IP Características 34
PROCESO DE ENCAPSULAMIENTO 36
LOS DISPOSITIVOS EN UNA RED 38
TOPOLOGÍA DE RED 42
TECNOLOGÍA ETHERNET 44
Direccionamiento de hardware Ethernet 48
FORMATO DE LA TRAMA ETHERNET 50
TIPOS DE ETHERNET 51
DIRECCIONAMIENTO IP 54
DIRECIONAMIENTO IP V4 56
Clases De Direcciones IP V4 57
MÁSCARA DE RED 59
Tipos De Mascara De Subred 60

CIDR: Ruteo Interno De Dominios Sin Clases 61
SUBREDES O SUBNETEO 63
DIRECCIONAMIENTO IPV6 66
CARACTERÍSTICAS DE IPV6 67
ORGANISMOS QUE REGULAN LAS DIRECCIONES IP EN EL MUNDO 70
PREGUNTAS SOBRE LA UNIDAD N°1 72
Redes LAN 75
Redes De Áreas Metropolitanas MAN 77
Red WAN 79
TOPOLOGÍAS DE REDES 81
Topología de red difusión: 81
Topología De Red Punto A Punto 83
Topologías De Redes Multipunto 84
Topología en bus 84
La Topología En Estrella 85
Topología En Anillo 86
Topología En Malla O Total 87
PROTOCOLO ENRUTADO 90
PROTOCOLOS DE ENRUTAMIENTO 91
PREGUNTAS SOBRE LA UNIDAD N°2: 95
CAPÍTULO III: REDES INALÁMBRICAS 96
Redes Inalámbricas De Área Personal (WPAN) 98
Bluetooth 99
LAS REDES INALÁMBRICAS DE ÁREA LOCAL WLAN 101
Redes De Área Metropolitana Inalámbricas (WMAN) 106
WIMAX 107
Redes inalámbricas de área amplia (WWAN) 109
PREGUNTAS SOBRE LA UNIDAD N°3: 115
CAPÍTULO IV: COMUNICACIONES SATELITALES 117
ELEMENTOS DE LAS REDES SATELITALES 119
TELEFONÍA CELULAR 124
Los Teléfonos Móviles En La Actualidad 126
FUNCIONAMIENTO TELEFONÍA CELULAR 127
Cobertura Territorial: Red De Celdas 128

EVOLUCIÓN DE LA TELEFONÍA CELULAR 129
2-G: Segunda Generación 130
3-G: Tercera Generación 131
4-G: Cuarta Generación 132
5-G: Quinta Generación 134
PREGUNTAS SOBRE LA UNIDAD N°4: 136
RESPUESTAS SOBRE LA UNIDAD N°1: 138
RESPUESTAS SOBRE LA UNIDAD N°2: 140
RESPUESTAS SOBRE LA UNIDAD N°3: 142
RESPUESTAS SOBRE LA UNIDAD N°4: 143
GLOSARIO DE TERMINOS 144
BIBLIOGRAFÍA: 150

INTRODUCCIÓN A LAS REDES DE COMUNICACIÓN

Las comunicaciones a través del tiempo fueron cambiando en cuanto a su estructura y funcionamiento, por medios de diferentes formas de comunicarse, el auge de nuevas tecnologías de la información y comunicación fueron un papel preponderante para que estos medios evolucionaran en nuestra sociedad.

El avance constante de la computación y su integración con las telecomunicaciones han proporcionado el surgimiento de nuevas formas de comunicarse, que son empleada cada vez más por diferentes personas en el mundo.

El desarrollo y la continua evolución de las redes informáticas e Internet posibilito que una computadora pueda intercambiar fácilmente información con otras situadas en diferentes regiones lejanas del planeta.

El último avance en nuevas formas de comunicación es la realidad virtual, que permite al usuario acceder a una simulación de la realidad en tres dimensiones, en la cual es posible realizar acciones y obtener inmediatamente una respuesta, o sea, interactuar con ella.

Las redes de computadoras son ahora parte indispensable en nuestras vidas, ya sea por la escuela, el trabajo o como un simple pasatiempo.

La comunicación entre los individuos es parte básica en nuestro desarrollo y gracias a las redes de computadoras podemos comunicarnos con gente que vive en diferentes lugares del mundo.

En el caso de Internet ha revolucionado la informática y las comunicaciones como ningún otro medio lo realizo anteriormente, la invención del telégrafo, el teléfono, la radio y el ordenador sentó las bases para esta integración de funcionalidades sin precedentes. Internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica.

Internet representa uno de los ejemplos más exitosos de los beneficios de una inversión y un compromiso continuos en el campo de la investigación y el desarrollo de la infraestructura de la información.

Internet ha cambiado mucho en las dos décadas desde que nació, se concibió en la época de tiempo compartido, pero ha sobrevivido a la época de los computadores personales, la informática cliente-servidor y par a par y la informática de redes. Se diseñó antes que existiesen las LAN, pero ha acomodado a esa tecnología nueva, además de los recientes cajeros y servicios de intercambio de marcos.

Se creó para soportar un rango de funciones tales como compartir archivos y acceso remota a distribución de recursos y colaboración, y ha creado el correo electrónico y más recientemente la World Wide Web.

La disponibilidad de una red dominante (es decir, Internet) junto con ordenadores potentes baratos y comunicaciones en dispositivos portátiles (es decir, portátiles, mensáfonos, PDA, teléfonos móviles) hace posible un nuevo paradigma de informática y comunicaciones nómadas, lo cual traerá nuevas aplicaciones; el teléfono de Internet y, en el futuro, la televisión de Internet.

Por último los sistemas de telecomunicaciones hoy en día son de vitales para cualquier empresa ya si son administrados adecuadamente pueden ser un gran aliado en el momento de economizar tiempo y dinero, las telecomunicaciones han ayudado a eliminar los obstáculos geográficos acelerando la producción y la toma de decisiones de las instituciones que las emplean.

Para obtener resultados positivos es indispensable tener un personal capacitado además de escoger adecuadamente el tipo de canal de comunicación y el tipo de red que se necesita dependiendo de la circunstancia. Por otro lado también es importante que se considere la distancia, si se va emplear correo electrónico o de voz o se van a usar videoconferencias, la seguridad es otro factor a tomar en cuenta al igual q la regularidad con la que se va emplear y el presupuesto que se maneja para el futuro mantenimiento.

CAPÍTULO N° 1

CAPÍTULO I: MEDIOS DE COMUNICACIÓN

En un sistema de transmisión se denomina medio de transmisión al soporte físico mediante el cual el emisor y el receptor establecen la comunicación.
Los medios de transmisión se clasifican en guiados y no guiados, y en ambos casos la transmisión se realiza mediante ondas electromagnéticas; en el caso de los medios guiados estas ondas se conducen a través de cables, la velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los elementos que caracterizan a los medios guiados.
Medios Guiados: Se conoce como medios guiados a aquellos que utilizan unos componentes físicos y sólidos para la transmisión de datos, también conocidos como medios de transmisión por cable.
Los medio no Guiados: Son los que no utilizan cable como medio de conectividad , emplean antenas, las cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones.

La evolución de la tecnología en lo que respecta a los cables ha estado orientada por la optimización de estas tres variables.

- **Velocidad de transmisión**: en la actualidad las velocidades alcanzadas difieren notablemente entre los diferentes tipos de cables, siendo la fibra óptica la que permite alcanzar una velocidad mayor.
- **Alcance de la señal**: está determinado por la atenuación que sufre dicha señal según va circulando por el cable y que es mayor cuanta más distancia debe recorrer, por lo que este factor limita considerablemente la longitud de cable que se puede instalar sin regenerar la señal.
- **Calidad de la señal**: uno de los principales problemas de la transmisión de un flujo de datos por un cable eléctrico consiste en el campo magnético que se genera por el hecho de la circulación de los electrones.

  Este fenómeno es conocido como inducción electromagnética. La existencia de un campo magnético alrededor de un cable va a generar interferencias en los cables próximos debido a este mismo fenómeno.

MEDIOS GUIADOS: EL CABLE COAXIAL

Es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla, blindaje o trenza, que sirve como referencia de tierra y retorno de las corrientes.

Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable; todo el conjunto suele estar protegido por una cubierta aislante (también denominada chaqueta exterior).

Debido a la necesidad de manejar frecuencias cada vez más altas y a la digitalización de las transmisiones, en años recientes se ha sustituido paulatinamente el uso del cable coaxial por el de fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de esta última es muy superior.

TIPOS DE CABLE COAXIAL

THICK: (grueso). Este cable se conoce normalmente como "cable amarillo", fue el cable coaxial utilizado en la mayoría de las redes. Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Este cable es empleado en las redes de área local conformando con la norma 10 Base 2.

THIN: (fino). Este cable se empezó a utilizar para reducir el coste de cableado de la redes. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo el cable es mucho más barato y fino que el thick y, por lo tanto, solventa algunas de las desventajas del cable grueso, siendo empleado en las redes de área local conformando con la norma 10 Base 5.

Imagen N° 1.1
En esta imagen podemos ver la estructura de un cable coaxial

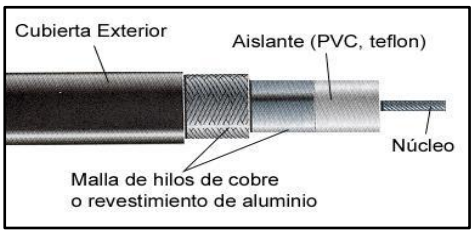
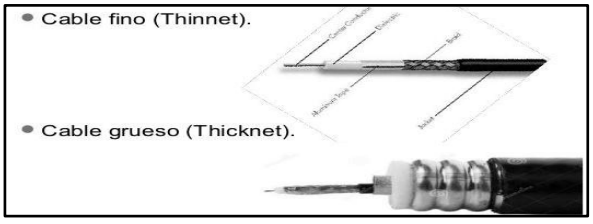


Imagen N° 1.2
Tipos de cable coaxial



CABLE DE PAR TRENZADO TP (UTP, STP, FTP)

Cable par trenzado TP

El cable de par trenzado es un medio de conexión usado en telecomunicaciones en el que dos conductores eléctricos aislados son entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes. **Fue inventado por Alexander Graham Bell.**

El entrelazado de los cables disminuye la interferencia debido a que el área de bucle entre los cables, la cual determina el acoplamiento eléctrico en la señal, se ve aumentada; en la operación de balanceado de pares, los dos cables suelen llevar señales paralelas y adyacentes (modo diferencial), las cuales son combinadas mediante sustracción en el destino; la tasa de trenzado, usualmente definida en vueltas por kilómetro, forma parte de las especificaciones de un tipo concreto de cable; cuanto mayor es el número de vueltas, menor es la atenuación de la diafonía; donde los pares no están trenzados, como en la mayoría de las conexiones telefónicas residenciales, un miembro del par puede estar más cercano a la fuente que el otro y, por tanto, expuesto a niveles ligeramente distintos de interferencias electromagnéticas.

Cable par trenzado UTP

Cada par de cables es un conjunto de dos conductores aislados con un recubrimiento plástico, este par se retuerce para que la señales transportadas por ambos conductores (de la misma magnitud y sentido contrario) no generen interferencias ni resulten sensibles a emisiones.

La u de UTP indica que este cable es sin blindaje o no blindado, esto quiere decir que este cable no incorpora ninguna malla metálica que rodee ninguno de sus elementos (pares) ni el cable mismo.

Características:

- Los cables de par retorcido por lo general tienen estrictos requisitos para obtener su máxima tensión, así como tener un radio de curvatura mínimo; esta relativa fragilidad de los cables de par retorcido hace que su instalación sea tan importante para asegurar el correcto funcionamiento del cable.
- La especificación 568ª constituida por Commercial Building Wiring Standardde y la asociación Industrias Electrónicas e Industrias de las

Telecomunicaciones (EIA/TIA) especifica el tipo de cable UTP que se utilizará en cada situación y construcción.

- Usos Comunes En Interiores: Se utiliza en telefonía y redes de ordenadores, por ejemplo en LAN Ethernet y fast Ethernet, actualmente ha empezado a usarse también en redes gigabit Ethernet.
- son cables de pares trenzados sin blindar que se utilizan para diferentes tecnologías de redes locales, son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.
- Es un tipo de cable de par trenzado que no se encuentra blindado y que se utiliza principalmente para comunicaciones, se encuentra normalizado de acuerdo a la norma estadounidense TIA/EIA-568-B y a la internacional ISO/IEC 11801.

Cable de par trenzado STP: (Shieldedtwistedpair o par trenzado blindado) se trata de cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor de un conjunto de cables.

STP es un cable de par trenzado similar al un shieldedtwistedpair con la diferencia de que cada par tiene una pantalla protectora, además de tener una lámina externa de aluminio o de cobre trenzado alrededor del conjunto de pares, diseñada para reducir la absorción del ruido eléctrico.

Este cable es más costoso y difícil de manipular que el cable sin blindaje, se emplea en redes de ordenadores como Ethernet o Token Ring y su coste en la nueva categoría 6A puede ser el mismo que la versión sin blindaje.

Cable de par trenzado FTP (Foiledtwistedpair o par trenzado con blindaje global): son unos cables de pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias y su impedancia es de 12 ohmios.

Imagen N° 2.1
Tipos de cable UTP

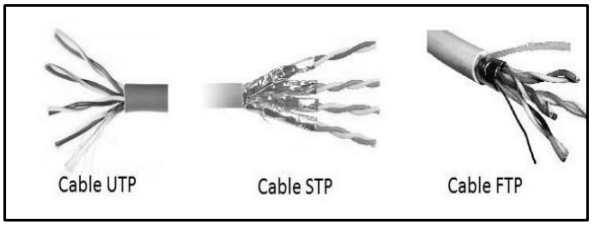
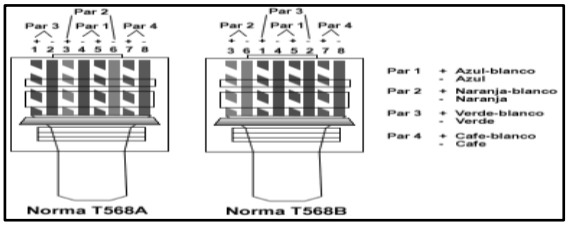


Imagen N° 2.2
Estructura de cable UTP



CABLE DE FIBRA ÓPTICA

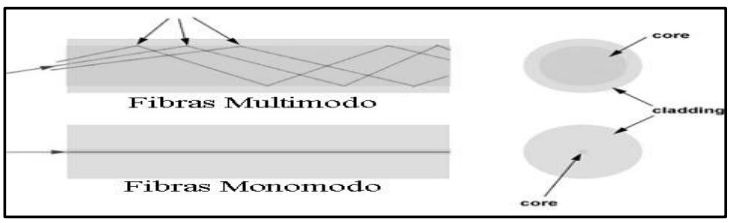
La Fibra Óptica: es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir, el haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell, la fuente de luz puede ser láser o un LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable; son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Tipos de cable

- **Fibra multimodo:** Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz, las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 km, es simple de diseñar y económico. b.
- **Fibra monomodo:** Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s).

Imagen N° 3
Tipos de fibra óptica



Componentes de la fibra óptica

Dentro de los componentes que se usan en la fibra óptica se destacan los siguientes:

- Los conectores, el tipo de emisor del haz de luz, los conversores.
- **Transmisor de energía óptica:** Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.
- **Detector de energía óptica:** Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para generar la señal), su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

Tipos de conectores: Estos elementos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor y en la cual podemos encontrar los siguientes:

- FC, que se usa en la transmisión de datos y en las telecomunicaciones.
- FDDI, se usa para redes de fibra óptica.
- LC y MT-Array que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC se usa en redes de edificios y en sistemas de seguridad.

Emisores del haz de luz: Estos dispositivos se encargan de convertir la señal eléctrica en señal luminosa, emitiendo el haz de luz que permite la transmisión de datos, estos emisores pueden ser de dos tipos:

- **LEDs.** Utilizan una corriente de 50 a 100 mA, su velocidad es lenta, solo se puede usar en fibras multimodo, pero su uso es fácil y su tiempo de vida es muy grande, además de ser económicos.
- **Lasers.** Este tipo de emisor usa una corriente de 5 a 40 mA, son muy rápidos, se puede usar con los dos tipos de fibra, monomodo y multimodo, pero por el contrario su uso es difícil, su tiempo de vida es largo pero menor que el de los LEDs y también son mucho más costosos.

Conversores luz-corriente eléctrica: Este tipo de dispositivos convierten las señales luminosas que proceden de la fibra óptica en señales eléctricas, se limitan a obtener una corriente a partir de la luz modulada incidente, esta corriente es proporcional a la potencia recibida, y por tanto, a la forma de onda de la señal moduladora; y Se fundamenta en el fenómeno opuesto a la recombinación, es decir, en la generación de pares electrón hueco a partir de los fotones.

El tipo más sencillo de detector corresponde a una unión semiconductora PN.

Las condiciones que debe cumplir un fotodetector para su utilización en el campo de las comunicaciones, son las siguientes:

- La corriente inversa (en ausencia de luz) debe ser muy pequeña, para así poder detectar señales ópticas muy débiles (alta sensibilidad).
- Rapidez de respuesta (gran ancho de banda).
- El nivel de ruido generado por el propio dispositivo ha de ser mínimo.
- Hay dos tipos de detectores: los fotodiodos PIN y los de avalancha APD.

Detectores PIN: Su nombre viene de que se componen de una unión P-N y entre esa unión se intercala una nueva zona de material intrínseco (I), la cual mejora la eficacia del detector. Se utiliza principalmente en sistemas que permiten una fácil discriminación entre posibles niveles de luz y en distancias cortas.

Detectores APD: Los fotodiodos de avalancha son fotodetectores que muestran, aplicando un alto voltaje en inversa, un efecto interno de ganancia de corriente (aproximadamente 100), debido a la ionización de impacto (efecto avalancha). El mecanismo de estos detectores consiste en lanzar un electrón a gran velocidad (con la energía suficiente), contra un átomo para que sea capaz de arrancarle otro electrón

Un cable de fibra óptica está compuesto por un grupo de fibras ópticas por el cual se transmiten señales luminosas. Las fibras ópticas comparten su espacio con hiladuras de aramida que le confieren la necesaria resistencia a la tracción.

Los cables de fibra óptica proporcionan una alternativa sobre los coaxiales en la industria de la electrónica y las telecomunicaciones. Así, un cable con 8 fibras ópticas tiene un tamaño bastante más pequeño que los utilizados habitualmente, puede soportar las mismas comunicaciones que 60 cables de

1623 pares de cobre o 4 cables coaxiales de 8 tubos, todo ello con una distancia entre repetidores mucho mayor.

Por otro lado, el peso del cable de fibra óptica es muchísimo menor que el de los coaxiales, ya que una bobina del cable de 8 fibras antes citado puede pesar del orden de 30 kg/km, lo que permite efectuar tendidos de 2 a 4 km de una sola vez.

Técnicas de empalme: Los tipos de empalmes pueden ser:

- Empalme mecánico con el cual se pueden provocar pérdidas del orden de 0.5 dB.
- Empalme con pegamentos con el cual se pueden provocar pérdidas del orden de 0.2 dB.
- Empalme por fusión de arco eléctrico con el cual se logran pérdidas del orden de 0.02 dB

Pérdida en los cables de Fibra Óptica: la pérdida de potencia a través del medio se conoce como Atenuación, es expresada en decibelios, con un valor positivo en dB, es causada por distintos motivos, como la disminución en el ancho de banda del sistema, velocidad, eficiencia.

La fibra de tipo multimodal, tiene mayor pérdida debido a que la onda luminosa se dispersa originada por las impurezas. Las principales causas de pérdida en el medio son:

- **Pérdidas por absorción.** Ocurre cuando las impurezas en la fibra absorben la luz, y esta se convierte en energía calorífica; las pérdidas normales van de 1 a 1000 dB/Km.
- **Pérdida de Rayleigh.** En el momento de la manufactura de la fibra, existe un momento donde no es líquida ni sólida y la tensión aplicada durante el enfriamiento puede provocar microscópicas irregularidades que se quedan permanentemente; cuando los rayos de luz pasan por la fibra, estos se difractan haciendo que la luz vaya en diferentes direcciones.
- **Dispersión cromática.** Esta dispersión sólo se observa en las fibras tipo unimodal, ocurre cuando los rayos de luz emitidos por la fuente y se propagan sobre el medio, no llegan al extremo opuesto en el mismo tiempo; esto se puede solucionar cambiando el emisor fuente.

- **Pérdidas por radiación.** Estas pérdidas se presentan cuando la fibra sufre de dobleces, esto puede ocurrir en la instalación y variación en la trayectoria, cuando se presenta discontinuidad en el medio.
- **Dispersión modal.** Es la diferencia en los tiempos de propagación de los rayos de luz.
- **Pérdidas por acoplamiento.** Las pérdidas por acoplamiento se dan cuando existen uniones de fibra, se deben a problemas de alineamiento.

Por último, todo cable posee una funda, generalmente de plástico cuyo objetivo es proteger el núcleo que contiene el medio de transmisión frente a fenómenos externos a éste como son la temperatura, la humedad, el fuego, los golpes externos, etc. Dependiendo de para qué sea destinada la fibra, la composición de la funda variará. Por ejemplo, si va a ser instalada en canalizaciones de planta exterior, debido al peso y a la tracción bastará con un revestimiento de polietileno extruido; si el cable va a ser aéreo, donde sólo importa la tracción en el momento de la instalación nos preocupará más que la funda ofrezca resistencia a las heladas y al viento.

Si va a ser enterrado, querremos una funda que, aunque sea más pesada, soporte golpes y aplastamientos externos; en el caso de las fibras submarinas la funda será una compleja superposición de varias capas con diversas funciones aislantes.

Imagen N° 4.1
Estructura del cable de fibra óptica

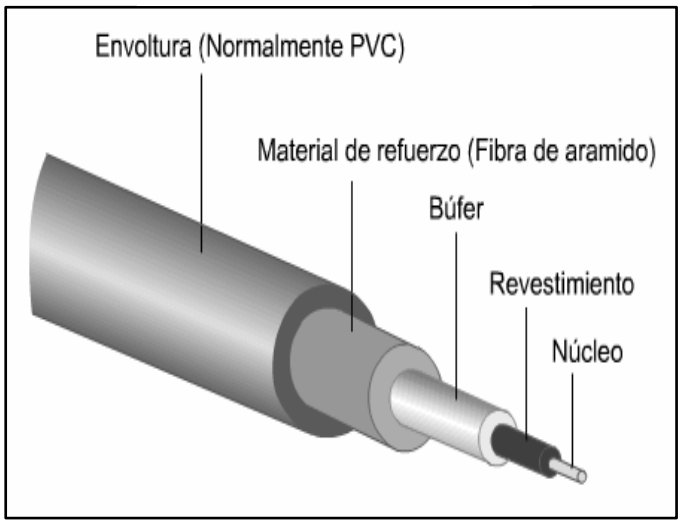
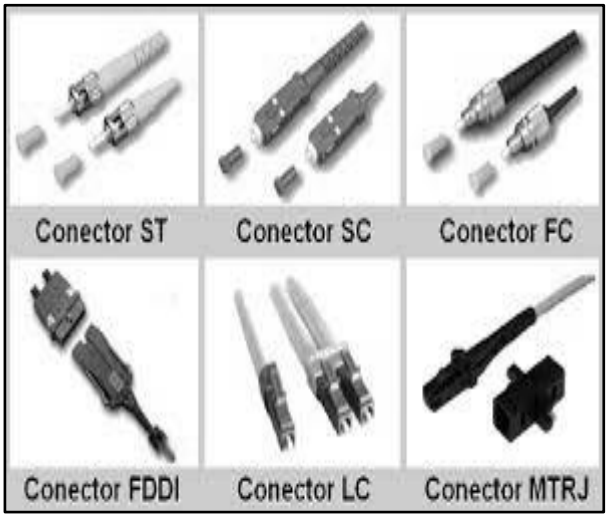


Imagen N° 4.2
Tipos de fibra óptica



SISTEMA DE CABLEADO ESTRUCTURADO

Es un sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio, donde la instalación y las características del sistema deben cumplir con ciertos estándares para formar parte de la condición de cableado estructurado.

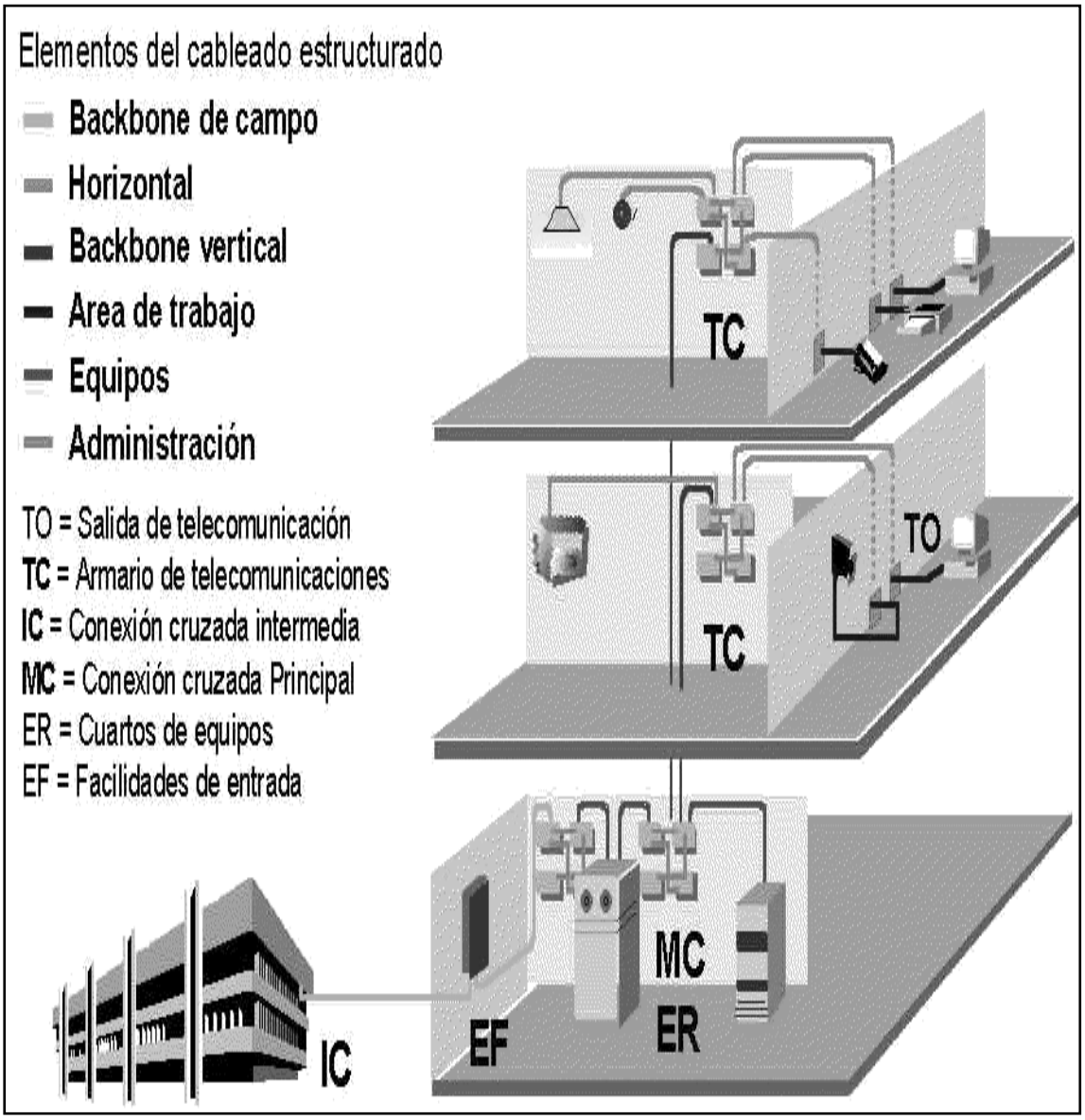
Permite dar una infraestructura flexible de cables que pueda aceptar y soportar múltiples sistemas de computación y de comunicación, permitiendo integrar los sistemas de automatización y de control de un edificio

Algunas características de cableado estructurado serian:

- Permitir la comunicación virtual con cualquier dispositivo en cualquier lugar y en cualquier momento
- Un plan de cableado bien diseñado puede incluir distintas soluciones de cableado independientes, utilizando diferentes tipos de medios e instalados en cada estación de trabajo para acomodar los requerimientos del funcionamiento del sistema
- El cableado estructurado tiene a estandarizar los sistemas de transmisión de información al integrar diferentes medios para soportar todo tipo de tráfico
- Es la solución ideal para Edificios, Campus e infraestructura en general, en la cual se requiera una alta especialización de servicios avanzados de comunicación
- Los primeros sistemas de cableado fueron concebidos por las compañías telefónicas, entrando posteriormente las compañías de sistemas de cómputo
- Fue hasta la publicación de la norma sobre tendido de cables en edificios ANSI/EIA/TIA 568 (1991) que se tuvo una especificación completa para guiar en la selección e instalado de los sistemas de cableado
- Capacidad: permite transmitir información de múltiples protocolos y tecnologías (permitan la fácil reubicación o reasignación de los usuarios)
- Flexibilidad: permite incorporar nuevos o futuros servicios a la red ya existente, así como modificar la distribución interna sin afectar el nivel de eficiencia

- Diseño: Permite optimizar la productividad al mínimo costo posible. Además, en la práctica ha demostrado requerir hasta un 50% de espacio menor al cableado tradicional „
- Integración de servicios: reúne en una misma infraestructura los servicios de datos, telefónico, audio y vídeo, seguridad, etc
- Administración: facilita al cliente el manejo y la administración de los servicios conectados „
- Modularidad: facilita el crecimiento „
- Compatibilidad: Cumple con los estándares internacionales de las industrias

Imagen N° 5
Estructura funcional de un cableado estructurado



Organismos

Luego de saber las características que nos brinda el mismo, es importante tener en cuenta quien regula el sistemas de cableado estructurado y cuáles son los organismos que se deben tener en cuenta para cualquier implementación, por ello a continuación se nombraran los mismos con sus respectivas características.

- **TIA (Telecommunications Industry Association),** fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

- **ANSI (American NationalStandardsInstitute),** es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International ElectrotechnicalCommission, IEC).

- **EIA (Electronic Industries Alliance),** es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

- **ISO (International Standards Organization),** es una organización no gubernamental creada en 1947 a nivel mundial, de cuerpos de normas nacionales, con más de 140 países.

- **IEEE (Instituto de Ingenieros Eléctricos y de Electrónica),** principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet,802.5TokenRing, ATM y las normas de Gigabit Ethernet.

Normas

- **ANSI/TIA/EIA-568-B:** Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el Cableado: TIA/EIA 568-B1 Requerimientos generales; TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado; TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.
- **ANSI/TIA/EIA-569-A:** Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.
- **ANSI/TIA/EIA-570-A:** Normas de Infraestructura Residencial de Telecomunicaciones.
- **ANSI/TIA/EIA-606-A:** Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-607:** Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-758:** Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.
- **ANSI/TIA/EIA TSB-36:** Especificaciones adicionales para cables de Par Trenzado sin blindaje „
- **ANSI/TIA/EIA TSB-40:** Especificaciones adicionales de Transmisión para Hardware de conexión de cables par trenzado sin blindaje .
- **ANSI/TIA/EIA TSB-67:** Especificación para las prueba en el campo del rendimiento de transmisión de sistemas de cableado par trenzado sin blindaje
- **ANSI/TIA/EIA TSB-72:** guía para el cableado de fibra óptica centralizada
- **ANSI/EIA 310-D-92:** gabinetes, andenes, paneles y equipo asociado
- **NFPA-75:** estándar para la protección de equipo de cómputo electrónico
- **NFPA-780:** estándar para la instalación de sistemas de protección contra rayos.

Cableado Horizontal o De Planta

El cableado horizontal es la porción del sistema de cableado que se extiende desde el closet de comunicaciones (Rack) hasta el usuario final en su estación de trabajo, es decir, el cableado que va desde el armario de Telecomunicaciones a la toma de usuario.

Algunas características de este tipo de cableado serian:

- El término “horizontal” se debe a que típicamente se instala a través del piso o del techo del edificio.
- Generalmente el cableado horizontal consta de cable par trenzado, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica
- Normalmente contiene más cable que el cableado “backbone” y es menos accesible .
- Normalmente se diseña para soportar transmisión de datos, aunque debe de pensarse en transmisión de video y audio, así como señales de control
- El cableado horizontal se implementa en topología estrella
- No se permiten empates (múltiples apariciones del mismo par de cables en diversos puntos de distribución)
- La distancia horizontal máxima es de 90 metros.Esta es la distancia desde el área de trabajo hasta el closet de comunicaciones
- En cada planta se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada dependencia, luego de estas rosetas parten los cables que se tienden por el falso suelo (o por el falso techo) de la planta.
- Todos los cables se concentran en el denominado armario de distribución de planta, es un bastidor donde se realizan las conexiones eléctricas de unos cables con otros.

Imagen N° 6.1
Ejemplo de cabreado horizontal
Servidor a PC

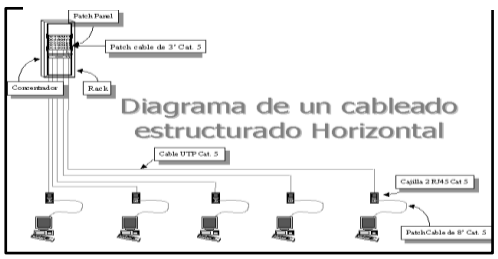
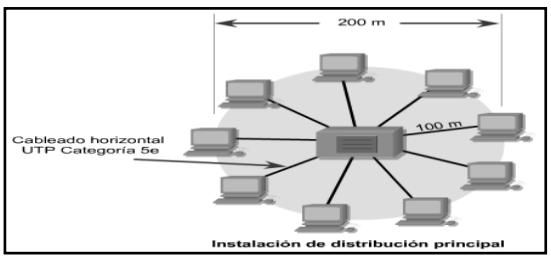


Imagen N° 6.2
Ejemplo de cabreado horizontal
Swiches a PC



Cableado vertical o troncal

El cableado vertical es conocido como cableado de backbone, es el sistema de conexión entre los distintos cuartos de comunicaciones hasta el cuarto de comunicaciones principal, incluyendo la interconexión vertical entre los pisos de un edificio; y dependiendo la instalación, por lo general suele implementarse usando fibra óptica, sin embargo en algunos casos puede usarse cable UTP, también interconecta los diferentes cableados horizontales de su empresa, independientemente si estos se encuentran instalados en los diferentes pisos de un solo edificio.

Características:

- Debido a que provee interconexión entre múltiples usuarios de diversos sectores, debe ser planeado para soportar un gran flujo de datos „
- tiene la ventaja con respecto a la poca cantidad de canales verticales en un edificio, por lo que se suele usar equipos más costosos que en el cableado horizontal
- En el cableado vertical, la fibra óptica se ha convertido en el medio más apropiado, debido a la capacidad y velocidad que ofrece
- El tendido físico se realiza en forma de estrella, es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

Imagen N° 7.1
Ejemplo de cableado vertical
Rack primario a rack secundarios

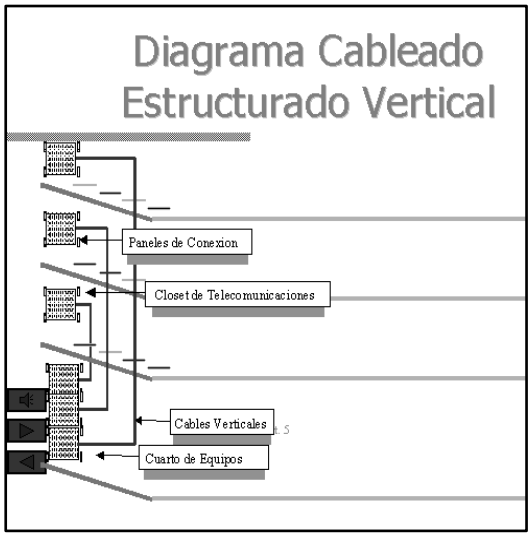
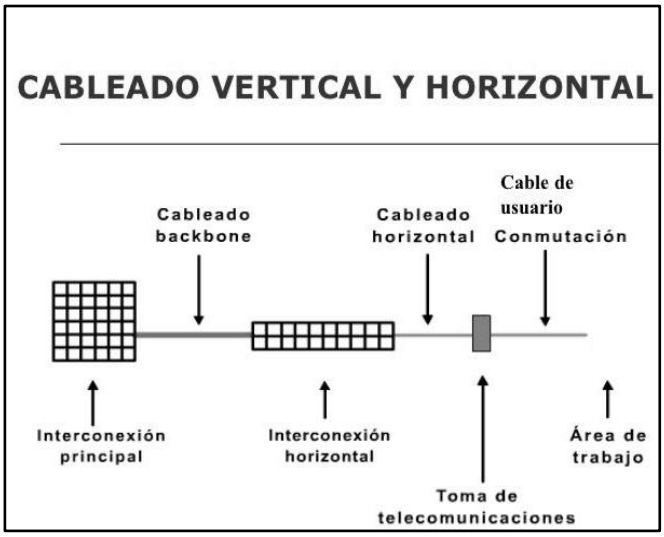


Imagen N° 7.2
Ejemplo de conexiones entren cableado vertical y cableado horizontal



Un sistema de cableado estructurado, bien diseñado e implementado, proporciona a las organizaciones una plataforma de comunicaciones estable y duradera para que las mismas se enfoque a la realización de sus objetivos productivos sin tener que estar ocupando personal, tiempo y dinero a corregir fallas y provocar pérdida de producción ó productividad, asociadas a fallas en las comunicaciones dentro de la empresa.

Un buen diseño en este aspecto permite que todas las áreas de la planta queden cubiertas con cableado o con la posibilidad de ser cubiertas en un futuro, esto se logra mediante un diseño que tome en cuenta necesidades y distancias para ubicar tanto el punto central del cableado (MDF) como los puntos de distribución (IDF).

IDF: Se denomina a los servicios de distribución intermedia (IDF), los cuales dependen del servicio de distribución principal. Una topología de este tipo se describe como una topología en estrella extendida.

MDF: Es común que las redes de gran tamaño tengan más de un centro de cableado. Normalmente, cuando esto sucede, uno de los centros de cableado se designa como el servicio de distribución principal (MDF).

Imagen N° 8.1
Ejemplo de cableados verticales
Y horizontales mediante MDF E IDF

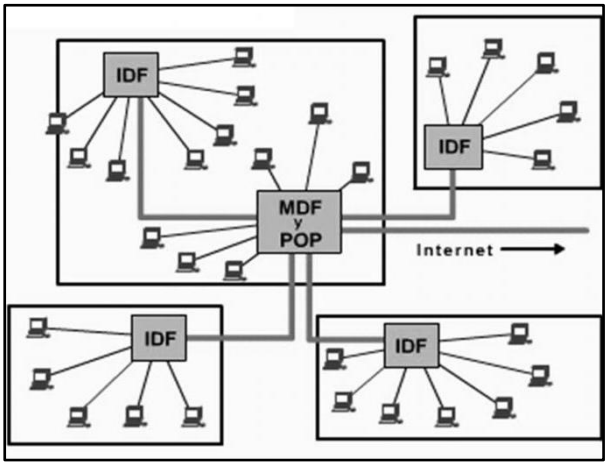
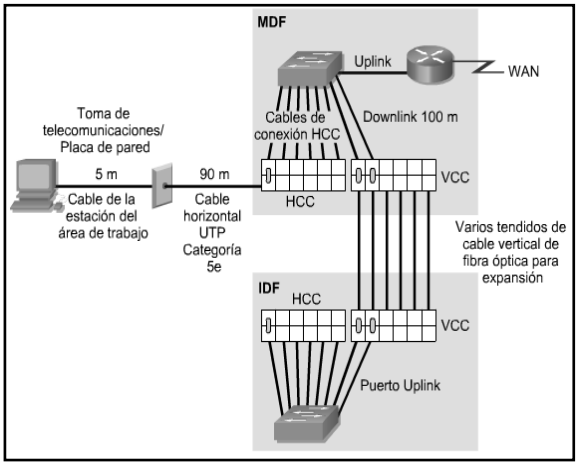


Imagen N° 8.2
Ejemplo de una estructura topológica, mediante
cableado horizontal y vertical



En un sistema de cableado se tienen que tener en cuentas elementos que son sumamente importante para su instalación y mantenimiento, a continuación se nombran algunos de ellos y los tipos de canalizaciones que se emplearían en el tendido de cables.

Cuarto de telecomunicaciones: Es el espacio asociado para las ubicaciones de las terminaciones de cableado, generalmente en armarios tipo RACK, donde se realizara la gestión de todo el cableado estructurado. Debe de ser un cuarto bien dimensionado para permitir posibles ampliaciones, así como instalación de equipos de red y telecomunicaciones, y en donde no es recomendable se comparta el cuarto eléctrico con el de telecomunicaciones.

Canalizaciones externas

Las canalizaciones externas entre edificios son necesarias para interconectar instalaciones de entradas de varios edificios de una misma empresa u organización, en ambientes del tipo campus. La recomendación ANSI/TIA/EIA-569 admite, para estos casos, cuatro tipos de canalizaciones: Subterráneas, directamente enterradas, aéreas, y en túneles.

Canalizaciones subterráneas: Las canalizaciones subterráneas consisten en un sistema de ductos y cámaras de inspección.

Canalizaciones directamente enterradas: En estos casos, los cables de telecomunicaciones quedan enterrados, es importante que los cables dispongan, en estos casos, de las protecciones adecuadas

Canalizaciones de túneles: La ubicación de las canalizaciones dentro de túneles debe ser planificada de manera que permita el correcto acceso al personal de mantenimiento, y también las separaciones necesarias con otros servicios.

Backbone aéreos: Algunas consideraciones a tener en cuenta al momento de tender cableas aéreos:

- Apariencia del edificio y las áreas circundantes
- Legislación aplicable
- Separación requerida con cableados aéreos eléctricos

Canalizaciones internas

Las canalizaciones internas de backbone, generalmente llamadas montantesson las que vinculan las instalaciones de entrada con la sala de equipos, y la sala de equipos con las salas de telecomunicaciones; estas canalizaciones pueden ser ductos, bandejas, escalerillas porta cables, etc.

Es muy importante que estas canalizaciones tengan los elementos cortafuegos de acuerdo a las normas corporativas y/o legales.

Canalizaciones montantes verticales

Estas se emplean para unir la sala de equipos con las salas de telecomunicaciones o las instalaciones de entrada con la sala de equipos en edificios de varios pisos, generalmente, en edificios de varios pisos, las salas de telecomunicaciones se encuentran alineados verticalmente, y una canalización vertical pasa por cada piso, desde la sala de equipos.

Estas canalizaciones pueden ser realizadas con ductos, bandejas verticales, o escalerillas porta cables verticales. No se admite el uso de los ductos de los ascensores para transportar los cables de telecomunicaciones.

Canalizaciones montantes horizontales

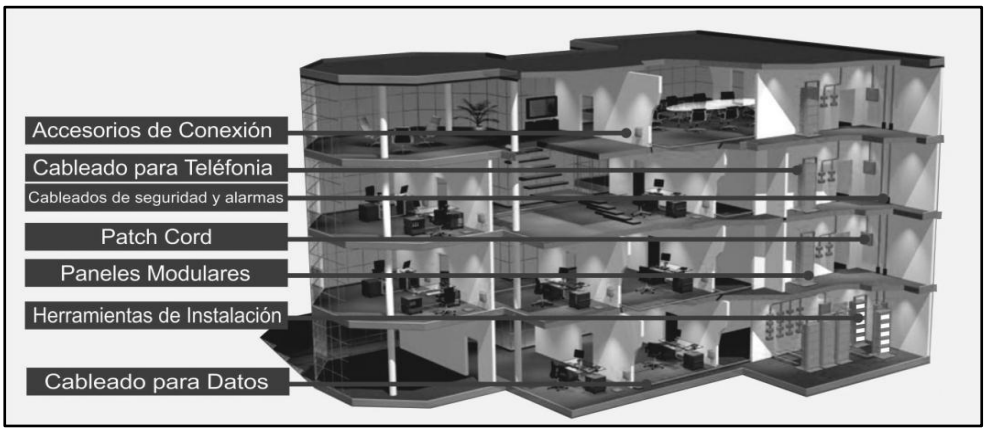
Si las salas de telecomunicaciones no están alineadas verticalmente, son necesarios tramos de montantes horizontales. Estas canalizaciones pueden ser realizadas con ductos, bandejas horizontales, o escalerillas porta cables. Pueden ser ubicadas sobre el cielorraso, debajo del piso, o adosadas a las paredes.

Certificación del cableado:

La certificación de un sistema de cableado estructurado nos muestra la calidad de los componentes y de la instalación, es decir, nos dice si la red de cableado cumple con la normativa y por tanto asegura una conectividad y un funcionamiento correcto.

La certificación del cableado es la única garantía para asegurar que la red cumple con todos los requisitos y soportará los equipos y aplicaciones correspondientes sin ningún tipo de problema, es una documentación imprescindible, y puede ser interna o externa.

Imagen N° 9
Estructura de un edificio mediante la conectividad de cableado estructurado



PUNTO DE DEMARCACIÓN

El punto de demarcación es el punto de la red donde termina la responsabilidad del proveedor del servicio o compañía telefónica; en los Estados Unidos, una compañía telefónica provee bucles locales a las instalaciones del cliente y el cliente provee el equipo activo, como por ejemplo la unidad de servicio del canal/unidad de servicio de datos (CSU/DSU) donde termina el bucle local. Esta terminación a menudo se produce en un armario de telecomunicaciones y el cliente es responsable de mantener, reemplazar y reparar el equipo.

En otros países del mundo, la compañía telefónica provee y administra la unidad de terminación de la red (NTU); esto permite que la compañía telefónica administre y diagnostique de forma activa los problemas en el bucle local cuando el punto de demarcación ocurre después de la NTU.

El cliente conecta un dispositivo del equipo terminal del abonado (CPE), como por ejemplo un router o un dispositivo de acceso de framerelay a la NTU por medio de una interfaz serial V.35 o RS-232.

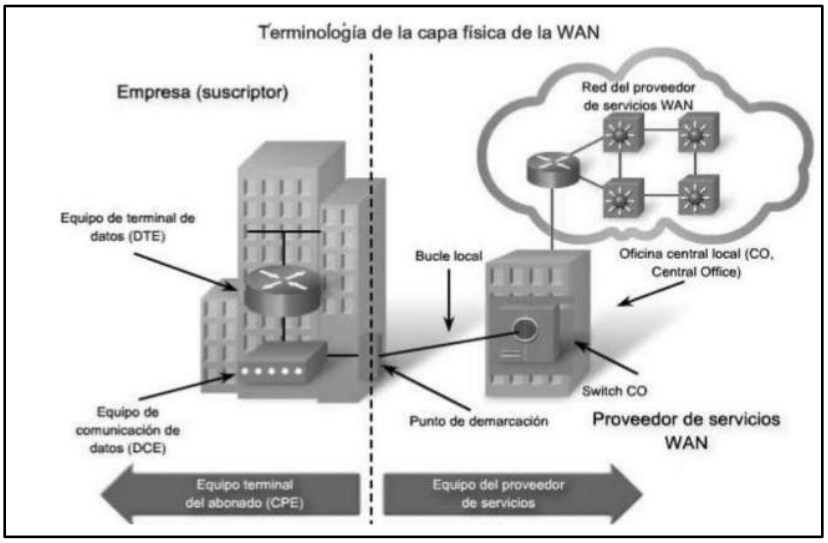


Imagen N° 10.1
Ejemplo de límite de la responsabilidad del servicio entre la empresa (ISP) Y el usuario

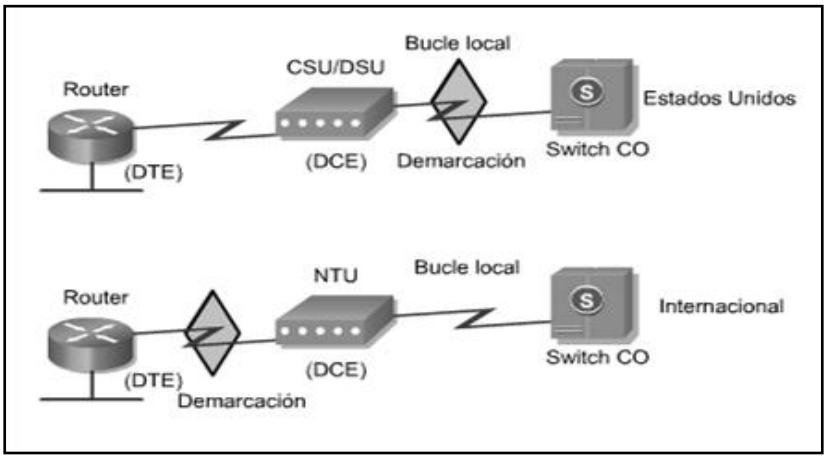


Imagen N° 10.2
Ejemplo del punto de demarcación entre un DCE y un DTE

.

TIPOS DE CONEXIONES EN CABLES HORIZONTALES

Para garantizar el éxito y el correcto funcionamiento de una instalación de cableado estructurado, hay que definir el uso para el cual se va a destinar la red, realizar un correcto dimensionado de los puestos de trabajo y hacer una previsión correcta de las estructuras necesarias para la instalación, las cuales se detallan a continuación:

Cable directo: El cable directo sirve para conectar dispositivos diferentes, como una computadora con switch o router, por ejemplo nuestra PC al modem/router de internet.

En este caso ambos extremos del cable deben de tener la misma distribución. No existe diferencia alguna en la conectividad entre la distribución 568B y la distribución 568A siempre y cuando en ambos extremos se use la misma.

Se utilizan cables de conexión directa para el siguiente cableado:

- Switch a router
- Switch a PC o servidor
- Hub a PC o servidor

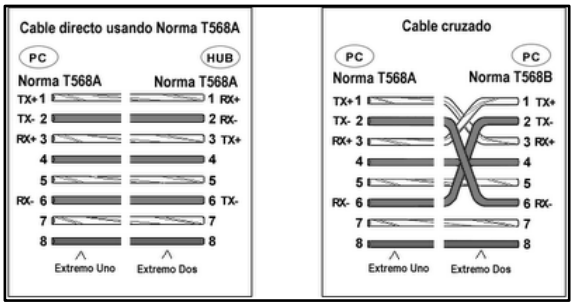


Imagen N° 11.1
Muestra una conexión directa y cruzada de un cable UTP

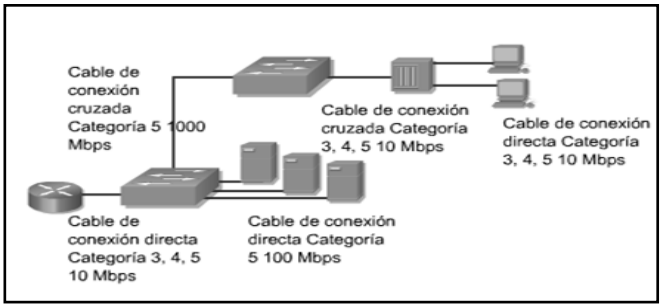
Conexiones cruzadas: Es aquel donde en los extremos la configuración es diferente; el cable cruzado, como su nombre lo dice, cruza las terminales de transmisión de un lado para que llegue a recepción del otro, y la recepción del origen a transmisión del final.

Para crear el cable de red cruzado, lo único que se debe hacer es ponchar un extremo del cable con la norma T568A y el otro extremo con la norma T568B.

Se utilizan cables de conexión cruzada para el siguiente cableado:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a router
- PC a PC
- Router a PC

Imagen N° 10.2
Ejemplo de directas y cruzadas con diferentes dispositivos de red



Estándares De Prueba De Cables

El estándar TIA/EIA-568-B especifica diez pruebas que un cable de cobre debe pasar si ha de ser usado en una LAN Ethernet moderna de alta velocidad; se deben probar todos los enlaces de cables a su calificación más alta aplicable a la categoría de cable que se está instalando.

Los diez parámetros de prueba principales que se deben verificar para que un enlace de cable cumpla con los estándares TIA/EIA son:

- Mapa de cableado
- Pérdida de inserción
- Paradiafonía (NEXT)
- Paradiafonía de suma de potencia (PSNEXT)
- Telediafonía del mismo nivel (ELFEXT)
- Telediafonía del mismo nivel de suma de potencia (PSELFEXT)
- Pérdida de retorno
- Retardo de propagación
- Longitud del cable
- Sesgo de retardo

El mapa del cableado verifica además que la totalidad de los ocho cables estén conectados a los pins correspondientes en ambos extremos del cable, y en donde son varias las fallas de cableado que el mapa de cableado puede detectar, además asegura que no existan circuitos abiertos o cortocircuitos en el cable.

Un circuito abierto ocurre cuando un hilo no está correctamente unido al conector.

Un cortocircuito ocurre cuando dos hilos están conectados entre sí.

La falla de par invertido ocurre cuando un par de hilos está correctamente instalado en un conector, pero invertido en el otro conector; si el hilo blanco/naranja se termina en el pin 1 y el hilo naranja se termina en el pin 2 en uno de los extremos de un cable, pero de forma invertida en el otro extremo, entonces el cable tiene una falla de par invertido.

Una falla de cableado de par dividido ocurre cuando un hilo de un par se cruza con un hilo de un par diferente; esta mezcla entorpece el proceso de cancelación cruzada y hace el cable más susceptible a la diafonía y la

interferencia. Observe con atención los números de pin en el gráfico para detectar la falla de cableado. Un par dividido da lugar a dos pares transmisores o receptores, cada uno con dos hilos no trenzados entre sí.

Las fallas de cableado de pares transpuestos se producen cuando un par de hilos se conecta a pins completamente diferentes en ambos extremos. Compare esto con un par invertido, en donde el mismo par de pins se usa en ambos extremos.

Imagen N° 11.1
Tipos de mapeo de cable UTP

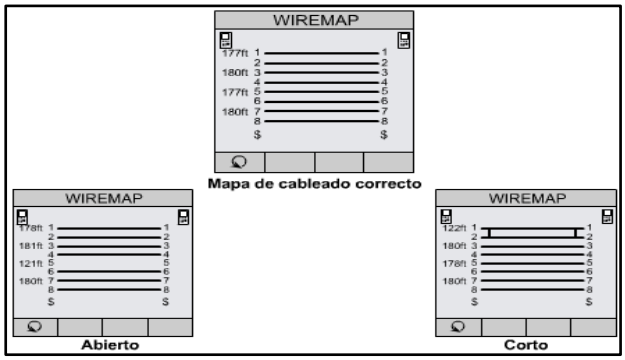
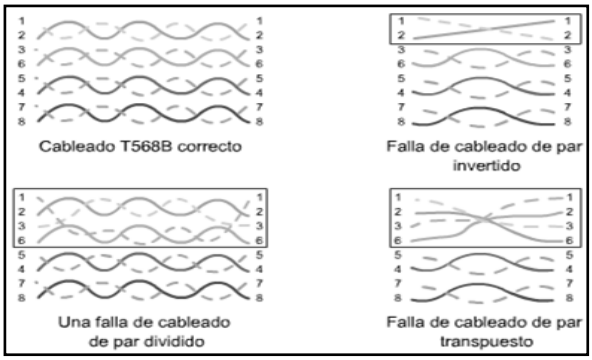


Imagen N° 11.2
Tipos de fallas cable UTP



Por último se podría decir que una vez instalado el sistema de cableado estructurado en la organización, se obtendría una serie de beneficios, que en su conjunto harán que la misma tenga un mejor resultado y eficacia con sus procesos internos y externos.

Dentro de los **Beneficios del Cableado Estructurado** se encuentran:

- Administración rápida y sencilla de cambios de ubicación del personal de la empresa; si se desean hacer cambios, un sistema de cableado de red bien definido permite que estos sean rápidos y sencillos.
- Es posible que exista la convivencia de varios servidores en red, como voz, datos e imagen, web, base de datos, http entre otros.
- Tienen un periodo largo de vida útil. Ofrece a la organización una topología de comunicaciones que se conoce como cableado abierto, porque soporta todas las tecnologías actuales y futuras , y en caso de ser necesario a partir de entonces se podrá reemplazar la vieja infraestructura por una más actualizada sin necesidad de realizar una gran inversión , en la restructuración total del cableado
- facilita y agiliza mucho las labores de mantenimiento

MODELO DE REFERENCIA OSI Y PROTOCOLO TCP/IP

Funciones y Capa

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO el cual proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

Tiene siete niveles y no es una arquitectura particular, porque no especifica los detalles de los niveles, sino que los estándares de ISO existen para cada nivel.

Nivel físico. Cuestiones: los voltajes, la duración de un bit, el establecimiento de una conexión, el número de polos en un enchufe, etc.

Nivel de enlace. El propósito de este nivel es convertir el medio de transmisión crudo en uno que esté libre de errores de transmisión.

- El remitente parte los datos de input en marcos de datos (algunos cientos de bytes) y procesa los marcos de acuse.
- Este nivel maneja los marcos perdidos, dañados, o duplicados.
- Regula la velocidad del tráfico.
- En una red de broadcast, un subnivel (el subnivel de acceso medio, o médium Access sublayer) controla el acceso al canal compartido.

Nivel de red. Determina el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez. Se incorpora la función de contabilidad.

Nivel de transporte. Es el primer nivel que se comunica directamente con su par en el destino (los de abajo son de máquina a máquina); provee varios tipos de servicio (por ejemplo, un canal punto-a-punto sin errores); podría abrir conexiones múltiples de red para proveer capacidad alta.

Se puede usar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples entrando en una máquina; provee el control de flujo entre los hosts.

Nivel de sesión. Parecido al nivel de transporte, pero provee servicios adicionales.; por ejemplo, puede manejar tokens (objetos abstractos y únicos) para controlar las acciones de participantes o puede hacer checkpoints (puntos de recuerdo) en las transferencias de datos.

Nivel de presentación. Provee funciones comunes a muchas aplicaciones tales como traducciones entre juegos de caracteres, códigos de números, etc.

Nivel de aplicación. Define los protocolos usados por las aplicaciones individuales, como e-mail, telnet, etc.

Imagen N° 12.1
El modelo OSI Y sus respectivos protocolos según su capa correspondiente

Capas Modelo OSI	Protocolos
APLICACIÓN	TELNET, FTP, SNMP, NNTP, SSH, SMTP, POP3, DNS, RTP, NFS, HTTP
PRESENTACIÓN	ASN.1
SESIÓN	NetBIOS
TRANSPORTE	TCP, UDP
RED	ARP, IP(IPv4/IPv6), ICMP, X.25
ENLACE DE DATOS	ETHERNET, FAST ETHERNET, GIGABIT ETHERNET, FDDI, ATM, HDLC
FISICA	CGI, MIME, IEEE

Existen diferentes formas de ampliar una red aislada o interconectar redes individuales, con dispositivos de interconexión de redes y son:

- **Repetidor (Repeater) :** Capa física del modelo OSI
- **Concentrador (Hub) :** Capa física del modelo OSI
- **Puente (Bridge):** Capa física y de enlace de datos capa 2 del modelo OSI.
- **Conmutador (switch):** Actúan como filtros en la Capa de enlace de datos (Capa2) del Modelo OSI.
- **Router:** Capa 3 del Modelo OSI (Físico, enlace de datos y red).
- **Pasarela (Gateway) :** Niveles de transporte, sesión, presentación y aplicación del modelo OSI

Imagen N° 12.2
El modelo OSI Y sus respectivos elementos de red según su capa correspondiente

COMUNICACIONES DE PAR A PAR

Para que los datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino, esta forma de comunicación se conoce como de par-a-par.

Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo (PDU), donde cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino.

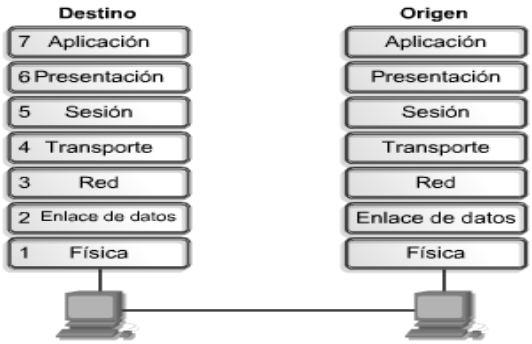


Imagen N° 12.1
Ejemplo de capa par a par mediante el modelo OSI

Las comunicaciones par a par se define también como una red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí, es decir actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

También se las llama redes peer-to-peer que aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, obteniendo más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.

Algunas características de comunicación par a par serian:

- Es un medio de comunicación emisor y receptor.
- También llamada P2P.
- A medida que la red crece las relaciones se vuelven complicadas de coordinar.
- No es necesario definir personal administrativo.

TCP/IP

El 1968 la Agencia de investigación de Proyectos Avanzados del Departamento de Defensa de EE.UU. (DARPA) comienza un programa de desarrollo que permitiese la transmisión de información entre redes de distintos tipos y características.

Se implementó una red punto a punto de líneas telefónicas denominada ARPANET, usando un conjunto de protocolos que posteriormente se denominarían TCP/IP, donde esta red formada por organizaciones educativas, militares y de investigación se convirtió en el núcleo de Internet hacia 1980, y en 1983, todos los hosts de ARPANET utilizaban dicho conjunto de protocolos

La Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos de Norteamérica definió un conjunto de reglas que establecieron cómo conectar computadoras entre sí para lograr el intercambio de información, soportando incluso desastres mayores en la subred. Fue así como se definió el conjunto de protocolos de TCP/IP (TCP/IP Internet Suite of Protocols).

Para los años 80 una gran cantidad de instituciones estaban interesadas en conectarse a esta red que se expandió por todo EEUU.

TCP/IP es un protocolo abierto, lo que significa que se publican todos los aspectos concretos del protocolo y cualquiera los puede implementar.

TCP/IP está diseñado para ser un componente de una red, principalmente la parte del software. Todas las partes del protocolo de la familia TCP/IP tienen unas tareas asignadas como enviar correo electrónico, proporcionar un servicio de acceso remoto, transferir datos, asignar rutas a los mensajes o gestionar caídas de la red.

Una red TCP/IP transfiere datos mediante el ensamblaje de bloque de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control, tal como la dirección del destino, seguida de los datos;cuando se envía un archivo a través de una red TCP/IP, su contenido se envía utilizando una serie de paquetes diferentes.

La Suite de TCP/IP consta de 4 capas principales que se han convertido en un estándar a nivel mundial.

Las siguientes cuatro capas se detallan a continuación:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red

Nivel de internet. Los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino; no hay garantías de entrega ni de orden. Este nivel define el Internet Protocol (IP), que provee el ruteo y control de congestión.

Nivel de transporte. Permite que pares en los hosts de fuente y destino puedan conversar. Hay dos protocolos:

- **Transmission Control Protocol (TCP).** Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la internet; parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.
- **UserDatagramProtocol (UDP).** Es un protocolo no confiable y sin conexión para la entrega de mensajes discretos. Se pueden construir otros protocolos de aplicación sobre UDP; también se usa UDP cuando la entrega rápida es más importante que la entrega garantizada.

Nivel de aplicación. Como en OSI. No se usan niveles de sesión o presentación.

Algunos de los protocolos de capa de aplicación más usados son:

- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Sistema de denominación de dominios (DNS)
- Protocolo Trivial de Transferencia de Archivos (TFTP)

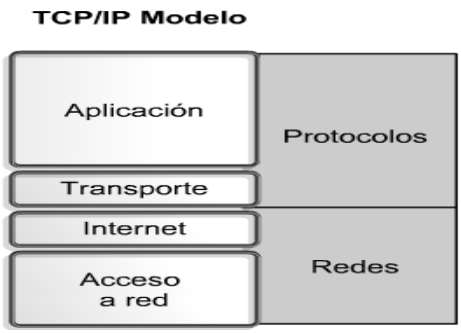


Imagen N° 13
Modelo TCP/IP y sus protocolos

TCP/IP Características

- Estándar en Estados Unidos desde 1983.
- Dispone de las mejores herramientas para crear grandes redes de ordenadores.
- Independencia del fabricante.

Ventajas

- Encaminable.
- Imprescindible para Internet.
- Soporta múltiples tecnologías.
- Puede funcionar en máquinas de todo tamaño (multiplataforma).

Desventajas

- El modelo no distingue bien entre servicios, interfaces y protocolos, lo cual afecta al diseño de nuevas tecnologías en base a TCP/IP.
- Peor rendimiento para uso en servidores de fichero e impresión.

OSI Características

- OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.
- Servicio: lo que un nivel hace.
- Interfaz cómo se pueden acceder los servicios.
- Protocolo: la implementación de los servicios.
- TCP/IP no tiene esta clara separación.

Ventajas

- Proporciona a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Desventajas

- Las capas contienen demasiadas actividades redundantes, por ejemplo, el control de errores se integra en casi todas las capas siendo que tener un único control en la capa de aplicación o presentación sería suficiente.
- La gran cantidad de código que fue necesario para implantar el modelo OSI y su consecuente lentitud hizo que la palabra OSI fuera interpretada como "calidad pobre", lo que contrastó con TCP/IP que se implantó exitosamente en el sistema operativo Unix y era gratis.

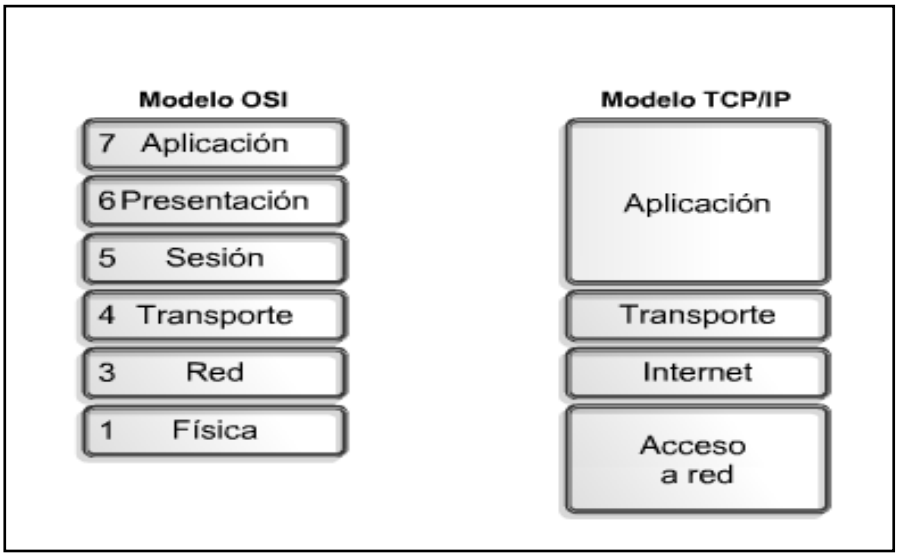
Semejanzas

- La funcionalidad de las capas es muy similar.
- Las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.
- Ambos se basan en el concepto de un gran números de protocolos independientes

Diferencias

- El modelo OSI se desarrolló antes de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos.
- En TCP/IP primero llegaron los protocolos. El modelo fue una descripción de los protocolos existentes.
- El modelo OSI apoya la conexión tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte que es más importante(por que el servicio de transporte es visible a los usuarios) lo hace únicamente con la comunicación orientada a las conexión.
- El modelo TCP/IP sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos en la capa de transporte, con lo que ofrece una alternativa a los usuarios.

Imagen N° 13
Comparación de las diferentes capas entre el OSI Y EL Modelo TCP/IP.



PROCESO DE ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear donde las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos, también asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto.

Luego la capa de red encapsula el segmento creando un paquete, le agrega al paquete una dirección de red destino y origen, por lo general IP.

En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino, luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino, pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).

Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet, donde la excepción principal a esto es un dispositivo denominado Gateway;. este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato.

Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

Crear los datos. Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.

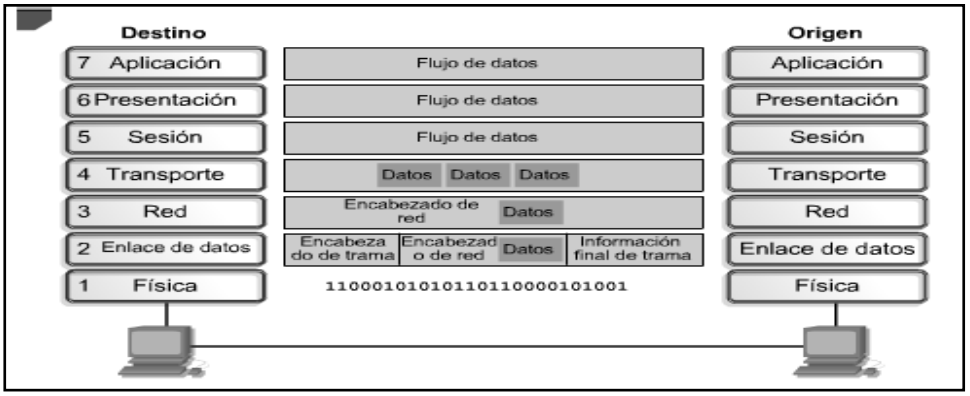
Empaquetar los datos para ser transportados de extremo a extremo. Los datos se empaquetan para ser transportados por la internetwork; al utilizar segmentos, la función de transporte asegura que los hosts de mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

Agregar la dirección de red IP al encabezado. Los datos se colocan en un paquete o datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y de destino; estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

Agregar el encabezado y la información final de la capa de enlace de datos. Cada dispositivo de la red debe poner el paquete dentro de una trama; la trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace; cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

Realizar la conversión a bits para su transmisión. La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio; una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada, por ejemplo, el mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de una universidad y salir por un enlace WAN hasta llegar a su destino en otra LAN remota.

Imagen N° 14
Ejemplo del proceso de encapsulamiento



LOS DISPOSITIVOS EN UNA RED

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo. Los dispositivos conectados a una red informática pueden clasificarse en dos tipos:

Los que gestionan el acceso y las comunicaciones en una red (dispositivos de red), como módem, router, switch, access point, bridge, etc.; y los que se conectan para utilizarla (dispositivos de usuario final), como computadora, notebook, tablet, teléfono celular, impresora, televisor inteligente, consola de videojuegos, etc.

Los que utilizan una red, a su vez, pueden cumplir dos roles (clasificación de redes por relación funcional): servidor, en donde el dispositivo brinda un servicio para todo aquel que quiera consumirlo; o cliente, en donde el dispositivo consume uno o varios servicios de uno o varios servidores. Este tipo de arquitectura de red se denomina cliente/ servidor.

Por otro lado, cuando todos los dispositivos de una red pueden ser clientes y servidores al mismo tiempo y se hace imposible distinguir los roles, estamos en presencia de una arquitectura punto a punto o peer to peer.

A continuación veremos los tipos de dispositivos que encontramos en una red:

Módems: Los populares módems, son dispositivos que tienen la importante función de comunicar los equipos informáticos que forman parte de una red con el mundo exterior, es decir, es el aparato en donde se conecta el cable principal de red y que recibe la información de la línea telefónica, donde también estos dispositivos pueden conectar varias redes entre sí.

El funcionamiento de los modem es simple. la computadora envía señales digitales que son convertidas a señales analógicas en el modem emisor y viajan a través de líneas telefónicas hasta su destino, donde el modem receptor convierte la señal analógica nuevamente en una señal digital que podrá ser interpretada por un ordenador.

El modem cuenta con una interfaz de comunicación en serie (RS-232) y una interfaz de línea telefónica RJ-11. Las velocidades de transmisión de datos de los modems actuales van desde 57500 bps hasta 76800 bps

Tarjeta de red: se suele asociar a una tarjeta de expansión insertada en una ranura interna de un computador o impresora, se suele utilizar para referirse también a dispositivos integrados (del inglés embebed) en la placa madre del equipo, como las interfaces presentes en la videoconsola Xbox o los notebooks, Igualmente se usa para expansiones con el mismo fin que en nada recuerdan a la típica tarjeta con chips y conectores soldados, como la interfaz de red para la Sega Dreamcast, las PCMCIA, o las tarjetas con conector y factor de forma CompactFlash y Secure Digital SIO utilizados en PDAs
Cada tarjeta de red tiene un número de identificación único de 48 bits, en hexadecimal llamado dirección MAC (no confundir con Apple Macintosh); estas direcciones hardware únicas son administradas por el Institute of Electronic and ElectricalEngineers (IEEE). Los tres primeros octetos del número MAC son conocidos como OUI e identifican a proveedores específicos y son designados por la IEEE.
Se denomina también NIC al chip de la tarjeta de red que se encarga de servir como interfaz de Ethernet entre el medio físico (por ejemplo un cable coaxial) y el equipo (por ejemplo un ordenador personal o una impresora); es un chip usado en computadoras o periféricos tales como las tarjetas de red, impresoras de red o sistemas intergrados (embebed en inglés), para conectar dos o más dispositivos entre sí a través de algún medio, ya sea conexión inalámbrica, cable UTP, cable coaxial, fibra óptica, etcétera.

Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

.

Un concentrador o hub es un dispositivo que permite centralizar el cableado de una red y poder ampliarla, esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

Un concentrador, o repetidor, es un dispositivo de emisión bastante sencillo. Los concentradores no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otro puerto (que no sea el puerto de entrada), dado que cada paquete está siendo enviado a través de cualquier otro puerto, aparecen las colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan; al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

Un repetidor es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable; en telecomunicación el término repetidor tiene los siguientes significados normalizados:

- **Un dispositivo analógico** que amplifica una señal de entrada, independientemente de su naturaleza (analógica o digital).
- **Un dispositivo digital** que amplifica, conforma, retemporiza o lleva a cabo una combinación de cualquiera de estas funciones sobre una señal digital de entrada para su retransmisión.

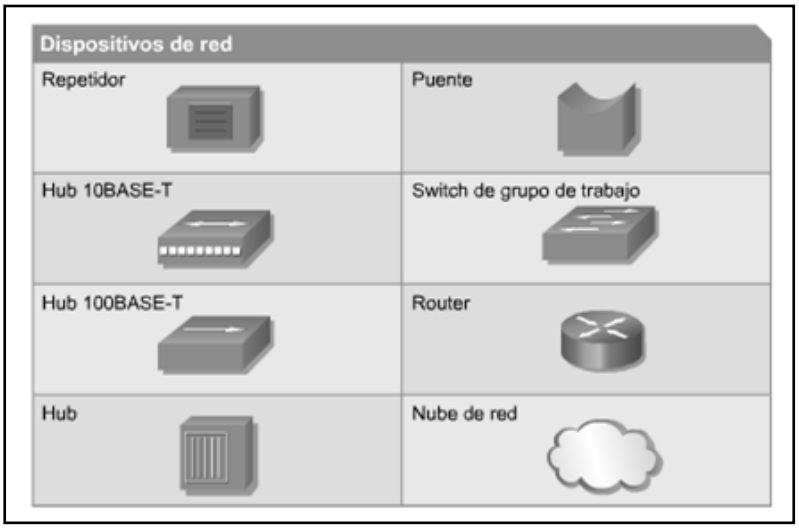
Bridges: Los Bridges son dispositivos que tiene una finalidad muy parecida a la de los repetidores, pero a diferencia de estos, pueden dividir una red para aislar un ala de esta y poder realizar las reparaciones que se requieran.

Los Bridges son utilizados, por lo general, para:

- Extender la longitud de un segmento de red.
- Incrementar el número de ordenadores de una red.
- Reducir el efecto de cuello de botella de una red.
- Dividir redes sobrecargadas.
- Enlazar medios físicos

Gateway: Son dispositivos activan la comunicación entre arquitecturas y entornos y realizan el empaquetado y conversión de paquetes de datos que se van a transmitir a través de una red.

Dispositivos de red inalámbricos: Son dispositivos de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. En ese sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, como por ejemplo: Antenas, Laptops, PDAs, Teléfonos Celulares, rotre inalámbricos acces point entre otros, los cuales se hablaran y detallaran en capítulos posteriores.



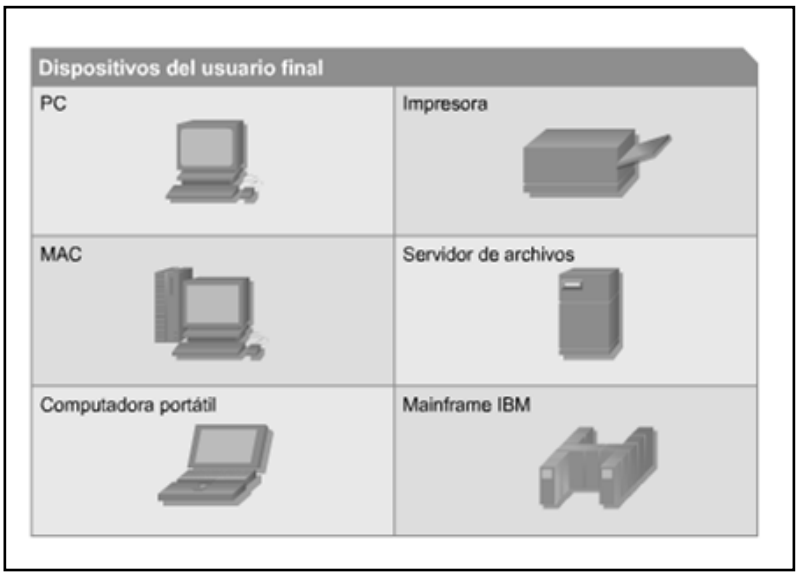


Imagen N° 15
Ejemplo del los diferentes elementos red que se utilizan en las s distintas topologías

TOPOLOGÍA DE RED

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medio; la otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Las topologías físicas más comúnmente usadas son las siguientes:

- **Una topología de bus** usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- **La topología de anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- **La topología en estrella** conecta todos los cables con un punto central de concentración.
- **Una topología en estrella extendida** conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- **Una topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- **La topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio; el uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Cada host tiene sus propias conexiones con los demás hosts, aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.
- **La topología lógica** de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.
- **La topología broadcast** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red; no existe una orden que las estaciones deban seguir para utilizar la red, es por orden de

llegada. Ethernet funciona así, tal como se explicará en el curso más adelante.

- **La segunda topología lógica** es la transmisión de tokens, la transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

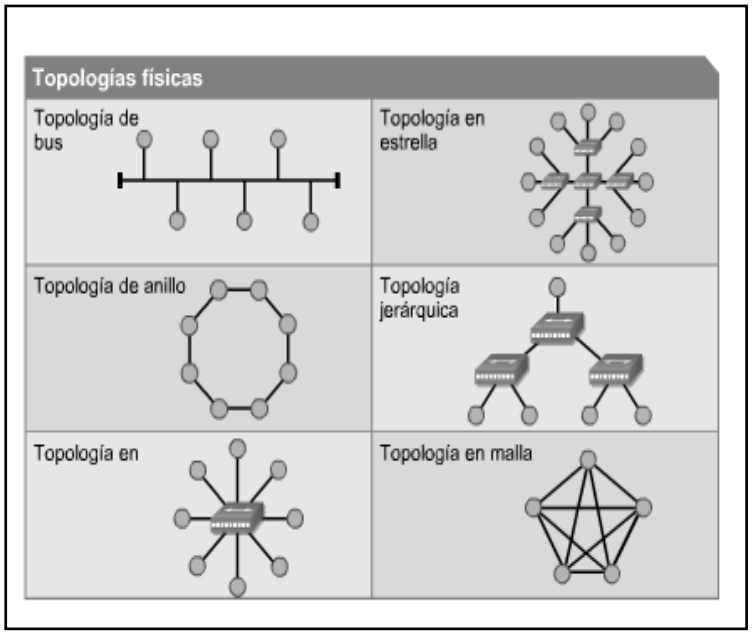


Imagen N° 14.1
Ejemplo de las diferentes topologías de red

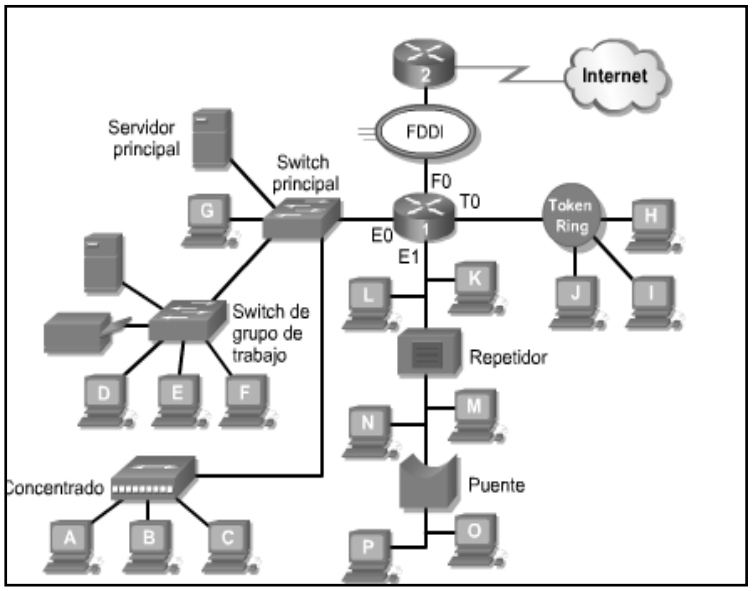


Imagen N° 14.2
Ejemplo de las diferentes redes, con diferentes topologías

TECNOLOGÍA ETHERNET

Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CDes Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. El nombre viene del concepto físico de ether, donde Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

La Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3 es además una especificación para redes de área local , que comprende el nivel físico y el nivel de enlace del modelo de referencia OSI, el cual se basa sobre una topología bus serie con mecanismo CSMA/CD para el acces o al medio. „

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet. Desde su inicio en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. Cuando se introdujo el medio de fibra óptica, Ethernet se adaptó a esta nueva tecnología para aprovechar el mayor ancho de banda y el menor índice de error que ofrece la fibra.

La primera LAN (Red de área local) del mundo fue la versión original de Ethernet; el primer estándar de Ethernet fue publicado por un consorcio formado por Digital EquipmentCorporation, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto; los primeros productos que se desarrollaron a partir del estándar de Ethernet se vendieron a principios de la década de 1980.

El IEEE tomó Ethernet como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos.

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

En Ethernet se separan las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC); las funciones descritas en el

modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC, el empleo de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

Control de acceso al medio

Algunas topologías de red, como ethernet, comparten un medio común con varios nodos. En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los medios de red, donde hay reglas que rigen cómo esos dispositivos comparten los medios.

Hay dos métodos básicos de control de acceso al medio para medios compartidos:

- **Acceso controlado para medios compartidos:** Al utilizar el método de acceso controlado, los dispositivos de red toman turnos, en secuencia, para acceder al medio, a este método se lo conoce como acceso programado o determinístico; si un dispositivo no necesita acceder al medio, la oportunidad de utilizar el medio pasa al siguiente dispositivo en línea, cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino.

Aunque el acceso controlado está bien ordenado y provee rendimiento predecible, los métodos determinísticos pueden ser ineficientes porque un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

- **Acceso por contención para medios compartidos:** Estos métodos por contención, también llamados no deterministas, permiten que cualquier dispositivo intente acceder al medio siempre que haya datos para enviar.

  Para evitar caos completo en los medios, estos métodos usan un proceso de Acceso múltiple por detección de portadora (CSMA) para detectar primero si los medios están transportando una señal, si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo; cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto, si no se detecta una señal portadora, el dispositivo transmite sus datos.
  Las redes Ethernet e inalámbricas utilizan control de acceso al medio por contención, es posible que el proceso CSMA falle si dos dispositivos transmiten al mismo tiempo; a esto se lo denomina colisión de datos, si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente; los métodos de control de acceso al medio por contención no tienen la sobrecarga de los métodos de acceso controlado.

  No se requiere un mecanismo para analizar quién posee el turno para acceder al medio. Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios.

  A medida que el uso y el número de nodos aumentan, la probabilidad de acceder a los medios con éxito sin una colisión disminuye, además, los mecanismos de recuperación requeridos para corregir errores debidos a esas colisiones disminuyen aún más el throughput.CSMA es generalmente implementado junto con un método para resolver la contención del medio.

Los dos métodos comúnmente utilizados son:

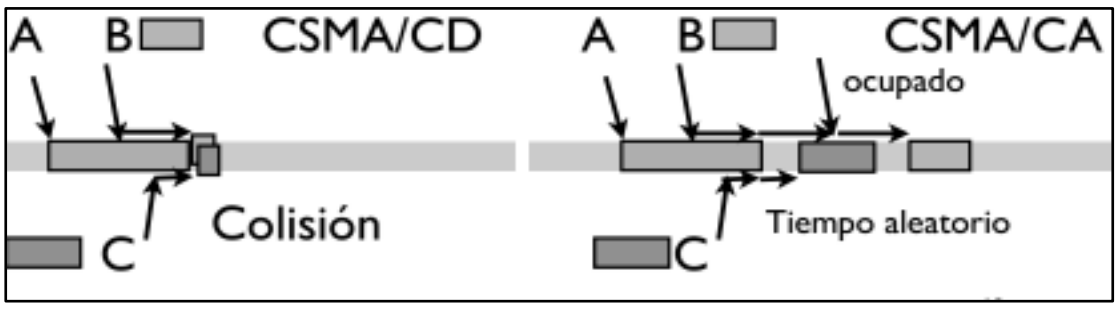
- **CSMA/Detección de colisión (CSMA/CD),** aquí el dispositivo monitorea los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet usan este método.
- **En CSMA/Prevención de colisiones (CSMA/CA),** 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 802.11.

Las primeras implementaciones de Ethernet se utilizaron en entornos LAN de bajo ancho de banda en los que el acceso a los medios compartidos se administraba mediante CSMA y, posteriormente, mediante CSMA/CD.

Los protocolos de control de acceso al medio para medios no compartidos requieren poco o ningún control antes de colocar tramas en los medios. Estos protocolos tienen reglas y procedimientos más simples para el control de acceso al medio. Tal es el caso de las topologías punto a punto.

En las topologías punto a punto, los medios interconectan sólo dos nodos. En esta configuración, los nodos no necesitan compartir los medios con otros hosts ni determinar si una trama está destinada para ese nodo; por lo tanto, los protocolos de capa de enlace de datos hacen poco para controlar el acceso a medios no compartidos.

Imagen N° 14.3
Ejemplo de métodos de acceso al medio de Ethernet



Direccionamiento de hardware Ethernet

Las redes Ethernet definen un esquema de direccionamiento de 48 bits, cada computadora conectada a una red Ethernet es asignada a un número único de 48 bits conocido como dirección Ethernet. Para asignar una dirección, los fabricantes de hardware de Ethernet adquieren bloques de direcciones Ethernet y las asignan en secuencia conforme fabrican el hardware de interfaz Ethernet. De esta manera no existen dos unidades de hardware de interfaz que tengan la misma dirección Ethernet.

Por lo general, las direcciones Ethernet se fijan en las máquinas en el hardware de interfaz de anfitrión de forma que se puedan leer; debido a que el direccionamiento Ethernet se da entre dispositivos de hardware, a estos se les llama a veces direccionamientos o direcciones físicas.

Las propiedades importantes de las direcciones físicas Ethernet son:

- Las direcciones físicas están asociadas con el hardware de interfaz Ethernet; cambiar el hardware de interfaz a una máquina nueva o reemplazar el hardware de interfaz que ha fallado provocará cambios en la dirección física de la máquina.
- Conociendo la dirección física Ethernet se pueden hacer cambios con facilidad porque los niveles superiores del software de red están diseñados para adaptarse a estos cambios.
- El hardware de interfaz anfitrión examina los paquetes y determina qué paquetes deben enviarse al anfitrión. Debe recordarse que cada interfaz recibe una copia de todos los paquetes aun cuando estén direccionados hacia otras máquinas. La interfaz de anfitrión utiliza el campo de dirección de destino de un paquete como filtro. La interfaz ignora los paquetes que esté direccionados hacia otra máquina y selecciona sólo los paquetes direccionados hacia el anfitrión.
- El mecanismo de direccionamiento y filtrado de hardware es necesario para prevenir que una computadora sea abrumada con la entrada de datos. Aun cuando el procesador central de la computadora podría realizar la verificación, ésta se realiza en la interfaz de anfitrión haciendo que el tráfico en la red Ethernet sea un proceso menos lento en todas las computadoras.

Una dirección Ethernet de 48 bits puede hacer más que especificar una sola computadora destino, pudiendo ser alguno de los tres tipos siguientes:

- La dirección física de una interfaz de red (dirección de unidifusión).
- La dirección de publidifusión de la red.
- Una dirección de multidifusión

Convencionalmente, la dirección de difusión se reserva para envíos simultáneos a todas las estaciones. Las direcciones de multidifusión proporcionan una forma limitada de difusión en la cual un subconjunto de computadoras en una red acuerda recibir una dirección de multidifusión dada. El conjunto de computadoras participantes se conoce como grupo de multidifusión, para unirse a un grupo de multidifusión, una computadora debe instruir a la interfaz anfitrión para aceptar las direcciones de multidifusión del grupo, la ventaja de la multidifusión reside en la capacidad para limitar la difusión: todas las computadoras en un grupo de multidifusión pueden ser alcanzadas con un solo paquete de transmisión, pero las computadoras que eligen no participar en un grupo de multidifusión en particular no recibirán los paquetes enviados al grupo.

Para adaptarse al direccionamiento de multidifusión y difusión, el hardware de interfaz Ethernet debe reconocer más que la dirección física; una interfaz anfitrión por lo general acepta hasta dos clases de paquete: los direccionados a la dirección física de la interfaz (esto es, unidifusión) y las direcciones hacia la dirección de difusión de la red.

Algunos tipos de interfaz pueden programarse para reconocer direcciones de multidifusión o para alternar entre direcciones físicas; y cuando el sistema operativo comienza a trabajar, éste inicia la interfaz Ethernet, haciendo que se reconozca un conjunto de direcciones.

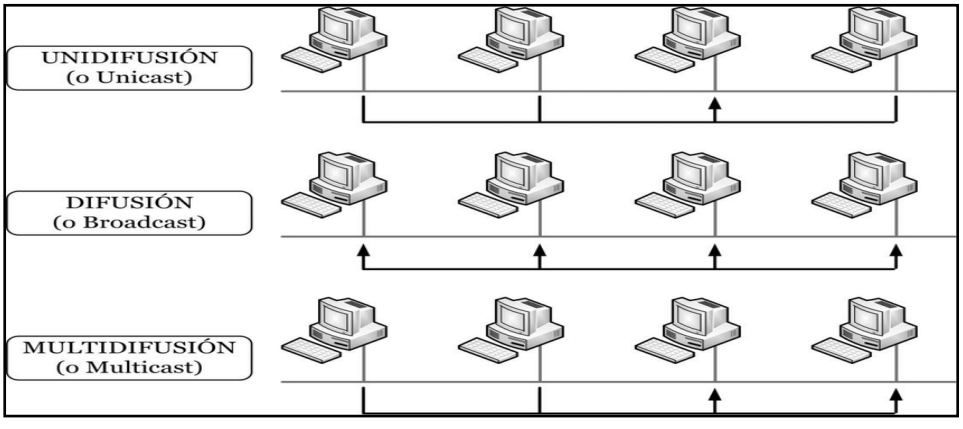


Imagen N° 14.4
Ejemplo de tipos de comunicación Ethernet

FORMATO DE LA TRAMA ETHERNET

La red Ethernet podría pensarse como una conexión de niveles enlazados entre máquinas, de esta manera, la información transmitida podría tener el aspecto de una trama. La trama Ethernet es de una longitud variable pero no es menor a 64 octetos ni rebasa los 1518 octetos (encabezado, datos y CRC). Como en todas las redes de conmutación de paquetes, cada trama Ethernet contiene un campo con la información de la dirección de destino.

Imagen N° 15
Ejemplo de una trama ETHERNET

Preámbulo	Destino	Fuente	Tipo	Datos	CRC
8 octetos	6 octetos	6 octetos	2 octetos	64-1500 octetos	4 octetos

Además de la información para identificar la fuente y el destino, cada trama transmitida a través de Ethernet contiene un preámbulo, un campo de tipo, un campo de datos y una CyclicRedundancyCheck (verificación por redundancia cíclica o CRC, por sus siglas en inglés).

El preámbulo consiste en 64 bits que alternan ceros y unos para ayudar a la sincronización de los nodos de recepción. El CRC de 32 bits ayuda a la interfaz a detectar los errores de transmisión: el emisor computa el CRC como una función de los datos de la trama y el receptor computa de nuevo el CRC para verificar que el paquete se ha recibido intacto.

El campo de tipo de trama contiene un entero de 16 bits que identifica el tipo de datos que se están transfiriendo en la trama; desde el punto de vista de Internet, el campo de tipo de trama es esencial porque significa que las tramas de Ethernet se auto identifican; cuando una trama llega a una máquina dada, el sistema operativo utiliza el tipo de trama para determinar que módulo de software de protocolo se utilizará para procesar la trama.

La mayor ventaja de que las tramas se auto identifiquen es que éstas permiten que múltiples protocolos se utilicen juntos en una sola máquina y sea posible entremezclar diferentes protocolos en una sola red física sin interferencia. Por ejemplo, uno podría tener un programa de aplicación que utiliza protocolos de Internet, mientras otro utiliza un protocolo experimental local, y el sistema operativo utiliza el campo de tipo de una trama entrante para decidir cómo procesar el contenido.

TIPOS DE ETHERNET

El modo en que las tramas IEEE 802.3 son puestas en el medio de transmisión físico depende de las especificaciones de hardware y de los requerimientos del tipo de cableado elegido; por lo tanto se definen varios estándares, todos ellos integrados dentro de la IEEE 802.3, que especifican el tipo de conector y de cable que es preciso para alcanzar los rendimientos previstos utilizando siempre el método CSMA/CD.

Algunos de estos estándares son los siguientes:

- **1BASE-5:** El estándar IEEE para Ethernet en banda base a 1Mb/s sobre cable par trenzado a una distancia máxima de 250m.
- **10BASE-5 :** Es el estándar IEEE para Ethernet en banda base a 10Mb/s sobre cable coaxial de 50 Ω troncal y AUI (attachmentunit interface) de cable par trenzado a una distancia máxima de 500m.
- **10BASE-2:** El estándar IEEE para Ethernet en banda base a 10MB/s sobre cable coaxial delgado de 50 Ω con una distancia máxima de 185m.
- **10BROAD-36:** El estándar IEEE para Ethernet en banda ancha a 10Mb/s sobre cable coaxial de banda ancha de 75 Ω con una distancia máxima de 3600m.
- **10BASE-T:** El estándar IEEE para Ethernet en banda base a 10 Mb/s sobre cable par trenzado sin blindaje (UnshieldedTwistedPair o UTP) siguiendo una topología de cableado horizontal en forma de estrella, con una distancia máxima de 100m desde una estación a un hub.
- **10BASE-F:** El estándar IEEE para Ethernet en banda base a 10Mb/s sobre fibra óptica con una distancia máxima de 2.000 metros (2Km).
- **FastEthernet : 100BASE-TX** El estándar IEEE para Ethernet en banda base a 100Mb/s sobre dos pares (cada uno de los pares de categoría 5 o superior) de cable UTP o dos pares de cable STP.
- **100BASE-T4:** El estándar IEEE para Ethernet en banda base a 100Mb/s sobre 4 pares de cable UTP de categoría 3 (o superior).
- **100BASE-FX:** Es el estándar IEEE para Ethernet en banda base a 100Mb/s sobre un sistema de cableado de dos fibras ópticas de 62.5/125 m.

- **100BASE-T2:** El estándar IEEE para Ethernet en banda base a 100Mb/s sobre 2 pares de categoría 3 (o superior) de cable UTP.
- **Gigabit Ethernet :** 1000BASE-SX El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 2 fibras multimodo (50/125 m o 62.5/125 m) de cableado de fibra óptica.
- **1000BASE-LX :** El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 2 fibras monomodo o multimodo (50/125 m or 62.5/125 m) de cableado de fibra óptica.
- **1000BASE-T :** El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 4 pares de categoría 5 o superior de cable UTP, con una distancia máxima de cableado de 100m.

Metro Ethernet: Metro Ethernet Es considerada como una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs Ethernet. Estas redes se basan en sistemas multiservicio, es decir que soportan una amplia gama de servicios, aplicaciones y mecanismos donde se incluye soporte de trafico "RTP" tiempo real, streaming, flujo de datos continuo como por ejemplo audio y vídeo, como puede ser Telefonía IP y Video IP, este tipo de trafico resulta especialmente sensible a retardo y al jitter.

- La utilización de las lineas de cobre (MAN BUCLE), garantiza el despliegue de un punto de red ethernet, en cualquier punto del casco urbano.
- Las redes Metro Ethernet, están soportadas por medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones de radio licenciada, los caudales proporcionados son de 10Mbps, 20Mbps, 34Mbps, 100Mbps, 1Gbps y 10Gbps.
- La tecnología de agregación de múltiples pares de cobre, (MAN BUCLE), permite la entrega de entre 10 Mbps, 20 Mbps, 34Mbps y 100Mbps, mediante la transmisión simultánea de multipleslineas de cobre, además esta tecnica cuenta con muy alta disponibilidad ya que imposible la rotura de todas las lineas de cobre y en caso de rotura parcial el enlace sigue transmitiendo y reduce el ancho de banda de forma proporcional.

Los beneficios que Metro Ethernet ofrece son:

- Presencia y capilaridad prácticamente universal en el ámbito metropolitano, en especial gracias a la disponibilidad de las líneas de cobre, con cobertura universal en el ámbito del urbano.
- Muy alta fiabilidad, ya que los enlaces de cobre certificados Metro Ethernet, están constituidos por múltiples pares de en líneas de cobre (MAN BUCLE) y los enlaces de Fibra Óptica, se coonfiguran mediante Spanningtree (activo-pasivo) o LACP (caudal Agregado).
- **Fácil uso:** Interconectando con Ethernet se simplifica las operaciones de red, administración, manejo y actualización
- **Economía:** los servicios Ethernet reducen el capital de suscripción y operación de tres formas:

  Amplio uso: se emplean interfaces Ethernet que son la más difundidas para las soluciones de Networking

  Bajo costo: Los servicios Ethernet ofrecen un bajo costo en la administración, operación y funcionamiento de la red.
- **Ancho de banda:** Los servicios Ethernet permiten a los usuarios acceder a conexiones de banda ancha a menor costo.
- **Flexibilidad:** Las redes de conectividad mediante Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, el ancho de banda y la cantidad de usuarios en corto tiempo.

DIRECCIONAMIENTO IP

Una dirección IP es una serie de números binarios que provee información sobre la red y el host (PC o dispositivo), se emplea también en todas las conexiones de red, ya sea inalámbrica, de cable local o en internet, autentificar los nodos o puntos desde los cuales nos conectamos e intercambiamos información, donde en la actualidad existen dos versiones de IP, las IPv4 (Protocolo de Internet Versión 4) y las IPv6 (Protocolo de Internet versión 6).

La asignación de la dirección IP a un dispositivo se puede hacer de dos formas:

- **Estática:** Una dirección **IP fija o estática** es una IP la cual es asignada por el usuario, o bien dada por el proveedor ISP en la primera conexión., donde se debe configurar manualmente todos los parámetros de red, incluyendo la dirección IP.
- **Dinámica:** Una dirección **IP dinámica** es una dirección IP que el ISP o proveedor de Internet asigna dinámicamente al dispositivo que pretende tener acceso a Internet. Cada vez que el dispositivo se reinicia, el ISP vuelve a asignar dinámicamente una dirección IP al dispositivo utilizando para ello el protocolo DHCP. Este protocolo, por su propia naturaleza, tiene tendencia a asignar la misma dirección IP, pero como decimos esto no es porque tu ISP te la quiera mantener sino por cómo es el protocolo DHCP. La realidad es que la posibilidad de que tras un reinicio el dispositivo deje de tener la misma IP que tenía anteriormente es alta. Por lo general un router en una empresa, nunca se apaga, y los proveedores de ISP siempre hacen barridos de IP.

En cuanto a su alcance se dividen en dos tipos de direcciones:

- **Direcciones públicas.** Las direcciones IP públicas son aquellas que permiten que cada dispositivo conectado a una red pueda ser identificado. Cuándo un dispositivo se conecta a internet se le asigna una dirección IP de las que disponga su proveedor de acceso (ISP, Internet ServiceProvider).

  La dirección IP del servidor es una dirección IP pública y el servidor utiliza la dirección IP pública del usuario para saber dónde enviar la información de vuelta.

- **Direcciones privadas.** Son direcciones asignadas a dispositivos dentro de una red que no tiene visibilidad con Internet. Los dispositivos que tienen asignada una dirección privada no pueden acceder a Internet con su dirección y necesitan un dispositivo que les asigne una dirección pública.

Diferencia entre IP pública y privada

- La pública es el identificador de nuestra red desde el exterior, es decir, la de nuestro router de casa, que es el que es visible desde fuera, mientras que la privada es la que identifica a cada uno de los dispositivos conectados a nuestra red, por lo tanto, cada una de las direcciones IP que el router asigna a nuestro ordenador, móvil, tablet o cualquier otro dispositivo que se esté conectado a él.
- Por lo tanto, todos los dispositivos conectados a un mismo router tienen distintas direcciones IP privadas, pero la misma IP pública, ya que es la del router, que actúa como puerta de enlace.

Imagen N° 16.1
Ejemplo de un direccionamiento IP de clase c

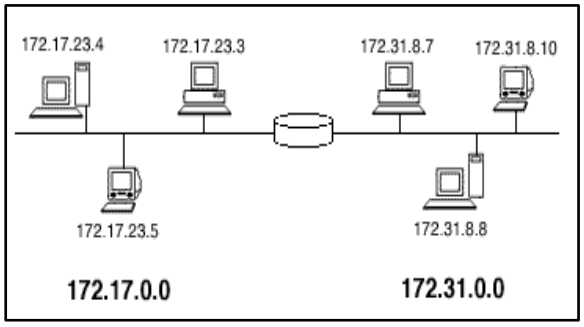


Imagen N° 16.2
Ejemplo de un direccionamiento IP mediante un servidor DHCP

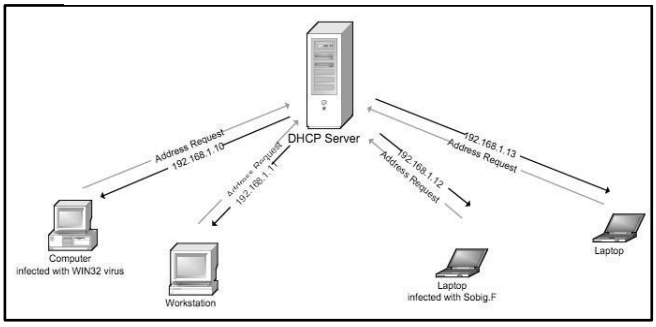
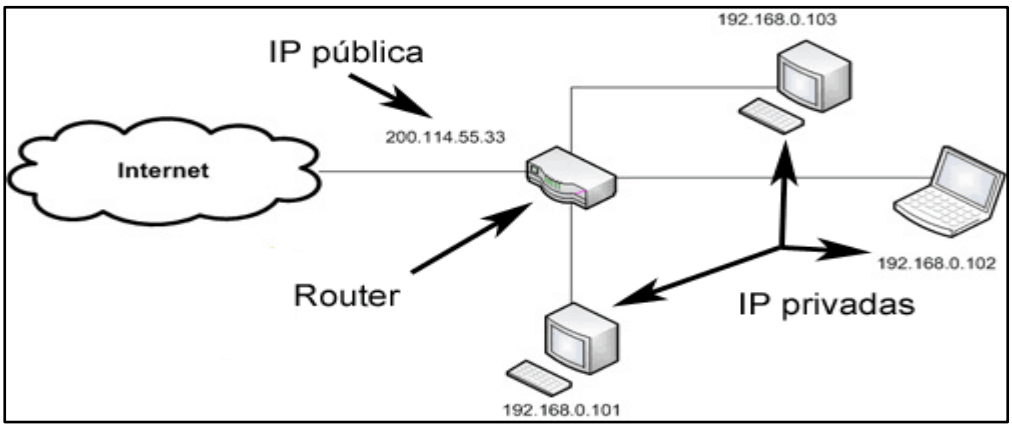


Imagen N° 16.3
Ejemplo de un direccionamiento IP público y privado



DIRECIONAMIENTO IP V4

Las direcciones IP se representan por 32 bits con 4 campos de 8 bits cada uno, aunque normalmente se pasan de binario a decimal. Cada número estará comprendido entre cero y 255, separados entre por puntos.

En una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111); los escribimos en la forma decimal para hacerlos más comprensibles, pero hay que tener bien claro que la red entiende sólo direcciones binarias.

Por ejemplo la dirección IP de clase c **197.9.7. 1** se representa en número binario de la siguiente forma:

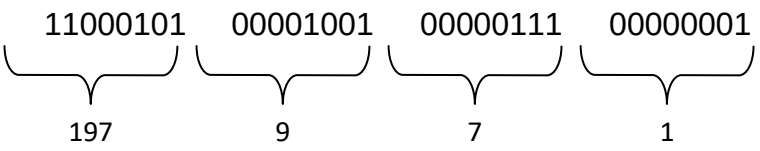


Imagen N° 17
Ejemplo de la estructura
En una dirección IPV 4

Dado que no puede haber dos interfaces con la misma dirección IP, dichas direcciones las otorgan organismos y entidades especialmente designadas, que delegan dicha autoridad jerárquicamente, de este modo, los ISPs (proveedores de Internet, Internet ServicesProvider) disponen de rangos de IP que pueden otorgar.

Cuando un equipo se conecta a Internet necesita una IP pública ya sea variable o fija, que le proporciona su ISP.

Existen rangos de direcciones IPv4 que no se utilizan en la red pública, sino que están reservadas para redes internas (intranets) cuyos equipos no disponen de conexión directa a Internet.

Al reutilizarse los mismos rangos en todas las organizaciones todavía se consigue disponer de suficientes direcciones IP públicas para quienes la soliciten, pero en la actualidad el límite de asignaciones ya se ha alcanzado.

Clases De Direcciones IP V4

En la actualidad, en el mundo de las redes, se utiliza la versión 4 de IP, conocida más comúnmente como IPv4, esta versión del protocolo IP está definida en el RFC 791 liberado en septiembre de 1981, la misma establece cinco clases de direcciones que se detallan a continuación:

- **Redes de clase A:** son aquellas redes que precisan un gran número de direcciones IP, debido al número de host que comprenden; a este tipo de redes se les asigna un rango de direcciones IP identificado por el primer octeto de la IP, de tal forma que disponen de los otros 3 octetos siguientes para asignar direcciones a sus host. Su primer byte tiene un valor comprendido entre 1 y 126, ambos inclusive, el número de direcciones resultante es muy elevado, más de 16 millones, por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.
- **Loopback** - La dirección IP 127.0.0.1 se utiliza como la dirección del loopback, esto significa que es utilizada por el ordenador huésped para enviar un mensaje de nuevo a sí mismo. Se utiliza comúnmente para localizar averías y pruebas de la red.

  Rango: 1.0.0.0 hasta: 127.255.255.255

  Privadas: 10.0.0.0 hasta: 10.255.255.255

  Redes Omitidas: 0.0.0.0 (default) y 127.0.0.1 (loopback).

  Máscara por defecto: 255.0.0.0
- **Redes de clase B:** son redes que precisan un número de direcciones IP intermedio para conectar todos sus host con Internet; a este tipo de redes se les asigna un rango de direcciones IP identificado por los dos primeros octetos de la IP de tal forma que disponen de los otros 2 octetos siguientes para asignar direcciones a sus host.

  Sus dos primeros bytes deben estar entre 128.1 y 191.254, por lo que el número de direcciones resultante es de 64.516. Las redes de clase B corresponden a grandes empresas, organizaciones o universidades etc.

  Rango: 128.0.0.0 hasta: 191.255.255.255

  Privadas: 172.16.0.0 hasta: 172.31.255.255

  Máscara por defecto: 255.255.0.0

- **Redes de clase C:** son redes que precisan un número de direcciones IP pequeño para conectar sus host con Internet, a este tipo de redes se les asigna un rango de direcciones IP identificado por los tres primeros octetos de la IP, de tal forma que disponen de un sólo octeto para asignar direcciones a sus host. Sus 3 primeros bytes deben estar comprendidos entre 192.1.1 y 223.254.254.

  El número de direcciones resultante es de 256 para cada una de las redes, por lo que éstas corresponden fundamentalmente a pequeñas empresas, organismos locales.

  Rango: 192.0.0.0 hasta: 223.255.255.255

  Privadas: 192.168.0.0 hasta: 192.168.255.255

  Máscara por defecto: 255.255.255.0
- **Clase D:** Utilizado para los multicast, la clase D es levemente diferente de las primeras tres clases; tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 0. Los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast está dirigido.

  La clase D totaliza 1/16ava (268,435,456 o 228) de las direcciones disponibles del IP.

  Rango: 224.0.0.0 hasta 239.255.255.255

  Máscara por defecto: 255.255.255.255
- **Clase E:** La clase E se utiliza para propósitos experimentales solamente. Como la clase D, es diferente de las primeras tres clases. Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 1. Los otros 28 bits se utilizan para identificar el grupo de computadoras que el mensaje del multicast está dirigido. La clase E totaliza 1/16ava (268,435,456 o 228) de las direcciones disponibles del IP.

  Rango: 240.0.0.0 hasta: 255.255.255.255

  Motivo de la Red: Investigación.
- **Broadcast -** Los mensajes que se dirigen a todas las computadoras en una red se envían como broadcast, y los mensajes utilizan siempre la dirección **IP 255.255.255.255.**

MÁSCARA DE RED

Cuando dos o más redes diferentes se encuentran conectadas entre sí por medio de un router, éste debe disponer de algún medio para diferenciar los paquetes que van dirigidos a los host de cada una de las redes, es aquí donde entra en juego el concepto de máscara de red, que es una especie de dirección IP especial que permite efectuar este enrutamiento interno de paquetes.

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras; su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

La máscara de red posee la importante propiedad de que cuando se combina con la dirección IP de un host se obtiene la dirección propia de la red en la que se encuentra el mismo; cuando al router que conecta varias redes le llega un paquete saca de él la dirección IP del host destino y realiza una operación AND lógica entre ésta IP y las diferentes máscaras de red de las redes que une, comprobando si el resultado coincide con alguna de las direcciones de red. Este proceso de identificación de la red destino de un paquete (y del host al que va dirigido el paquete) se denomina enrutamiento.

Ejemplo

8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)

8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)

8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)

8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)

Imagen N° 18

Ejemplo de las diferentes clases de direcciones IPV4 y su respectiva mascara de subred y formato diagonal

Classes IPv4 e Máscara de Rede

Classe	Início	Fim	Máscara de Subrede padrão	Notação CIDR	OBS
A	1.0.0.1	126.255.255.254	255.0.0.0	/8	
B	128.0.0.1	191.255.255.254	255.255.0.0	/16	
C	192.0.0.1	223.255.255.254	255.255.255.0	/24	
D	224.0.0.0	239.255.255.255			Multicast
E	240.0.0.0	247.255.255.255			Uso futuro; atualmente reservada a testes pela IETF

Tipos De Mascara De Subred

El número de bits correspondientes a la subred y al número de host son elegidos libremente por el administrador.

Esta división se realiza utilizando una **máscara de subred**. Esta es un número binario de 32 bits. Los bits que estén a '1' indicarán el campo de la dirección IP dedicada a la red y los bits puestos a '0' indicarán la parte dedicada al host.

La máscara de subred se representa normalmente en notación decimal, por ejemplo, si no utilizamos subredes y dejamos la red como una sola, para una red Clase A y B, la máscara será:

Clase A

11111111	00000000	00000000	00000000
255	0	0	0

Clase B

11111111	11111111	00000000	00000000
255	255	0	0

Si queremos dividirla en subredes, tomaremos 16 bits de la parte local y pondremos a '1' la parte que queremos represente a las subredes, por ejemplo, si queremos 8 subredes, necesitaremos en binario 3 bits para referenciarlas.

La máscara que necesitamos será: **11111111.11111111.11100000.00000000** es decir, **255.255.224.0** en decimal, al emplear 13 bits para el host podríamos tener hasta $2^{13} – 2 = 8.190$ máquinas en cada subred.

La máscara quedaría de la siguiente manera

11111111	11111111	11100000	00000000
255	255	224	0

Si tenemos una red Clase C cuya máscara sin subredes es 255.255.255.0 y queremos dividirla en 4 subredes, solo necesitamos 2 bits para definirlas:

11111111	11111111	11111111	11000000
255	255	255	192

Esta máscara permitiría hasta $2^6 – 6 = 62$ host en cada subred.

CIDR: Ruteo Interno De Dominios Sin Clases

A partir de 1993, ante la previsible futura escasez de direcciones IP debido al crecimiento exponencial de hosts en Internet, se empezó a introducir el sistema CIDR, que pretende en líneas generales establecer una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y desperdiciando las mínimas posibles, para rodear el problema que las distribución por clases había estado gestando.

CIDR es un estándar de red para la interpretación de direcciones IP, que facilita el encaminamiento al permitir agrupar bloques de direcciones en una sola entrada de tabla de rutas, dichos grupos, comúnmente llamados Bloques CIDR, comparten una misma secuencia inicial de bits en la representación binaria de sus direcciones IP.

Los bloques CIDR IPv4 se identifican usando una sintaxis similar a la de las direcciones IPv4: cuatro números decimales separados por puntos, seguidos de una barra de división y un número de 0 a 32; A.B.C.D/N.

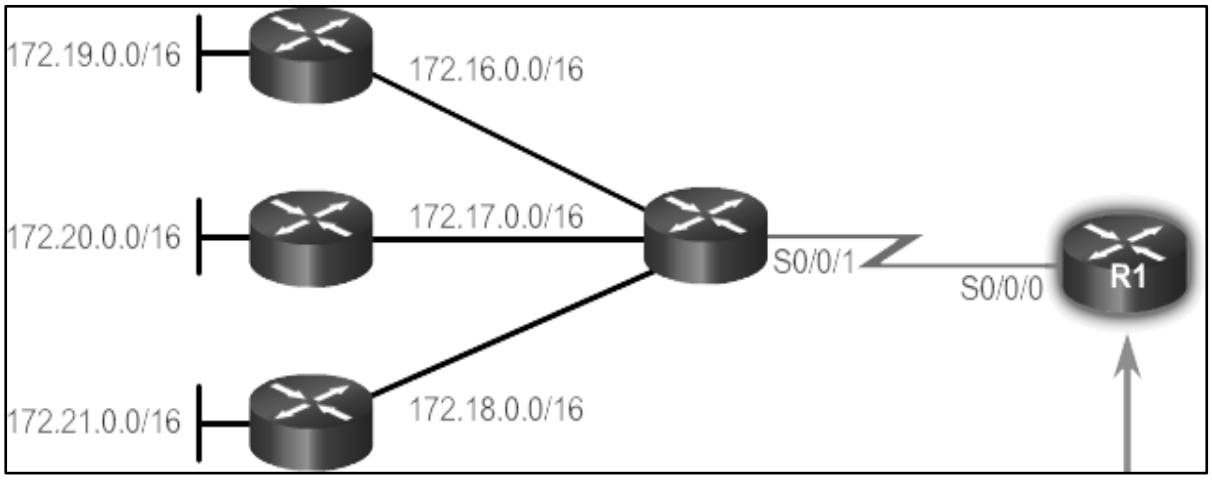
Los primeros cuatro números decimales se interpretan como una dirección IPv4, y el número tras la barra es la longitud de prefijo, contando desde la izquierda, y representa el número de bits comunes a todas las direcciones incluidas en el bloque CIDR.

Esto viene a decir que lo que antes era: **192.168.0.1**

Con máscara de subred: **255.255.255.0**

Ahora con CIDR es: **192.168.0.1/24**

Imagen N° 19
Ejemplo de CIDR en una dirección IPV 4 clase c



Como podemos ver en la siguiente gráfico, diferentes direcciones de clase B están contempladas bajo un mismo formato CDIR /16 enviando información hacia el router R1, esto quiere decir que las direcciones 172.19.0.0, 172.20.0.0, 172.21.0.0, tienen la máscara de subred 2555.255.0.0 con el formato de barra diagonal **CDIR /16**

.

Imagen N° 20
Cuadro en donde nos muestra el formato CDIR con los diferentes bits que toma en su diferente estructura

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

En la siguiente tabla podemos ver que en la primera columna **network bits**, está representada por los bits tomados de la parte de red, en la segunda columna **subnetmask** representa la máscara de subred según su clase, en la tercera columna **bits borrowed** los bits tomados de la parte de host según su clase, en el cuarta columna **subnet** la cantidad de subredes disponibles y por último en la quinta columna **host/subnets,** la cantidad de host disponibles en cada red

SUBREDES O SUBNETEO

La función del Subneteo o subredes es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabajen en el nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

Las **subredes** permiten maximizar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una interred mayor.

En cualquier clase de dirección, las subredes proporcionan un medio para asignar parte del espacio de la dirección host a las direcciones de red, lo cual permite tener más redes. La parte del espacio de dirección de host asignada a las nuevas direcciones de red se conoce como número de subred.

Características de las subredes:

- Permite crear múltiples redes lógicas de un único bloque de direcciones.
- Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.
- El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función.
- Mejora la performance de la red al reducir el tráfico de broadcast de nuestra red.
- Permite tener una más fácil administración de la red.
- Permite organizar de manera jerárquica la red.
- Permite Optimizar su Rendimiento de las direcciones IP.
- Cuando se segmenta una red, se están creando subredes que se autogestionan, de forma que la comunicación entre segmentos solo se realiza cuando es necesario, mientras tanto, la subred está trabajando de forma independiente.
- El dispositivo utilizado para segmentar la red debe ser inteligente, ya que debe ser capaz de decidir a qué segmento va a enviar la información que llego a el.
- Para realizar el subneteo se manipulan los bits que están a la derecha del Network Id, es decir, a la derecha del octeto 255 de la máscara de subred. Es decir, para las redes clase A, se manipulan los tres octetos

restantes; para las redes clase B, se manipulan los dos octetos a la derecha; para las redes clase C, el octeto que se utiliza es el último.

- Para direcciones de subred, lo normal es asignar un número de subred a una red física (por ejemplo, un número a cada departamento) .Por ejemplo, cuando se unen las redes de tres edificios con repetidores, puede suceder que en el futuro se decida separarlas, por lo que el uso de múltiples números de subred desde el inicio evitará modificar la dirección de cada host

Ejemplo de subneteo:

Vamos a crear una red local con 2 departamentos separados entre sí.

Diseñar una tabla con todas las direcciones: En primer lugar, elegimos la clase de la red que vamos a preparar; para este caso y sabiendo que se trata de una red local pequeña, elegimos una clase C:

- **Por ejemplo 192.168.1.0 con máscara 255.255.255.0**

Para montar 2 subredes se requieren:

- **2bits = 2^2=4 totales, de las que usaremos 2.**

Pasamos la máscara a binario:

- **255.255.255.0 = 11111111.11111111.11111111.00000000**

Tomamos dos bits de la parte hosts:

- **11111111.11111111.11111111.11000000 = 255.255.255.192**

En esta ocasión no necesitamos saber a qué subred pertenece la dirección IP192.168.1.0, pero si fuera necesario porque no lo hemos ubicado, haríamos una multiplicación (AND) de la dirección por la máscara de subred:

- **11000000.10101000.00000001.00000000 ->192.168.1.0**
- **11111111.11111111.11111111.11000000 ->255.255.255.192**
- **11000000.10101000.00000001.00000000 -> 192.168.1.0**

Las subredes posibles son:

- **11000000.10101000.00000001.00000000 -> 192.168.1.0/26**
- **11000000.10101000.00000001.01000000 -> 192.168.1.64/26**
- **11000000.10101000.00000001.10000000 -> 192.168.1.128/26**
- **11000000.10101000.00000001.11000000 -> 192.168.1.192/26**

Y su dirección se obtiene poniendo a cero todos los bits correspondientes a host

Para obtener el primer host de la subred, ponemos todos los bits de la parte de host a 0 excepto el último:

- **11000000.10101000.00000001.00000001**
- **11000000.10101000.00000001.01000001**
- **11000000.10101000.00000001.10000001**
- **11000000.10101000.00000001.11000001**

Para obtener la dirección del último host, ponemos todos los bits de la parte host a 1, excepto el último, que será 0:

- **11000000.10101000.00000001.00111110**
- **11000000.10101000.00000001.01111110**
- **11000000.10101000.00000001.10111110**
- **11000000.10101000.00000001.11111110**

Para obtener la dirección de multidifusión o broadcast, ponemos a 1 todos los bits de host:

- **11000000.10101000.00000001.00111111**
- **11000000.10101000.00000001.01111111**
- **11000000.10101000.00000001.10111111**
- **11000000.10101000.00000001.11111111**

Por último debido a que la primera dirección se guarda para red en este caso estaría representada por su formato binario y decimal seria:

- **11000000.10101000.00000001.00000000 -> 192.168.1.0/26**

La dirección de brodcast seria la ultima de la subred representada por su formato binario y decimal seria:

- **11000000.10101000.00000001.11000000 -> 192.168.1.192/26**

Las direcciones que quedarían disponibles de acuerdo a su formato binario y decimal seria:

- **11000000.10101000.00000001.01000000 -> 192.168.1.64/26**
- **11000000.10101000.00000001.10000000 -> 192.168.1.128/26**

DIRECCIONAMIENTO IPV6

IPv6 (Internet ProtocolVersion 6) es la nueva versión del protocolo IP que ha sido diseñado por el IETF para reemplazar en forma gradual atreves del tiempo a la versión actual, del protocolo de direccionamiento IPv4.

La mayor capacidad del espacio para direcciones de IPv6 proporciona una solución para el problema de escasez de direcciones, es una solución muy importante ya que cada vez que más personas utilizan sistemas móviles, como teléfonos móviles, agendas personales, tablet, notebook entre otros.

IPv6 tiene un conjunto de normas técnicas que define la forma en que las computadoras se comunican dentro de la red, donde el principal motivo para el desarrollo de IPv6 fue el de la expansión del espacio de direccionamiento disponible en Internet, posibilitando que nuevos dispositivos se puedan incorporar.

IPv6 está desarrollada especialmente para redes de alto rendimiento (ATM), pero manteniendo la eficiencia en las redes de bajo ancho de banda (redes inalámbricas).

Esta nueva versión tiene un tamaño de dirección de 128 bits, lo que significa que existen 2^{128} (16 trillones aprox.) direcciones diferentes, esta cantidad sobrepasa con creses a las de la versión anterior, la cual tiene un tamaño de 32 bits (4 mil millones aprox.).

Actualmente las nuevas tendencias en el mundo de las telecomunicaciones como la movilidad de los usuarios (acceder en cualquier momento y lugar), las redes domésticas avanzadas y la convergencia de voz, video y datos en infraestructuras basadas en IP originan la necesidad de migrar a IPv6.

La creciente demanda de usuarios que utilizan dispositivos sin cable contribuye al agotamiento de direcciones IPv4; la mayor capacidad para direcciones IP de IPv6 proporciona suficientes direcciones IP para el número creciente de dispositivos sin cable, además de este mayor espacio para direcciones, IPv6 proporciona funciones nuevas que simplifican las tareas de configurar y gestionar las direcciones en la red.

La configuración y el mantenimiento de redes es una actividad laboriosa. IPv6 reduce parcialmente el volumen de trabajo automatizando algunas de las tareas del administrador de red.

CARACTERÍSTICAS DE IPV6

- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado.
- La difusión ARP es reemplazada por el uso de multicast en el link local.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- IPv6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que el protocolo IPv4.
- Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6.

Tipos de direcciones IPv6

Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados:

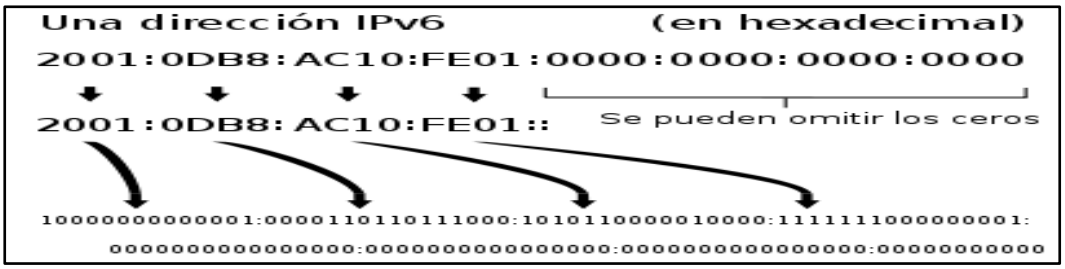
- **Unicast.** Se utiliza únicamente para identificar una interface de un nodo IPv6.

  Un paquete enviado a una dirección unicast es entregado a la interface identificada por esa dirección.**[RFC 2373] [RFC 2374]**
- **Multicast.** Se utiliza para identificar a un grupo de interfaces IPv6.

  Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.**[RFC 2526]**
- **Anycast.** Se asigna a múltiples interfases (usualmente en múltiples nodos).

  Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.**[RFC 2375]**

Imagen N° 20
Formato de direccionamiento IPV6 y su diferente estructura



Como podemos ver en la siguiente esquema , la estructura que posee el protocolo de internet versión 6 , su formato es hexadecimal, dividida por dos puntos, se pueden suprimir los 0 mediante la notación de dos puntos seguidos **::** y en la parte inferior la representación en formato binario.

Existen tres formas de representar las direcciones IPv6 como strings de texto. x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

- **FEDC:BA98:7654:3210:FEDC:BA98:7654:3210**
- **1080:0:0:0:8:800:200C:417A**

Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente **:** para representarlos, el uso de **::** indica uno o más grupos de 16 bits de ceros, dicho símbolo podrá aparecer una sola vez en cada dirección.

Por ejemplo :

- **1080:0:0:0:8:800:200C:417A unicast address**
- **FF01:0:0:0:0:0:0:101 multicast address**
- **0:0:0:0:0:0:0:1 loopback address**
- **0:0:0:0:0:0:0:0 unspecified addresses**

Podrán ser representadas como:

- **1080:: 8:800:200C:417A unicastaddress**
- **FF01::101 multicastaddress**
- **::1 loopbackaddress**
- **:: unspecifiedaddresses**

Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.

Ejemplos:

- **0:0:0:0:0:0:13.1.68.3**
- **0:0:0:0:0:FFFF:129.144.52.38**

O en la forma comprimida

- **::13.1.68.3**
- **::FFFF:129.144.52.38**

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6, por ejemplo: si la dirección decimal **IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34),** puede ser convertida a:

- **0000:0000:0000:0000:0000:0000:874B:2B34 o ::874B:2B34**.
  Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser **::135.75.43.52.**

Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Por último para tener un panorama más claro cuáles serían las diferencias más significativas que tienen los protocolos de internet versión 4 y 6, se muestra en la siguiente tabla las características que posee cada uno de ellos.

IPV4	IPV6
Formato de 32 bits (4 bytes)	Formato de 128 bits (16 bytes)
Formato decimal	Formato hexadecimal
Encabezado de 20 bytes	Encabezado de 40 bytes
Protocolo no escalable	Protocolo escalable
Comunicación por medio de Brodcast	Comunicación por medio de Unicast, multicas y Anicasst
Fragmentación de paquetes realizado por host y router	Fragmentación de paquetes realizado solo host
Configuración manual	Configuración automática

ORGANISMOS QUE REGULAN LAS DIRECCIONES IP EN EL MUNDO

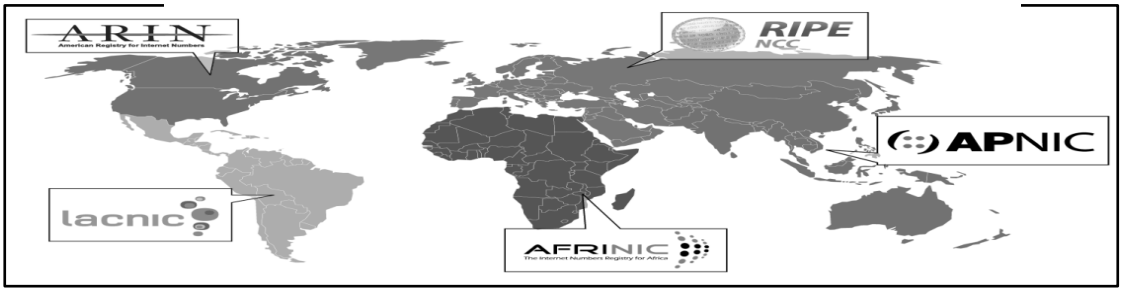
En el caso que queramos solicitar un numero IP para nuestra organización u empresa, es preciso saber qué organismo es el que asigna las direcciones, y cuáles son los que regulan de acuerdo a la parte del mundo donde estemos establecidos.

- **IANA:** es la Autoridad para la Asignación de Números de Internet (del Inglés: responsable de la coordinación global de los protocolos de Raíz DNS, direccionamiento IP y otros recursos del Protocolo de Interne. **www.iana.org**
- **ICANN**: La Corporación de Internet para la Asignación de nombres y números de Dominios del Inglés: (Nternet Corporation for Assigned Names and Numbers) es una organización sin fines de lucro que opera a nivel de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las administración del sistema de servidores raíz. Aunque en un principio estos servicios los desempeñaba (IANA) y otras entidades bajo contrato con el gobierno de EE.UU., actualmente son responsabilidad de ICANN. **www.icann.org**
- **Registro Americano para Números de Internet (ARIN).** El Registro Americano para Números de Internet (ARIN) es un RIR responsable de la administración de direcciones y dominios de Internet para América del Norte, incluyendo Canadá, Estados Unidos, y partes del Caribe; fundada en 1997, ARIN fue el resultado de la decisión del gobierno estadounidense de separar el apoyo a la Internet comercial de los Estados Unidos Departamento de Defensa (DoD). El original de la transferencia de responsabilidades se produjo en 1991, cuando el gobierno adjudicó a un contratista privado, Network Solutions, un contrato para realizar direccionamiento de Internet y los servicios de registro, incluyendo registro de dominios, direcciones, registro de usuarios y de apoyo, y el apoyo a la distribución y archivo de documentos RFC. **www.arin.net**
- **ReseauxEuropeens IP Red de Coordinación de Centro (RIPE NCC).** La IP R Red de Centros de Coordinación (RIPE NCC) es un RIR responsable de la administración de direcciones y dominios de Internet

para Europa, Oriente Medio y Asia Central. Con sede central en Amsterdam, Holanda, RIPE NCC se creó en 1992 con la financiación de plena competencia del consorcio europeo de redes de investigación y un grupo de empresas más pequeñas y de redes comerciales. RIPE NCC es una organización basada en la responsabilidad de coordinar y gobernar las actividades de la comunidad RIPE. RIPE NCC fue considerado el RIR primero como el gobierno de Estados Unidos aún estaba activamente involucrado en la gestión de Internet para hacer frente a gran parte de América del Norte en ese momento.**www.ripe.net**

- **Asia-Pacific Network Information Centre (APNIC):** El Centro de Asia y el Pacífico Red de Información es un RIR responsable de la administración de direcciones de Internet y los dominios de Asia y la Cuenca del Pacífico. Fundada en Tokio, Japón, APNIC fue el segundo RIR que se establezcan. En 1993, se convirtió en activo APNIC y fue originalmente diseñado como un ensayo para satisfacer las necesidades de direccionamiento de las infraestructuras de redes regionales en ese momento. APNIC se mudó a Brisbane, Australia, en 1998.**www.apnic.net**
- **América Latina y el Caribe Registro de Direcciones de Internet (LACNIC)-:** Fundada en 2001, América Latina y el Caribe del Registro de Direcciones de Internet (LACNIC), es un RIR responsable de la administración de direcciones y dominios de Internet para América Latina y el Caribe. Con sede en Montevideo, Uruguay, LACNIC es una organización sin fines de lucro responsables de la dirección regional de Internet y registros de dominio y participa activamente en la promoción de iniciativas de expansión de Internet en la región.**www./lacnic.net/sp/index.html**

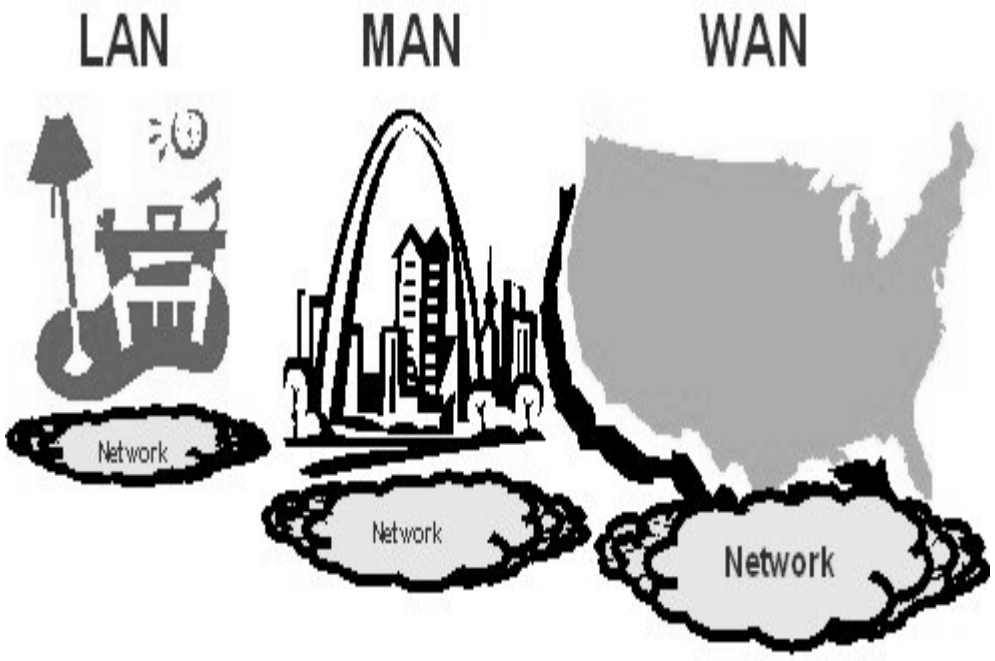
Imagen N° 21
Ejemplo de las diferentes organizaciones de asignaciones IP en el mundo.



PREGUNTAS SOBRE LA UNIDAD N°1

1. ¿Las direcciones lógicas están ubicadas dentro de que capa del modelo OSI?
2. ¿Las direcciones Físicas están ubicadas dentro de que capa del modelo OSI?
3. ¿El cable coaxial THICK pertenece a que norma?
4. ¿El cable coaxial THIN pertenece a que norma?
5. ¿En Ethernet se separan las funciones de la capa de Enlace de datos en dos subcapas. ¿cuáles son?
6. ¿Cuál es la diferencia entre **CSMA/CD y CSMA/CA?**
7. ¿Cuántos bits tiene la dirección MAC?
8. ¿Cuántos bits tiene la dirección IP?
9. ¿Cuáles son las direcciones IP estáticas?
10. ¿Cuáles son las direcciones IP dinámicas?
11. ¿Cuáles son las direcciones IP públicas?
12. ¿Cuáles son las direcciones IP privadas?
13. ¿Cuántos bytes contiene la dirección IPV4?
14. ¿Cuántos bits contiene la dirección IPV6?
15. ¿Cuál es la dirección de loopbak que pertenece a IPV4?
16. ¿Cuál es el rango de direcciones IPV4 de clase A de acuerdo a la RFC 4291?
17. ¿Cuál es el rango de direcciones IPV4 de clase B de acuerdo a la RFC 4291?
18. ¿Cuál es el rango de direcciones IPV4 de Clase C de acuerdo a la RFC 4291?
19. ¿Cuál es el rango de direcciones IPV4 de clase D de acuerdo a la RFC 4291?
20. ¿Cuál es el rango de direcciones IPV4 de clase E de acuerdo a la RFC 4291?
21. ¿Como trabaja en IPV6 el sistema unicast?
22. ¿Como trabaja en IPV6 el sistema Multicast?
23. ¿Como trabaja en IPV6 el sistema Anycast?
24. ¿En IPV6 la configuración es automática o manual?
25. ¿En IPV6 el formato es decimal o hexadecimal?

CAPÍTULO N° 2



CAPÍTULO II: REDES DE COMUNICACIÓN DE DATOS

La forma en que se comunican las redes de datos ha evolucionado notablemente a través del tiempo, permitiendo conectar equipos, casa, edificios, ciudades y continentes, en donde la caracterización fundamental se basa de acuerdo a su tecnología y alcance que brindan alrededor del mundo.

Las redes pueden intercambiar información entre ellas mediante diversos protocolos, que son conjuntos de reglas, como el indispensable TCP/IP (Transmission Control Protocol / Internet Protocolo de Control de Transmisión /Protocolo de Internet) que permite a dos máquinas establecer una conexión e intercambiar datos, no importando que sean de marcas, modelos, años o con sistemas operativos diferentes.

Las mismas se dividen de la siguiente manera:

LA RED PAN: Una red de área personal es una red de computadora utilizada para la comunicación entre los dispositivos de información de la computadora y diferentes tecnologías cerca de una persona.

PAN representa el concepto de redes centradas en las personas, y que les permiten a dichas personas comunicarse con sus dispositivos personales ejemplo, PDAs, tableros electrónicos de navegación, agendas electrónicas, computadoras portátiles entre otras.

Algunos ejemplos de dispositivos que se utilizan en un PAN son las computadoras personales, impresoras, máquinas de fax, teléfonos, PDA, escáneres y consolas de videojuegos., con un alcance que se extiende normalmente a 10 metros.

Un cable PAN se construye generalmente con conexiones USB y Firewire, mientras que las tecnologías tales como Bluetooth y la comunicación por infrarrojos forman típicamente una red inalámbrica PAN

Imagen N° 22
Ejemplo de los diferentes dispositivos conectado a una red blueooth.

Redes LAN

La redes LAN: Una red de área local, red local o LAN (del inglés local área network) es la interconexión de varias Computadoras y Periféricos, donde su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o 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, etc., para compartir recursos e intercambiar datos y aplicaciones.

Las LAN están restringidas por la infraestructura, lo cual significa que sus tiempos de retransmisión están limitados y son conocidos y por lo tanto pueden ser controlados en base a diseños adecuados de la red, a menudo usan una tecnología de transmisión que consiste en un cable sencillo, compartido al cual están conectadas todas las máquinas, con sistemas de difusión

Características de una red LAN

- Interconexión Local de una o varias computadoras y periféricos.
- Mantienen la red en forma privada y con un ancho de banda.
- Permite el mismo manejo de la base de datos mediante la instalación de programas específicos en los computadores que lo requieran donde se puede centralizar los movimientos y la información para el manejo de la gestión empresarial.
- Utiliza una sola conexión telefónica o de ancho de banda para todas las computadoras conectadas en la red.
- Capacidad de 1 Mbps a 1Gbps.
- Su servicio utiliza conexión de fibra óptica, cable coaxial y cable telefónico.
- Tecnología Broadcast (difusión) con el medio de transmisión compartido.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Uso de un medio de comunicación privado
- La simplicidad del medio de transmisión que utiliza Cable coaxial, Cables telefónicos y Fibra óptica
- Gran variedad y número de dispositivos conectados
- Posibilidad de conexión con otras redes
- Limitante de 100 m, puede llegar a más si se usan Repetidores.

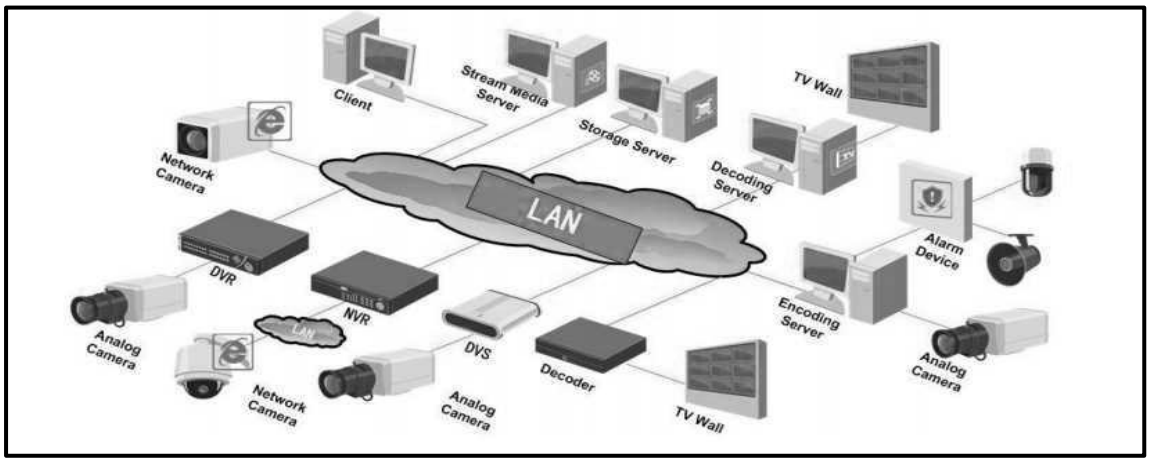
En la actualidad podemos encontrar dos tipos básicos de red LAN:

- A través de cable, llamada conexión por Ethernet, y en el cual se deben interconectar entre si todos los dispositivos que la conforman mediante un dispositivo llamado router.
- A través de ondas de radio, llamada LAN inalámbrica o WLAN" lo que nos permite prescindir de cables e instalaciones costosas y complicadas.

Elementos básicos de una red LAN:

- Estaciones de trabajo o terminales: Cada ordenador conectado a la red.
- Servidor: El equipo principal de la red.
- Rack: Es un armario que recoge de modo ordenado todas las conexiones y los extremos de cables finales de toda la red LAN.
- Canaleta: Es una estructura metálica o de plástico, adosada al suelo o pared. Los cables se disponen en su interior. De esta forma evitamos posibles deterioros indeseados o saber con facilidad donde se encuentran los cables.
- Placas de conectores y rosetas: Son conectores que se insertan en las canaletas o se adosan a la pared y que sirve de interface entre el latiguillo que lleva la señal al nodo y el cable de red.
- ROUTER: Es el dispositivo necesario para conectar nuestra red LAN a internet.
- BackBone: Este es el cable principal de la red LAN, Vendría a ser como el tronco de un árbol.

Imagen N° 23
Ejemplo de los diferentes dispositivos conectado a una red LAN.



Redes De Áreas Metropolitanas MAN

MAN: Es una red que abarca un área metropolitana, como una ciudad o una zona suburbana. Una MAN, por lo general, consta de una o más LAN dentro de un área geográfica común. Este tipo de redes son administradas por un proveedor de servicios (ISP). Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se recurre a un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos; también se puede crear una MAN por medio de tecnologías de puente inalámbrico, enviando haces de luz a través de áreas públicas.

La misma ofrece velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica, ó 16 hilos se averíen de forma simultánea.

Una red de área metropolitana permite la interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Las características principales son:

- Puede alcanzar una distancia de 500 km, dependiendo del alcance entre nodos y utilizando repetidores
- Interconexión de redes de área local (RAL)
- Son implementadas por los proveedores de servicio de Internet, que son normalmente los proveedores del servicio telefónico
- Interconexión de centralitas telefónicas digitales (PBX y PABX)
- Interconexión ordenador a ordenador
- Transmisión de vídeo e imágenes
- Transmisión CAD/CAM
- Pasarelas para redes de área extensa (WANs)
- Es normal que en una MAN un proveedor de servicios monte su red telefónica, su red de datos y los otros servicios que ofrezca.

- Permite el despliegue de servicios de VoIP, en el ámbito metropolitano, permitiendo eliminar las obsoletas líneas tradicionales de telefonía analógica o RDSI, eliminando el gasto corriente de estas líneas
- El objetivo de las redes de área metropolitana es ofrecer sobre el área urbana el nivel de ancho de banda requerido para tareas tales como: aplicaciones cliente servidor, intercambio de documentos, transferencia de mensajes, acceso a base de datos y transferencia de imágenes.
- Las redes MAN son apropiadas para entornos como control de tráfico aéreo, aprovisionamiento de almacenes, bancos y otras aplicaciones comerciales donde la indisponibilidad de la red tiene graves consecuencias.

Una red de área metropolitana puede ser pública o privada.

- **Una MAN privada** sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos. Los datos podrían ser transportados entre los diferentes edificios, bien en forma de paquetes o sobre canales de ancho de banda fijos. Aplicaciones de vídeo pueden enlazar los edificios para reuniones, simulaciones o colaboración de proyectos.
- **Una MAN pública** es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

Imagen N° 24.1
Ejemplo de las diferentes dispositivos conectado a una red MAN en diferentes edificios

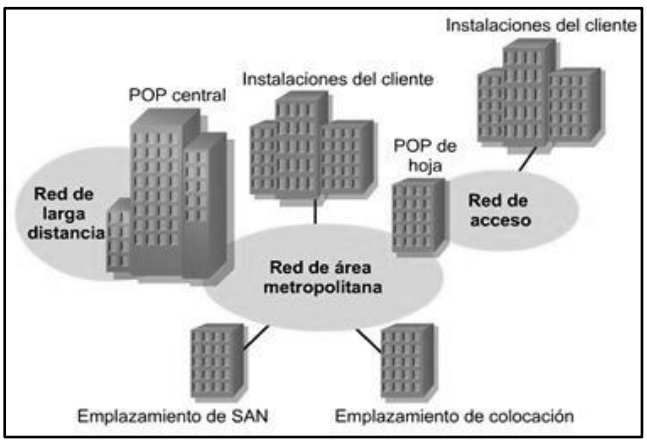
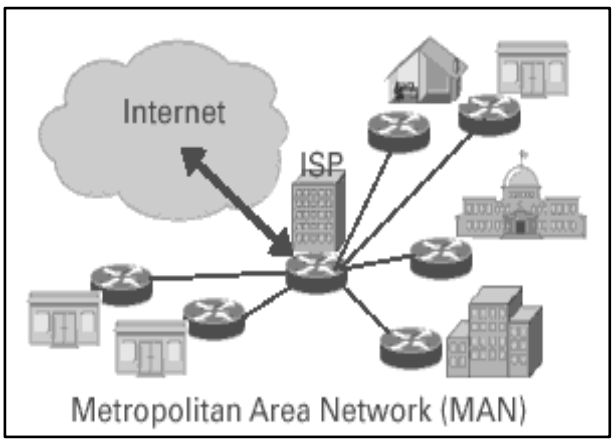


Imagen N° 24.2
Ejemplo de las diferentes dispositivos conectado a una red MAN en diferentes routers



Red WAN

Una red WAN es una red de área extensa se extiende sobre un país o un continente, donde su función fundamental está orientada a la interconexión de redes o equipos que se encuentran ubicados a grandes distancias entre sí.

Las distancias puede ir entre unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente, empleando una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continúa.

Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro.

Existen muchas redes WAN que son desarrolladas y configuradas especialmente para empresas y organizaciones privadas, existen también casos en los que estas redes son construidas por empresas proveedoras de Internet con el fin de proveer de dicho servicio a sus clientes.

Este tipo de redes se caracterizan por estar interconectadas punto a punto, en otras palabras usan nodos de conmutación y que deben tener la capacidad para soportar un alto volumen de tráfico de información, un nodo de conmutación es un dispositivo que justamente se encarga de manejar dicho tráfico de datos, tienen una línea de entrada y otra de salida la cual usan para reenviar.

También hay que tener en cuenta que las redes WAN pueden usar diferentes tipologías entre las cuales están la topología de anillo que básicamente consta en la conexión de un nodo con otros dos y así sucesivamente aunque los problemas de conexión se incrementan por la complejidad de este tipo de red, otra conocida es la topología de estrella en la cual un nodo es el centro de muchos otros pues los interconecta en una estructura conocida también como malla por su forma.

Existen también las redes Wan conmutadas por circuitos, las conmutadas por mensaje, conmutadas por paquetes, las redes orientadas a conexión y las redes no orientadas a conexión.

Tipos de redes WAN

Conmutadas por Circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por Mensaje: En este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo; esta tecnología permite grabar la información para atenderla después, y el usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por Paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños; donde estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Redes Orientadas a Conexión: En estas redes existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión: Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos.

Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular, un ejemplo de este tipo de red es Internet.

Red Pública de Conmutación Telefónica (PSTN): Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos.

La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación

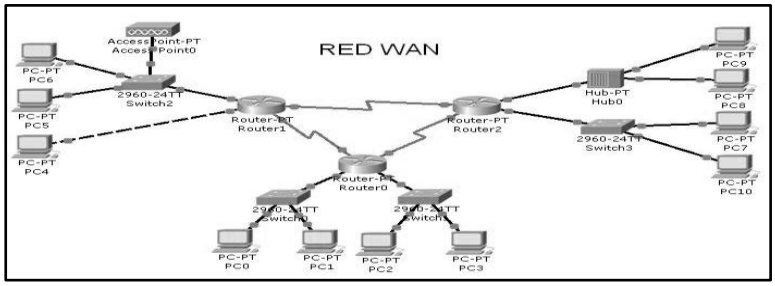


Imagen N° 25
Ejemplo de los diferentes dispositivos conectados a una red WAN

TOPOLOGÍAS DE REDES

Las topologías de red son muy importantes en las comunicaciones ya que permiten estructurar los diferentes nodos que se encuentran en una organización, empresa, casa, universidades, escuelas, de acuerdo al funcionamiento que se pretenda implementar.

Dependiendo de la forma en que estos nodos estén interconectados, y de las características de estos nodos, obtendremos una red más o menos compleja, con mayor o menor rendimiento, además de condicionar otros aspectos, como la forma en que se implementan las posibles políticas de seguridad, sobre la misma.

Cuando nos referimos a una determinada topología, podemos utilizarla para representar la forma de conexionado y el flujo físico de los datos, como por ejemplo: punto a punto y punto a multipunto; o también podemos abstraernos al movimiento lógico de la información, sin importar la forma en que están conectados los elementos físicos que realizan la tarea de transportarla, como por ejemplo: peer-to-peer.

Topología de red difusión:

Las redes de difusión tienen un solo canal de difusión compartido por todas las máquinas de la red. Los mensajes cortos (paquetes) que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quien se dirige; al recibir un paquete, una máquina verifica el campo de dirección; y si el paquete está dirigido a ella, lo procesa; si está dirigido a otra máquina lo ignora.

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección; cuando se transmite un paquete con este código, cada máquina lo recibe y lo procesa, y este modo de operación se le llama difusión .

Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo conocido como multidifusión.

Las redes de difusión se dividen en estáticas y dinámicas, dependiendo de cómo se asigna el canal. Una asignación estática típica, divide los intervalos discretos y ejecuta un algoritmo de asignación cíclica, permitiendo a cada máquina trasmitir únicamente cuando llega su turno.

La asignación estática, desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante su segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente.

Los métodos de asignación dinámica, pueden ser centralizados o descentralizados.

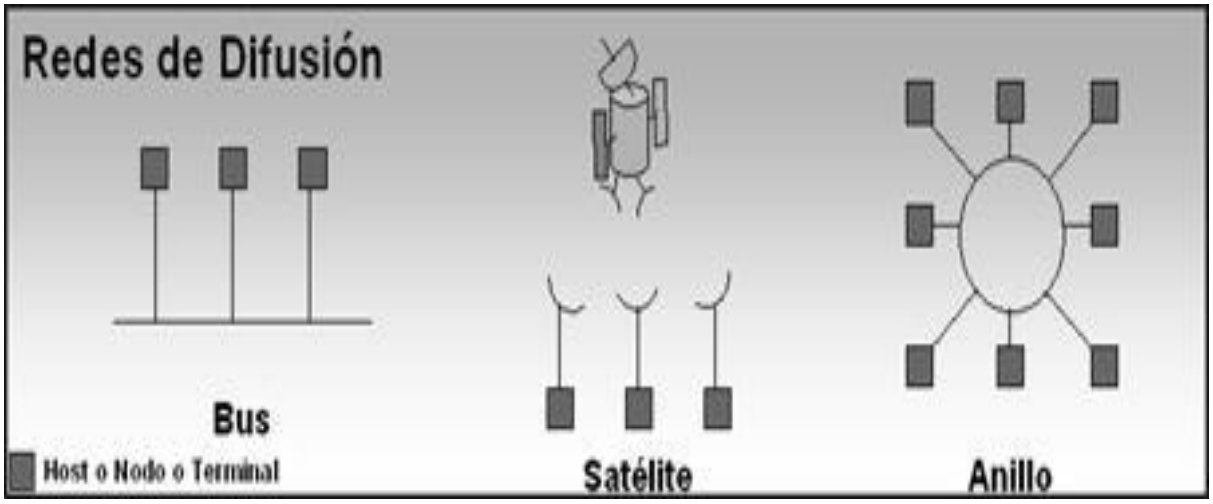
- En el método de asignación de canal centralizado hay una sola entidad, la cual determina quién es la siguiente.
- En el descentralizado no existe una unidad central, cada máquina debe decidir por sí misma si transmite o no.

Sus características son:

- Empleadas en redes locales
- Software de admisión es simple porque no requiere de algoritmos de routing y el control de errores es de extremo a extremo.
- Se requiere reconocer la dirección destino.
- Existe el único medio de transmisión, es decir solo hay un canal de comunicación.

  Los principales retrasos: espera de ganar el canal.
- El medio de transmisión puede ser totalmente pasivo, es decir solo está conduciendo la información.
- Se necesitaran duplicar las líneas en caso en que se requiera asegurar la funcionalidad ante fallas.
- Aumenta el costo, para poder asegurar más tarjetas de red.

Imagen N° 26
Ejemplo de los diferentes tipos de topología de red



Topología De Red Punto A Punto

Las redes punto a punto (llamadas a veces de igual a igual) proporcionan muchas características avanzadas y la flexibilidad requerida hasta por las instalaciones más exigentes; la función general de todas las redes punto a punto es la misma:

Que los nodos de la red compartan dispositivos como son las impresoras y lo más importante que es la información, la cual esta contenida en las unidades de disco.

Al evaluar las redes punto a punto, son varios los factores que determinan si este tipo de red satisface nuestras necesidades. Basadas principalmente en cable y en cada conexión intervienen solo dos equipos.

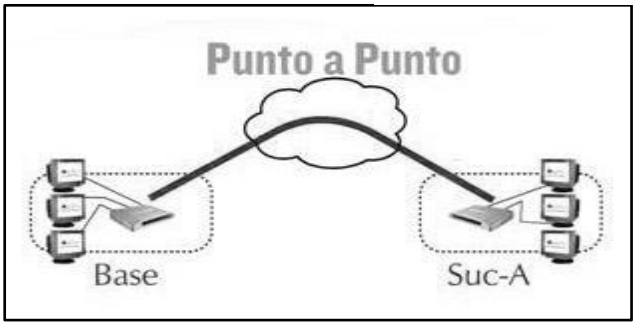
Se dividen en:

- Simplex: inútil en redes de computadores (monodireccional).
- Semi-dúplex (Half-duplex): envía datos cada vez en un sentido.
- Dúplex (Full-duplex): envía datos en los dos sentidos a la vez.

Sus características son:

- Empleadas en redes WAN
- Los algoritmos de routing son complejos, se necesitan 2 niveles de control de errores.
- Se distribuye el mensaje a la estación indicada.
- Existen varias líneas de comunicación.
- El principal retraso es debido a la retransmisión del mensaje entre nodos intermedios.
- Medio de transmisión: nodos intermedios.
- La redundancia es inherente siempre que el número de conexión de cada nodo sea mayor de 2.

Imagen N° 27
Ejemplo de redes punto a punto



Topologías De Redes Multipunto

En una red multipunto sólo existe una línea de comunicación cuyo uso está compartido por todas las terminales en la red, y la información fluye de forma bidireccional y es disernible para todas las terminales de la red.

Lo típico es que en una conexión miltipunto las terminales compiten por el uso del medio (líenea) de forma que el primero que lo encuentra disponible lo acapara, aunque también puede negociar su uso.

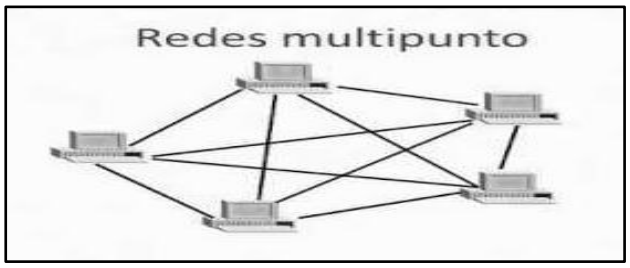


Imagen N° 28
Ejemplo de redes multipunto

Cuando se selecciona la topología que va a tener una red, se deben considerar dos aspectos importantes:

- La topología física o la disposición real de los componentes de la red, y
- La topología lógica o arquitectura de la red, que es la forma en que las maquinas se comunicaran dentro de la red.

Topología en bus

La topología en bus tiene todos sus nodos conectados directamente a un cable central y lineal, donde físicamente cada dispositivo está conectado a un cable común, el cable o canal propaga las señales en ambas direcciones, de manera que todos los dispositivos puedan ver todas las señales de todos los demás dispositivos.

Esta característica puede ser ventajosa si se requiere que todos los dispositivos obtengan esa información, pero podría representar una desventaja debido al tráfico y podrían presentarse colisiones que afecten a la red.

Las ventajas de la topología en canal o bus son:

- La facilidad de incorporar o quitar dispositivos de la red.
- se requiere una menor cantidad de cableado que en otras topologías.

Su principal desventaja es:

- La ruptura del cableado hace que se rompa toda la comunicación dentro de la red que se encuentra conectado.

La Topología En Estrella

La topología en estrella se caracteriza por tener todos sus nodos conectados a un controlador central: donde todas las transacciones pasan a través del nodo central, siendo éste el encargado de gestionar y controlar todas las comunicaciones, por este motivo, el fallo de un nodo en particular es fácil de detectar y no daña el resto de la red, pero un fallo en el nodo central desactiva la red completa.

Las ventajas de la topología en estrella son:

- Facilidad para incorporar o eliminar dispositivos de la red.
- La ruptura del cableado de un dispositivo, solo afecta a éste.
- Se detecta con facilidad alguna desconexión.

Las desventajas que presenta, son las siguientes:

- La cantidad de cableado requerido es superior a cualquier otra topología.
- Una falla en el hub o swiche, afecta a toda la red.

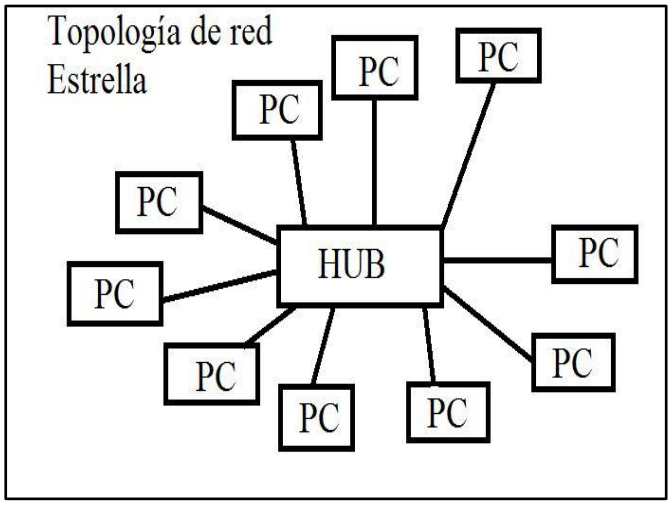


Imagen N° 29.1
Ejemplo de un hub conectado a una topología estrella

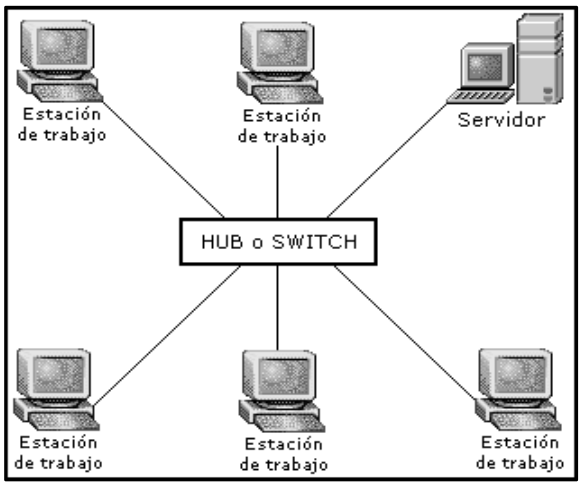


Imagen N° 29.2
Ejemplo de un switch conectado a una topología estrella

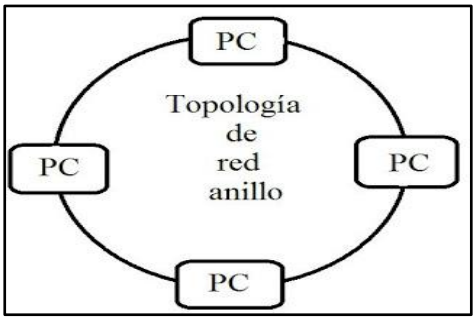
Topología En Anillo

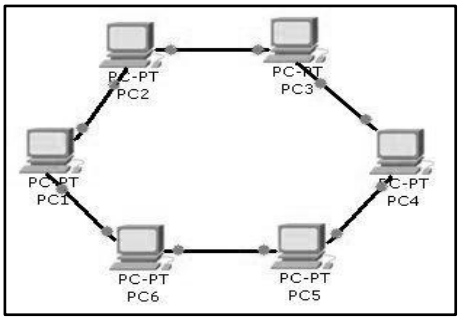
La topología en anillo se caracteriza por un camino unidireccional cerrado que conecta todos los nodos, dependiendo del control de acceso al medio, se dan nombres distintos a esta topología: Bucle; se utiliza para designar aquellos anillos en los que el control de acceso está centralizado (una de las estaciones se encarga de controlar el acceso a la red).

La principal ventaja en redes con topología en anillo, es la estabilidad con respecto al tiempo que tardan las señales en llegar a su destino, sin que se presenten colisiones.

La desventaja que tiene esta topología es que la ruptura en la conexión de un dispositivo, tira toda la red.

Imagen N° 30
Ejemplo de una topología anillo conectados a diferentes PC



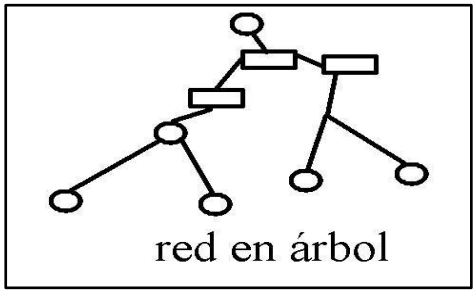


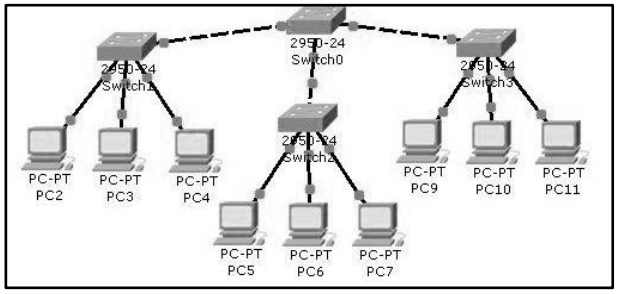
La topología en árbol

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

La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central.

Imagen N° 31
Ejemplo de dispositivos conectados a una topología de árbol

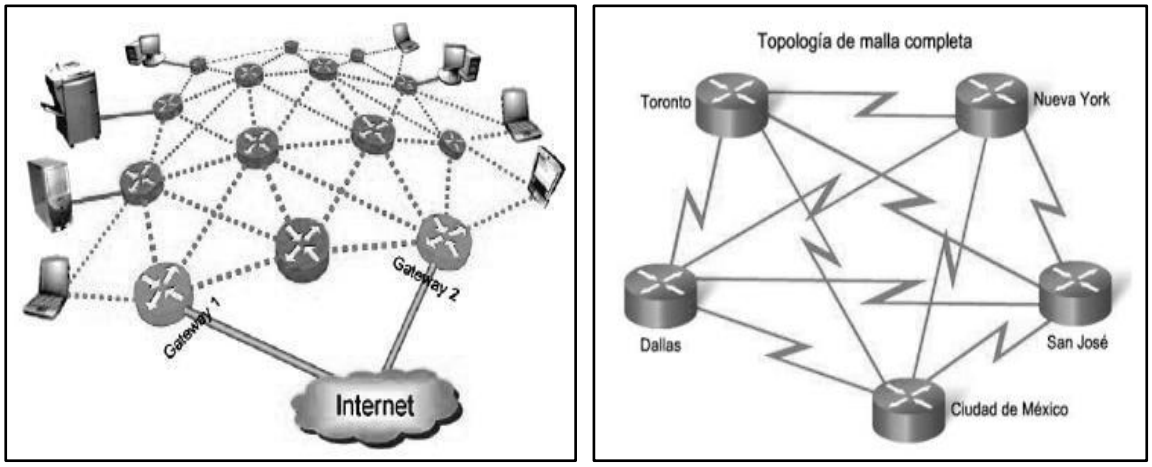




Topología En Malla O Total

En esta topología, de uso común en redes tipo WAN, todos los nodos de la red están interconectados entre sí, formando una malla de conexiones similar a una tela de araña. La redundancia de conexiones busca que siempre exista un camino viable entre un nodo y otro.

Imagen N° 32
Ejemplo de topologías malla o total



Tipos de topología hibrida o mixta

Como su nombre lo indica, es una combinación de dos o más topologías de red diferentes**,** para adaptar la red a las necesidades del cliente, de este modo, podemos combinar las topologías que deseemos, obteniendo infinitas variedades, las cuales, deben ajustarse a la estructura física del lugar en donde estará la red y los equipos que estarán conectados en dicha red.

En una topología mixta, se combinan dos o más topologías para formar un diseño de red completo, esta combinación puede darse en diferentes tipos de redes, LAN, MAN y WAN, dependiendo del diseño y funcionamiento que presente cada una de ellas.

Ventajas

Las redes híbridas o mixtas ofrecen múltiples posibilidades para la transmisión de datos entre nodos de la red; el fallo de cualquier componente simple de hardware (tal como una impresora o un cable) no afecta al rendimiento de la red, y en tal caso, la red híbrida evita el nodo/cable afectado y desplaza los datos a una ruta de transmisión alternativa.

Las redes híbridas son versátiles y pueden adaptarse a una amplia variedad de requerimientos y tamaños de red.

Desventaja

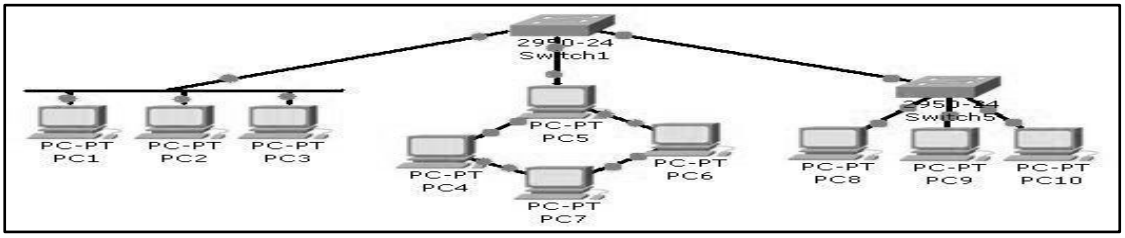
Una red híbrida requiere más cableado entre sus nodos que otros tipos de redes; las inconsistencias y errores en los nodos individuales de una red híbrida son a menudo difíciles de aislar y reparar.

Las redes híbridas eficientes requieren puntos o centros inteligentes de concentración; los concentradores inteligentes están diseñados para proporcionar aislamiento de fallos y procesamiento automáticos. Constantemente escanean la red, recogen información sobre todos los nodos, detectan errores, aislan los nodos defectuosos y convierten el tráfico de red a rutas alternas. Los concentradores inteligentes, aunque eficientes, son más caros que los pasivos y los activos.

Las redes híbridas de gran tamaño comúnmente requieren varios concentradores inteligentes

La topología híbrida anillo – estrella, consiste físicamente en una estrella centralizada en un concentrador, mientras que a nivel lógico, la red funciona como un anillo.

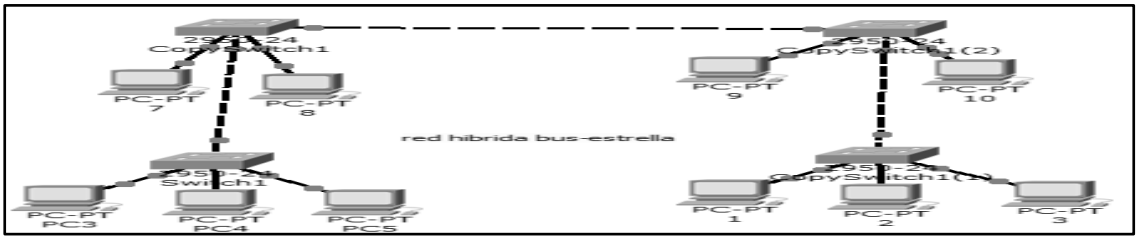
Imagen N° 33
Ejemplo de topologías hibrida anillo- estrella



La topología híbrida bus – estrella es un canal o bus que se cablea físicamente como una estrella mediante concentradores, es decir consiste en la unión de dos o más redes con topología en estrella unidas mediante un cable lineal central que utiliza la topología en canal.

En esta topología, la señal generada por un dispositivo, es enviada al concentrador, el cuál la transmite al otro hub, conectado en el canal, y de este concentrador llega al dispositivo destino.

Imagen N° 34
Ejemplo de topologías hibrida bus- estrella



Topología de red jerárquica - arbol

Es la topología de red en la que los nodos están colocados en forma de árbol, y desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

Tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos; es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones, y se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

Los problemas asociados a las topologías anteriores radican en que los datos son recibidos por todas las estaciones sin importar para quien vayan dirigidos.

Ventajas de Topología de Árbol

- El Hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.
- Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Desventajas de Topología de Árbol

- Se requiere mucho cable.
- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.

PROTOCOLO ENRUTADO

Un protocolo enrutado permite que un Router envíe datos entre nodos de diferentes redes, trabaja en el nivel 3 utilizado para transferir información desde un dispositivo a otro a través de la red, es un datagrama que lleva información de la aplicación además de información de los niveles superiores.

Cualquier protocolo de red que proporcione suficiente información en su dirección de capa de red para permitir que un paquete se envíe desde un host a otro tomando como base el esquema de direccionamiento.

Los protocolos enrutados definen el formato y uso de los campos dentro de un paquete, y donde generalmente se transfieren de un sistema final a otro.

IP es un ejemplo de protocolo enrutado.

Funciones:

- Incluir cualquier conjunto de protocolos de red que ofrece información suficiente en su dirección de capa para permitir que un Router lo envíe al dispositivo siguiente y finalmente a su destino.
- Definir el formato y uso de los campos dentro de un paquete.
- El Protocolo Internet (IP) y el intercambio de paquetes de internetworking (IPX) de Novell son ejemplos de protocolos enrutados. Otros ejemplos son DEC net, Apple Talk, Banyan VINES y Xerox Network Systems (XNS).
- Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host.
- En la actualidad solo hay un protocolo enrutado en uso, y es IP (versión 4 y versión 6). Las direcciones IP tienen una parte de red y una parte de host (la máscara de subred le indica cómo separar las dos).

  La parte de red de la dirección le permite al host buscar en su tabla de enrutamiento para determinar cuál es la mejor manera de reenviar el paquete.

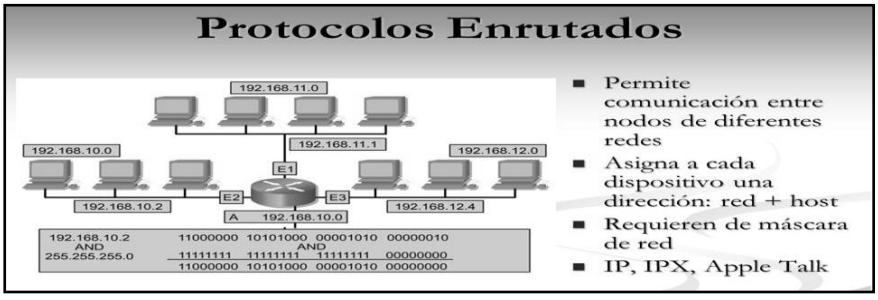


Imagen N° 35
Ejemplo de protocolo enrutado con su respectivo direccionamiento

PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento proporcionan información para elaborar las tablas de enrutamiento y además determinan la mejor ruta a través de la conexión entre redes que deben seguir los paquetes de datos desde la computadora transmisora hasta la computadora receptora.

Los protocolos de enrutamiento utilizan algoritmos ya sea estático o dinámico según el caso para encaminar los paquetes de una máquina a otra.

Enrutamiento Estático. El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red.

Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Existe una sola conexión con un solo ISP.
- En lugar de conocer todas las rutas globales
- se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

Enrutamiento Predeterminado. Es una ruta estática que se refiere a una conexión de salida o Gateway de último recurso, y donde el tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida.

Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino **0.0.0.0/0.0.0.0.**

Enrutamiento Dinámico. Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

La principal diferencia entre los **protocolos estáticos y dinámicos,** es que en los estáticos los router no pueden adaptarse a los cambios que puedan producirse en la topología de red, esto quiere decir que si un router queda desactivado o una porcion de la red deja de funcionar, no hay forma de que los

routers se adapten a estos cambios y actualicen sus tablas de enrutamiento para que los paquetes puedan seguir su camino hasta el final.

Los algoritmos dinámicos se construyen y mantienen por medio de mensajes de actualización de enrutamiento; estos mensajes que contienen información acerca de los cabios que han operado en la red, indican al software de enrutamiento que vuela a calcular su algoritmo y actualice la tabla de enrutamiento del routers.

Los algoritmos de enrutamiento se dividen en:

a) Vector Distancia: Determina la dirección y la distancia hacia cualquier enlace de la red. Su métrica se basa en lo que se le llama en redes **Numero de Saltos**, es decir la cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino, la ruta que tenga el menor número de saltos es la más optima y la que se publicará.

- Visualiza la red desde la perspectiva de los vecinos
- Actualizaciones periódicas
- Transmite copias completas o parciales de las tablas de enrutamiento Convergencia lenta
- Incrementa las métricas a través de las actualizaciones

b) Estado de enlace: También llamado Primero la Ruta Libre Mas Corta (OSPF), recrea la topología exacta de toda la red, donde su métrica se basa el retardo, ancho de banda , carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra.

Estos protocolos utilizan un tipo de publicaciones llamadas Publicaciones de estado de enlace (LSA),que intercambian entre los routers, mediante estas publicación cada router crea una base datos de la topología de la red completa.

- Buscan una unión común de la topología de la red.
- Cada dispositivo calcula la ruta más corta a los otros routers.
- Las actualizaciones se activan por los eventos (cambios en la topología) de la red.

METRICA: La métrica es el análisis, y en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta por sobre

otra, basándose en eso el protocolo creará la tabla de enrutamiento en el routers, publicando sólo las mejores rutas.

Un protocolo de enrutamiento utiliza métrica para determinar qué vía utilizar para transmitir un paquete a través de un Intercambio

La métrica utilizada por protocolos de enrutamiento incluyen:

- Numero de saltos: Número de routers por los que pasará un paquete.
- Pulsos: Retraso en un enlace de datos usando pulsos de reloj de PC.
- Coste: Valor arbitrario, basado generalmente en el ancho de banda, el coste económico u otra medida.
- Ancho de banda: Capacidad de datos de un enlace.
- Retraso: Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- Carga: Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- Fiabilidad: Se refiere al valor de errores de bits de cada enlace de red.
- MTU: Unidad máxima de transmisión. Longitud máxima de trama en octetos que puede ser aceptada por todos los enlaces de la ruta.

Distancia administrativa y métrica: Es una medida de la confianza otorgada a cada fuente de información de enrutamiento; cada protocolo de enrutamiento lleva asociado una distancia administrativa, y los valores más bajos significan una mayor fiabilidad.

Un enrutador puede ejecutar varios protocolos de enrutamiento a la vez, obteniendo información de una red por varias fuentes.; y en estos casos usará la ruta que provenga de la fuente con menor distancia administrativa de los protocolos de enrutamiento

RIP (Routing Information Protocol): El método más común para transferir información de enrutamiento entre routers ubicados en la misma red es el RIP, y este protocolo de gateway interior calcula las distancias hacia un destino.

El RIP permite que los routers que usan este protocolo actualicen sus tablas de enrutamiento a intervalos programables, normalmente cada treinta segundos. Sin embargo, como el router se conecta constantemente con otros routers vecinos, esto puede provocar el aumento del tráfico en la red.

Por esto RIP permite que los routers determinen cuál es la ruta que usarán para enviar datos, basándose en un concepto que se conoce como vector-distancia. Siempre que los datos viajan a través de un router, y por lo tanto a través de un nuevo número de red, se considera que han efectuado un salto. Una ruta cuyo número de saltos es cuatro indica que los datos que se transportan a través de la ruta deben pasar a través de cuatro routers antes de llegar a su destino final en la red, si hay múltiples rutas hacia un destino, el router, usando RIP, selecciona la ruta que tiene el menor número de saltos.

El IGRP se desarrolló específicamente para ocuparse de los problemas relacionados con el enrutamiento en redes compuestas por productos de varios fabricantes, que no se podían manejar con protocolos como, por ejemplo, RIP. Como RIP, IGRP es un protocolo de vector de distancia, sin embargo, al determinar cuál es la mejor ruta también tiene en cuenta elementos como, por ejemplo, el ancho de banda, la carga, el retardo y la confiabilidad.
Los administradores de red pueden determinar la importancia otorgada a cualquiera de estas métricas, o bien, permitir que IGRP calcule automáticamente la ruta óptima.

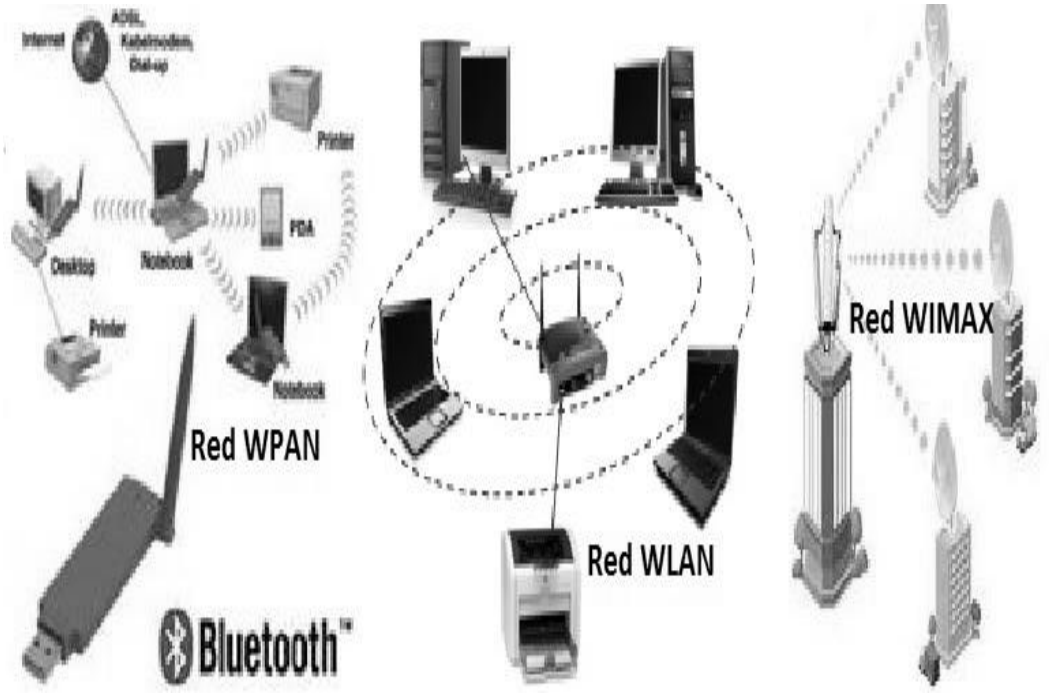
El EIGRP es una versión avanzada del IGRP. Específicamente, EIGRP suministra una eficiencia de operación superior y combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector de distancia.

Imagen N° 36
Ejemplo de protocolo de enrutamiento exterior, interior y diferentes sistemas autónomos

PREGUNTAS SOBRE LA UNIDAD N°2:

1. ¿Cual es la distancia máxima de una red 10 base 2?
2. ¿Cual es la distancia máxima de una red 10 base 5?
3. ¿Cuál es la distancia máxima de una red 10 base T?
4. ¿Cuál es la distancia máxima de una red 10 base F?
5. ¿Cuál es la distancia máxima de una red 100 base TX?
6. ¿Cuál es la distancia máxima de una red 100 base FX?
7. ¿Cuál es la distancia máxima de una red 1000 BASE T**?**
8. ¿Cuál es la distancia máxima de una red 1000 BASE SX?
9. ¿Cuál es la distancia máxima de una red 1000 BASE LX?
10. ¿Qué es una topología de difusión?
11. ¿Que es una Topología en bus?
12. ¿Qué es una Topología en estrella?
13. ¿Qué es una Topología en anillo?
14. ¿Qué es una Topología total o malla?
15. ¿Qué es un protocolo de enrutado?
16. ¿Qué es un protocolo de enrutamiento?
17. ¿Qué es un vector a distancia?
18. ¿Que es un estado de enlace?
19. ¿Cuáles son los algoritmos que utilizan los protocolos de enrutamiento?
20. ¿Cuál es la característica del protocolo RIP?
21. ¿Cuál es la característica del protocolo IGRP?
22. ¿Qué es la métrica

CAPÍTULO N° 3


Internet
ADSL
Kabelmodem
Dial-up
Printer
PDA
Desktop
Notebook
Printer
Notebook
Red WPAN
Bluetooth
Red WLAN
Red WIMAX

CAPÍTULO III: REDES INALÁMBRICAS

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales computadoras portátiles, agendas electrónicas, etc.; y se pueden comunicar sin la necesidad de una conexión por cable.

Gracias a las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica, y por esta razón, a veces se utiliza el término movilidad cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas por medio de un radio infrarrojo en lugar de cableado estándar, donde existen muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros; así mismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas.

Los tipos de onda posibles son:

Ondas de radio: Son omnidireccionales, no necesita de parabólicas y no es sensible a los cambios climáticos como la lluvia. Hay varios tipos de banda, se puede transmitir con una frecuencia de 3 a 30 Hz y un máximo de 300 a 3000 MHz .

Microondas terrestres: Las antenas parabólicas se envían la información, alcanza kilómetros pero emisor y receptor deben estar perfectamente alineados, y su frecuencia es de 1 a 300 GHz .

Microondas por satélite: la información se reenvía de un satélite, es de las ondas más flexibles pero es fácil que sufra interferencias, para este tipo de conectividad uno de los servicios de Red que se puede utilizar es BGAN.

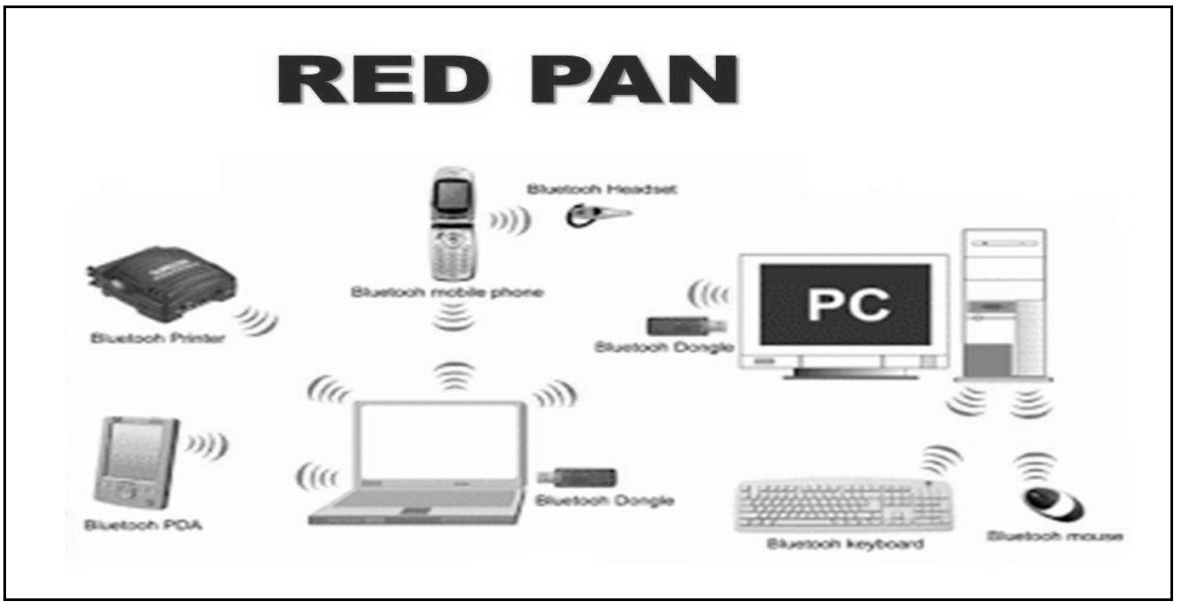
Infrarrojos: deben estar alineados directamente, no atraviesan paredes y tienen una frecuencia de 300 GHz a 384 THz.

Redes Inalámbricas De Área Personal (WPAN)

Las redes inalámbricas de área personal se basan en el estándar IEEE 802.15 Las redes inalámbricas permiten la comunicación en un rango de distancias muy corto, unos 10 metros, y a diferencia de otras redes inalámbricas, una conexión realizada a través de una WPAN implica, por lo general, poca o ninguna infraestructura o conectividad directa fuera del enlace establecido. Esto permite soluciones pequeñas, eficientes en energía y de bajo coste que pueden ser implementadas en una amplia gama de dispositivos, como por ejemplo teléfonos inteligentes, PDAs, entre otros, y se caracterizan por:

- Este tipo de redes se caracterizan por su bajo consumo de energía y también una baja velocidad de transmisión; se basan en tecnologías como Bluetooth, IrDA, ZigBee o UWB.
- Desde un punto de vista de aplicación, Bluetooth está destinado a un ratón, un teclado, unas manos libres.
- **IrDA** está pensado para enlaces punto a punto entre dos dispositivos para la transferencia de datos simples y sincronización de archivos.
- **ZigBee** está diseñado para redes inalámbricas fiables para el seguimiento y control de procesos, mientras que UWB está orientado a enlaces multimedia de gran ancho de banda.

Imagen N° 37.1
Ejemplo de una red PAN conectada a diferentes dispositivos según su alcance.



Bluetooth

La nueva versión 1.2, incorpora la función de salto de frecuencia adaptiva, la cual minimiza la interferencia mutua con sistemas de frecuencia estática (802.11) y hace posible la coexistencia de diferentes sistemas inalámbricos en el mismo entorno.

Esta función permite a los dispositivos Bluetooth, operar mas efectivamente en donde existen redes inalámbricas, como en los grandes supermercados y en muchos almacenes.

La versión 1.2 también ha corregido los problemas asociados con la transmisión de voz, y soporta mejor los audífonos inalámbricos, como los de los teléfonos celulares y los sistemas basados en voz utilizados en los almacenes.

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 las sincronización de datos entre nuestros equipos personales

Bluetooth proporciona una vía de interconexión inalámbrica entre diversos aparatos que tengan dentro de sí esta tecnología, como celulares, computadoras de mano (Palm, Pocket PC) , cámaras, computadoras portátiles, impresoras y simplemente cualquier cosa que a un fabricante le de por colocarle Bluetooth, usando por supuesto una conexión segura de radio de muy corto alcance. El alcance que logran tener estos dispositivos es de 10 metros. Para mejorar la comunicación es recomendable que nada físico (como una pared) se interponga.

El primer objetivo para los productos Bluetooth de primera generación eran los entornos de la gente de negocios que viaja frecuentemente. Por lo que se debería pensar en integrar el chip de radio Bluetooth en equipos como: PCS portátiles, teléfonos móviles, PDAs y auriculares.

Esto originaba una serie de cuestiones previas que deberían solucionarse tales como:

- El sistema debería operar en todo el mundo.
- El emisor de radio deberá consumir poca energía, ya que debe integrarse en equipos alimentados por baterías.
- La conexión deberá soportar voz y datos, y por lo tanto aplicaciones multimedia. y se a crea una gran popularidad con dicho sistema.

La tecnología

- La especificación de Bluetooth define un canal de comunicación de máximo 720Kb/seg con rango óptimo de 10 metros (opcionalmente 100m).
- La frecuencia de radio con la que trabaja está en el rango de 2.4 a 2.48Ghz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex con un máximo de 1600 saltos/seg.
- Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz; esto permite dar seguridad y robustez.

Imagen N° 37.2
Ejemplo: En esta imagen podemos ver los diferentes dispositivos electrónicos e informáticos que puede interconectar la tecnología Bluetooth

LAS REDES INALÁMBRICAS DE ÁREA LOCAL WLAN

WLAN por sus siglas en inglés Wirless Local Area Network, son redes que comúnmente cubren distancias de los 10 a los 100 de metros.

Esta pequeña cobertura contiene una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia.

Debido a que las LAN a menudo son utilizadas para comunicaciones de una relativa alta capacidad de datos, normalmente tienen índices de datos más altos, por ejemplo 802.11, una tecnología WLAN, tiene un ámbito nominal de 100 metros e índices de transmisión de datos de hasta 11Mbps, y los dispositivos que normalmente utilizan WLAN son los que tienen una plataforma más robusta y abastecimiento de potencia como son las computadoras personales en particular.

Las Redes de Área Local Inalámbricas (WLAN), según definición anterior, son un sistema de comunicación que transmite y recibe datos utilizando ondas electromagnéticas (aunque también es posible con luz infrarroja), en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (peer to peer), dentro de un edificio o en un área de cobertura. Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE para redes locales inalámbricas .

Las WLAN constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha, estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado permitiéndole competir con otro tipo de tecnologías de acceso.

Sus características más destacadas son:

- **Movilidad:** permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario, al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, reduciendo el tiempo de instalación, y permitiendo el acceso instantáneo a usuarios temporales de la red.

- **Flexibilidad:** puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes, siendo útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas

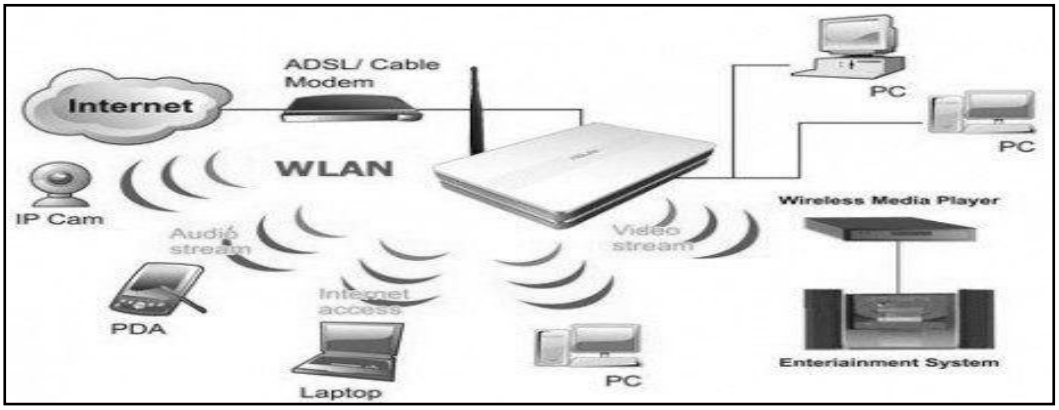
Imagen N° 38
Ejemplo de Comparación de una WLAN y una red cableada LAN

Aspecto	WLAN	LAN cableada
Velocidad de transmisión	11-54Mbps	100/1000Mbps
Costes de instalación	Bajo	Alto
Movilidad	Sí	No
Flexibilidad	Muy alta	Baja
Escalabilidad	Alta	Muy alta
Seguridad	Media	Alta
Demanda	Alta	Muy alta
Configuración e instalación	Fácil	Compleja
Presencia en empresas	Media	Alta
Coste de expansión	Bajo	Alto
Licencia	No regulado	No

Los principales problemas o debilidades, digámoslo así, que tiene una WLAN:

- **Seguridad:** Se considera que esta es mucho más vulnerable que otras redes, por lo que se hace necesario tomar todas las medidas posibles en pro de evitar que cualquiera pueda acceder a la misma. De ahí que se opte, por ejemplo, por lo que es el cifrado y el empleo de distintas claves y algoritmos.
- **Velocidad:** De la misma manera, aún queda mucho por mejor las WLAN en cuanto a este aspecto se refiere. Y es que se considera que, en la actualidad, aún no ha conseguido alcanzar la velocidad que sí ofrecen y tienen otros tipos de redes locales.

Imagen N° 39
Ejemplo de una red WLAN conectada a sus diferentes dispositivos



Estándares

Varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativa de WLAN y han generado un abanico de nuevos estándares.

802.11 legacy: Esta versión original del estándar IEEE 802.11 publicada en 1997, especifica dos velocidades de transmisión teóricas, 1Mbps y 2Mbps, que se transmiten mediante infrarrojos en la banda 2,4GHz, también define el protocolo CSMA/CA como método de acceso.

Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas.

A continuación se nombrara los diferentes estándares de la 802.11

- **802.11a** fue aprobada en 1999. Utiliza la banda de frecuencias de 5GHz con una velocidad máxima de transmisión de 54 Mbps, utiliza la tecnología de transmisión OFDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio, dividiendo la señal y transportándola mediante 52 subportadoras a diferentes frecuencias que son transmitidas simultáneamente hacia el receptor.
  La utilización de la banda de 5GHz representa la ventaja de recibir menos interferencias, pero también el inconveniente de que el rango de cobertura que ofrece es menor ya que penaliza mucho la potencia de la señal en función de la distancia.

- **802.11b** La revisión 802.11b, al igual que la 802.11, fue aprobada en 1999, utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 11Mbps. Los productos de este estándar aparecieron en el mercado muy rápido debido a que es una extensión directa de la técnica de modulación DSSS definida en el estándar original. por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b; y el rápido incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación del 802.11b como la tecnología WLAN definitiva.

- **802.11c** La revisión 802.11c fue aprobada en 1998. Especifica métodos para la conmutación inalámbrica, es decir, métodos para conectar diferentes tipos de redes mediante redes inalámbricas. 1.3.5 IEEE 802.11d La revisión 802.11d fue aprobada en 2001.
  También conocido como “Método Mundial” está pensado para permitir el uso internacional de las redes 802.11 locales; y p ermite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

- **802.11e** La revisión 802.11e fue aprobada en 2005. Define los mecanismos utilizados en una WLAN para proporcionar QoS a aplicaciones en tiempo real como voz y video. Para proporcionar soporte QoS se introduce una tercera función de coordinación, llamada HCF (Hybrid Coordination Function), que incorpora dos nuevos mecanismos de acceso al canal: EDCA (Enhanced Distributed Channel Access) y HCCA (HCF Controlled Channel Access).

- **802.11f** La recomendación 802.11f fue aprobada en el año 2000 y va dirigida a proveedores de puntos de acceso. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red; en definitiva permite que los productos sean más compatibles.

- **802.11g** La revisión 802.11g fue aprobada en 2003, utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 54Mbps; es compatible con el estándar 802.11b y utiliza las mismas frecuencias, y en buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. El rango máximo de los dispositivos 802.11g es ligeramente mayor al de los 802.11b, pero el rango en el que el cliente puede alcanzar 54Mbps es mucho más corto que en el que puede alcanzar 11Mbps en 802.11b.

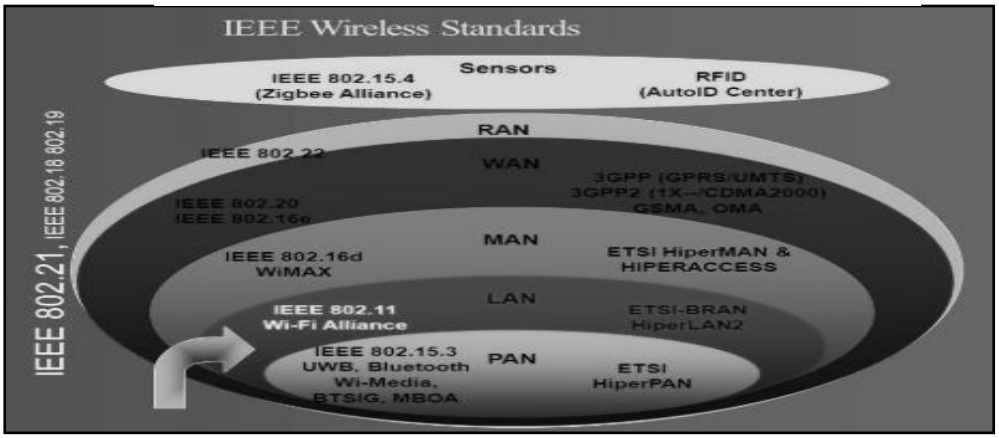
- **802.11h** La revisión 802.11h fue aprobada en 2003. Aparece como una modificación del estándar 802.11a para resolver problemas derivados de este tipo de redes con sistemas de radares y satélites debido a que la banda 5GHz era la utilizada por estos sistemas en el ámbito militar.

- **802.11i** La revisión 802.11i fue aprobada en 2004. Surgió con el fin de resolver los problemas de seguridad que comprometieron en su momento las WLAN. Integra todo lo que el mundo de la seguridad ofrece; esto incluye la autenticación IEEE 802.1x con protocolo de Integridad de claves Temporales (TKIP), Protocolo de Autenticación Extendido (EAP), RADIUS, Kerberos y encriptación basada en el algoritmo AES.

- **802.11j** La revisión 802.11j fue aprobada en 2002 y hace referencia a lo mismo que la 802.11h pero en Japón.

- **802.11 n** El estándar 802.11n fue ratificado por el IEEE en el año 2009. Mejora significativamente el rendimiento de la red con un incremento significativo de la velocidad máxima de transmisión de hasta 600Mbps en capa física. Puede trabajar en las bandas de frecuencia 2,4GHZ y 5GHz, lo que lo hace compatible con los dispositivos basados en estándares anteriores. La incorporación también de la tecnología MIMO (Multiple Input – Multiple Output) que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de 3 antenas, hace que el alcance del radio de las redes sea mucho mayor.

Imagen N° 40
Ejemplo de una red WLAN conectada a sus diferentes dispositivos



Redes De Área Metropolitana Inalámbricas (WMAN)

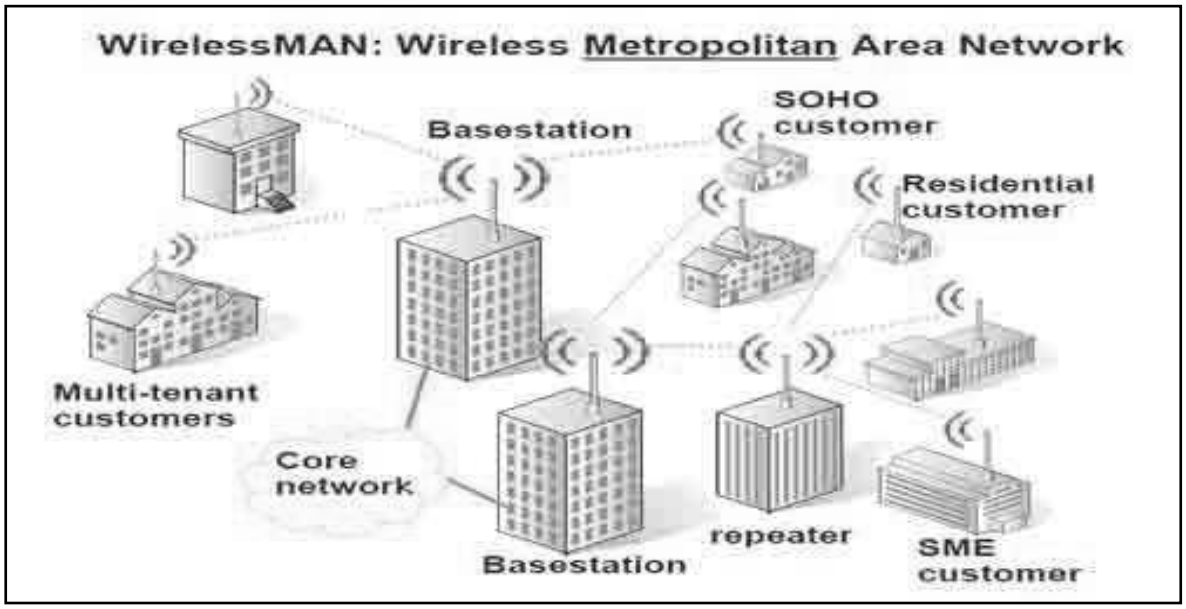
Las tecnologías WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas, además, WMAN puede servir como copia de seguridad para las redes con cable, en caso de que las líneas alquiladas principales para las redes con cable no estén disponibles. WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos.

Las redes de acceso inalámbrico de banda ancha, que proporcionan a los usuarios acceso de alta velocidad a Internet, tienen cada vez mayor demanda. Aunque se están utilizando diferentes tecnologías, como el servicio de distribución multipunto de canal múltiple (MMDS) y los servicios de distribución multipuntos locales (LMDS), el grupo de trabajo de IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Tienen un radio de acción mayor que el de las WLAN. Del orden de varias decenas de kilómetros.

Lo suficiente para cubrir una población completa, y las WMAN pueden interconectar unas WLAN con otras.

Imagen N° 41
Ejemplo de una red WPAN conectando varios edificios en una ciudad



WIMAX

Es una tecnología de banda ancha que te permite conectarte a la red a través de ondas electromagnéticas y en donde su nombre proviene de Worl wide Inter operabilty for Microwave Access en inglés, lo que en español se traduce como Interoperabilidad mundial para acceso por microondas.

En la actualidad, existen dos tipos principales de tecnología WiMAX:

WIMAX fija (802.16d-): es una tecnología de punto a varios puntos, en tanto que la WiMAX móvil es una tecnología de varios puntos a varios puntos, que se asemeja a la de una infraestructura celular. Estas dos soluciones fueron diseñadas para brindar servicios inalámbricos de Banda Ancha de alto rendimiento a costos reducidos.

WIMAX móvil (802.16e-): se basa en la tecnología OFDMA (acceso múltiple por división de frecuencia ortogonal) que ofrece ventajas inherentes en términos de latencia, eficiencia en el uso del espectro de frecuencia de radio y soporte avanzado de antenas, lo que en definitiva se traduce en un desempeño superior al de las actuales tecnologías de redes inalámbricas de área amplia. Por otra parte, las tecnologías inalámbricas 4G de próxima generación están evolucionando hacia OFMDA y redes IP ya que son ideales para proporcionar servicios inalámbricos de datos a un costo razonable.

Entre las principales características de la tecnología WIMAX se encuentran:

- Dependiendo de la version que se utilice, WiMAX podría alcanzar velocidades máximas de hasta 1 Gbit/seg para usuarios que se encuentren en una localización fija y 365 Mbit/seg para clientes en movilidad.
- La WiMAX pertenece a la familia de tecnologías 4G.
- El estándar que utiliza es el IEEE 802.16MAN.
- Se utiliza, principalmente, en zonas rurales en donde la instalación de otro tipo de tecnologías representarían un alto costo para el cliente.
- El organismo que certifica el cumplimiento de las normas es el Wimax Forum.
- Puede alcanzar distancias de hasta 80 kilómetros.

- Dependiendo de la regulación de cada país, tiene buena facilidad para agregar canales.
- Los anchos de banda son configurables y no cerrados, sujetos a la relación de espectro.
- WiMAX tiene una velocidad de transferencia bastante alta, pero en general debe repartirse entre múltiples usuarios. En teoría, WiMAX proporciona velocidades de aproximadamente 70 mbps en un rango de 50 kilómetros. En realidad, WiMAX sólo puede eludir obstáculos pequeños, como árboles o una casa y no puede atravesar montañas ni edificios altos. Cuando se presentan obstáculos, el rendimiento total real puede ser inferior a 20 mbps.

Imagen N° 42.1
Ejemplo de una red WMAX conectando diferentes estaciones y dispositivos

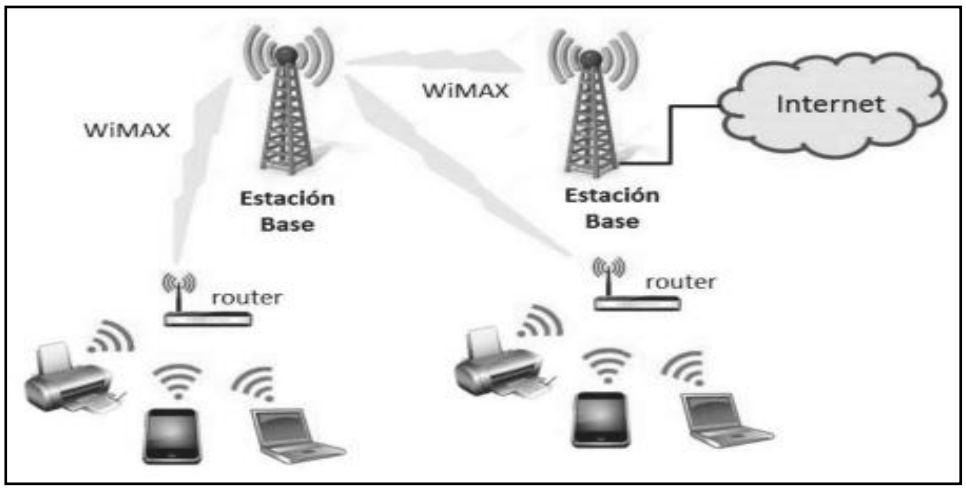
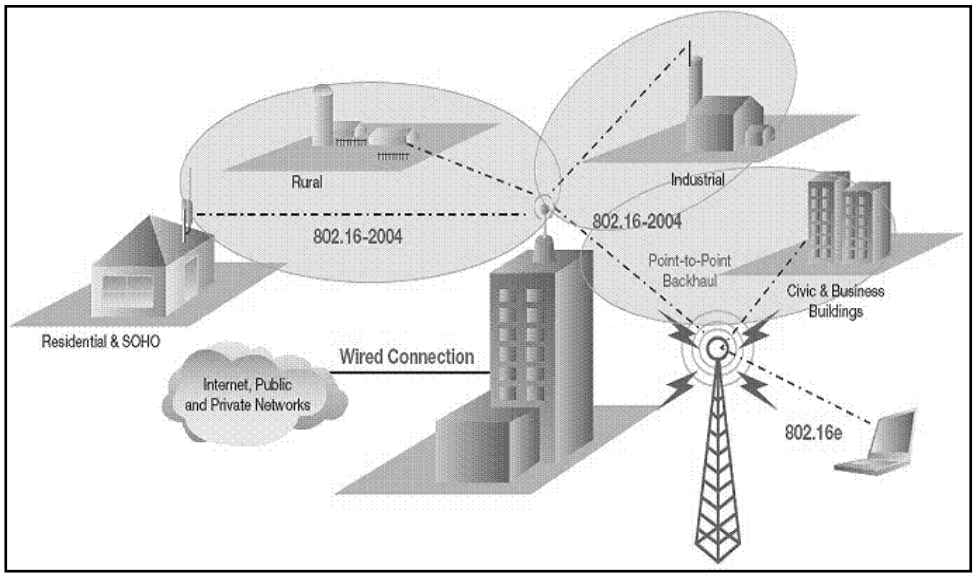


Imagen N° 42.2
Ejemplo de una red WMAX c conectando diferentes edificios y su correspondiente norma



Redes inalámbricas de área amplia (WWAN)

Las redes inalámbricas de área amplia se extienden más allá de los 50 kilómetros y suelen utilizar frecuencias con licencia.

Este tipo de redes se pueden mantener en grandes áreas, tales como ciudades o países, a través de los múltiples sistemas de satélites o ubicaciones con antena atendidos por un proveedor de servicios de Internet.

Existen principalmente dos tecnologías disponibles: la telefonía móvil y los satélites.

Red de telefonía móvil

En la red de telefonía móvil, el área de cobertura se divide en celdas; un transmisor de celda o estación base, en el centro de la celda, está diseñado para servir a una celda individual. Los dispositivos móviles están conectados a una estación base y estas últimas a una central de conmutación de telefonía móvil que une el teléfono móvil y la red cableada de telefonía.

El sistema pretende hacer un uso eficiente de los canales disponibles mediante el uso de transmisores de baja potencia para permitir la reutilización de frecuencias a distancias mucho más pequeñas.

- Las diferentes generaciones de telefonía móvil se han desarrollado desde principios de 1980.
- La primera generación, 1G, era analógica y fue concebida y diseñada exclusivamente para las llamadas de voz casi sin consideración de servicios de datos, con una velocidad de hasta 2,4 kbps. La segunda generación, 2G, está basada en tecnología digital y la infraestructura de red (GSM), permitiendo mensajes de texto con una velocidad de datos de hasta 64 Kbps. La generación 2.5G se sitúa entre la 2G y la 3G.
- También se la conoce como 2G + GPRS. Se trata de una versión mejorada de 2G, con una velocidad de hasta 144 Kbps. La generación 3G fue introducida en el año 2000, con una velocidad de datos de hasta 2 Mbps.
- Ls cuarta generación, 4G, es capaz de proporcionar velocidades de hasta 1 Gbps y cualquier tipo de servicio en cualquier momento de acuerdo con las necesidades del usuario, en cualquier lugar.

MECANISMOS DE SEGURIDAD

Para poder considerar una red inalámbrica como segura se deberían de cumplir entre otros los siguientes requisitos fundamentales.

- Las ondas de radio deben confinarse tanto como sea posible, esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación mutua, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Tipos De Autenticación Y Asociación

- **No autenticado y no asociado:** El nodo está desconectado de la red y no está asociado a un punto de acceso.
- **Autenticado y no asociado:** El nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso.
- **Autenticado y asociado:** El nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.

Los principales mecanismos de seguridad son:

- **SSID** Es uno de los mecanismos básicos de seguridad que contempla el estándar IEEE 802.11. El (SSID) es una cadena de generalmente 32 caracteres, utilizada para establecer un dominio de desplazamiento común a través de múltiples Puntos de Acceso.

  El SSID puede actuar como una simple contraseña sin la cual el cliente no podrá conectarse a la red.

  Los puntos de acceso retransmiten el SSID varias veces en las tramas broadcast de gestión, por lo que es sencilla su obtención.

- **Filtrado de direcciones MAC** Es otro de los mecanismos básicos de seguridad empleado por el estándar IEEE 802.11; este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso de la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso, donde todas las tarjetas de red, inalámbricas y no inalámbricas, poseen una dirección MAC, que es un número hexadecimal de doce dígitos único para cada tarjeta. Debido a esa exclusividad en la dirección MAC, un punto de acceso podría limitar las comunicaciones a sólo los usuarios cuya dirección MAC poseyera de antemano, es decir, a sólo aquellos clientes que estuvieran autorizados a comunicarse con y a través de él. Este método de filtrar las direcciones MAC está siendo muy utilizado por los fabricantes e instaladores de productos inalámbricos.

- **WEP** El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de los vendedores de soluciones inalámbricas. WEP puede ser utilizado tanto para autenticación como para encriptación.

  Generalmente, la autenticación se utiliza para protegerse contra accesos no autorizados a la red, mientras que la encriptación se usa para evitar que de una señal capturada se puedan obtener los datos en ella contenidos, y se basa en la encriptación de los paquetes de datos antes de ser transmitidos.

  Cuando se desea establecer una comunicación entre dos dispositivos, debe establecerse primero una asociación, para ello el cliente solicita la autenticación y el AP responde identificando el tipo de autenticación presente en la red.

  El funcionamiento de WEP se implementa en la capa MAC del estándar 802.11, y consiste en la encriptación de los datos, utilizando el algoritmo RC4 de RSA Security, que no es más que un generador de números pseudoaleatorios, alimentado por una clave que hará de semilla.

En primer lugar se genera una llave de 40 bits a partir de una clave estática de forma automática, aunque existe software que permite introducir esta llave manualmente.

La clave debe ser conocida por todos los clientes que quieran conectarse a la red inalámbrica que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente, aunque esto sea un problema para la seguridad.

A partir de la clave se generan 4 llaves de 40 bits, y sólo una de ellas se utilizará para la encriptación WEP.

- **WEP2** utiliza una clave secreta de 104 bits, donde el atacante que quiera hacerse con la clave secreta por medio de la fuerza bruta, es decir, probando a partir de algoritmos que contrarresten el RC4, tardará unas veinte semanas en obtener resultados, lo cual, en comparación con los pocos días que se tarda en descifra la clave en el protocolo WEP simple, supone una eternidad, y aún así, todavía existen hackers a los que les vale la pena este tipo de ataques, sin embargo, al igual que en WEP, hay gran cantidad de métodos que permiten acceder a la clave de forma mucho más rápida.

  Existen dos contratiempos o problemas en el uso de WEP2:

  El primero de ellos no es un problema en sí, sino una falta de mejora con respecto a WEP, muchos de los ataques a WEP no dependen más que del vector de inicialización; y éste, tanto en WEP como en WEP2 tiene el mismo número de bits, es decir, 24, con lo cual no estamos añadiendo nada nuevo en cuanto a seguridad; esta falta de mejora se debe a que cambiar la longitud del IV implicaría cambios sustanciales en el hardware.

  El **segundo** problema es que, debido a la mayor longitud de la clave secreta, existe una carga añadida en el proceso de encriptación de cada trama, la cual reduce el throughput.

  A pesar de los problemas que implica el uso de WEP2, es conveniente usarlo en lugar de WEP; y esto se debe a que, con el avance de las tecnologías, los equipos informáticos son cada vez más potentes, repercutiendo esto en dos aspectos distintos: dentro de poco, con la

potencia ofrecida por los ordenadores futuros, se podrá descifrar una clave WEP de 40 bits en unos pocos minutos, lo cual no ofrece prácticamente ninguna seguridad.

- **WPA** (Wi-Fi Protected Access) WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE.
  Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación más robust; y trata por lo tanto de una actualización de WEP mientras se desarrollaba el estándar 802.11i. WPA es compatible con el hardware existente y sólo requiere cambios en el software
  En WPA se encuentra con las siguientes mejoras respecto a WEP:
  1. WPA soluciona la debilidad del vector de inicialización de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados.
     El algoritmo utilizado por WPA sigue siendo RC4, y la secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas.
  2. Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 cuyas debilidades se demostraron en WEP y se ha incluido un nuevo código denominado MIC.
  3. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP. d) Para la autentificación, se sustituye el mecanismo de autentificación de WEP por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

- **WPA2** se recomienda generalmente sobre su predecesor WPA; ya que se trata del último protocolo desarrollado y diseñado para cubrir los defectos de sus antecesores. Probablemente el único inconveniente de WPA2 es cuánta potencia de procesamiento se necesita para proteger su red, esto significa que se necesita hardware más potente para no experimentar un menor rendimiento de la red. Por otro lado, la mayoría de los puntos de acceso actuales se han suministrado con hardware más que capaz.

  En síntesis es conveniente usar WPA2 si puede y sólo use WPA si no hay manera de que su punto de acceso soporte WPA2.

  El uso de WPA también es una posibilidad cuando su punto de acceso experimenta regularmente altas cargas y la velocidad de la red sufre del uso de WPA2.

  Cuando la seguridad es la principal prioridad, entonces el retroceso no es una opción, sino que uno debería considerar seriamente la posibilidad de obtener mejores puntos de acceso.

  Por último WEP tiene que ser utilizado si no hay posibilidad de usar cualquiera de los estándares WPA.

Imagen N° 43
Tabla Comparativa De Los Mecanismo De Seguridad

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
IV Size	24 bits	48 bits	48 bits
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-Based	EAP-Based

PREGUNTAS SOBRE LA UNIDAD N°3:

1. ¿Sobre qué norma se basan las redes wpan?
2. ¿sobre qué norma se basan las redes wlan?
3. ¿sobre qué norma se basan las redes wman?
4. ¿sobre qué norma se basan las redes wwan?
5. ¿cuáles son los tipos de ondas posibles?
6. ¿cuál es la distancia máxima que alcanza una red pan?
7. ¿cuál es el rango de frecuencia de radio que trabaja la tecnología bluetooth?
8. ¿en que frecuencia se basa el estándar IEEE 802.11 n?
9. ¿cuáles son las dos tipos principales de tecnología wimax?
10. ¿a qué tipo de tecnología pertenece wimax?
11. ¿cuáles son las principales tecnología de las redes wwan?
12. ¿Cuáles son los principales mecanismo de seguridad de las redes inalámbricas?
13. ¿Cuale s son los tipos de autenticación y asociación en una red inalámbrica?
14. ¿cuántos bits utiliza WEP para su clave secreta?
15. ¿cuántos bits utiliza WEP 2 para su clave secreta?
16. ¿cuántos bits utiliza WAP para su clave secreta?
17. ¿cuántos bits utiliza WAP 2 para su clave secreta?
18. ¿cuántos bits utiliza el filtrado MAC y x que medio lo realiza?

CAPÍTULO N° 4

LÍNEA TELEFÓNICA
ADSL
CABLE
Fibra óptica
Fibra + coaxial
SATÉLITE
Tipos de
CONEXIONES a INTERNET
econectia
TELEFONÍA MÓVIL
GSM, GPRS, 4G
REDES INALÁMBRICAS
LMDS, PLC, WIMAX

CAPÍTULO IV: COMUNICACIONES SATELITALES

Un satélite se define, de acuerdo al DRAE, como un cuerpo celeste opaco que solo brilla por la luz refleja del Sol y gira alrededor de un planeta primario.

En un concepto más amplio, un satélite se define como un cuerpo que gira alrededor de otro (denominado principal o primario) de masa preponderante, y cuyo movimiento se determina principalmente por la fuerza de atracción de éste ultimo.

Un satélite es por tanto un cuerpo que orbita alrededor de otro, fabricado por el ser humano para la realización de unas funciones determinadas, describiendo una trayectoria determinada en el espacio exterior.

Satélite artificial

Es un elemento físico capaz de recibir y transmitir señales en forma analógica o digital de alta calidad, está colocado en órbita por las necesidades que tiene el hombre para recibir y transmitir información a cualquier punto de la Tierra.

La mayoría de los satélites de comunicación se colocan en el arco satelital; es decir, se encuentran en la órbita geo síncrona o geoestacionaria, a una altura aproximada de 36,000 Km sobre el Ecuador; su velocidad es igual a la de la rotación terrestre y giran sobre su propio eje; por ello, cada satélite parece inmóvil con respecto a la Tierra, permitiendo que las antenas fijas apunten directamente hacia cualquier satélite.

- Un satélite es capaz de recibir y transmitir datos, audio y video en forma analógica o digital de alta calidad y en forma inmediata.
- Está formado por transponedores.
- El satélite toma su energía de la radiación solar, cada satélite tiene un tiempo de vida determinado que varía según la cantidad de combustible que posee; dicho combustible sirve para mover al satélite cada vez que éste se sale de su órbita, si el satélite pierde su posición y no tiene combustible, no hay manera de regresarlo ya que es atraído por las fuerzas espaciales hasta que se pierde.
- El satélite tiene un margen bien determinado en el espacio, como un cubo imaginario de aproximadamente 75 Km por lado, en el cual se desplaza sin salirse de control.

Servicios que brindan los satélites artificiales:

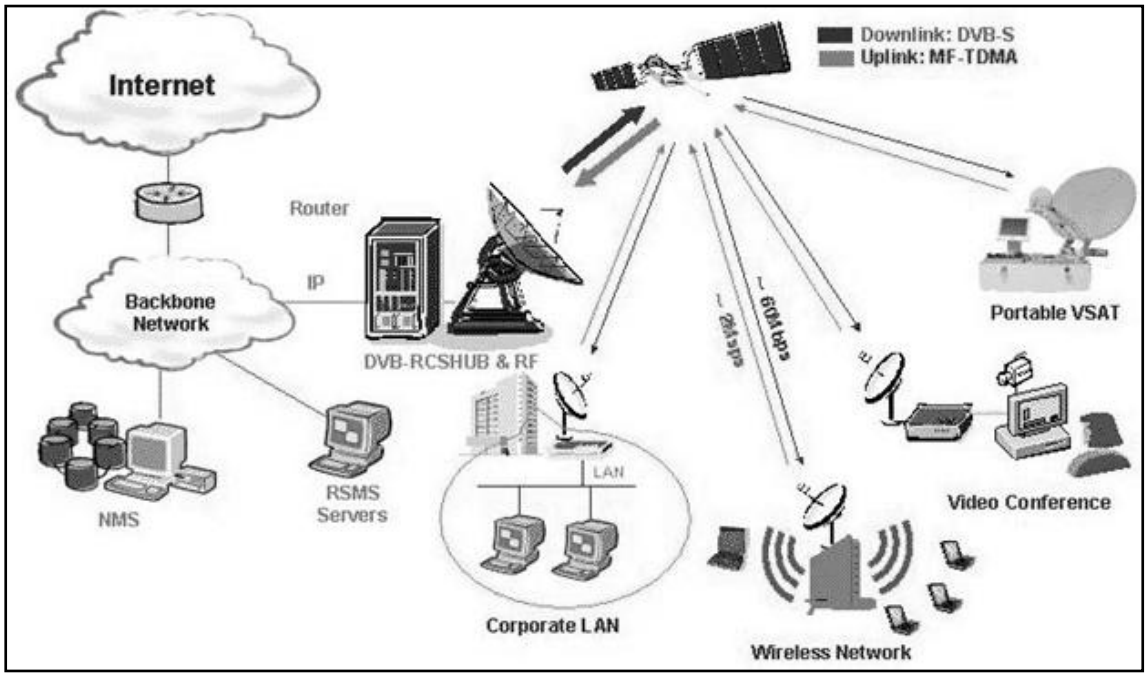
Los usos y servicios que brindan varían dependiendo el tipo de servicio, algunos son útiles para elaborar mapas, otros para obtener información específica de la Tierra u otros planetas y unos más para recopilar datos que ayuden a prever las condiciones del tiempo en el planeta.

El famoso Sistema de Posicionamiento Global (GPS, por sus siglas en inglés), que determina la ubicación/posición de un objeto en el planeta, funciona a partir de una red de satélites artificiales, y de hecho, los sistemas de telecomunicaciones actuales que incluyen la televisión y los teléfonos celulares, funcionan gracias a satélites artificiales.

Algunos servicios que brindan serian:

- Radioenlaces entre estaciones fijas o móviles, a través de alrededor de la Tierra.
- Servicio de radiodifusión por satélite, de tipo punto a zona.
- Servicios de meteorología por satélite.
- Servicio móvil por satélite entre estaciones de base fija y tele servicio fijo por satélite entre múltiples puntos fijos.
- Servicios de localización y navegación por satélite.
- Servicios de exploración de la Tierra por satélite.

Imagen N° 44.1
Ejemplo de un sistema de comunicación satelital



ELEMENTOS DE LAS REDES SATELITALES

Es importante a la hora de entender el funcionamiento de un satélite, en cuáles son sus componentes principales y cuál sería su órbita de funcionamiento alrededor de la tierra, por eso a continuación veremos estos elementos y su tipo órbita alrededor de la tierra.

Transponders: Es un dispositivo que realiza la función de recepción y transmisión. Las señales recibidas son amplificadas antes de ser retransmitidas a la tierra, y para evitar interferencias les cambia la frecuencia.

Estaciones terrenas: Las estaciones terrenas controlan la recepción con el satélite y desde el satélite, regula la interconexión entre terminales, administra los canales de salida, codifica los datos y controla la velocidad de transferencia.

Consta de 3 componentes principales:

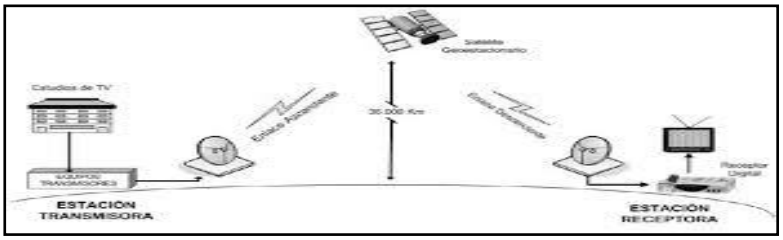
Estación receptora: Recibe toda la información generada en la estación transmisora y retransmitida por el satélite.

Antena: Debe captar la radiación del satélite y concentrarla en un foco donde está ubicado el alimentador. Una antena de calidad debe ignorar las interferencias y los ruidos en la mayor medida posible; estos satélites están equipados con antenas receptoras y con antenas transmisoras. Por medio de ajustes en los patrones de radiación de las antenas pueden generarse cubrimientos globales, cubrimiento a solo un país (satélites domésticos), o conmutar entre una gran variedad de direcciones.

Estación emisora: Esta compuesta por el transmisor y la antena de emisión. La potencia emitida es alta para que la señal del satélite sea buena; esta señal debe ser captada por la antena receptora, y para cubrir el trayecto ascendente envía la información al satélite con la modulación y portadora adecuada.

Imagen N° 44.2

Ejemplo de cómo interactúan los componentes de un satélite



Las orbitas de un satélite

Una órbita es una trayectoria que describe, en relación a un sistema de referencia dado, el centro de gravedad de un satélite o de otro objeto espacial, por la acción principal de fuerzas naturales, en particular la de gravitación.

El período orbital o de revolución de un satélite es el intervalo de tiempo que transcurre entre dos pasos consecutivos de un satélite por un punto característico de su órbita.

Las órbitas pueden clasificarse de acuerdo a diversos criterios:

- Según el centro (cuerpo primario) de la órbita. Puede ser galactocéntrica (galaxia), heliocéntrica (Sol), geocéntrica (Tierra), areocéntrica (Marte) o lunar (Luna).
- Según su excentricidad. Existen circulares (cerradas), elípticas (cerradas), parabólicas (abiertas), hiperbólicas (abiertas) o radiales (abiertas o cerradas).
- Según su inclinación. Son inclinadas (por ejemplo la órbita polar se encuentra inclinada 90° respecto del plano ecuatorial) o no inclinada (por ejemplo la órbita ecuatorial en el plano del ecuador terrestre).
- Según la sincronía del período de rotación del satélite respecto del cuerpo primario. Son síncronas, subsíncronas o supersíncronas.
- Según el sentido de rotación son prógradas o retrógradas.

Tipos de satélite según su órbita:

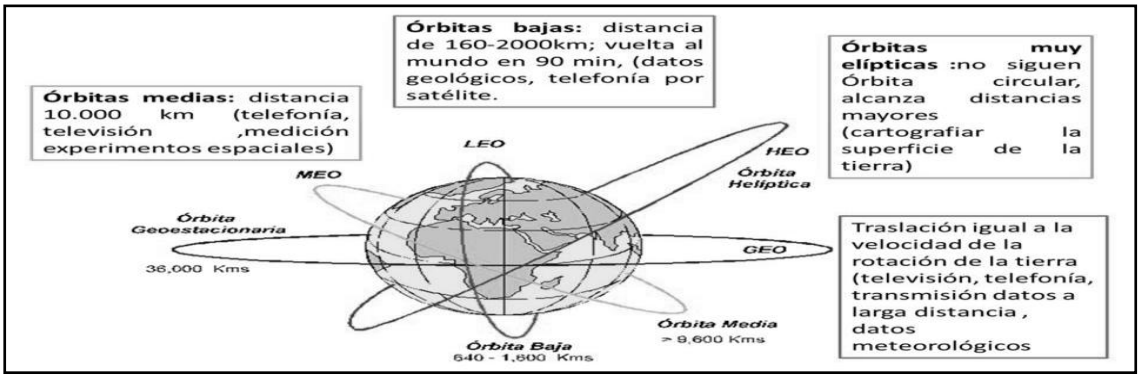
Clasificación por centro

- **Órbita galactocéntrica:** órbita alrededor del centro de una galaxia. El Sol terrestre sigue éste tipo de órbita alrededor del centro galáctico de la Vía Láctea.
- **Órbita heliocéntrica:** una órbita alrededor del Sol. En el Sistema Solar,los planetas, cometas y asteroides siguen esa órbita, además de satélites artificiales y basura espacial.
- **Órbita geocéntrica:** una órbita alrededor de la Tierra. Existen aproximadamente 2.465 satélites artificiales orbitando alrededor de la Tierra.

Clasificación por altitud

- **Órbita baja terrestre (LEO):** una órbita geocéntrica a una altitud de 0 a 2.000 km.
- **Órbita media terrestre (MEO):** una órbita geocéntrica con una altitud entre 2.000 km y hasta el límite de la órbita geosíncrona de 35.786 km. También se la conoce como órbita circular intermedia.
- **Órbita alta terrestre (HEO):** una órbita geocéntrica por encima de la órbita geosíncrona de 35.786 km; también conocida como órbita muy excéntrica u órbita muy elíptica.

Imagen N° 44
Ejemplo de un sistema de comunicación satelital de acuerdo a su órbita



Clasificación por inclinación.

- **Órbita inclinada:** una órbita cuya inclinación orbital no es cero.
- **Órbita polar:** una órbita que pasa por encima de los polos del planeta. Por tanto, tiene una inclinación de 90º o aproximada.
- **Órbita polar heliosíncrona:** una órbita casi polar que pasa por el ecuador terrestre a la misma hora local en cada pasada.

Clasificación por excentricidad.

- **Órbita circular:** una órbita cuya excentricidad es cero y su trayectoria es un círculo.
- **Órbita de transferencia de Hohmann:** una maniobra orbital que traslada a una nave desde una órbita circular a otra.
- **Órbita elíptica:** una órbita cuya excentricidad es mayor que cero pero menor que uno y su trayectoria tiene forma de elipse.

- **Órbita de transferencia geosíncrona**: una órbita elíptica cuyo perigeo es la altitud de una órbita baja terrestre y su apogeo es la de una órbita geosíncrona.
- **Órbita de transferencia geoestacionaria:** una órbita elíptica cuyo perigeo es la altitud de una órbita baja terrestre y su apogeo es la de una órbita geoestacionaria.
- **Órbita de Molniya:** una órbita muy excéntrica con una inclinación de 63,4º y un período orbital igual a la mitad de un día sideral (unas doce horas).
- **Órbita tundra:** una órbita muy excéntrica con una inclinación de 63,4º y un período orbital igual a un día sideral (unas 24 horas).
- **Órbita hiperbólica:** una órbita cuya excentricidad es mayor que uno.
  En tales órbitas, la nave escapa de la atracción gravitacional y continua su vuelo indefinidamente.
- **Órbita parabólica:** una órbita cuya excentricidad es igual a uno.
  En estas órbitas, la velocidad es igual a la velocidad de escape.
- **Órbita de escape:** una órbita parabólica de velocidad alta donde el objeto se aleja del planeta.
- Órbita de captura: una órbita parabólica de velocidad alta donde el objeto se acerca del planeta.

Clasificación por sincronía.

- **Órbita síncrona:** una órbita donde el satélite tiene un periodo orbital igual al periodo de rotación del objeto principal y en la misma dirección. Desde el suelo, un satélite trazaría una analema en el cielo.
- **Órbita semisíncrona:** una órbita a una altitud de 12.544 km aproximadamente y un periodo orbital de unas 12 horas.
- **Órbita geoestacionaria:** una órbita geosíncrona con inclinación cero. Para un observador en el suelo, el satélite parecería un punto fijo en el espectro terrestre.
- **Órbita cementerio:** una órbita a unos cientos de kilómetros por encima de la geosíncrona donde se trasladan los satélites cuando acaba su vida útil deja de servir.

- **Órbita areosíncrona:** una órbita síncrona alrededor del planeta Marte con un periodo orbital igual al día sideral de Marte, 24,6229 horas.
- **Órbita areoestacionaria:** una órbita areosíncrona circular sobre el plano ecuatorial a unos 17.000 km de altitud. Similar a la órbita geoestacionaria .

Los satélites artificiales poseen diversas ventajas que los hacen idóneos para su empleo radiocomunicaciones:

- No dependen de fronteras ni barreras físicas.
- Son muy estables en su funcionamiento. La señal se propaga por el espacio libre, con márgenes de desvanecimiento muy reducidos.
- Sustituyen o complementan las comunicaciones terrenas, inalámbricas o cableadas.
- Permiten grandes coberturas, alcanzando el 100% de la población con pocos satélites.
- Permiten comunicaciones de gran ancho de banda.

TELEFONÍA CELULAR

Concepto de Telefonía Celular

Un teléfono celular es un dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil, se denomina celular debido a las antenas repetidoras que conforman la red, cada una de las cuales es una célula, si bien existen redes telefónicas móviles satelitales.

Su principal característica es su portabilidad, que permite comunicarse desde casi cualquier lugar; aunque su principal función es la comunicación de voz, como el teléfono convencional, su rápido desarrollo ha incorporado otras funciones como son cámara fotográfica, agenda, acceso a internet, reproducción de video e incluso GPS y reproductor mp3.

La telefonía móvil se divide en dos partes bien diferenciadas, los teléfonos móviles o equipos terminales a un lado, y al otro toda la red que permite interconectarlos transmitiendo la información.

Historia

La historia del celular, del teléfono celular o teléfono móvil, es la secuencia de desarrollos, innovaciones tecnológicas y descubrimientos científicos que han permitido la creación de los teléfonos móviles**, t**ambién incluye su evolución en el tiempo hasta convertirse en las herramientas polifacéticas que manejamos hoy en día.

En la actualidad los sistemas de telefonía celular nos comunican a diversas personas y ciudades alrededor del mundo, donde su evolución se produce forma vertiginosa en los últimos años, pero que su origen se remonta hace varias décadas y su tecnología de trasmisión se basa en antiguas tecnologías de comunicación

La comunicación inalámbrica tiene sus raíces en la invención del radio por Nikola Tesla en los años 1880, aunque formalmente presentado en 1894 por un joven italiano llamado Guglielmo Marconi.

El teléfono móvil se remonta a los inicios de la Segunda Guerra Mundial, donde ya se veía que era necesaria la comunicación a distancia, es por eso que la compañía Motorola creó un equipo llamado Handie Talkie H12-16, que es un

equipo que permite el contacto con las tropas vía ondas de radio que en ese tiempo no superaban más de 600 kHz.

Fue sólo cuestión de tiempo para que las dos tecnologías de Teslay Marconi se unieran y dieran a la luz la comunicación mediante radio-teléfonos..

Martin Cooper fue el pionero en esta tecnología, a él se le considera como "el padre de la telefonía celular" al introducir el primer radioteléfono, en 1973, en Estados Unidos, mientras trabajaba para Motorola; pero no fue hasta 1979 cuando aparecieron los primeros sistemas comerciales en Tokio, Japón por la compañía NTT.

En 1981, los países nórdicos introdujeron un sistema celular similar a AMPS (Advanced Mobile Phone System); por otro lado, en Estados Unidos, gracias a que la entidad reguladora de ese país adoptó reglas para la creación de un servicio comercial de telefonía celular, en 1983 se puso en operación el primer sistema comercial en la ciudad de Chicago.

Con ese punto de partida, en varios países se diseminó la telefonía celular como una alternativa a la telefonía convencional inalámbrica

Imagen N° 45
Imagen del creador de la telefonía celular Martin Cooper

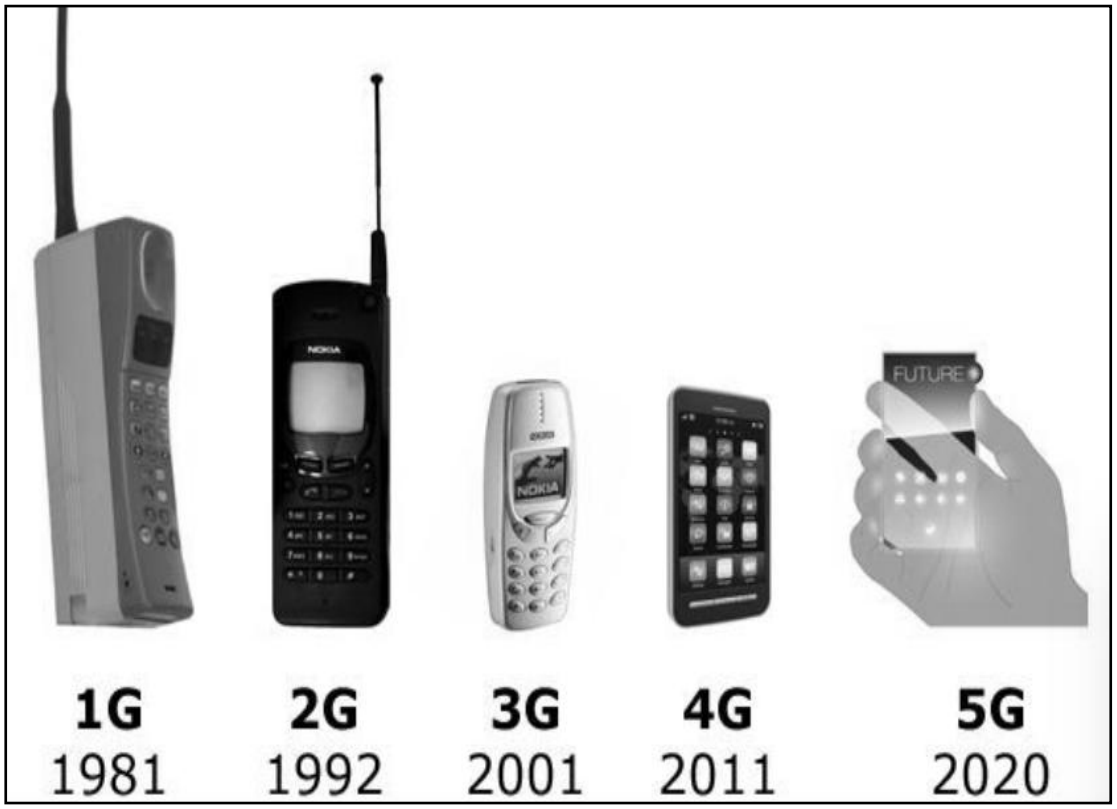
Los Teléfonos Móviles En La Actualidad

Que la telefonía móvil a cambiado de manera más que sustancial, es un hecho constatado en el cual caemos sin necesidad de tener que leer ningún estudio ni investigación al respecto, tan solo hace falta mirar la imagen y el diseño del primer Motorola y compararla con cualquier teléfono móvil de última generación que tengamos disponible en el mercado tecnológico actual.

Además de las funciones propias de cualquier teléfono convencional, los últimos y más avanzados modelos de telefonía móvil o mejor conocidos como teléfonos inteligentes o Smartphones, nos ofrecen infinidad de servicios y aplicaciones móviles.

Más que unos simples teléfonos, son auténticos ordenadores que funcionan con sistemas operativos específicos y optimizados según las condiciones de cada terminal, además de la propia antena emisora y receptora de señal. Los Smartphones de hoy en día vienen equipados con antenas de posicionamiento GPS, conectividad WiFi, capacidad para enviar y recibir archivos de manera inalámbrica en diferentes formatos, por medio de la tecnología Wifi, Bluetooth, cámaras integradas de gran calidad etc.

Imagen N° 46
Imagen de las diferentes generaciones de celulares atreves del tiempo



FUNCIONAMIENTO TELEFONÍA CELULAR

En esencia, un teléfono móvil es un receptor-transmisor que recibe y envía ondas electromagnéticas de radiofrecuencia; el terminal convierte las ondas sonoras de nuestra voz en ondas electromagnéticas, que viajan a través del aire, siendo recibidas y reenviadas hasta el destinatario del mensaje mediante una o más antenas repetidoras, y una vez alcanzan el teléfono del destinatario, son convertidas nuevamente en sonido para que este pueda escuchar el mensaje.

Al hacer una llamada, el teléfono móvil emite ondas de sonido que viajan a través del aire y son recibidas como señales electromagnéticas, mismas que se transforman por medio de antenas satelitales para recibirlas como sonidos inteligibles nuevamente, todo este proceso es posible gracias a la combinación de redes de estaciones receptoras y transmisoras de radio así como de centrales telefónicas de comunicación.

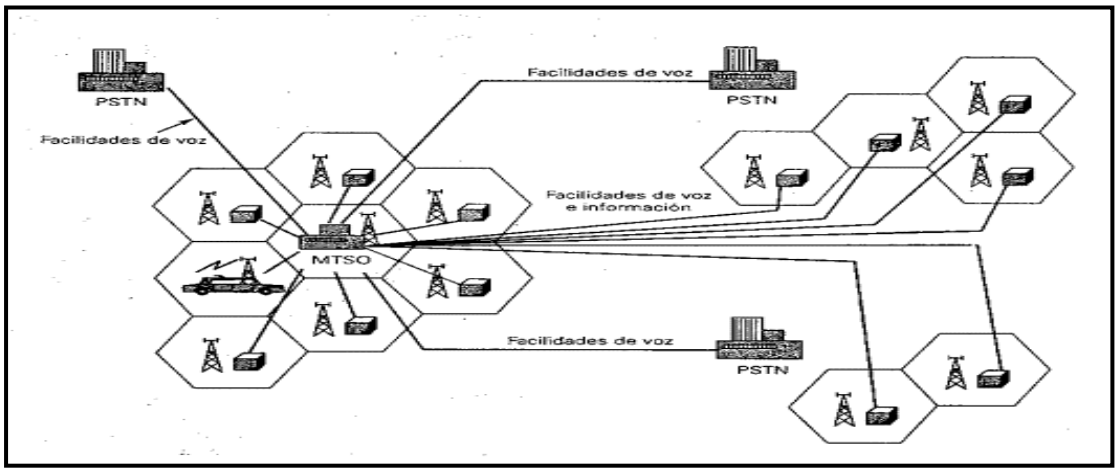
Los sistemas digitales usan estaciones bases dispuestas en celdas pequeñas conectadas en forma de red, cada estación se ubica en el centro recibiendo un número específico de transmisiones de su red.

Al momento de que un teléfono móvil sale de una celda la estación base transfiere la posesión a la celda que esté recibiendo la señal más potente, o sea, la celda donde se encuentra el teléfono.

Por esto es que cada ciudad necesita de al menos una oficina central que maneje todas las conexiones telefónicas y las estaciones de la región.

Los sistemas digitales usan celdas pequeñas que por sus dimensiones imposibilita que algún sistema aledaño use el mismo conjunto de frecuencias.

Imagen N° 47
Imagen de un sistema de comunicación celular



Cobertura Territorial: Red De Celdas

Para poder dar servicio a un territorio determinado sin que haya zonas fuera de cobertura, las redes inalámbricas operan dividiendo el terreno en cuadrículas llamadas celdas o células, en cada una de las que se instalan una o más antenas repetidoras; cada celda puede cubrir desde unas pocas manzanas de una ciudad densamente poblada hasta extensiones de 200 km^2; generalmente son de forma hexagonal, ya que esa figura geométrica permite cubrir una región geográfica con el menor número de celdas posible sin dejar áreas sin cobertura, permitiendo que la distancia entre las antenas de las celdas sea la misma en todo el territorio, evitando problemas de mala recepción de la señal.

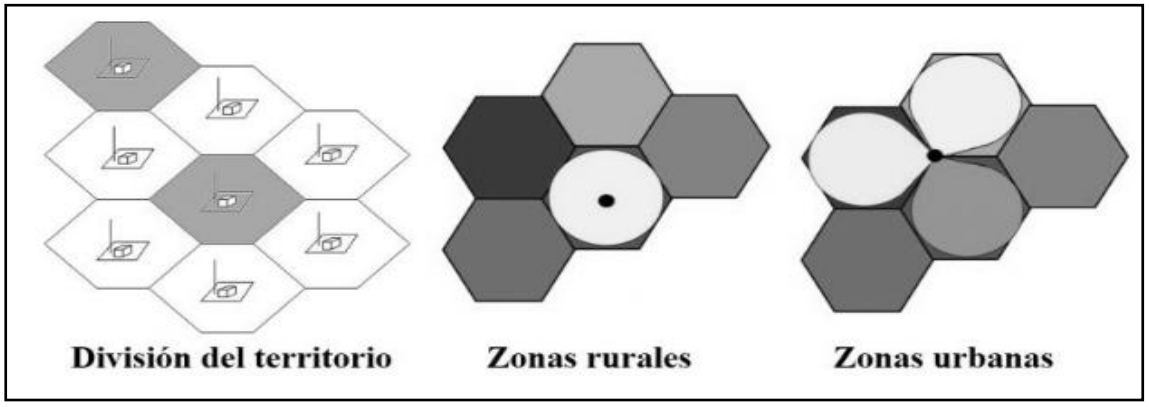
Cada celda utiliza un conjunto de frecuencias de radio para facilitar la comunicación en su área específica; el alcance de estas frecuencias se limita a la celda donde dan servicio y con objeto de evitar problemas de interferencia, una misma frecuencia puede ser usada simultáneamente en celdas cercanas pero no contiguas, a su vez, dentro de una celda cada frecuencia tiene lo que se conoce como un ancho de banda, lo que permite incluir dentro un elevado número de canales para que un gran número de usuarios puedan hablar sin interferirse entre ellos.

División de un territorio en celdas: La celda central opera a una frecuencia y cada una de las celdas contiguas trabaja a frecuencias cercanas, pero diferentes, hay una celda que vuelve a usar la misma frecuencia que la central.

A**éreas rurales**, las antenas son omnidireccionales y se sitúan en el centro de cada celda.

Áreas urbanas: con gran cantidad de usuarios potenciales, las antenas se suelen colocar en tres vértice no consecutivos de cada hexágono.

Imagen N° 48
Imagen de la división de celdas según su área de cobertura



EVOLUCIÓN DE LA TELEFONÍA CELULAR

A través del tiempo y debido al enorme avance de las comunicaciones y tecnologías, la telefonía celular fue evolucionando en el tiempo de forma vertiginosa alrededor del mundo, los servicios básicos de comunicación que en un principio brindaban, fueron mejorando sustancialmente en el tiempo, hasta llegar hoy en día a una de las tecnologías más usadas en la actualidad.

Esta evolución ha permitido no solo comunicarnos, si no poder compartir diferentes recursos multimediales entre diferentes personas, organizaciones y países alrededor del mundo, cambiando la forma de vida en algunos casos

Generaciones:

1-G: Móviles de Primera Generación

Surgidos a partir de 1973 y con un tamaño y peso inmanejable, los móviles de primera generación funcionaban de manera analógica, es decir que la transmisión y recepción de datos se apoyaba sobre un conjunto de ondas de radio que cambiaban de modo continuo.

El hecho de que fueran analógicos traía consigo una serie de inconvenientes, tales como que solo podían ser utilizados para la transmisión de voz (el uso de Mensajería instantánea era algo solo visible en un futuro muy lejano) o su baja seguridad, la cual hacia posible a una persona escuchar llamadas ajenas con un simple sintonizador de radio o, incluso hacer uso de las frecuencias cargando el importe de las llamadas a otras personas.

Estándares y características:

- Año - 1970 - 1980
- NMT: Nordic Mobile Telephone
- Estándares - AMPS (Advanced Mobile Phone System).
- Servicios - Sólo voz
- Tecnología - analógica
- Velocidad - 1kbps a 2,4 kbps
- Multiplexación - FDMA
- Conmutación - conmutación de circuitos
- Core Network – PSTN y Frecuencia - 800- 900

2-G: Segunda Generación

Al contrario de lo que pasa en otras generaciones, la denominada segunda generación no es un estándar concreto, sino que marca el paso de la telefonía analógica a la digital, que permitió, mediante la introducción de una serie de protocolos, la mejora del manejo de llamadas, más enlaces simultáneos en el mismo ancho de banda y la integración de otros servicios adicionales al de la voz, de entre los que destaca el Servicio de Mensajes Cortos

Estos protocolos fueron implementados por diversas compañías, siendo este hecho el origen de uno de los principales problemas de esta generación la incompatibilidad entre protocolos, debido a que el radio de utilización del teléfono quedaba limitado al área en el que su compañía le diera soporte.

Estándares y características:

- GSM: Global System for Mobile Communications - Sistema Global para Comunicaciones Móviles.
- CDMA (Code Division Multiple Access) : La multiplexación por división de código, acceso múltiple por división de código.
- GPRS: General Packet Radio Service - Servicio General de Radio por Paquetes
- Se basan en un ancho de banda de 9,6 kbps para datos y fax
- Los sistemas básicos usaron frecuencias de banda de 900MHz, mientras otros de 1800 y 1900MHz.
- Año - 1980 -1990
- Tecnología - Digital
- Velocidad - 14kbps a 64 Kbps

Imagen N° 49
Imagen del servicio brindado por la 2G

3-G: Tercera Generación

El objetivo de los sistemas 3G fue ofrecer aumento de las tasas de datos, facilitar el crecimiento, mayor capacidad de voz y datos, soporte a diversas aplicaciones y alta transmisión de datos a bajo coste, donde los datos se envían a través de la tecnología de una tecnología llamada Packet Switching, y las llamadas de voz se traducen mediante conmutación de circuitos.

Estándares y características:

- UMTS (WCDMA) basado en GSM (Global Systems for Mobile) infraestructura del sistema 2G, estandarizado por el 3GPP.
- CDMA 2000 basado en la tecnología CDMA (IS-95) estándar 2G, estandarizada por 3GPP2.
- Velocidad: 384KBPS 2Mbps y Frecuencia: aproximadamente 8 a 2,5 GHz
- Ancho de banda: de 5 a 20 MHz
- Tecnologías de multiplexación y acceso
- interfaz de radio llamada WCDMA (Wideband Code División Multiple Access)
- HSPA es un actualización de W-CDMA que ofrece velocidades de 14,4 Mbit / s de bajada y 5,76 Mbit / s de subida.
- HSPA + puede proporcionar velocidades de datos pico teóricas de hasta 168 Mbit / s de bajada y 22 Mbit / s de subida.
- CDMA2000 1X: Puede soportar tanto servicios de voz como de datos. La máxima velocidad de datos puede llegar a 153 kbps
- Servicios - telefonía móvil de voz, acceso a Internet de alta velocidad, acceso fijo inalámbrico a Internet, llamadas de video, chat y conferencias, televisión móvil, vídeo a la carta, servicios basados en la localización, telemedicina, navegación por Internet, correo electrónico, buscapersonas, fax y mapas de navegación, juegos, música móvil, servicios multimedia, como fotos digitales y películas. servicios localizados para acceder a las actualizaciones de tráfico y clima, servicios móviles de oficina, como la banca virtual.

4-G: Cuarta Generación

En telecomunicaciones, **4G** es la sigla utilizada para referirse a la cuarta generación de tecnologías de telefonía móvil, siendo la sucesora de las tecnologías 2G y 3G, y precede a la próxima generación, la 5G.

Es una tecnología basada por completo en IP (Internet Protocol) y está siendo desarrollada para mejorar el sistema de comunicaciones inalámbricas que se tiene en la actualidad, el cual es conocido como 3G.

La tecnología de redes 4G, fue creada por compañías de teléfonos celulares, con el principal objetivo de proporcionar soluciones completas a los usuarios de redes inalámbricas, las cuales han siendo desarrolladas para ofrecer un alto nivel de seguridad del protocolo IP.

Las redes 4G, tienen como característica principal una velocidad de transmisión de datos muy superior a la de las generaciones de redes inalámbricas anteriores, ofreciendo una mayor calidad de servicio y una recepción de datos superior a la actual tecnología 3G.

El principal uso que se le dará a esta tecnología de redes, es mejorar la comunicación entre los teléfonos celulares de todo el mundo, mejorando considerablemente la recepción y manteniendo una velocidad de transmisión de datos alta (100Mbps), aún si el usuario se encuentra en movimiento.

Otro uso que se le dará con mucha frecuencia a las redes 4G, es la ejecución de aplicaciones multimedia, ya que están pensadas para ofrecer el mejor soporte multimedia que se ha visto hasta la fecha; además, mejorarán las conexiones Wi-Fi y las conexiones inalámbricas entre ordenadores.

Estándares y características:

- Inicio - años de 2010. En 2008, la UIT-R especifica los requisitos para los sistemas 4G
- Estándares - Long-Term Evolution Time-Division Duplex (LTE-TDD y LTE-FDD) estándar WiMAX móvil (802.16m estandarizado por el IEEE)
- Velocidad - 100 Mbps en movimiento y 1 Gbps cuando se permanece inmóvil.
- Telefonía IP
- Nuevas frecuencias, ancho de banda de canal de frecuencia más amplia.

- Tecnologías de multiplexación / acceso - OFDM, MC-CDMA, CDMA y LAS-Red-LMDS
- Ancho de Banda - 5-20 MHz, opcionalmente hasta 40 MHz
- Bandas de frecuencia: - LTE cubre una gama de diferentes bandas. En América del Norte se utilizan 700, 750, 800, 850, 1900, 1700/2100 (AWS), 2300 (WCS) 2500 y 2600 MHz (bandas 2, 4, 5, 7, 12, 13, 17, 25, 26 , 30, 41); 2500 MHz en América del Sur; 700, 800, 900, 1800, 2600 MHz en Europa (bandas 3, 7, 20); 800, 1800 y 2600 MHz en Asia (bandas 1, 3, 5, 7, 8, 11, 13, 40) 1800 MHz y 2300 MHz en Australia y Nueva Zelanda (bandas 3, 40).
- Servicios - acceso móvil web, telefonía IP, servicios de juegos, TV móvil de alta definición, videoconferencia, televisión 3D, computación en la nube, gestión de flujos múltiples de difusión y movimientos rápidos de teléfonos móviles, Digital Video Broadcasting (DVB), acceso a información dinámica, dispositivos portátiles

5-G: Quinta Generación

La capa física y de enlace de datos define la tecnología inalámbrica 5G indicando que es una tecnología Open Wireless Architecture (OWA). Para realizar esto, la capa de red está subdividida en dos capas; capa de red superior para el terminal móvil y un menor nivel de red para la interfaz. Aquí todo el enrutamiento se basa en direcciones IP que serían diferentes en cada red IP en todo el mundo.

En la tecnología 5G la pérdida de velocidad de bits se supera mediante el Protocolo de Transporte Abierta (OTP). El OTP es soportado por Transporte y capa de sesión; la capa de aplicación es para la calidad de la gestión de servicio a través de varios tipos de redes. 5G adelanta un verdadero mundo inalámbrico Wireless-World Wide Web.

Estándares y características:

- Velocidad - 1 a 10 Gbps.
- Ancho de Banda - 1.000x ancho de banda por unidad de superficie.
- Frecuencia - 3 a 300 GHz
- Tecnologías de multiplexación / Access - CDMA y BDMA
- Estándares - banda ancha IP LAN / W AN / PAN & WWWW
- Características: rendimiento de tiempo real - de respuesta rápida, de baja fluctuación, latencia y retardo
- Muy alta velocidad de banda ancha - velocidades de datos Gigabit, cobertura de alta calidad, multi espectro
- Infraestructura virtualizada - Software de red definido, sistema de costes escalable y bajo.
- Soporta Internet de las Cosas y M2M - 100 veces más dispositivos conectados, Cobertura en interiores y eficiencia de señalización
- Reducción de alrededor del 90% en el consumo de energía a la red.
- Su tecnología de radio facilitará versión diferente de las tecnologías de radio para compartir el mismo espectro de manera eficiente.
- Servicios: - Algunas de las aplicaciones son importantes - personas y dispositivos conectados en cualquier lugar en cualquier momento.
- Su aplicación hará que el mundo real sea una zona Wi Fi.

- Dirección IP para móviles asignada de acuerdo con la red conectada y la posición geográfica.
- Señal de radio también a mayor altitud.
- Múltiples servicios paralelos, con los que se puede saber el tiempo meteorológico y la posición geográfica que se está situado.
- El diagnóstico remoto es una gran característica de 5G, debido a que un Médico puede tratar al paciente situado en la parte remota del mundo.
- El seguimiento será más fácil, una organización gubernamental y otros investigadores pueden monitorear cualquier parte del mundo.

PREGUNTAS SOBRE LA UNIDAD N°4:

1. ¿Cómo funciona el sistema GPRS?
2. ¿Cuáles son los componentes de las estaciones terraneas?
3. ¿Qué es la orbitas de un satélite?
4. ¿Cuáles son los tipos de orbita de un satélite por el centro?
5. ¿Cuáles son los tipos de orbita de un satélite por altitud?
6. ¿Cuáles son los tipos de orbita de un satélite por inclinación?
7. ¿Cuáles son los tipos de orbita de un satélite por sincronía?
8. ¿Quién es el creador de la telefonía celular?
9. ¿Quién es el pionero en las comunicaciones inalámbricas?
10. ¿Cómo es la la división territorial en las celdas una telefonía celular?
11. ¿Qué tipo de tecnología utilizaba la primera generación de celulares?
12. ¿Qué tipo de tecnología utilizaba la segunda generación de celulares?
13. ¿Qué tipo de tecnología utilizaba la tercera generación de celulares?
14. ¿Qué tipo de tecnología utilizaba la cuarta generación de celulares?
15. ¿Qué tipo de tecnología utilizaba la quinta generación de celulares?

RESULTADO DE LAS PREGUNTAS

RESPUESTAS SOBRE LA UNIDAD N°1:

1. Capa de red
2. Capa de enlace de datos
3. Norma 10 base 2
4. Norma 10 base 5
5. En capa (LLC) capa de enlace lógico y (MAC) control de acceso al medio
6. **CSMA/Detección de colisión (CSMA/CD),** aquí el dispositivo monitorea los medios para detectar la presencia de una señal de datos.
   En CSMA/Prevención de colisiones (CSMA/CA), el dispositivo examina los medios para detectar la presencia de una señal de datos.
7. 48 bits
8. 32 bits
9. Una dirección **IP fija o estática** es una IP la cual es asignada por el usuario, o bien dada por el proveedor ISP en la primera conexión.,
10. Una dirección **IP dinámica** es una dirección IP que el ISP o proveedor de Internet asigna dinámicamente al dispositivo que pretende tener acceso a Internet.
11. Las direcciones IP públicas son aquellas que permiten que cada dispositivo conectado a una red pueda ser identificado. Cuándo un dispositivo se conecta a internet se le asigna una dirección IP de las que disponga su proveedor de acceso
12. Son direcciones asignadas a dispositivos dentro de una red que no tiene visibilidad con Internet. Los dispositivos que tienen asignada una dirección privada no pueden acceder a Internet con su dirección y necesitan un dispositivo que les asigne una dirección pública.
13. 4 byte
14. 128 bits
15. 127.0.0.1
16. **Rango**: 1.0.0.0 hasta: 127.255.255.255
17. **Rango:** 128.0.0.0 hasta: 191.255.255.255
18. **Rango:** 192.0.0.0 hasta: 223.255.255.255
19. **Rango:** 224.0.0.0 hasta 239.255.255.255

20. **Rango:** 240.0.0.0 hasta: 255.255.255.255
21. Se utiliza únicamente para identificar una interface de un nodo IPv6.
22. Se utiliza para identificar a un grupo de interfaces IPv6.
23. Se asigna a múltiples interfaces (usualmente en múltiples nodos).
24. Automática
25. Hexadecimal

RESPUESTAS SOBRE LA UNIDAD N°2:

1. 185 metros
2. 500 metros
3. 100 metros
4. 2000 metros
5. 100 metros
6. 2000 metros
7. 100 metros
8. 550 metros
9. 5000 metros
10. Las redes de difusión tienen un solo canal de difusión compartido por todas las máquinas de la red.
11. La topología en bus tiene todos sus nodos conectados directamente a un cable central y lineal, donde físicamente cada dispositivo está conectado a un cable común, el cable o canal propaga las señales en ambas direcciones, de manera que todos los dispositivos puedan ver todas las señales de todos los demás dispositivos.
12. La topología en estrella se caracteriza por tener todos sus nodos conectados a un controlador central. Todas las transacciones pasan a través del nodo central, siendo éste el encargado de gestionar y controlar todas las comunicaciones
13. La topología en anillo se caracteriza por un camino unidireccional cerrado que conecta todos los nodos, dependiendo del control de acceso al medio, se dan nombres distintos a esta topología
14. En esta topología, de uso común en redes tipo WAN, todos los nodos de la red están interconectados entre sí, formando una malla de conexiones similar a una tela de araña.
15. Un protocolo enrutado permite que un Router envíe datos entre nodos de diferentes redes, trabaja en el nivel 3 utilizado para transferir información desde un dispositivo a otro a través de la red, es un datagrama que lleva información de la aplicación además de información de los niveles superiores.

16. Los protocolos de enrutamiento proporcionan información para elaborar las tablas de enrutamiento y además determinan la mejor ruta a través de la conexión entre redes que deben seguir los paquetes de datos desde la computadora transmisora hasta la computadora receptora .
17. Determina la dirección y la distancia hacia cualquier enlace de la red. Su métrica se basa en lo que se le llama en redes “Numero de Saltos”, es decir la cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino
18. También llamado “Primero la Ruta Libre Mas Corta” (OSPF – Open Shortest Path First), recrea la topología exacta de toda la red. Su métrica se basa el retardo ,ancho de banda , carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra.
19. Los protocolos de enrutamiento utilizan algoritmos ya sea estáticos o dinámicos según el caso para encaminar los paquetes de una máquina a otra.
20. El método más común para transferir información de enrutamiento entre routers ubicados en la misma red es el RIP. Este protocolo de gateway interior calcula las distancias hacia un destino. El RIP permite que los routers que usan este protocolo actualicen sus tablas de enrutamiento a intervalos programables, normalmente cada treinta segundos.

21. se desarrolló específicamente para ocuparse de los problemas relacionados con el enrutamiento en redes compuestas por productos de varios fabricantes, que no se podían manejar con protocolos como, por ejemplo, RIP. Como RIP, IGRP es un protocolo de vector de distancia, sin embargo, al determinar cuál es la mejor ruta también tiene en cuenta elementos como, por ejemplo, el ancho de banda, la carga, el retardo y la confiabilidad. Los administradores de red pueden determinar la importancia otorgada a cualquiera de estas métricas.
22. La métrica es el análisis, y en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta por sobre otra, basándose en eso el protocolo creará la tabla de enrutamiento en el router, publicando sólo las mejores rutas.

RESPUESTAS SOBRE LA UNIDAD N°3:

1. IEEE 802.15
2. IEEE 802.11
3. IEEE 802.16
4. IEEE 802.20
5. Ondas de radio, Microondas terrestres y Microondas por satélite
6. 10 metros
7. rango de 2.4 a 2.48Ghz
8. 2,4GHZ y 5GHz
9. WIMAX fija y WIMAX móvil
10. tecnologías 4G de banda ancha
11. la telefonía móvil y los satélites
12. SSID, Filtrado de direcciones MAC , WEP, WEP2, WPA Y WPA2
13. No autenticado y no asociado, Autenticado y no asociado y Autenticado y asociado
14. WEP combina claves de 64 o 128 bits
15. WEP2 combina claves de 128 bits
16. WAP combina claves de 128 bits
17. WAP combina claves de 128 bits
18. 48 bits por medio de la tarjeta de red

RESPUESTAS SOBRE LA UNIDAD N°4:

1. **GPRS:** determina la ubicación/posición de un objeto en el planeta, funciona a partir de una red de satélites artificiales, y de hecho, los sistemas de telecomunicaciones actuales que incluyen la televisión y los teléfonos celulares, funcionan gracias a satélites artificiales.
2. Estación receptora, antena y estación emisora
3. Una órbita es una trayectoria que describe, en relación a un sistema de referencia dado, el centro de gravedad de un satélite o de otro objeto espacial, por la acción principal de fuerzas naturales, en particular la de gravitación.
4. Órbita galactocéntrica, Órbita heliocéntrica y Órbita geocéntrica
5. Órbita baja terrestre (LEO), Órbita media terrestre (MEO) y Órbita alta terrestre (HEO)
6. Órbita inclinada, Órbita polar y Órbita polar heliosíncrona
7. Órbita síncrona, Órbita semisíncrona, Órbita geoestacionaria, Órbita cementerio, Órbita areosíncrona y Órbita areoestacionaria
8. Martin Cooper
9. Nikola Tesla
10. Aéreas rurales, División de un territorio en celdas y Áreas urbanas
11. Tecnología - analógica
12. Tecnología – inalámbrica
13. Tecnologías de multiplexación y acceso
14. Tecnologías de multiplexación / acceso - OFDM, MC-CDMA, CDMA y LAS-Red-LMDS
15. Tecnologías de multiplexación / Access - CDMA y BDMA

GLOSARIO DE TERMINOS

- **Bps:** bits por segundo.
- **Byte:** unidad de información utilizada por las computadoras. Cada byte está compuesto por ocho bits.
- **Cable coaxial:** es el tipo de cable usado por las compañías de televisión por cable para establecer la conexión entre la central emisora y el usuario. La compañía telefónica AT&T usó el cable coaxial para la primera conexión transcontinental en 1941. También se lo utiliza mucho en las conexiones de redes de área local (lan). Según el tipo de tecnología que se use, se lo puede reemplazar por fibra óptica.
- **Cable-módem:** módem que conecta una computadora con Internet a alta velocidad, por medio de una línea de TV por cable.
- **Clave pública y clave privada:** esquema de encriptación en el que cada persona tiene dos claves: la pública y la privada. Los mensajes se encriptan usando la clave pública del destinatario y sólo pueden ser descifrados usando su clave privada.
- **Cliente/servidor:** este término define la relación entre dos programas de computación en el cual uno, el cliente, solicita un servicio al otro, el servidor, que satisface el pedido.
- **CIFRADO**: Es la manipulación de datos para evitar que cualquiera de los usuarios a lo que no están dirigidos los datos puedan realizar una interpretación precisa.
- **DHCP**: (Protocolo de configuración dinámica de host) protocolo que permite a un dispositivo de una red, conocido como servidor dhcp, asignar direcciones ip.
- **E-mail:** correo electrónico.
- **Encriptar:** proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.
- **Enlace:** link.
- **Ethernet:** tecnología para red de área local. Fue desarrollada originalmente por Xerox y posteriormente por Xerox, DEC e Intel. Ha sido aceptada como estándar por la IEEE.

- **Explorer:** Microsoft Internet Explorer. Navegador de la empresa Microsoft que, a partir de Windows98, viene integrado al sistema operativo.
- **Extranet:** parte de una intranet de acceso disponible a clientes y otros usuarios ajenos a la compañía
- **Fibra óptica:** tecnología para transmitir información como pulsos luminosos a través de un conducto de fibra de vidrio. La fibra óptica transporta mucha más información que el cable de cobre convencional. La mayoría de las líneas de larga distancia de las compañías telefónicas utilizan la fibra óptica.
- **FTP:** File Transfer Protocol: Protocolo de Transferencia de Archivos. Sirve para enviar y recibir archivos de Internet.
- **Gateway:** puerta; acceso; pasarela. Punto de enlace entre dos sistemas de redes.
- **Gusano:** programa que se copia a sí mismo hasta ocupar toda la memoria. Es un virus que suele llegar a través del correo electrónico, en forma de archivo adjunto.
- **Hipertexto:** textos enlazados entre sí. Haciendo clic con el mouse el usuario pasa de un texto a otro, vinculado con el anterior.
- **Hipervínculo:** link
- **Hosting:** alojamiento. Servicio ofrecido por algunos proveedores, que brindan a sus clientes (individuos o empresas) un espacio en su servidor para alojar un sitio web.
- **HTML:** Hyper Text Mark-up Language. Lenguaje de programación para armar páginas web.
- **HTTP:** Hypertext Transfer Protocol. Protocolo de transferencia de hipertextos. Es un protocolo que permite transferir información en archivos de texto, gráficos, de video, de audio y otros recursos multimedia.
- **Internet:** red de redes. Sistema mundial de redes de computadoras interconectadas. Fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Se la llamó primero ARPAnet y fue pensada para cumplir

funciones de investigación. Su uso se popularizó a partir de la creación de la WorldWideWeb. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

- **Intranet: r**ed de redes de una empresa. Su aspecto es similar al de las páginas de Internet.
- **IP:** Protocolo de Internet. ISO: International Organization for Standardization. Fundada en 1946, es una federación internacional que unifica normas en unos cien países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de comunicación.
- **ISP:** Internet Service Provider. Proveedor de servicios de Internet.
- **Jitter:** variación en la cantidad de latencia entre paquetes de datos recibidos.
- **Kilobit:** 1.024 bits.
- **Kilobyte (KB):** unidad de medida de una memoria. l kilobyte = 1024 bytes.
- **LAN Manager:** sistema operativo de red.
- **LAN:** Local Area Network: Red de Área Local. Red de computadoras interconectadas en un área reducida, por ejemplo, una empresa.
- **MB:** megabyte.
- **Megabit:** Aproximadamente 1 millón de bits. (1.048.576 bits).
- **Megabyte (MB):** unidad de medida de una memoria. 1 megabyte = 1024 kilobytes = 1.048.576 bytes.
- **Módem:** modulador-demodulador. Dispositivo periférico que conecta la computadora a la línea telefónica.
- **Navegador:** programa para recorrer la World Wide Web. Algunos de los más conocidos son: Google Chrome, Microsoft Explorer, Opera y Mozilla.
- **Net:** WorldWideWeb.
- **Netiquette:** conjunto de reglas de etiqueta tácitas dentro de Internet.
- **Newsgroup:** grupo de discusión sobre determinado tema, en Internet u otras redes.

- **Online:** en línea, conectado. Estado en que se encuentra una computadora cuando se conecta directamente con la red a través de un dispositivo, por ejemplo, un módem.
- **Outbox:** buzón de salida.
- **Página web:** una de las páginas que componen un sitio de la WorldWideWeb. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".
- **Paquete (packet):** la parte de un mensaje que se transmite por una red. Antes de ser enviada a través de Internet, la información se divide en paquetes.
- **Password:** contraseña.
- **Placa Ethernet:** placa que se inserta en una computadora para conectarla en red con otras a través de un cable.
- **PoP:** Punto de acceso a Internet.
- **POP3** (**Post Office Protocol 3):** Protocolo 3 de Correo. Es un protocolo estándar para recibir e-mail.
- **Portal:** sitio web que sirve de punto de partida para navegar por Internet. Los portales ofrecen una gran diversidad de servicios: listado de sitios web, buscador, noticias, e-mail, información meteorológica, chat, newsgroups (grupos de discusión) y comercio electrónico. En muchos casos el usuario puede personalizar la presentación del portal. Algunos de los más conocidos son Altavista, Yahoo!, Netscape y Microsoft.
- **Protocolo:** lenguaje que utilizan dos computadoras para comunicarse entre sí.
- **Proveedor de servicios de Internet:** compañía que ofrece una conexión a Internet, e-mails y otros servicios relacionados, tales como la construcción y el hosting de páginas web.
- **Puerto:** en una computadora, es el lugar específico de conexión con otro dispositivo, generalmente mediante un enchufe. Puede tratarse de un puerto serial o de un puerto paralelo.
- **PROXY:** Software que permite a varios ordenadores acceder a Internet a través de una única conexión física. Según lo avanzado que sea, puede permitir acceder a páginas Web, FTP, correo electrónico, etc.

- **Red:** en tecnología de la información, una red es un conjunto de dos o más computadoras interconectadas.
- **RED CLIENTE/SERVIDOR:** es en la que se distingue entre las computadoras que ponen a disposición los recursos de la red (los servidores) y aquellas que utilizan los recursos (los clientes o las estaciones de trabajo).
- **Red de área local:** LAN
- **Router:** ruteador. Sistema constituido por hardware y software para la transmisión de datos en Internet. El emisor y el receptor deben utilizar el mismo protocolo.
- **Servidor:** computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas.
- **Sistema operativo:** programa que administra los demás programas en una computadora.
- **SWITCHES:** como su nombre lo indica, pueden conmutar conexiones de un puerto a otro y lo pueden hacer de manera muy rápida. Están orientados a la conexión y, de forma dinámica, conmutan entre sus diferentes puertos para crear estas conexiones.
- **SMTP:** Simple Mail Transfer Protocol. Es un protocolo estándar para enviar email. Software: término general que designa los diversos tipos de programas usados en computación.
- **Spam:** correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a Internet.
- **Socket:** (soporte) conector eléctrico, toma de corriente, enchufe. / Un socket es el punto final de una conexión. / Método de comunicación entre un programa cliente y un programa servidor en una red (véase cliente/servidor).
- **TCP/IP:** Transfer Control Protocol / Internet Protocol. Es el protocolo que se utiliza en Internet.
- **Telemática:** combinación de las palabras "telecomunicaciones" e "informática". Disciplina que asocia las telecomunicaciones con los recursos de la informática.

- **TOPOLOGIA:** Configuración formada por las conexiones entre los dispositivos de una red.
- **WAP (Wireless Application Protocol):** norma internacional para aplicaciones que utilizan la comunicación inalámbrica, por ejemplo el acceso a Internet desde un teléfono celular.
- **WAN:** es simplemente la conexión de varias redes de área local (LAN) entre sí. Este mega sistema puede construirse de muchas formas en función de la frecuencia con que sea necesario conectar las LAN entres si, cuanta capacidad de datos (ancho de banda) se requiere y cuál es la distancia entre las LAN.
- **Web page:** página web.
- **Web site:** sitio web.
- **Web:** World Wide Web.
- **Webmail:** servicio que ofrecen ciertos sitios web para crear una cuenta gratuita de e-mail. Mediante el webmail el correo electrónico se revisa con el navegador. Se puede acceder a él desde cualquier computadora situada en cualquier lugar.
- **Webmaster:** persona responsable de la creación, administración, programación y control técnico de un sitio web.
- **Wireless:** inalámbrico.
- **World Wide Web:** red mundial; telaraña mundial. Es la parte multimedia de Internet. Es decir, los recursos creados en HTML y sus derivados. Sistema de información global desarrollado en 1990 por Robert Cailliau y Tim Berners-Lee en el CERN (Consejo Europeo para la Investigación Nuclear). Con la incorporación de recursos gráficos e hipertextos, fue la base para la explosiva popularización de Internet a partir de 1993.

BIBLIOGRAFÍA:

- Pérez Alcalá, María Del Socorro; Ortiz Ortiz, María Gloria; Flores Briseño, María Mirna. Redes sociales en Educación y propuestas metodológicas para su estudio. vol. 26, núm. 50, mayo, 2015. ISSN: 0327-5566
- Calzadilla, María Eugenia: Aprendizaje colaborativo y tecnologías-OEI-Revista Iberoamericana de Educación 10 JONHSON, y JONHSON (1992). (ISSN: 1681-5653)
- Arboleda, T.N. (2008). Modelo Integral para el aseguramiento de la calidad en educación superior virtual y a distancia. En La educación a distancia en el ámbito de la educación superior. Las nuevas tecnologías de información y comunicación (TIC´S) (pp. 23-51) Argentina. Editorial Croquis S.R.L
- Orihuela, J. L. (2008): Internet: la hora de las redes sociales. Nueva revista, 119, 57-62.
- Parra Castrillón, E. (2010). Las redes sociales de Internet: también dentro de los hábitos de los estudiantes universitarios. Anagramas, 9 (17), 107-116. Medellín.
- De Haro, J.J. (2010). Las redes sociales en educación. Recuperado de http://jjdeharo.blogspot.com.es/2008/11/la-redes-sociales-en educacin.html.
- Herrera Echeverri, H. (2009). Investigación sobre redes sociales y emprendimiento: revisión de la literatura y agenda futura. Innovar, 19 (33), 19-33.
- Koper, R. (Ed.) (2009). Learning Network Services for Professional Development. Berlin: Heidelberg: Springer. Lampe, C., Ellison, N. y Steinfield, C. (2006). A Facein the crowd: Social searching vs. social browsing. Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work, 167–170. New York: ACM
- Tanenbaum andrew s- año 2003- redes de ordenadores - méxico - ISBN: 970-26-0162-2.- editorial pearson educación- 4 edición- página 912
- Academia de networking de cisco systems- fundamento de las redes inalàmbricas - madrid - pearson educación -página 820

- Academia de networking de cisco systems, ccna 1 y 2,año 2004- tercera edición- madrid - pearson educación --página 1008
- Academia de networking de cisco systems, ccna 3 y 4, tercera edición- año 2004- Madrid - pearson educación- página 1010
- Ernesto ariganelo- año 2013 -redes cisco- guía de estudio para la certificación ccna security - mexico - ISBN 978-84-9964214-7 - alfaomega grupo editor -página 400
- Antonio perpinan - año 2004 -administración de es gnu/linux- ISBN 88-9 9 9 9 9 -9 9 -9- santo dom ingo-república dominicana- impresos gamm a- páginas 450 Enzo augusto marchionni -año 2011- administrador de servidores: instalación y virtualización- buenos aires- ISBN: 978-987177-319-0 - editorial users páginas: 352
- Marchionni, enzo augusto- administrador de servidores: herramientas y consejos para a la actividad diaria -buenos airesISBN: 978-987-1773-19-0 -editorial users páginas: 352
- DE HARO, J. (2010). *Redes sociales en educación*. Barcelona: Colegio Amor de Dios. Disponible en: http://jjdeharo.blogspot.com.ar/2010/05/redes-socialesen-educacion.html [24 de mayo 2014]
- STATISTA (2015). Leading social networks worldwide as of January 2015, ranked by number of active users (in millions). Disponible en: http://www.statista.com/statistics/272014/global-social-networksranked-by-number-of-users/. 9 de marzo del 2015
- ABUIN, N. (2009). Las redes sociales como herramienta educativa en el ámbito universitario. Disponible en: < http:// moodle.upm.es/adamadrid/file.php/1/web_ IV_jornadas_ADA/comunicaciones/30_ Abuin.pdf > [15 de mayo de 2014].
- FERNÁNDEZ, I. (2012). Potencialidad educativa de las redes sociales, en: Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 8 (1). Disponible en: http://www.ride.org.mx/pdf/globalizacion/02_ globalizacion.pdf .7 de mayo de 2014.