Apuntes de la Asignaturas de

Redes de Datos I
Y
Redes de Datos II

Ing. Ma. Eugenia Macías Ríos
Ayte. Edwin Rentería Anguiano
Departamento de Ingeniería en Computación

Dr. Victor Rangel Licea
Depto. Ing. en Telecomunicaciones

Facultad de Ingeniería
Universidad Nacional Autónoma de México

Octubre de 2009

AGRADECIMIENTOS

ESTE MATERIAL FUE ELABORADO CON EL APOYO DEL PROYECTO PAPIME PE103807: INTEGRACIÓN DE NUEVAS TÉCNOLOGIAS Y ELABORACIÓN DE MATERIAL DIDÁCTICO PAR UN LABORATORIO MULTIDISCIPLINARIO DE REDES DE LA FACULTAD DE INGENIERIA 2007-2010

SE AGRADECE EL APOYO DE LA DGAPA-UNAM POR LOS RECUROS PROPORCIONADOS PARA LA ELABORACION DE ESTE MATERIAL.

 © DGAPA-PAPIME

APUNTES DE REDES DE DATOS I Y II

Contenido

 © DGAPA-PAPIME

 © DGAPA-PAPIME

 © DGAPA-PAPIME

1. Conceptos básicos

1.1 Redes de comunicaciones de datos. Panorama general

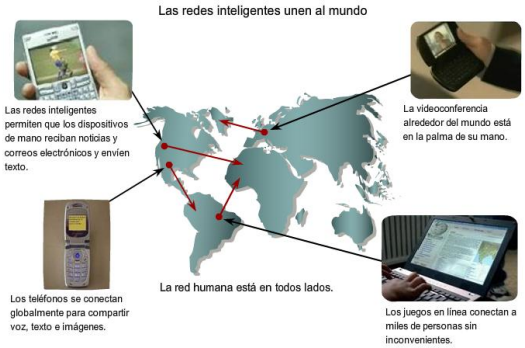
Han pasado muchos avances tecnológicos. Entre los acontecimientos vimos la instalación de redes de telefonía, el radio, la televisión y el crecimiento de la industria de la computadora, así como el avance de las comunicaciones.

Para los humanos la comunicación es casi tan importante como el aire, el agua, los alimentos y un lugar para vivir. Los métodos que utilizamos para compartir ideas e información están en constante cambio y evolución, desde las conversaciones cara a cara, hasta las comunicaciones satelitales; el avance de los medios ha extendido el alcance de las comunicaciones.

Con cada avance en la tecnología de comunicación, la creación e interconexión de redes de datos sólidas tiene un profundo efecto en la humanidad.

Las redes de datos actuales evolucionaron para agregarle voz y flujos de video, a los diferentes tipos de dispositivos. Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común: Internet.

La manera en que se producen las interacciones comerciales, sociales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. En la siguiente etapa de nuestro desarrollo, los innovadores verán a Internet como punto de inicio para sus esfuerzos, creando nuevos productos y servicios diseñados específicamente para aprovechar los recursos de la red. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman parte de nuestra vida cotidiana tendrán una función cada vez más importante en el desarrollo de la humanidad.



Conceptos básicos

La ***comunicación*** en nuestra vida cotidiana tiene diferentes formas y existe en muchos entornos. Tenemos diferentes expectativas según si estamos conversando por Internet o participando de una entrevista de trabajo. Cada situación tiene su comportamiento y estilo correspondiente.

Antes de comenzar a comunicarnos, establecemos reglas o acuerdos que rigen la conversación. Estas reglas o protocolos deben respetarse para que el mensaje se envíe y comprenda correctamente. Algunos de los protocolos que rigen con éxito las comunicaciones humanas son:

- Emisor y receptor identificados,
- Método de comunicación consensuado (cara a cara, teléfono, carta, fotografía),
- Idioma y gramática comunes,
- Velocidad y puntualidad en la entrega, y
- Requisitos de confirmación o acuse de recibo.

La comunicación es exitosa cuando el mensaje deseado se ha recibido y confirmado.

Las reglas de comunicación pueden variar según el contexto. Si un mensaje transmite un hecho o concepto importante, se necesita una confirmación de que el mensaje se recibió y comprendió correctamente. Los mensajes menos importantes pueden no requerir acuse de recibo por parte del receptor.

Las técnicas utilizadas en las comunicaciones de red comparten estos fundamentos con las conversaciones humanas. Para las redes de datos, utilizamos los mismos criterios básicos que para juzgar el éxito.

Los ***datos*** se refieren a hechos, conceptos e instrucciones presentados en cualquier formato acordado entre las partes que crean y utilizan dichos datos. En los sistemas de información basados en computadoras, los datos se representan como unidades de información binaria (o bits) producidos y consumidos en forma de ceros y unos.

La ***transmisión de datos*** es el intercambio de datos entre dos dispositivos a través de alguna forma de medio de transmisión.

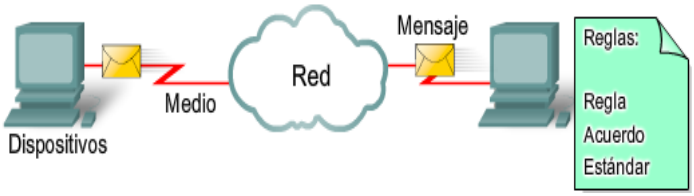
Podemos definir a las ***redes de computadoras*** como un conjunto de dispositivos conectados entre sí mediante uno o más medios de transmisión a fin de llevar a cabo la transferencia eficiente y confiable de información.

© DGAPA-PAPIME

Los ***elementos de una red*** son:

- Reglas
- Medios
- Mensajes
- Dispositivos

Los elementos de una red típica, incluyen dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar mensajes*.*



1.2 Beneficios de las redes locales. Usadas y aplicaciones

Uno de los principales beneficios de las redes locales es precisamente compartir recursos y dispositivos.

Cuando se comparten recursos se hace que los programas, el equipo y en particular los datos estén disponibles para todos los que se conecten a la red local. Un ejemplo muy claro puede ser cuando compartimos la misma impresora en la oficina para varios usuarios, el uso de un equipo especial para almacenar respaldos, registros de clientes, inventarios, información de impuestos, etc.

1.3 Topologías Importantes consideraciones de diseño

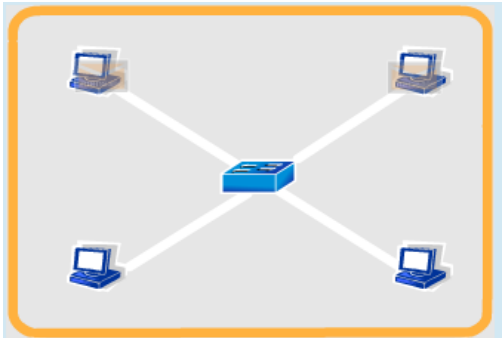
El término topología se refiere a la forma en la que está diseñada la red, esto es, tanto físicamente o lógicamente. Dos o más dispositivos se conectan a un enlace; dos o más enlaces forman una topología.

La topología de una red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente llamados nodos).

Hay cinco posibles topologías físicas básicas: malla, estrella, anillo, árbol y bus además existe la posibilidad de combinarlas lo que se conoce como topología hibrida. Estas cinco clases describen cómo están interconectados los dispositivos de una red, lo que no indica su posición física.

1.3.1 Estrella

La propiedad más importante de la topología de estrella es que cada estación se enlaza en forma radial a un nodo central a través de una conexión directa de punto a punto. En la configuración de estrella, una transmisión de una estación entra al nodo central, de donde se retransmite a todos los enlaces de salida. Por consiguiente, aunque el arreglo físico del circuito se asemeje a una estrella, se configura lógicamente como un bus, es decir, las transmisiones desde cualquiera de las estaciones las reciben todas las demás estaciones.

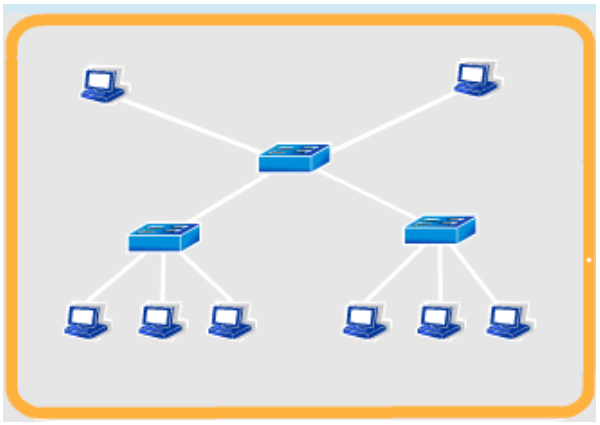


Ventajas	Desventajas
• Sí este tipo de red falla, solamente el enlace con problemas se verá afectado. Todos los demás enlaces permanecen activos. • Este tipo de topología es más barata, ya que cada dispositivo necesita solamente un enlace y un puerto de entrada/salida para conectarse a cualquier número de dispositivos.	• La red sólo es tan confinable como el nodo central. Cuando falla el nodo central, falla el sistema. • Cuando es crítica la falla de cualquier entidad dentro de la red, hasta el grado de interrumpir el servicio de toda la red, a esa entidad se le llama recurso crítico. Así, el nodo central en una configuración de estrella es un recurso crítico.

1.3.2 Árbol

Una topología árbol es una configuración jerárquica. 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.

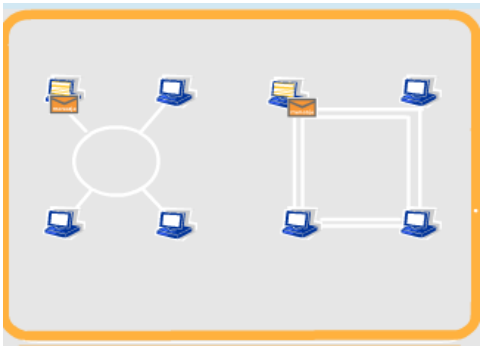
© DGAPA-PAPIME



Ventajas	Desventajas
• Permite que se conecten más dispositivos a un único concentrador central. • Incrementar la distancia que puede viajar la señal entre dos dispositivos. • Permite aislar y priorizar las comunicaciones de distintas computadoras.	• La red sólo es tan confiable como el nodo central. Cuando falla el nodo central, falla el sistema.

1.3.3 Anillo

En la topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor. Cuando un dispositivo recibe una señal para otro dispositivo, su repetidor regenera los bits y los retransmite al anillo.



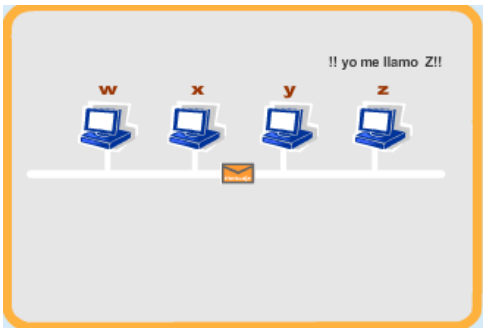
Ventajas	Desventajas
• Es relativamente fácil de instalar y reconfigurar una topología en anillo. • Para añadir o quitar dispositivos, solamente hay que mover dos conexiones. • Las fallas se pueden aislar de forma sencilla.	• El tráfico unidireccional puede ser una desventaja. En anillos sencillos, una rotura del anillo (como por ejemplo una estación inactiva) puede inhabilitar toda la red. Esta debilidad se puede resolver usando un anillo dual o un conmutador capaz de puentear la rotura.

© DGAPA-PAPIME

1.3.4 Bus

Una topología bus es una topología de difusión. En esta topología todos los nodos están conectados al mismo canal.

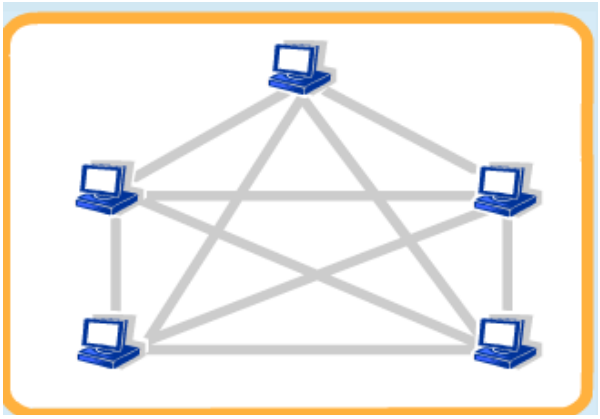
Es necesario conectar terminadores a cada extremo de la topología para absorber las señales que se reflejen. Si se usa cable coaxial sin terminadores, las señales que se reflejen se repetirán por la red, dejando la red inutilizable. La propiedad más característica de una topología bus es que el control se distribuye entre todos los nodos interconectados



Ventajas	Desventajas
• El coste y la facilidad de instalación. Dado que esta topología utiliza una distribución de cableado sencilla, cuesta menos y es más fácil de implementar que otras topologías.	• Si un segmento de cable o de backbone se rompe o falla, la red también fallará. • Sólo un nodo puede transmitir datos a la vez. Si dos o más nodos tratan de enviar datos al mismo tiempo, se producirá una colisión; esto requerirá un procedimiento de recuperación, con lo que se alentará la red. • Cuando se produce una colisión, todos los datos deben ser reenviados. Un proceso llamado acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) impide que se produzca otra colisión. CSMA/CD es un proceso en virtud del cual cada nodo espera su turno para transmitir datos.

1.3.5 Malla

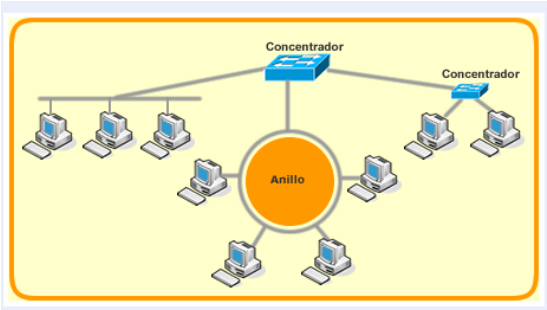
En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta. Por tanto, una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos.



Ventajas	Desventajas
• El uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos • Una topología en malla es robusta. Si un enlace falla, no inhabilita todo el sistema. • Otra ventaja es la privacidad o la seguridad. Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado.	• La cantidad de cable y el número de puertos de entrada/salida necesarios. • La instalación y reconfiguración de la red es difícil, debido a que cada dispositivo debe estar conectado a cualquier otro. • La masa de cables puede ser mayor que el espacio disponible para acomodarla (en paredes, techos o suelos). • Finalmente, el hardware necesario para conectar cada enlace (puertos de E/S y cables) puede ser extremadamente caro. • Por tanto, el mantenimiento de la red puede ser muy complejo.

1.3.6 Hibridas

A menudo, una red combina varias topologías mediante subredes enlazadas entre sí para formar una topología mayor. Por ejemplo, un departamento de una empresa puede decidir usar una topología de bus mientras otro puede tener un anillo. Ambas pueden ser conectadas entre sí a través de un controlador central mediante una topología en estrella.



1.4 Evolución de las redes de datos. Principales características: cobertura geográfica, velocidad, control de errores, enlaces, etc.

Las redes de computadoras no son el único tipo de redes que los humanos han creado. Es posible que el ejemplo más antiguo de una red que haya abarcado grandes territorios y ofrecido servicios a múltiples clientes haya sido el sistema de suministro de agua en la antigua

Roma. Pero, sin importar que tan diferentes o diversas puedan ser las redes, todas tienen algo en común: todas ofrecen algún servicio para diferentes tipos de clientes.

Las redes de computadoras, también conocidas como redes de comunicación de datos o de transmisión de datos, representan el resultado lógico de la evolución de dos de las ramas científicas y tecnologías más importantes de la civilización moderna: las tecnologías de las computadoras y de las telecomunicaciones.

Clasificación de redes por cobertura geográfica.

Distancia entre procesadores	Ubicados en el mismo	Red
1m	m^2	Red de área personal
10m	Habitación-laboratorio	Red de área local (LAN)
100m	Edificio	LAN
1km	Campus	LAN
10km	Cuidad	MAN
100km	País	MAN
1000 km	Continente	Red de área amplia WAN
10000 km	Planeta	Red de área global GAN

Clasificación de redes por cobertura geográfica.

1.4.1 PAN´s

Las PAN (Personal Area Networks o redes de área personal) están destinadas para comunicaciones entre dispositivos pertenecientes a un solo propietario a través de distancias pequeñas, por lo regular de 10 metros. Ejemplos de dispositivos de esta clase son computadoras portátiles, teléfonos móviles, impresoras, asistentes personales (PDA), equipos de televisión y numerosos aparatos domésticos de alta tecnología, como refrigeradores.

1.4.2 LAN´s

Las infraestructuras de red pueden variar en gran medida en términos de:

- el tamaño del área cubierta,
- la cantidad de usuarios conectados, y
- la cantidad y tipos de servicios disponibles.

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

1.4.3 MAN´s

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos

de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP.

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

La MAN es una red cuyo diámetro no va más allá de 50 km, y responde claramente a la necesidad de un sistema de comunicación de tamaño intermedio con beneficios que superan a los que pueden ofrecer las redes LAN o WAN.

1.4.4 GAN´s

La Red GAN (Red de Área Global) permite la conexión de una o varias LAN pertenecientes a diferentes países. GAN es un servicio de comunicación móvil que ofrece datos, voz y fax de alta calidad a velocidades de hasta 64 kbps. Los usuarios pueden elegir el servicio ISDN móvil de GAN (Red Digital de Servicio Integrado) para la transferencia rápida de grandes archivos de datos o el servicio móvil de datos por paquete (Mobil Packet Data Service) para aplicaciones de datos de uso variable como es el acceso a Internet y a correo electrónico. GAN también ofrece comunicaciones por voz con calidad de difusión.

1.4.5 WAN´s

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP (proveedor de servicios de telecomunicaciones).

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

© DGAPA-PAPIME

2. Estándares y arquitecturas

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

Un estándar es un proceso o protocolo que ha sido certificado por los especialistas de las redes y ratificado por una organización de estándares. El uso de estándares en el desarrollo y la aplicación de protocolos aseguran que los productos de diversos fabricantes puedan funcionar en conjunto para lograr comunicaciones satisfactorias. Por ejemplo si un protocolo no es observado estrictamente por un fabricante en particular, probablemente sus equipos o aplicaciones software no podrán establecer la comunicación de manera con productos hechos por otros fabricantes**.**

2.1.1 ISO

ISO es la Organización Internacional para la Estandarización surge después de la segunda guerra mundial, y este organismo se encarga de promover el desarrollo de las normas de fabricación internacionalmente, además promueve el comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

Su objetivo principal es la búsqueda de la estandarización de normas de productos y seguridad para las organizaciones a nivel internacional. La ISO se conforma de institutos de normas nacionales de diferentes países, 146 en total, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema.

La Organización Internacional de Normalización, es compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental. Es importante decir que las normas desarrolladas son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país.

2.1.2 ITU

La ITU es la organización más sobresaliente e importante de las Naciones Unidas enel ámbito de las tecnologías de la información y la comunicación. Tiene su sede en Ginebra, Suiza y está conformad por 191 estados miembros y más de 700 Miembros de Sector y Asociados. Como coordinador mundial de gobiernos y sector privado, sus funciones principales son enfocados en tres sectores: radiocomunicaciones, desarrollo y normalización. La ITU organiza eventos TELECOM.

2.1.3 IEEE

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), es la mayor sociedad mundial profesional de ingeniería. Sus objetivos son el desarrollo, la creatividad y la calidad de los productos en el campo de la ingeniería eléctrica, la electrónica y la radio. Uno de sus objetivos principales es impulsar el desarrollo y la adopción de estándares internacionales para la

© DGAPA-PAPIME

computación y comunicación. Su misión es Fomentar el conocimiento y los avances científicos y tecnológicos, los cuales, la membrecía del IEEE transforma en productos, y en procedimientos que favorecen la calidad de la vida

El IEEE atiende a más de 367,395cientificos, ingenieros, estudiantes de ingeniería, y diversos profesionistas en más de 150 países, divididos en:

- 10 Regiones
- 17 Consejos
- 382 Capítulos Técnicos de Ramas Estudiantiles
- 60 Grupos Afines de Ramas Estudiantiles
- 217 Grupos Afines
- 311 Secciones
- 34 Sub-secciones
- 1,570 Capítulos Técnicos
- 1,434 Ramas Estudiantiles

2.1.4 ANSI

El Instituto Nacional Americano para la Estandarización (ANSI) es una corporación en su totalidad privada pero sin ánimo de lucro la cual no tiene ninguna relación con el gobierno de los Estados Unidos, y sus ciudadanos tienen una importancia primordial.

Los objetivos fundamentales por ANSI incluyen servir como una institución de coordinación nacional para la estandarización voluntaria dentro de los Estados Unidos.

Los integrantes de ANSI son en su mayoría sociedades profesionales, asociaciones de la industria, agencias gubernamentales y reguladoras y grupos de consumidores. Éntre los tópicos actuales de discusión incluyen planificación e ingeniería de interconexión de redes; servicios, señalización y arquitecturas RDSI; y jerarquía óptica (SONET).

2.1.5 NOM

Norma Oficial Mexicana (NOM) es una regulación técnica de observancia de carácter obligatorio expedida por dependencias normalizadoras competentes a través de sus respectivos Comités Consultivos Nacionales de Normalización, de conformidad con las finalidades establecidas en el artículo 40 de la Ley Federal.

La NOM establece tanto reglas, especificaciones, atributos, directrices, características como prescripciones aplicables a un producto, proceso, instalación, sistema, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado.
Una NOM tiene el mismo poder que una ley. Es por esto que la mayor parte de las leyes mexicanas incluyen varias NOM, algunas leyes incluyen varias de ellas. Cada una de las NOM observa y atiende a un tipo en particular de actividades. En el caso específico de las NOM relativas a productos, describen todos los reglamentos que son obligatorios en cuanto a su uso, manejo, descripción, mantenimiento y garantía, a fin de poder venderse en el mercado mexicano.

2.1.6 EIA

© DGAPA-PAPIME

La asociación de Industrias Electrónicas (EIA) es una organización dedicada a la promoción de aspectos de la fabricación electrónica sin ánimos de lucro.

Su objetivo es despertar el interés de la educación y hacer esfuerzos para el desarrollo de los estándares. Además en el campo de la tecnología de la información, ha hecho contribuciones significativas mediante la definición de interfaces de conexión física y de especificaciones de señalización eléctrica para la comunicación de datos. En particular, el EIA-232-D, EIA-449 y EIA-530, en donde se establece la transmisión serie entre dos dispositivos digitales.

2.1.7 EL FORUM ATM.

El foro ATM es una organización de carácter internacional, la cual promueve el desarrollo y empleo de productos y servicios para ATM, acelerando la emisión de estándares.

ATM cuenta con más de 400 miembros activos, con representantes de la industria de telecomunicación, fabricantes de semiconductores ordenadores, así mismo operadores de redes, etc. Trabaja en estrecha cooperación con otros organismos oficiales de normalización como ITU-T, ISO/IEC, ANSI, ETSI

Entre sus trabajos más importantes son los relativos a las especificaciones UNI (User Network Interface) tanto público como privado. Su misión es desarrollar normas por medio de los diversos estándares de la industria, y con la contribución de los órganos del foro, crear especificaciones sobre la manera de construir, crear y ofrecer programas de educación para capacitar a la industria.

2.2 Modelo de referencia: OSI

En las redes existen dos tipos de modelos, los modelos de referencia y los de referencia.

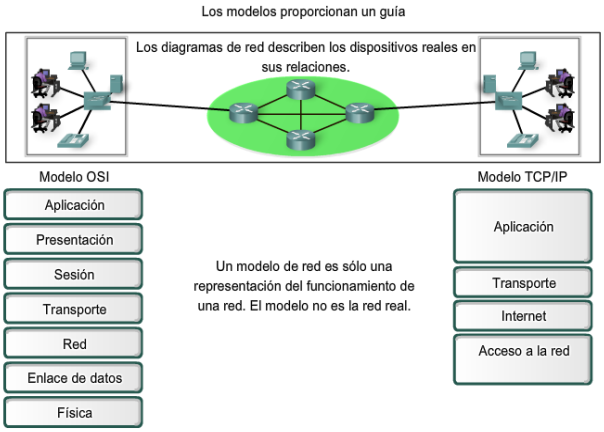
Los modelos de protocolo proporcionan un modelo que representa con exactitud la estructura de una suite de protocolo en particular. Un modelo de referencia da una referencia común para mantener coherencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia más usado y por ende mas conocido y se utiliza para diseñar redes de datos, especificaciones de funcionamiento y resolución de problemas.OSI fue aprobado por ISO (International Standards Organization) en el año 1984, bajo la norma ISO 7498.

Existen siete capas en el modelo de referencia OSI: aplicación, presentación, sesión, transporte, red, enlace de datos, física. Y cada una de las cuales proporciona una función de red específica. Ha la división de las funciones se le denomina división en capas.

Ventajas de la división por capas
Divide la comunicación de red en partes más pequeñas y sencillas. • Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes. • Permite a los distintos tipos de hardware y software de red comunicarse entre sí.

- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.



2.2.1 Definición de Sistemas Abiertos

Las capas del modelo OSI son siete y con frecuencia se mencionan por número y no por nombre, estas son:

Modelo OSI
7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace
1. Física

2.2.2 Capas del Modelo OSI

2.2.2.1 Capa Física

La capa física cubre las interfaces físicas entre los dispositivos y las reglas bajo las cuales cadenas de bits son transferidas de un dispositivo a otro. Los protocolos de la capa Física describen los medios mecánicos, funcionales, eléctricos y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia y desde un dispositivo de red.

La función de la capa física de OSI es la de codificar en señales los dígitos binarios que representan las tramas de la capa de Enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos (alambres de cobre, fibra óptica o medio inalámbrico) que conectan los dispositivos de la red.

2.2.2.2 Capa de Enlace

La capa de enlace controla la capa física (activándola, manteniéndola y desactivándola) y provee mecanismos necesarios que convierten a la comunicación en una transferencia confiable. Los protocolos de la capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes.

La capa de enlace de datos realiza dos servicios básicos:

- Permite a las capas superiores acceder a los medios usando técnicas, como tramas.
- Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

2.2.2.3 Capa de Red

La capa de red se encarga de encaminar los paquetes de información buscando para ello la mejor ruta. Proporciona los servicios para intercambiar los datos individuales en la red entre dispositivos finales identificándolos.

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

Direccionamiento, encapsulamiento, enrutamiento, y desencapsulamiento.

Protocolos de capa de Red

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- versión 4 del Protocolo de Internet (IPv4),
- versión 6 del Protocolo de Internet (IPv6),
- intercambio Novell de paquetes de internetwork (IPX),
- AppleTalk, y
- servicio de red sin conexión (CLNS/DECNet).

2.2.2.4 Capa de Transporte

La capa de transporte provee un mecanismo confiable para el intercambio de datos entre procesos y se encarga de segmentar y resemblar segmentos de información.

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son: seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino, segmentación de datos y gestión de cada porción, reensamble de segmentos en flujos de datos de aplicación, e identificación de las diferentes aplicaciones.

© DGAPA-PAPIME

Los dos protocolos más comunes de la capa de Transporte son el Protocolo de control de transmisión (TCP) y el Protocolos de datagramas de usuario (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

Protocolo de datagramas de usuario (UDP)

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

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión, descrito en la RFC 793. TCP incurre en el uso adicional de recursos para agregar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de Aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga. Ver la figura para obtener una comparación

2.2.2.5 Capa de Sesión

2.2.2.6 Capa de Presentación

2.2.2.7 Capa de Aplicación

2.2.2.8 Funciones de los Protocolos

2.2.2.9 Encapsulamiento

2.2.2.10 Control de Conexión

2.2.2.11 Detección de Errores

2.2.2.12 Encaminamiento

2.2.2.13 Transmisión punto a punto

2.3 Modelos de protocolos: TCP/IP

© DGAPA-PAPIME

Los Protocolos de Internet fueron el resultado del trabajo llevado a cabo por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA por sus siglas en inglés) a principios de los 70.

Este modelo define 4 categorías de funciones que deben tener lugar para que las comunicaciones sean satisfactorias.. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

La mayoría de los modelos de protocolos describen una pila de protocolos específicos del proveedor. Sin embargo TCP/IP es un estándar abierto, es decir, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFCS). En estos documentos se tienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

2.3.1 Capa del Modelo TCP/IP

Las capas del modelo TCP/IP son Aplicación, transporte, internet y acceso a la red.

Modelo TCP/IP	
1. Aplicación	Representa datos para el usuario mas el control de codificación y de dialogo
2. Transporte	Admite la comunicación entre distintos dispositivos de distintas redes.
3. Internet	Determina la mejor ruta a través de la red
4. Acceso a la red	Controla los dispositivos del hardware y los medios que conforman la red

Comparación entre el modelo OSI y TCP/IP

Modelo OSI	Modelo TCP/IP
7. Aplicación	1. Aplicación
6. Presentación	
5. Sesión	
4. Transporte	2. Transporte
3. Red	3. Internet
2. Enlace	4. Acceso a la red
1. Física	

2.4 Modelo SNA

Systems Network Architecture (SNA), es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus propios dispositivos por ejemplo sus hosts o mainframes, grandes ordenadores y servidores muy robustos que soportan millones de transacciones que por lo general son utilizados en el área bancaria

Al inicio fue diseñado para permitir la comunicación con un host. Cada red o subred eran controladas por este host. Los ordenadores se podían comunicar con dicho host, sin embargo no podían establecer comunicación directa con otros ordenadores. Este estilo de red recibe el nombre de subárea SNA. SNA describe los estándares, protocolos y funciones usadas por los dispositivos para permitirles la comunicación entre ellos en las redes SNA.

La arquitectura SNA

Es un modelo que presenta similitudes con el modelo de referencia OSI. Se compone de las siguientes capas:

Modelo OSI	SNA
7. Aplicación	7. Servicios de transacción
6. Presentación	6. Servicios de presentación
5. Sesión	5. Control de flujo de datos
4. Transporte	4. Control de transmisión
3. Red	3. Control de rutas
2. Enlace	2. Control de enlace de Datos
1. Física	1. Física

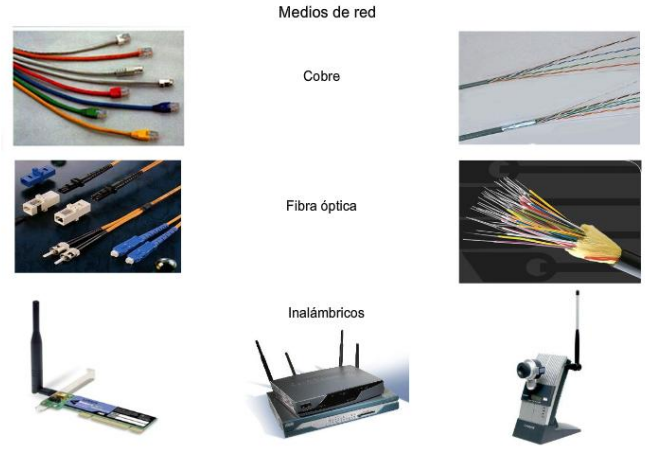
© DGAPA-PAPIME

3. Capa física

Cuando nos comunicación a través de la red la información es transportada por un medio. Éste proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes actuales utilizan fundamentalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son: hilos metálicos dentro de los cables, fibras de vidrio o plásticas (cable de fibra óptica), y transmisión sin cables, es decir, inalámbrica.

Cuando hablamos de medios de transmisión guiados nos referimos a los medios constituidos por un cable que se encarga de la conducción de las señales desde un extremo al otro. A diferencia de los medios guiados los medios no guiados son medios que no tienen cable y han tenido gran penetración al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar.



3.1 Medios de transmisión terrestres o guiados

3.1.1 Cable Coaxial

Descripción Física.	Características de transmisión.	Conectividad y Alcance Geográfico de acuerdo a IEEE 802.3.
Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un	Hay dos tipos de cable coaxial: • Cable fino (Thinnet). 10 base 2 • Cable grueso (Thicknet). 10 base 5 10 BASE T:	

Parámetro/Tipo de Cable	10Base5	10Base2
Longitud máxima	500 mts.	185 mts.
Impedancia	50 Ω	50Ω, RG58
Diámetro del conductor	2.17 mm	0.9 mm

aislamiento de protección para reducir las emisiones eléctricas. El ejemplo más común de este tipo de cables es el coaxial de televisión.	Velocidad 10 Mbps

3.1.2 Par Trenzado

Descripción Física.	Características de transmisión.	Conectividad y Alcance Geográfico de acuerdo a IEEE 802.3, 802.3u, 802.3z.
Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado. Cada cable de este tipo está compuesto por un serie de pares de cables trenzados. Los pares se trenzan para reducir la interferencia entre pares adyacentes. Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto.	UTP acrónimo de *Unshielded Twisted Pair* o Cable trenzado sin apantallar. Son cables que se utilizan para diferentes tecnologías de red local. STP, acrónimo de *Shielded Twisted Pair* o Par trenzado apantallado. Son cables de cobre aislados dentro de una cubierta protectora, 100 BASE T: Velocidad 100 Mbps 10 BASE T: Velocidad 10 Mbps	Distancia máxima por segmento : 100 m Número de nodos máxima por segmento: 30 Diámetro: .4 y .9 Conectores: RJ45

3.1.3 Fibra Óptica

Descripción Física.	Características de transmisión.	Conectividad y alcance geográfico de acuerdo a IEEE 802.3.
Este cable está constituido por uno o más hilos de fibra de vidrio, cada fibra de vidrio consta de: • Un núcleo central de fibra con un alto índice de refracción. • Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor. • Una envoltura que aísla las fibras y evita que se produzcan interferencias	Ancho de banda: 2 GHz Capacidad Máxima: 2 Gbps Capacidad usada: 100 Mbps Observaciones: Pequeño tamaño y peso, inmune a ruidos e interferencias, atenuación pequeña.	Velocidades muy altas, superiores al GHz. Tienen un Bc enorme (50Ghz máx., 2Ghz típico), Rmax enorme (2Gbps máx.), pequeño tamaño y peso, y una atenuación pequeña. Es un medio muy apropiado para largas distancias e incluso últimamente para

© DGAPA-PAPIME

entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.	Caras. Manipulación complicada	LAN's.

3.2 Medios de transmisión aéreos o no guiados

3.2.1 Redes inalámbricas

Descripción Física.	Características de Transmisión.
Se comunican por un medio de transmisión no guiado mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas. Tienen ventajas como la rápida instalación de la red sin la necesidad de usar cableado, permite la movilidad y tienen menos costos de mantenimiento que una red convencional. Otra de las ventajas de redes inalámbricas es la movilidad. Red inalámbrica los usuarios puedan conectarse a las redes existentes y se permite que circulen libremente.	Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos, por ejemplo. Dependiendo del medio, la red inalámbrica tendrá unas características u otras

3.2.2 Microondas

Descripción Física.	Características de Transmisión
En un sistema de microondas se usa el espacio aéreo como medio físico de transmisión. La información se transmite en forma digital a través de ondas de radio de muy corta longitud (unos pocos centímetros). Pueden direccionarse múltiples canales a múltiples estaciones dentro de un enlace dado, o pueden establecer enlaces punto a punto. Las estaciones consisten en una antena tipo plato y de circuitos que interconectan la antena con la terminal del usuario	Se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz. • Distancia máx.: 40 KM • Ancho de banda: 50 GHz • Ancho de banda: 500 Mbps

© DGAPA-PAPIME

3.2.3 Enlaces satelitales

Descripción Física.	Características de transmisión.
El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada .Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario. Se suele utilizar este sistema para: • Difusión de televisión. • Transmisión telefónica a larga distancia. Redes privadas.	Distancia entre satélites: 35680 km Ancho de banda: 100 MHz Capacidad max: 275 Gbps Capacidad usada: 275 Gbps

3.2.4 Rayo láser

Descripción Física	Características de transmisión
Un rayo láser (Light Amplification by Stimulated Emission of Radiation, Amplificación de Luz por Emisión Estimulada de Radiación) es un dispositivo que utiliza un efecto de la mecánica cuántica, la emisión inducida o estimulada, para generar un haz de luz coherente de un medio adecuado y con el tamaño, la forma y la pureza controlados.	El rayo láser es una luz muy potente y coherente (que no se dispersa fácilmente con la distancia). El rayo láser es unidireccional y para hacer LANs se necesitan dos rayos por cada nodo. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

3.2.5 Infrarrojo

Descripción Física.	Características de transmisión
El infrarrojo es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Consecuentemente, tiene menor frecuencia que la luz visible y mayor que las microondas.	Su rango de longitudes de onda va desde unos 700 nanómetros hasta 1 milímetro. • No hay interferencias • Distancia 200 metros • Línea de vista • No atraviesan obstáculos

© DGAPA-PAPIME

3.3 Estándares de capa física: RS-232, RS-422, RS-449

RS-232	RS-422 y RS-423	RS-449
Es una interfaz que da una norma para el intercambio serie de datos binarios entre un DTE (Equipo terminal de datos) y un DCE (*Data Communication Equipment*, Equipo de Comunicación de datos). RS-232 está diseñada para distancias cortas, de hasta 15 metros según la norma, y para velocidades de comunicación bajas, de no más de 20 Kbps. A pesar de ello, muchas veces se utiliza a mayores velocidades con un resultado aceptable. La interfaz puede trabajar en comunicación asíncrona o síncrona y tipos de canal simplex, half duplex o full duplex.	Interfaces normales aprobadas por la Asociación de Industrias Electrónicas (EIA) para los dispositivos de conexión serial . Las RS-422 y RS-423 normas se diseñan para reemplazar el más viejo RS-232 estándar porque se busca la mayor transmisión de datos y mayor inmunidad a la interferencia eléctrica. Todas las computadoras Macintosh de Apple contienen un puerto RS-422 que también puede usarse para comunicación RS-232C. RS-422 apoyan conexiones del multipoint considerando que RS-423 realiza sólo conexiones del punto-a-punto.	El RS-449 es una interfaz que designa las características mecánicas y funcionales de la interfaz entre Equipo Terminal de Datos (DTE) y Equipo Terminal de Circuito de Datos (DCE). Los componentes estándar para el uso junto con el RS-449 son el RS-422 para señales balanceadas, y el RS-423 para señales no balanceadas, con velocidades de transmisión de datos a 2.000.000 bits por segundo. El estándar especifica dos conectores D-sub con 37 y 9 pines para los circuitos de datos primarios y secundarios. Aunque no se implementa en computadores personales, esta interfaz se encuentra en algunos equipos de red. Este estándar se retiró en septiembre de 1992.

3.4 Cableado estructurado.

El cableado estructurado es una infraestructura de medios físicos destinada a transportar en un área limitada las señales que envía un emisor hasta el correspondiente receptor. Físicamente es una red de cable única y completa con un largo tiempo de vida útil, flexible, que soporta cambios y crecimiento a futuro y cumple con ciertas normas locales o internacionales. El diseño de esta infraestructura esta planeado para maximizar la velocidad, eficiencia y seguridad de una red.

Los principales estándares que se refieren al cableado de telecomunicaciones en edificios son:

ANSI/EIA/TIA 568-A: Alambrado de Telecomunicaciones para Edificios Comerciales.
ANSI/EIA/TIA 569: Rutas y Espacios de Telecomunicaciones para Edificios Comerciales.
ANSI/EIA/TIA 606: Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

© DGAPA-PAPIME

ANSI/EIA/TIA 607: Requerimientos de Puesta a Tierra y Puenteado de Telecomunicaciones para Edificios Comerciales.

3.4.1 Estándar EIA/TIA 568.

Especifica un sistema genérico de cableado de telecomunicaciones para edificios comerciales que soporta un ambiente de productos y fabricantes múltiples. Esta norma permite la planeación e instalación de cableado en edificios comerciales contando con poca información de los productos de telecomunicaciones que serán instalados posteriormente. Especifica los requerimientos mínimos del cableado de espacios de oficinas, incluyendo salidas y conectores, para que soporte distintos tipos de edificios y aplicaciones de usuario, así como los parámetros de medios de comunicación que determinan el rendimiento. La vida útil de los sistemas de cableado de telecomunicaciones que especifica esta norma debe ser mayor a diez años.

Esta norma determina los criterios técnicos y de desempeño para varias configuraciones de sistemas de cableado. Establece que un sistema de cableado estructurado consta de seis subsistemas funcionales:

- Subsistema de cableado horizontal.
- Subsistema de cableado vertical (*backbone*).
- Subsistema de área de trabajo.
- Subsistema de cuarto de telecomunicaciones.
- Subsistema de cuarto de equipos.
- Subsistema de entrada de servicios.

3.4.1.1 Subsistema horizontal.

Es la porción del cableado que conecta cada salida en el área de trabajo a la conexión cruzada horizontal en el armario de telecomunicaciones. Está formado por los cables horizontales, las salidas de telecomunicaciones en el área de trabajo, la terminación mecánica y los puentes en el armario de telecomunicaciones, así como las rutas y espacios horizontales que soportan el medio o cableado horizontal.

El diseño del sistema de cableado horizontal considera los siguientes servicios y sistemas comunes:

- Servicio vocal de telecomunicaciones.
- Elementos del equipo de interconexión.
- Comunicaciones de datos.
- Redes de área local.
- Otros sistemas de señalización del edificio.

El objetivo del cableado horizontal es satisfacer los requerimientos de telecomunicaciones, así como facilitar las actividades de mantenimiento, reubicación, instalación de nuevos equipos y cambios futuros en los servicios. Debido a la complejidad de la instalación del cableado horizontal y a la poca accesibilidad para realizar cambios se deben contemplar las diversas necesidades presentes y futuras de los usuarios antes de realizar la implementación.

Topología: El cableado horizontal se implementa con una topología física de estrella y se diseña para soportar aplicaciones como comunicaciones de datos, comunicaciones de voz, seguridad y sistemas de

control. Cada área de trabajo recibe los servicios desde un armario de telecomunicaciones situado en el mismo piso. En el área de trabajo cada conector de telecomunicaciones se conecta directamente a una conexión cruzada en el armario de telecomunicaciones.

Distancias horizontales: La distancia máxima desde el área de trabajo hasta el cuarto de telecomunicaciones es de 90 metros y se consideran 10 metros adicionales en cada canal horizontal para cables en el área de trabajo, puentes, cuerdas auxiliares y cuerdas de equipo en el armario de telecomunicaciones.

Los cordones en el área de trabajo deben ser de conductores flexibles y cumplir los requerimientos de longitud máxima que se determina con las siguientes formulas:

$$C = \frac{(102 - H)}{1.2} \qquad W = C - 7 \leq 20$$

Donde:

C es la máxima longitud combinada del cordón del área de trabajo y el cordón de parcheo, expresada en metros.

W es la máxima longitud del cordón del área de trabajo, expresada en metros.

H es la longitud del cable horizontal, expresada en metros.

Se asume que el cordón de parcheo mide un total de 5 metros en el distribuidor de cableado por piso, y que la longitud del cordón del área de trabajo no debe exceder los 10 metros.

Longitud del cable horizontal H	Longitud máxima del cordón del área de trabajo W	Longitud máxima combinada entre el cordón del área de trabajo y el patch C
90	5	10
85	9	14
80	13	18
75	17	22
70	22	27

Tabla 1.1. Distancias horizontales.

Cables aceptados:

- Se especifican tres tipos de cables para uso en el subsistema de cableado horizontal:
- Cable de par trenzado sin blindaje (UTP) de cuatro pares, 100 ohms, 22/24 AWG.
- Cable de par trenzado con blindaje (STP-A) de dos pares, 150 ohms, 22 AWG.
- Fibra óptica multimodo de dos fibras, 62.5/125 ó 50/125 µm.

También se pueden usar cables híbridos, compuestos de más de uno de los cables aceptados, los cuales deben satisfacer las especificaciones de transmisión y código de color correspondientes a ese tipo de

cable, así como los niveles permitidos de interferencia para cada tipo de cable reconocido en todas las frecuencias especificadas.

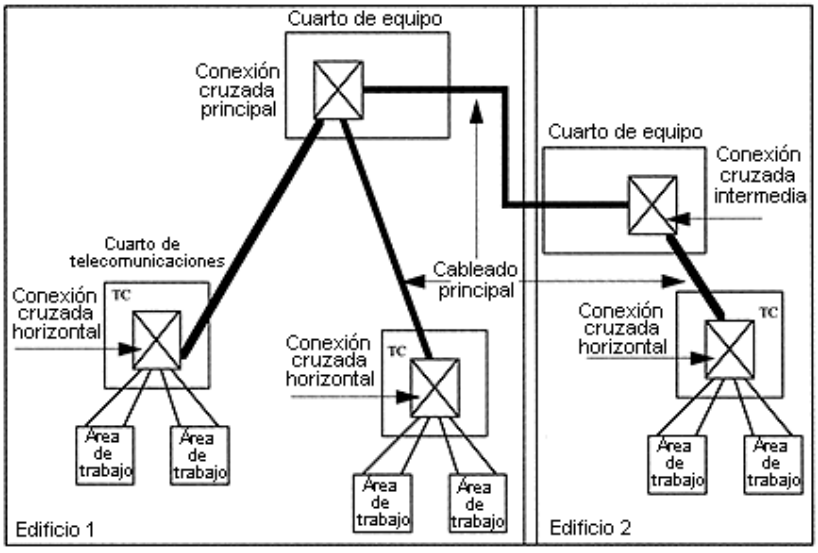
Las salidas para cableado horizontal en el área de trabajo cuentan con un mínimo de dos conectores. Un conector puede asociarse con voz y el otro con datos. Uno de los conectores debe estar sostenido por un cable UTP de cuatro pares, 100 Ω, de categoría 3 ó superior. Conectores adicionales deben estar sostenidos por un mínimo de uno de los medios horizontales aceptados. No existe más de un punto de transición o empalmes en cableados de distribución horizontal por cobre. Cuando se requieren adaptadores para los conectores estos se instalan de manera externa a la salida en el área de telecomunicaciones.

3.4.1.2 Subsistema vertical

Es la parte del sistema de cableado que proporciona la conexión entre el cuarto de entrada de servicios al edificio, los cuartos de equipo y los cuartos de telecomunicaciones. Realiza la conexión entre los gabinetes de telecomunicaciones ubicados en los distintos pisos, así como la conexión entre edificios de un medio tipo *Campus*. El cableado vertical o de *backbone* se compone de los cables medulares o de sostén, las conexiones cruzadas intermedias y principales, terminaciones mecánicas y alambres auxiliares. También incluye el cableado entre edificios.

La vida útil de un sistema de cableado vertical se mide en uno o varios periodos de planeación en los que los cambios en los requerimientos de servicios se satisfacen sin la necesidad de instalaciones adicionales. La duración de cada periodo se basa en la estabilidad y crecimiento de la organización del usuario. Se debe considerar también el número máximo de conexiones para cada armario de telecomunicaciones, cuarto de equipos y entrada para el periodo planeado.

Topología: El tendido del *backbone* de datos se realiza en una topología física de estrella jerárquica, en donde el gabinete con el equipamiento electrónico y de comunicaciones más complejo es el centro de la estrella. Cada conexión cruzada horizontal en un armario de telecomunicaciones está cableada a una conexión cruzada principal o a una conexión cruzada intermedia y de ahí a una conexión cruzada principal. No existen más de dos niveles jerárquicos de conexión cruzada para limitar la degradación de la señal en sistemas pasivos y simplificar movimientos, adiciones y cambios.



Distribución de cableado vertical en una topología de estrella jerárquica.

Cables aceptados: Usualmente el *backbone* de datos se implementa con cable UTP categoría 5 o superior, o con fibra óptica. Para ello se coloca un cable desde cada gabinete hasta el centro de la estrella. Los medios reconocidos que pueden ser usados individualmente o en combinación en el sistema de cableado vertical son:

- Cable de par trenzado sin blindaje (UTP), 100 ohms, 24 AWG.
- Cable de par trenzado con blindaje (STP-A), 150 ohms, 22 AWG.
- Cable de fibra óptica multimodal, 62.5/125 µm.
- Cable de fibra óptica unimodal.

Al hacer la elección de los medios de transmisión se deben considerar factores como la flexibilidad del medio con respecto a los servidores, la vida útil requerida del cableado medular y el tamaño del lugar y de la población usuaria. En la planeación es conveniente agrupar los servicios similares en categorías específicas, como voz, despliegue terminal, redes de área local y otras categorías digitales, identificando en cada grupo los tipos individuales y proyectando las cantidades requeridas.

Distancias de cableado vertical: Distancias Intra e Inter-Edificios: Las distancias máximas dependen de la aplicación. Para minimizarlas, la conexión cruzada principal se sitúa cerca del centro del lugar. La distancia máxima para el uso de cableado principal UTP multipar categoría 3 ó superior y STP-A 150 Ω es de 90 metros. Se asume que 5 m de la distancia total son necesarios en cada extremo para cables del equipo conectados a la médula. Para fibra óptica multimodo de 62.5 µm, la distancia máxima es de 2000 metros y para fibra óptica unimodo es de 3000 metros.
Conexión cruzada principal al punto de entrada: La distancia entre el punto de entrada y la conexión cruzada principal se incluye en los cálculos de la distancia total cuando por la ubicación del punto de demarcación sea necesario.

Conexiones cruzadas: Las longitudes de la cuerda auxiliar y alambre de puente no deben ser mayores de 20 metros en la conexión cruzada principal e intermedia.

Cableado hacia el equipo de telecomunicaciones: Los cables que conectan al equipo de telecomunicaciones con las conexiones cruzadas principales e intermedias tienen una longitud máxima de 30 metros.

3.4.1.3 Subsistema de Entrada del edificio.

Se define como el punto en donde la instalación exterior y los servicios de telecomunicaciones entran al edificio. Es un área destinada para la instalación de cables de telecomunicaciones y equipo de los proveedores de servicios externos y sistemas auxiliares de soporte para su operación. Puede contener interfaces de acceso a redes públicas o privadas y dispositivos de protección también. Incorpora el cableado de *backbone* que conecta con otros edificios del campus. Este subsistema comprende desde el punto de entrada a través del muro hasta el cuarto de entrada de servicios. Es aquí en donde se encuentran los dispositivos de protección para sobrecargas de voltaje.

Las instalaciones de entrada pueden incluir el punto de demarcación entre los proveedores de servicios y las instalaciones y equipos del cliente en cuanto al cableado. La ubicación del punto de demarcación para compañías locales de teléfono se determina por regulaciones y normas federales o estatales.

Entre los elementos de entrada al edificio se incluyen las conexiones entre el cableado usado en el exterior y el cableado especificado para la distribución en el interior del edificio. Las conexiones se realizan mediante empalmes o uniones.

© DGAPA-PAPIME

3.4.1.4 Subsistema del cuarto de telecomunicaciones.

Es el área del edificio usada como el punto de conexión entre el *backbone* y el cableado horizontal. En el cuarto de telecomunicaciones se alberga equipo de telecomunicaciones, terminaciones de cable y el cableado de interconexión asociado. Es ahí en donde se realiza la conexión cruzada de las terminaciones del cableado horizontal y *backbone* mediante *jumpers* o cordones de parcheo, permitiendo una conectividad flexible de servicios hacia las tomas de telecomunicaciones en el área de trabajo. Constituye un medio controlado para colocar el equipo de telecomunicaciones y los dispositivos de conexión que sirven a una porción del edificio. Existe al menos un cuarto de telecomunicaciones por piso.

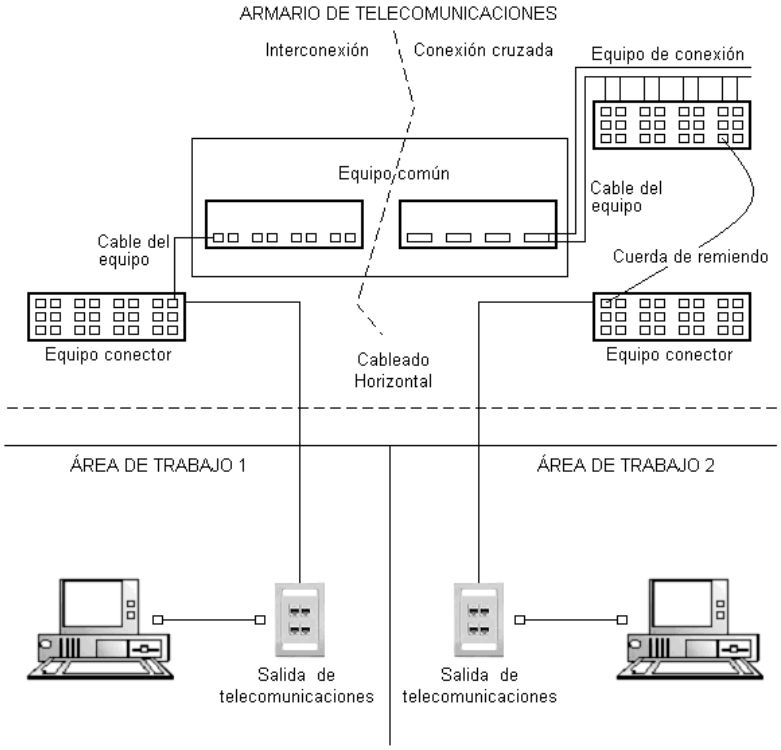
La terminación de la distribución del cableado horizontal, así como los tipos reconocidos de cableado medular llegan al armario de telecomunicaciones en un equipo conector compatible. El equipo de conexión, los puentes y las cuerdas auxiliares que enlazan los subsistemas de cableado con el armario de telecomunicaciones reciben el nombre de conexión cruzada horizontal. El armario de telecomunicaciones también puede contener la conexión cruzada principal e intermedia para diferentes secciones del sistema de cableado vertical. Las terminaciones de cables horizontales y verticales no se usan para administrar o realizar adiciones, traslados o cambios en el sistema de cableado.

Un armario de telecomunicaciones puede albergar equipo de telecomunicaciones, elementos de conexión, y en algunos casos, el punto de demarcación y el equipo de protección asociado.

Durante la instalación de equipo en un armario de telecomunicaciones se debe tener precaución en el manejo de los cables evitando exceder la tensión permitida.

El número de ductos que ingresan a un cuarto de telecomunicaciones depende del número de áreas de trabajo que atiende, pero se recomiendan al menos tres ductos de 4 pulgadas para distribuir el cable del *backbone*. Los *racks* de telecomunicaciones cuentan con más de 82 cm. libres alrededor como espacio de trabajo. Existen al menos dos tomacorrientes de 110 V C.A. dedicados de tres hilos, a partir de los cuales los equipos electrónicos se alimentan con UPS y regletas montadas a los *racks*. La temperatura del cuarto se mantiene continuamente entre 18°C y 24°C, con una humedad relativa entre 30% y 55%. A menudo se aplica un tratamiento especial a las paredes, pisos y techo para reducir el polvo y la electricidad estática.

© DGAPA-PAPIME



Esquemas de interconexión cruzada en un armario de telecomunicaciones.

3.4.1.5 Subsistema del área de trabajo.

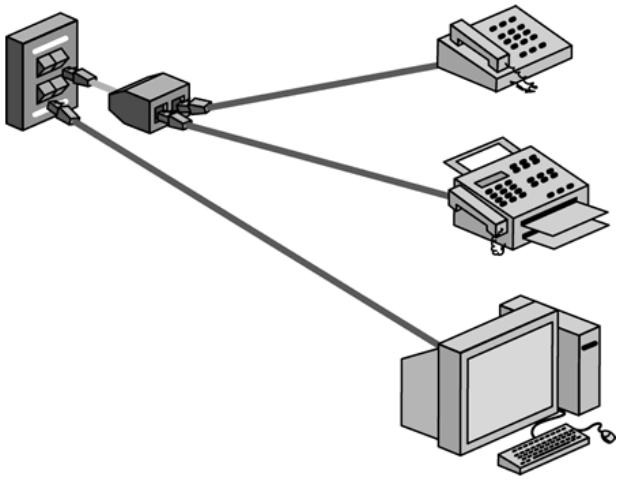
Es la zona en donde están ubicados los distintos puestos de trabajo de la red. Comprende todo aquello que se conecta desde la toma de telecomunicaciones, como computadoras, terminales de datos y teléfonos, así como adaptadores, filtros o acopladores en caso de ser requeridos. El cableado que se extiende a partir de la roseta de conexión no es permanente por lo que los cambios en esta zona son rápidos y sencillos.

Los ductos que llegan hasta las salidas en el área de trabajo tienen capacidad para manejar tres cables. Las salidas de telecomunicaciones cuentan al menos con dos conectores; uno de ellos del tipo RJ-45 siguiendo el código de colores de cableado T568A ó T568B.

La longitud máxima para el cable auxiliar en el área de trabajo es de 3 metros. Las características del cableado varían dependiendo de la aplicación. Comúnmente se usa una cuerda con conectores iguales en ambos extremos, pero es posible utilizar adaptaciones específicas externas a la salida de telecomunicaciones. Las adaptaciones más frecuentes en el área de trabajo son:

- Uso de un adaptador cuando es diferente el conector en el equipo al conector de telecomunicaciones.
- Adaptador en “Y” para conectar dos servicios en un cable singular.
- Adaptadores pasivos para conectar tipos de cables distintos del cableado horizontal y el equipo.
- Adaptadores activos con esquemas de señalamiento.
- Transposición del par por razones de compatibilidad.
- Resistores de terminación en el área de trabajo para algunos equipos de telecomunicaciones como terminales ISDN.

© DGAPA-PAPIME



Componentes del área de trabajo.

3.4.1.6 Subsistema del cuarto de equipo.

Es el espacio centralizado donde residen los equipos de telecomunicaciones comunes al edificio como PBX, servidores centrales, central telefónica, conmutadores de video, etc., así como los cables y conectores que permiten enlazarlos con otros dispositivos para compartir servicios. La naturaleza, costo y complejidad del equipo que contiene un cuarto de equipo lo diferencia de los cuartos de telecomunicaciones. Las funciones de un cuarto de telecomunicaciones pueden estar disponibles en un cuarto de equipos.

El cuarto de equipos proporciona un medio controlado para almacenar equipo de telecomunicaciones, conectar equipo, empalmar cierres y vincular medios y aparatos de protección. Contiene los componentes necesarios para realizar una conexión cruzada principal o intermedia. También puede tener terminaciones de equipo así como terminaciones troncales y auxiliares de redes.

A veces el cuarto de equipos es unido a la entrada de servicios o a una sala de cómputo para compartir aire acondicionado, seguridad, control de fuego, iluminación y acceso limitado. Típicamente se localiza lejos de fuentes de interferencia electromagnética. Incluye espacio de trabajo para personal de telecomunicaciones.

Los sistemas auxiliares para la operación de los equipos, como tableros de alimentación eléctrica, aire acondicionado y unidades de suministro de energía de hasta 100 KVA pueden instalarse en el cuarto de equipos.

Se recomienda un tamaño de 0.07 m^2 de uso de espacio para equipo por cada 10 m^2 de área utilizable. No se permite el uso de techo falso y la temperatura se mantiene entre 18°C y 24°C. Las paredes se pintan de blanco o colores claros para mejorar la visibilidad.

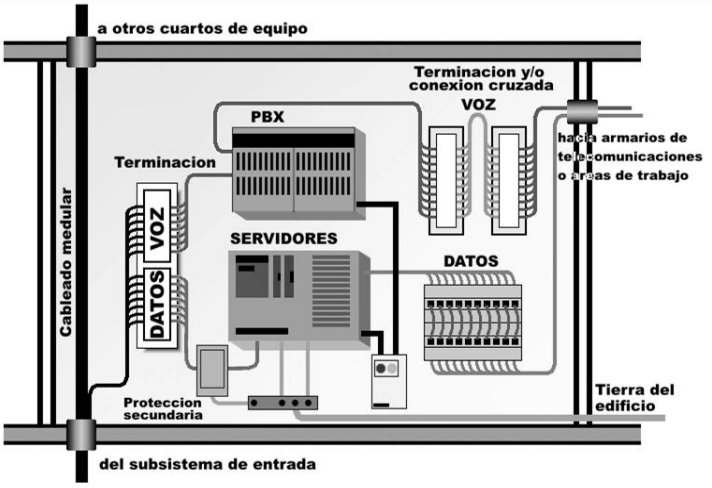
Se recomiendan las siguientes dimensiones de acuerdo al número de estaciones de trabajo:

Número de estaciones de trabajo	Dimensiones del distribuidor principal (m^2)

1 - 100	10
101 - 400	20
401 - 800	40
801 - 1200	70

Dimensiones recomendadas para un cuarto de equipos.

La siguiente figura muestra la conformación típica de un cuarto de equipos.



Subsistema de cuarto de equipos.

3.4.2 Estándar EIA/TIA 569.

Este estándar describe los aspectos de diseño de los recorridos de cableado y los cuartos destinados a albergar el equipo de telecomunicaciones. Provee una estructura genérica para el cableado, capaz de soportar cualquier aplicación de datos y voz previsible en un periodo de 10 a 15 años. Establece tres conceptos fundamentales para las telecomunicaciones en edificios comerciales:

Los edificios son dinámicos: Las remodelaciones se presentan de manera frecuente durante la existencia de un edificio. En este estándar se reconoce positivamente la recurrencia del cambio.

Los sistemas de telecomunicaciones y los medios son dinámicos: Los equipos de telecomunicaciones cambian de manera dramática durante la existencia de un edificio. Este estándar reconoce este hecho y establece que los cambios deben ser tan independientes como sea posible de los proveedores de equipo.

Telecomunicaciones no son solo datos y voz: Las telecomunicaciones del edificio incorporan también otros sistemas de bajo voltaje que transportan información, como la seguridad, el control ambiental, audio, video y alarmas.

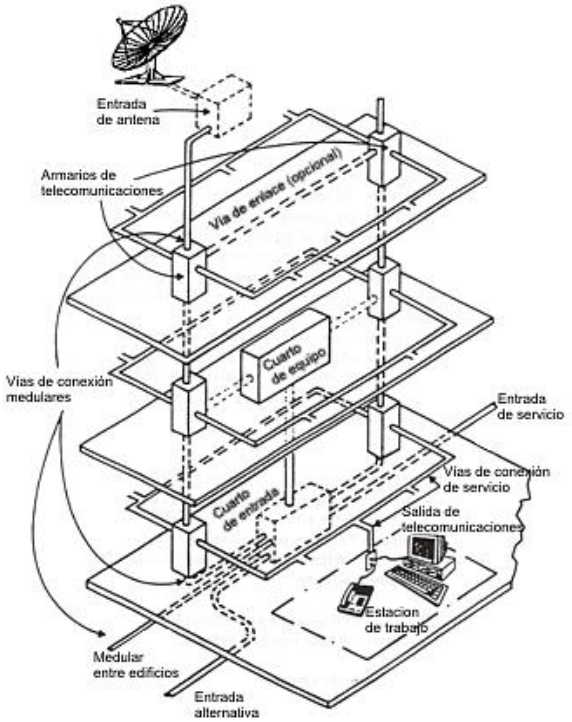
Un diseño exitoso de la infraestructura para telecomunicaciones se logra en la medida en que este se incorpora durante la fase preliminar del diseño arquitectónico del edificio.

La norma tiene por objetivo estandarizar prácticas específicas de diseño e instalación en edificios comerciales, que apoyen equipos y medios de telecomunicaciones, mediante normas para cuartos, áreas y conductos usados para la instalación de equipos y medios de transmisión.

Los componentes de telecomunicaciones que se contemplan en esta norma incluyen las vías o conductos en los que se encuentran localizados los medios de transmisión, así como las áreas destinadas a la instalación de los equipos de telecomunicaciones.

Esta norma identifica seis componentes fundamentales del sistema de cableado del edificio:

- Vías de telecomunicaciones horizontales.
- Vías de telecomunicaciones medulares.
- Estación de trabajo.
- Armario de telecomunicaciones.
- Cuarto de equipos.
- Instalaciones de entrada.



Componentes del sistema de cableado del edificio.

3.4.3 Estándar EIA/TIA 606.

Define un esquema de administración uniforme independiente de las aplicaciones que hacen uso del sistema de cableado, las cuales están sujetas a cambios durante la existencia del edificio. Este estándar establece las características que debe cumplir la codificación de colores, etiquetado y documentación de un sistema de cableado estructurado.

Especifica cuatro clases de administración para el mantenimiento de la infraestructura de telecomunicaciones. Estas clases se basan en el tamaño y la complejidad de la infraestructura que se administra y aseguran una implementación modular y escalable.

La **clase 1**, administra a un cuarto de equipos considerándolo el único espacio de telecomunicaciones en tanto no existan cuartos de telecomunicaciones, cableado de *backbone* o sistemas de cableado externo de planta que administrar.

La **clase 2,** define las necesidades de etiquetado para un edificio que es atendido por uno o más espacios de telecomunicaciones, como lo son un cuarto de equipos con uno o más cuartos de telecomunicaciones. Administra todos los elementos de la clase 1 e incluye identificadores para el cableado de *backbone*, elementos de aterrizaje, puntos de demarcación y protecciones contra fuego.

La **clase 3**, establece los elementos para la administración de un campus, incluyendo sus edificios y elementos de cableado externo. La administración clase 3 se aplica a todos los elementos de la clase 2 además de incluir identificadores para edificios y cableado de *backbone* de campus.

La **clase 4**, administra elementos de redes WAN (*Wide Area Network*) como sistemas de interconexión entre *Campus*. Para sistemas de misión crítica y edificios grandes se recomienda administrar recorridos, espacios y elementos de exterior de planta.

La administración de sistemas de cableado estructurado se simplifica con el uso de un código de colores para los elementos de la infraestructura de telecomunicaciones. Esa codificación se basa en la topología de estrella jerárquica de dos niveles del cableado de *backbone*. El primer nivel incluye el cableado de la conexión cruzada principal hacia un cuarto de telecomunicaciones en el mismo edificio. El segundo nivel incluye el cableado entre dos cuartos de telecomunicaciones en un edificio.

Para el uso adecuado del código de colores deben seguirse algunas reglas:

- Las etiquetas de terminación identificando dos extremos de un mismo cable deben ser del mismo color.
- A cada componente de la infraestructura de telecomunicaciones se le asigna una etiqueta única que lo relaciona con su registro correspondiente.
- Los identificadores en la etiqueta deben poder leerse con facilidad y ser resistentes a las condiciones del entorno.
- Todas las etiquetas deben ser impresas o generadas por algún dispositivo mecánico.

En la tabla muestra la correspondencia entre el código de colores y los elementos de telecomunicaciones.

Color	Elemento identificado
Naranja	Punto de demarcación (terminación central)
Verde	Terminación de conexiones de red
Púrpura	Terminaciones de cables originados de equipo común
Blanco	Terminación de *backbone* de primer nivel
Gris	Terminación de *backbone* de segundo nivel
Azul	Terminación del cableado horizontal en el cuarto de telecomunicaciones
Café	Terminaciones de cable de *backbone* Inter-edificios
Amarillo	Terminación de circuitos auxiliares
Rojo	Terminación de sistemas de equipo telefónico de seguridad

Código de colores para la identificación de los elementos de cableado.

Los registros contienen información sobre componentes específicos. Esta información puede incluir identificadores de enlaces horizontales, tipos de cables, salidas de hardware, longitud de los cables,

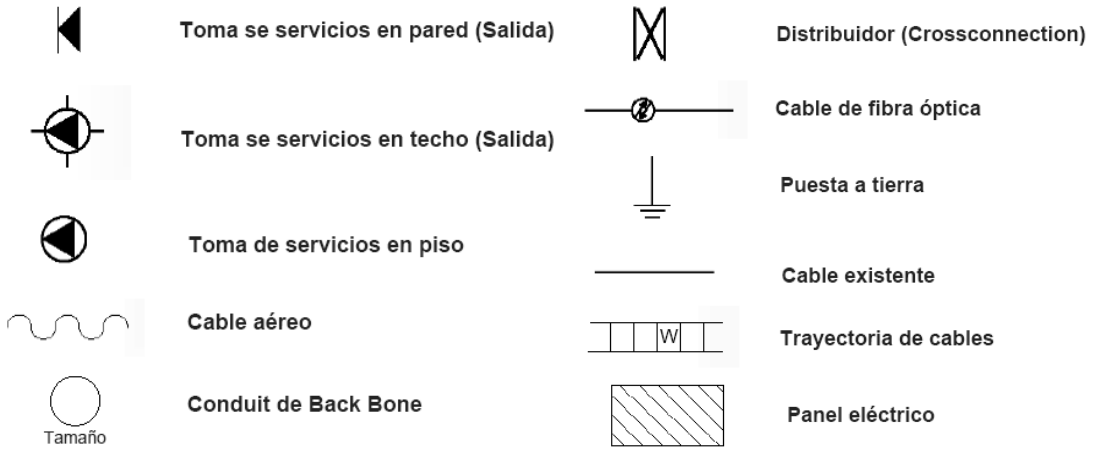
 © DGAPA-PAPIME

hardware de conexión cruzada y localización de salidas de telecomunicaciones. Además de la información requerida contienen los enlaces necesarios y otra información opcional. Los enlaces constituyen la conexión lógica entre identificadores y registros, así como el enlace entre un registro y otro.

El estándar establece la elaboración de reportes, mediante los cuales se puede consultar la información sobre la infraestructura de telecomunicaciones. Un reporte puede consistir en un registro individual, un grupo de registros, o fragmentos seleccionados de uno o más registros.

La nomenclatura para la identificación de cada servicio es única. Los servicios en el área del usuario se identifican con la misma nomenclatura que poseen en el panel de parcheo del que provienen. También se identifican los cordones de parcheo en el cuarto de distribución. Los conductos que requieren etiquetado comprenden a las charolas porta-cable, ductos conduit, canaletas superficiales y canaletas de muebles modulares. Para la identificación en paneles el cableado debe estar perfectamente ordenado.

El esquema de administración también incluye la elaboración de planos, dibujos de detalle, isométricos y diagramas de conexión de las canalizaciones, trayectorias de cableado, tipos de cables, capacidad de ductos, porcentajes de saturación y sistemas de tierra. La simbología empleada debe ser clara y la elaboración se debe realizar mediante software de CAD.



Simbología para planos y diagramas.

3.5 Equipo.

3.5.1 Repetidor.

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.

El término repetidor se creó con la telegrafía y se refería a un dispositivo electromecánico utilizado para regenerar las señales telegráficas. El uso del término ha continuado en telefonía y transmisión de datos.

En telecomunicación el término repetidor tiene los siguientes significados normalizados:

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

En el modelo de referencia OSI el repetidor opera en el nivel físico.

3.5.2 Hub.

Un Hub o concentrador Es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs han dejado de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician.

3.6 ATM.

El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Descripción del proceso ATM

Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.

3.7 Frame Relay

Frame Relay o (*Frame-mode Bearer Service*) es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("*frames*") para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.

© DGAPA-PAPIME

Las conexiones pueden ser del tipo permanente, (PVC, *Permanent Virtual Circuit*) o conmutadas (SVC, *Switched Virtual Circuit*). Por ahora solo se utiliza la permanente. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red.

El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red, puede manejar tanto tráfico de datos como de voz.

Al contratar un servicio Frame Relay, contratamos un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Commited Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas, pero en media en el intervalo Tc no deberá superarse la cantidad estipulada Bc.

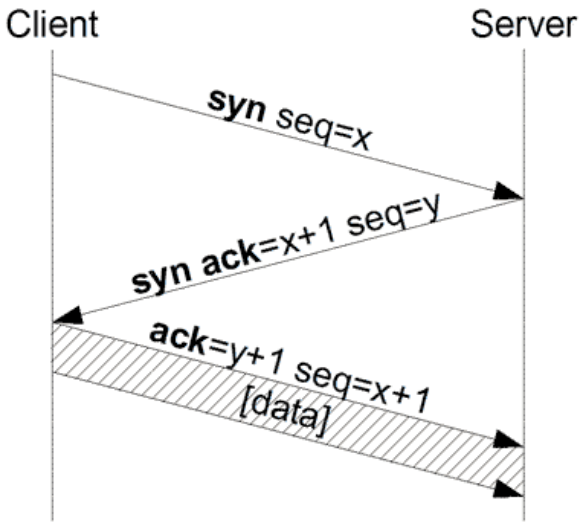
Estos Bc bits, serán enviados de forma transparente. No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante los Be (*Excess Burst*). Estos datos que superan lo contratado, serán enviados en modo *best-effort*, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo.

© DGAPA-PAPIME

4. Capa de enlace

4.1 Hand-shaking

Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión. Para establecer la conexión se usa el procedimiento llamado *negociación en tres pasos* (3-way handshake). Una *negociación en cuatro pasos* (4-way handshake) es usada para la desconexión. Durante el establecimiento de la conexión, algunos parámetros como el número de secuencia son configurados para asegurar la entrega ordenada de los datos y la robustez de la comunicación.



El proceso se describe a continuación:

El host receptor, que en el caso de más común será un servidor, espera pasivamente una conexión ejecutando las primitivas LISTEN y ACCEPT

En primer lugar, el host que desea iniciar la conexión ejecuta una primitiva CONNECT especificando la dirección IP y el puerto con el que se desea conectar, el tamaño máximo del segmento que está dispuesto a aceptar y opcionalmente otros datos, como alguna contraseña de usuario. Entonces la primitiva CONNCET hace una apertura activa, enviando al otro host un paquete que tiene el bit SYN (ver formato de un segmento TCP más abajo) activado, indicándole también el número de secuencia inicial "x" que usará para enviar sus mensajes.

El host receptor recibe el segmento revisa si hay algún proceso activo que haya ejecutado un LISTEN en el puerto solicitado, es decir, preparado para recibir datos por ese puerto. Si lo hay, el proceso a la escucha recibe el segmento TCP entrante, registra el número de secuencia "x" y, si desea abrir la conexión, responde con un acuse de recibo "x + 1" con el bit SYN activado e incluye su propio número de secuencia inicial "y", dejando entonces abierta la conexión por su extremo. El número de acuse de recibo "x + 1" significa que el host ha recibido todos los octetos hasta e incluyendo "x", y espera "x + 1" a continuación. Si no desea establecer la conexión, envía una contestación con el bit RST activado, para que el host en el otro extremo lo sepa.

La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión, por lo que a partir de ese momento también puede ella enviar datos. Con esto, la conexión ha quedado abierta en ambos sentidos

4.2 Transmisión asíncrona y síncrona.

La transmisión de datos síncrona involucra una continua y consistente (en tiempo) transferencia de datos. La duración del tiempo entre cada bit ó carácter mandado es pre asignado por el sistema receptor y el transmisor. Esto provee un medio para el sistema de recepción para conocer cuando buscar cada carácter ó bien que tanto tiempo tomará transmitir un carácter.

Los módems que pueden ser sincronizados de esta manera son llamados *módems síncronos.* Dependiendo del protocolo usado, el tiempo de sincronización es usualmente afectado por una especial señal de información que preceda a una transferencia de datos o por información contenida en un grupo de bytes (llamados BLOQUES). Esta señal habilita los sistemas para sincronizar sus relojes internos y puede venir de la computadora o el módem.

La transmisión asíncrona es un modo de transferencia de datos que notifica al sistema de recepción, cuando cada carácter empieza y termina, acompañado con bits adicionales. Esos extra bits incluyen un bit de empiezo, bit de paridad y un bit de paro. A estos bits junto con el carácter se les conoce como TRAMA. Los módems que operan en modo asíncrono son llamados *módems asíncronos.*

La transmisión síncrona es 20 porciento más rápida que la asíncrona. Pero la transmisión síncrona requiere de equipo más caro. Mientras tanto el equipo asíncrono no requiere de circuitos de reloj, razón por la cual los módems asíncronos son más baratos. Razón por la cual la mayoría de la microcomputadoras que usan módems usa este tipo de transmisión.

4.3 Analizar el funcionamiento del Protocolo HDLC y SDLC.

HDLC (High-Level Data Link Control, control de enlace síncrono de datos) es un protocolo de comunicaciones de propósito general punto a punto, que opera a nivel de enlace de datos. Se basa en ISO 3309 e ISO 4335. Surge como una evolución del anterior SDLC. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor.

Por otra parte el acrónimo SDLC (del inglés *Synchronous Data Link Controller*, controlador de enlace de datos síncrono) se utiliza para nombrar el protocolo diseñado por IBM para enlaces síncronos a través de una línea para la capa 2 del modelo OSI de comunicaciones. Como su nombre implica, es un protocolo síncrono, lo que supone la transmisión de la señal de reloj con los datos.

4.4 Protocolo ALOHA.

El protocolo ALOHA es un protocolo del nivel de enlace de datos para redes de área local con topología de difusión.

La primera versión del protocolo era básica:

- Si tienes datos que enviar, envíalos.
- Si el mensaje colisiona con otra transmisión, intenta reenviarlos más tarde.

La diferencia entre ALOHA y Ethernet en un medio compartido es que Ethernet usa CSMA/CD: comprueba si alguien está usando el medio antes de enviar, y detecta las colisiones desde el emisor.

Aloha puro tiene aproximadamente un 18'4% de rendimiento máximo. Esto significa que el 81'6% del total disponible de ancho de banda se está desperdiciando básicamente debido a estaciones tratando de emitir al mismo tiempo. El cálculo básico del rendimiento implica la asunción de que el proceso de llegada de tramas sigue una distribución de Poisson con un número medio de llegadas de 2G por cada 2X segundos. Por tanto, el parámetro lambda en la distribución de Poisson será 2G. Dicho máximo se alcanza para G = 0'5, obteniendo un rendimiento máximo de 0'184, es decir, del 18'4%.

Una versión mejorada del protocolo original fue el Aloha ranurado, que introducía ranuras de tiempo e incrementaba el rendimiento máximo hasta 36'8%. Una estación no puede emitir en cualquier momento, sino justo al comienzo de una ranura, y así las colisiones se reducen. En este caso, el número promedio de llegadas es de G por cada 2X segundos. Esto disminuye el parámetro lambda a G. El rendimiento máximo se alcanza para G = 1.

Debe apreciarse que estas características de ALOHA no difieren mucho de las experimentadas hoy día con Ethernet centralizado, Wi-Fi y sistemas similares. Existe una cierta cantidad de ineficiencia inherente a estos sistemas. Por ejemplo, 802.11b otorga alrededor de 2-4 Mbps de rendimiento real con unas pocas estaciones emitiendo, en contra del máximo teórico de 11 Mbps. Es común ver cómo el rendimiento de estos tipos de redes desciende significativamente a medida que el número de usuarios y mensajes aumenta. Por ello, las aplicaciones que requieren un comportamiento altamente determinístico a menudo usa esquemas de paso de testigo (como Token Ring) en su lugar. Por ejemplo, ARCNET es muy popular en aplicaciones empotradas. No obstante, los sistemas basados en *disputa* (como ALOHA) también tienen ventajas significativas, incluyendo la facilidad de gestión y la velocidad en una comunicación inicial.

Debido a que los sistemas de *escucha antes de enviar* (CSMA), como el usado en Ethernet, trabajan mucho mejor que ALOHA para todos los casos en los que todas las estaciones pueden escuchar a cada una de las demás, sólo se usa Aloha ranurado en redes tácticas de satélites de comunicaciones del ejército de los Estados Unidos con un bajo ancho de banda.

4.5 Control de Acceso al medio.

4.5.1 CSMA/CD y CSMA/CA.

CSMA/CD, siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció en primer lugar la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD.

CSMA/CA *Carrier Sense, Multiple Access, Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones)* es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para

transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no.

4.5.2 Token.

Dentro de una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso al medio llamada paso de tokens.

4.6 Protocolo LLC y MAC del estándar IEEE 802 para redes de área local

4.6.1 Capa LLC (IEEE 802.2).

El control de enlace lógico (LLC) coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

El control de acceso al medio (MAC) proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

4.6.2 Ethernet (IEEE 802.3).

A los inicios la primera LAN (Red de área local) del mundo fue la versión original de Ethernet. En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO). Para garantizar la compatibilidad, los estándares IEEE 802.3 debían cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

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

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

© DGAPA-PAPIME

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Para Ethernet en la Capa 2 se ocupa de algunas limitaciones. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

Ethernet separa 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. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

4.6.3 Token Bus y Token Ring (IEEE 802.4 y 802.5).

Token Bus es un protocolo para redes de área local con similitudes a Token Ring, pero en vez de estar destinado a topologías en anillo está diseñado para topologías en bus.

Es un protocolo de acceso al medio en el cual los nodos están conectados a un bus o canal para comunicarse con el resto. En todo momento hay un testigo (*token*) que los nodos de la red se van pasando, y únicamente el nodo que tiene el testigo tiene permiso para transmitir. El bus principal consiste en un cable coaxial.

Token bus está definido en el estándar IEEE 802.4. Se publicó en 1980 por el comité 802 dentro del cual crearon 3 subcomites para 3 propuestas que impulsaban distintas empresas. El protocolo ARCNET es similar, pero no sigue este estándar. Token Bus se utiliza principalmente en aplicaciones industriales. Fue muy apoyado por GM. Actualmente en desuso por la popularización de Ethernet.

Token Ring es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; Actualmente no es empleada en diseños de redes.

Token Bus	Token Ring

© DGAPA-PAPIME

- Tiene una topografía en bus (configuración en bus física), pero una topología en anillo. Las estaciones están conectadas a un bus común pero funcionan como si estuvieran conectadas en anillo.
- Todas las estaciones o nodos conocen la identidad de los nodos siguiente y anterior. El último nodo conoce la dirección del primero y de su anterior, así como el primer nodo conoce la dirección del último y de su sucesor.
- La estación que tiene el testigo o *token* tiene el control sobre el medio y puede transmitir información a otro nodo.
- Cada estación tiene un receptor y un transmisor que hace las funciones de repetidor de la señal para la siguiente estación del anillo lógico.
- No existen colisiones.
- Todas las estaciones tienen igual probabilidad de envio.
- Es un protocolo eficaz en la producción en serie.
- Utiliza una topología lógica en anillo, aunque por medio de una unidad de acceso de estación múltiple (MSAU), la red puede verse como si fuera una estrella. Tiene topología física estrella y topología lógica en anillo.
- Utiliza cable especial apantallado, aunque el cableado también puede ser par trenzado.
- La longitud total de la red no puede superar los 366 metros.
- La distancia entre una computadora y el MAU no puede ser mayor que 100 metros.
- A cada MAU se pueden conectar ocho computadoras.
- Estas redes alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps.
- Posteriormente el High Speed Token Ring (HSTR) elevó la velocidad a 100 Mbps la mayoría de redes no la soportan.

4.6.4 Redes Inalámbricas (802.11)

El estándar IEEE 802.11 o Wi-Fi de IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

Wifi n ó 802.11n, en la actualidad la mayoría de productos son de la especificación b y de la g , sin embargo ya se ha ratificado el primer borrador del estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen un primer borrador del estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5,4 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empieza a fabricar de forma masiva y es objeto de promociones de los operadores ADSL, de forma que la masificación de la citada tecnología, parece estar de camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre si, de forma que el usuario no necesitara nada mas que su adaptador wifi integrado, para poder conectarse a la red.

4.6.5 MAC Address

© DGAPA-PAPIME

La dirección MAC (Media Access Control) es un identificador de 48 bits (6 octetos) que corresponde de forma única a una ethernet de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits)

4.7 Bridges.

Un bridge es un dispositivo que se utilizaba con mayor frecuencia en los inicios de la LAN para conectar dos segmentos de red física. Los switches pueden utilizarse para realizar esta operación, a la vez que permiten la conectividad del dispositivo final con la LAN. Muchas otras tecnologías se desarrollaron en torno a los switches LAN.

4.8 Técnicas de Conmutación.

Conmutación es la conexión que realizan los diferentes nodos que existen en distintos lugares y distancias para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones. La conmutación permite la descongestión entre los usuarios de la red disminuyendo el tráfico y aumentando el ancho de banda. Es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda.

4.8.1 Conmutación de circuitos.

Es aquella en la que los equipos de conmutación deben establecer un camino físico entre los medios de comunicación previo a la conexión entre los usuarios. Este camino permanece activo durante la comunicación entre los usuarios, liberándose al terminar la comunicación. Ejemplo: Red Telefónica Conmutada.

Su funcionamiento pasa por las siguientes etapas: solicitud, establecimiento, transferencia de archivos y liberación de conexión.

4.8.2 Conmutación de mensajes.

Este método era el usado por los sistemas telegráficos, siendo el más antiguo que existe. Para transmitir un mensaje a un receptor, el emisor debe enviar primero el mensaje completo a un nodo intermedio el cual lo encola en la cola donde almacena los mensajes que le son enviados por otros nodos. Luego, cuando llega su turno, lo reenviará a otro y éste a otro y así las veces que sean necesarias antes de llegar al receptor. El mensaje deberá ser almacenado por completo y de forma temporal en el nodo intermedio antes de poder ser reenviado al siguiente, por lo que los nodos temporales deben tener una gran capacidad de almacenamiento.

4.8.3 Conmutación de paquetes.

El emisor divide los mensajes a enviar en un número arbitrario de paquetes del mismo tamaño, donde adjunta una cabecera y la dirección origen y destino así como datos de control que luego serán transmitidos por diferentes medios de conexión entre nodos temporales hasta

llegar a su destino. Este método de conmutación es el que más se utiliza en las redes de ordenadores actuales. Surge para optimizar la capacidad de transmisión a través de las líneas existentes.

Al igual que en la conmutación de mensajes, los nodos temporales almacenan los paquetes en colas en sus memorias que no necesitan ser demasiado grandes.

4.8.3.1 Conmutación de Circuitos Virtuales.

En la conmutación de circuitos virtuales cada paquete se encamina por el mismo circuito virtual que los anteriores. Por tanto se controla y asegura el orden de llegada de los paquetes a destino

4.8.3.2 Conmutación de Paquetes Datagrama.

En la conmutación de datagramas cada paquete se encamina de manera independiente de los demás. Por tanto la red no puede controlar el camino seguido por los paquetes, ni asegurar el orden de llegada a destino.

4.9 Analizar el protocolo X.25.

X.25 es un estándar para redes de área amplia de conmutación de paquetes. Su protocolo de enlace, LAPB, está basado en el protocolo HDLC. En el cual se establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación, técnicas de recuperación de errores. Los servicios públicos de conmutación de paquetes admiten numerosos tipos de estaciones de distintos fabricantes. Por lo tanto, es de la mayor importancia definir la interfaz entre el equipo del usuario final y la red.

OSI ha sido la base para la implementación de varios protocolos. Entre los protocolos comúnmente asociados con el modelo OSI, el conjunto de protocolos conocido como X.25 es probablemente el mejor conocido y el más ampliamente utilizado. X.25 fue establecido como una recomendación de la ITU-TS (Telecommunications Section de la International Telecommunications Union), una organización internacional que recomienda estándares para los servicios telefónicos internacionales. X.25 ha sido adoptado para las redes públicas de datos y es especialmente popular en Europa.

4.10 Equipo.

4.10.1 Switch.

Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas

en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs (*Local Area Network*- Red de Área Local).

Los switches permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

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

4.10.2 NIC (Network Interface Card)

Tarjeta de interfaz de red (NIC): una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo host. El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.

© DGAPA-PAPIME

5. Capa de red

5.1 Protocolos del Nivel Red.

5.1.1 Protocolo IP.

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos: direccionamiento, encapsulamiento, enrutamiento, y des encapsulamiento.

IPv4 es la versión 4 del Protocolo IP (Internet Protocol)version anterior de ipv6. Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

Direccionamiento

La Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación

La capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de Red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen.

Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

Enrutamiento

La capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

© DGAPA-PAPIME

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto.

A medida que el paquete es enviado, su contenido (la PDU de la Capa de transporte) permanece intacto hasta que llega al host destino.

Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

5.1.2 Protocolo IPX.

IPX es un protocolo de comunicaciones de NetWare que se utiliza para transportar mensajes de un nodo a otro. Los paquetes IPX incluyen direcciones de redes y pueden enviarse de una red a otra. Ocasionalmente, un paquete IPX puede perderse cuando cruza redes, de esta manera el IPX no garantiza la entrega de un mensaje completo. La aplicación tiene que proveer ese control o debe utilizarse el protocolo SPX de NetWare. IPX provee servicios en estratos 3 y 4 del modelo OSI. Actualmente este protocolo esta en desuso y solo se utiliza para juegos en red antiguos

5.1.3 Netbios.

NetBIOS, "*Network Basic Input/Output System*", es, en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. NetBIOS fue originalmente desarrollado por IBM y Sytek como API/APIS para el software cliente de recursos de una Red de área local (LAN). Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red.

De forma sencilla, NetBIOS, permite a las aplicaciones 'conversar' con la red. Su intención es conseguir aislar los programas de aplicación de cualquier tipo de dependencia del hardware. También evita que los desarrolladores de software tengan que desarrollar rutinas de recuperación ante errores o de enrutamiento o direccionamiento de mensajes a bajo nivel. Coloquialmente hablando, NetBIOS hace el 'trabajo sucio'.

En una red local con soporte NetBIOS, las computadoras son conocidas e identificadas con un nombre. Cada computador de la red tiene un único nombre.

Cada PC de una red local NetBIOS se comunica con los otros bien sea estableciendo una conexión (sesión), usando datagramas NetBIOS o mediante broadcast. Las sesiones permiten, como en el protocolo TCP, mandar mensajes más largos y gestionar el control y recuperación de errores. La comunicación será punto a punto. Por otro lado, los métodos de datagramas y broadcast permiten a un ordenador comunicarse con otros cuantos al mismo tiempo, pero estando limitados en el tamaño del mensaje. Además, no hay control ni recuperación de errores

(al igual que ocurre en UDP). A cambio, se consigue una mayor eficiencia con mensajes cortos, al no tener que establecer una conexión.

5.2 Redes y subredes.

Una de las principales funciones de la capa de Red es proveer un mecanismo para direccionar hosts. A medida que crece el número de hosts de la red, se requiere más planificación para administrar y direccionar la red.

División de redes

En lugar de tener todos los hosts conectados en cualquier parte a una vasta red global, es más práctico y manejable agrupar los hosts en redes específicas. Históricamente, las redes basadas en IP tienen su raíz como una red grande. Como esta red creció, también lo hicieron los temas relacionados con su crecimiento. Para aliviar estos problemas, la red grande fue separada en redes más pequeñas que fueron interconectadas. Estas redes más pequeñas generalmente se llaman subredes.

Red y subred son términos utilizados indistintamente para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP.

De manera similar, a medida que nuestras redes crecen, pueden volverse demasiado grandes para manejarlas como una única red. En ese punto, necesitamos dividir nuestra red. Cuando planeamos la división de la red, necesitamos agrupar aquellos hosts con factores comunes en la misma red.

5.3 Administración de tablas de ruteo.

En un router la tabla de enrutamiento almacena la información sobre las redes conectadas y remotas. Las redes conectadas está directamente adjuntas a una de las interfaces del router. Estas interfaces son los gateways para los hosts en las diferentes redes locales. Las redes remotas son redes que no están conectadas directamente al router. Las rutas a esas redes se pueden configurar manualmente con un protocolo estático por el administrador de red o aprendidas automáticamente utilizando protocolos de enrutamiento dinámico.

5.4 Protocolos de enrutamiento.

5.4.1 Algoritmos de Enrutamiento Estático.

Los algoritmos de enrutamiento estático no tienen en cuenta el estado de la subred al tomar las decisiones de encaminamiento. Las tablas de encaminamiento de los nodos se configuran de forma manual y permanecen inalterables hasta que no se vuelve a actuar sobre ellas. Por tanto, la adaptación en tiempo real a los cambios de las condiciones de la red es nula.

El cálculo de la ruta óptima es también off-line por lo que no importa ni la complejidad del algoritmo ni el tiempo requerido para su convergencia. Ejemplo: algoritmo de Dijkstra.

 © DGAPA-PAPIME

Estos algoritmos son rígidos, rápidos y de diseño simple, sin embargo son los que peores decisiones toman en general.

5.4.1.1 Camino más corto.

La identificación de la mejor ruta de un router implica la evaluación de múltiples rutas hacia la misma red de destino y la selección de la ruta óptima o "la más corta" para llegar a esa red.

Cuando existen múltiples rutas para llegar a la misma red, cada ruta usa una interfaz de salida diferente en el router para llegar a esa red. La mejor ruta es elegida por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Algunos protocolos de enrutamiento, como RIP, usan un conteo de saltos simple, que consiste en el número de routers entre un router y la red de destino. Otros protocolos de enrutamiento, como OSPF, determinan la ruta más corta al analizar el ancho de banda de los enlaces y al utilizar dichos enlaces con el ancho de banda más rápido desde un router hacia la red de destino.

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. Una métrica es un valor cuantitativo que se usa para medir la distancia hacia una ruta determinada. La mejor ruta a una red es la ruta con la métrica más baja. Por ejemplo, un router preferirá una ruta que se encuentra a 5 saltos antes que una ruta que se encuentra a 10 saltos.

5.4.1.2 Camino múltiple o bifurcado.

Hasta ahora se ha supuesto tácitamente que existe un solo "mejor" camino entre cualquier par de nodos y que todo el tráfico entre ellos deberá utilizarlo. En muchas redes hay varios caminos entre pares de nodos, que son casi igualmente buenos. Con frecuencia, se puede obtener un mejor rendimiento al dividir el tráfico entre varios caminos, para reducir la carga en cada una de las líneas de comunicación. La técnica de utilizar encaminamiento múltiple entre un sólo par de nodos se conoce como encaminamiento de camino múltiple, o algunas veces encaminamiento bifurcado.

El encaminamiento de camino múltiple se aplica tanto en subredes con datagramas, como en subredes con circuitos virtuales. Para el caso de subredes con datagramas virtuales (en beneficio de los diferentes usuarios) se lleva a cabo en forma independiente., cuando un paquete llega a un IMP para su reexpedición, se hace una selección entre varias alternativas, para ese paquete en particular, en forma independiente de las selecciones que se hicieron para otros paquetes que se dirigieron al mismo destino, en el pasado. Para subredes con circuitos virtuales, cada vez que se establece un circuito virtual, se selecciona una ruta, pero el encaminamiento para los diferentes circuitos

5.4.1.3 Centralizado.

Los algoritmos de encaminamiento anteriores necesitan tener información acerca de la topología y el tráfico de la red, para poder ' tomar las mejores decisiones. Si la topología es de característica estática y el tráfico, cambia muy rara vez, la construcción de las tablas de encaminamiento es muy sencilla, y se realiza una sola vez, fuera de línea, cargándolas en los IMP (procesador de mensajes de interfaz). Sin embargo, si los IMP y las líneas se desactivan y después se restablecen, o bien, si el tráfico varia violentamente durante todo el día, se

necesitará algún mecanismo para adaptar las tablas a las circunstancias que imperan en ese momento. Sin embargo se pueden construcción las tablas de encaminamiento en un lugar central. A continuación se verá la manera cómo este trabajo puede realizarse en una forma total o parcialmente descentralizada.

Cuando se utiliza un encaminamiento centralizado, en alguna parte de la red hay un RCC (Centro de control del enrutamiento). Periódicamente, cada IMP transmítela información de su estado al RCC (por ejemplo, una lista de sus vecinos activos, las longitudes actuales de las colas de espera, la cantidad de tráfico procesado por línea desde el último informe, etc.) El RCC recoge toda esta información, y después, con base en el conocimiento total de la red completa, calcula las rutas óptimas de todos los IMP a cada uno de los IMP restantes, utilizando por ejemplo el algoritmo del camino más corto, que se estudió anteriormente. A partir de esta información puede construir nuevas tablas de encaminamiento y distribuirlas a todos los IMP.

El encaminamiento centralizado parece atractivo a primera vista: dado que el RCC tiene la información completa, y puede tomar decisiones perfectas. Otra ventaja es que alivia a los IMP de la carga de calcular el encaminamiento.

Sin embargo, el encaminamiento centralizado también tiene algunos problemas serios, si no es que fatales, inconvenientes. Por una razón, si la subred se tiene que adaptar a un tráfico variable, el cálculo del encaminamiento tendrá que efectuarse con bastante frecuencia. Para una red grande, este cálculo tomará muchos segundos, incluso cuando se tenga un CPU razonablemente rápido. Si el propósito de correr el algoritmo consiste en adaptarlo a cambios en la topología de la red; y no tanto a cambios en el tráfico, podría ser adecuado si se llegara a ejecutar cada minuto aproximadamente, dependiendo de cuán estable sea dicha topología.

La vulnerabilidad del RCC resulta ser un problema más serio; si éste se desactiva o llega a aislarse, debido a fallos en las líneas, la subred estará súbitamente en una situación problemática. Una solución consiste en tener una segunda máquina disponible como respaldo, pero esto conlleva a desperdiciar un ordenador de gran tamaño. También, se necesitará establecer un método de arbitraje para tener la seguridad de que el RCC primario y el de respaldo no lleguen a entrar en conflicto para saber quién es el jefe.

5.4.1.4 Inundación.

La inundación es un caso extremo del encaminamiento aislado, en el cual cada paquete que llega se transmite en todas las líneas de salida, exceptuando aquélla por el que llega. Obviamente, con la inundación se genera un número considerable de paquetes duplicados; de hecho, un número infinito, a menos que se tomen algunas medidas para amortiguar el proceso. Una de tales medidas consiste en tener un contador de saltos contenido en la cabecera de cada uno de los paquetes, el cual se decrementa con cada salto que se lleve a cabo, y el paquete se desecha en el momento en que el contador alcance el valor de cero. Idealmente, el contador de saltos deberá iniciarse con un valor correspondiente a la longitud del camino que existe entre el origen y el destino. Si el emisor no conoce la longitud del camino, puede iniciar el contador con el valor del peor caso, es decir, el valor del diámetro completo de la subred.

Una técnica alternativa para retener la inundación consiste en hacer que el IMP de origen ponga un número de secuencia en cada paquete que recibe de su hostal. De esta forma,

 © DGAPA-PAPIME

cada IMP necesitará una lista por IMP origen, indicando qué números de secuencia originados en la fuente ya fueron vistos. Para evitar que la lista crezca sin límite, cada lista deberá aumentarse por medio de un contador, k, indicando que todos los números de secuencia hasta k ya fueron vistos. En el momento en que un paquete llega, resulta muy fácil verificar si éste es un duplicado; si es el caso, se desechará.

En varias aplicaciones, la inundación no resulta ser muy práctica, pero sí tiene algunos usos importantes. Por ejemplo, en aplicaciones militares, en donde un gran número de IMP puede desintegrarse en pedazos en cualquier instante, la robustez de la inundación es una característica altamente deseable. En aplicaciones de bases de datos distribuidas, algunas veces se necesita actualizar todas las bases de datos en forma concurrente, en cuyo caso la inundación puede ser de gran utilidad. Una tercera forma posible de utilización de la inundación es como un sistema de medición contra el cual otros algoritmos de encaminamiento se pueden comparar. La inundación siempre escoge el camino más corto, porque selecciona todos los posibles caminos en paralelo, por consiguiente, ningún otro algoritmo puede producir un retardo más corto

5.4.2 Algoritmos de Enrutamiento Adaptativo.

5.4.2.1 Enrutamiento Distribuido.

El encaminamiento mediante algoritmos distribuidos constituye el prototipo de modelo de encaminamiento adaptativo. Los algoritmos se ejecutan en los nodos de la red con los últimos datos que han recibido sobre su estado y convergen rápidamente optimizando sus nuevas rutas.

El resultado es que las tablas de encaminamiento se adaptan automáticamente a los cambios de la red y a las sobrecargas de tráfico. A cambio, los algoritmos tienen una mayor complejidad. Existen dos tipos principales de algoritmos de encaminamiento adaptativo distribuido.

5.4.2.2 Enrutamiento Óptimo.

5.4.2.3 Enrutamiento basado en Flujo.

Este algoritmo toma en cuenta la cantidad de tráfico medio que soportan las líneas, y en base a esta información intenta optimizar el conjunto de las rutas para utilizar el camino menos congestionado en cada caso. Para aplicarlo se ha de conocer bastante bien el tráfico, y éste ha de ser muy regular. Se pueden aplicar algoritmos relativamente sofisticados ya que el cálculo de rutas se hace offline y se carga en el router después. Este algoritmo sólo se aplica en algunos casos de routing estático. Puede ser útil para diseñar la topología de una red. Por ejemplo, si se conectan una serie de oficinas y se dispone de la matriz de tráfico previsto entre cada par de oficinas se pueden plantear diversas topologías y estudiar cuál es la más adecuada.

5.4.2.4 Enrutamiento por difusión.

© DGAPA-PAPIME

En algunas aplicaciones, los *host* necesitan enviar mensajes a varios otros *host* o a todos los demás. Por ejemplo, el servicio de distribución de informes ambientales, la actualización de los precios de la bolsa o los programas de radio en vivo podrían funcionar mejor difundiéndolos a todas las máquinas y dejando que aquellas interesadas lean los datos. El envío simultáneo de un paquete a todos los destinos se llama *difusión.* Hay varios métodos para llevarlo a cabo.

Un método de difusión que no requiere características especiales de la red es que el origen simplemente envíe copias del paquete a todos los destinos. El método no sólo desperdicia ancho de banda, sino que también requiere que el origen tenga una lista completa de todos los destinos. En la práctica, este es el método menos deseable.

5.4.3 Aleatorio.

5.4.4 Híbridos.

En el enrutamiento hibrido se pueden tener combinaciones de distintos tipos de algoritmos de enrutamiento en un mismo router, en redes grandes o complejas, en general los routers contienen una combinación de algoritmos estáticos y dinámicos.

5.5 Control de la congestión.

La congestión de redes es el fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede cursar. El control de la congestión comprende todo un conjunto de técnicas para detectar y corregir los problemas que surgen cuando no todo el tráfico de una red puede ser cursado.

Las soluciones para el problema de la congestión se pueden dividir en dos clases: Open Loop y Closed Loop. Con open loop se tratan de resolver el problema con un buen diseño. Usan algoritmos para decidir cuando aceptar más paquetes, cuando descartarlos, etc. Pero no utilizan el actual estado de la red. Con closed loop La solución en este caso se basa en la retroalimentación de la línea.

Por lo general tienen tres partes:
1. Monitorean el sistema para detectar cuándo y dónde ocurre la congestión.
2. Se pasa esta información hacia donde se puedan tomar acciones.
3. Se ajustan los parámetros de operación del sistema para corregir los problemas.

5.6 Servicios orientados a conexión.

Los protocolos orientados a la conexión, como TCP, requieren el intercambio del control de datos para establecer la conexión así como también los campos adicionales en el encabezado de la PDU.

5.7 Servicios no orientados a conexión.

© DGAPA-PAPIME

Un ejemplo de comunicación sin conexión es enviar una carta a alguien sin notificar al receptor con anticipación. Como se muestra en la figura, el servicio postal aún lleva la carta y la entrega al receptor. Las comunicaciones de datos sin conexión funcionan en base al mismo principio. Los paquetes IP se envían sin notificar al host final que están llegando.

Como IP trabaja sin conexión, no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que los paquetes sean enviados, ni requiere campos adicionales en el encabezado de la PDU para mantener esta conexión. Este proceso reduce en gran medida la sobrecarga del IP.

Sin embargo, la entrega del paquete sin conexión puede hacer que los paquetes lleguen a destino fuera de secuencia. Si los paquetes que no funcionan o están perdidos crean problemas para la aplicación que usa los datos, luego los servicios de las capas superiores tendrán que resolver estas cuestiones.

5.8 Ruteadores.

El router es una computadora diseñada para fines especiales que desempeña una función clave en el funcionamiento de cualquier red de datos. Los routers son los principales responsables de la interconexión de redes por medio de: la determinación de la mejor ruta para enviar paquetes el envío de paquetes a su destino.

Los routers envían paquetes al aprender sobre redes remotas y al mantener la información de enrutamiento. El router es la unión o intersección que conecta múltiples redes IP. La principal decisión de envío de los routers se basa en la información de Capa 3, la dirección IP de destino.

La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla de enrutamiento. La tabla de enrutamiento determinará finalmente la interfaz de salida para enviar el paquete y el router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.

6. Capa de transporte

6.1 Servicios de la capa transporte.

6.2 Fragmentación de paquetes.

6.3 Secuenciamiento.

6.4 Reensamble de paquetes.

6.5 Control de flujo.

6.5.1 Stop-wait.

 © DGAPA-PAPIME

9. Capa de aplicación

9.1 HTTP.

Protocolo de transferencia de hipertexto (HTTP) es un protocolo común que regula la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. El protocolo HTTP se basa en otros protocolos para regir de qué manera se transportan los mensajes entre el cliente y el servidor

Cuando se escribe una dirección Web (o URL) en un explorador de Internet, el explorador establece una conexión con el servicio Web del servidor que utiliza el protocolo HTTP. URL (o Localizador uniforme de recursos) y URI (Identificador uniforme de recursos) son los nombres que la mayoría de las personas asocian con las direcciones Web.

Los exploradores Web son las aplicaciones de cliente que utilizan nuestras computadoras para conectarse con la World Wide Web y para acceder a los recursos almacenados en un servidor Web. Al igual que con la mayoría de los procesos de servidores, el servidor Web funciona como un servicio básico y genera diferentes tipos de archivos disponibles.

Para acceder al contenido, los clientes Web realizan conexiones al servidor y solicitan los recursos deseados. El servidor responde con los recursos y, una vez recibidos, el explorador interpreta los datos y los presenta al usuario.

Los exploradores pueden interpretar y presentar muchos tipos de datos, como texto sin formato o Lenguaje de marcado de hipertexto (HTML, el lenguaje que se utiliza para construir una página Web). Otros tipos de datos, sin embargo, requieren de otro servicio o programa. Generalmente se los conoce como plug-ins o complementos. Para ayudar al explorador a determinar qué tipo de archivo está recibiendo, el servidor especifica qué clase de datos contiene el archivo.

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

HTTP especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador Web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página Web y envía los tipos de mensajes que el servidor utiliza para responder. Los tres tipos de mensajes más comunes son GET, POST y PUT.

GET es una solicitud de datos del cliente. Un explorador Web envía el mensaje GET para solicitar las páginas desde un servidor Web. Como se muestra en la figura, una vez que el servidor recibe la solicitud GET , responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje solo, cuyo cuerpo puede ser el archivo solicitado, un mensaje de error o alguna otra información.

POST y PUT se utilizan para enviar mensajes que cargan los datos al servidor Web. Por ejemplo, cuando el usuario ingresa datos en un formulario incorporado en una página Web, POST incluye los datos en el mensaje enviado al servidor. PUT carga los recursos o el contenido al servidor Web.

Aunque es muy flexible, HTTP no es un protocolo seguro. Los mensajes POST cargan información al servidor en un texto sin formato que puede ser interceptado y leído. De forma similar, las respuestas del servidor, generalmente páginas HTML, también son descifradas.

9.2 SMTP.

El E-mail, el servidor de red más conocido, ha revolucionado la manera en que nos comunicamos, por su simpleza y velocidad. Inclusive para ejecutarse en una computadora o en otro dispositivo, los e-mails requieren de diversos servicios y aplicaciones. Dos ejemplos de protocolos de capa de aplicación son Protocolo de oficina de correos (POP) y Protocolo simple de transferencia de correo (SMTP).

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres digitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

9.3 TELNET.

Mucho antes de que existieran las computadoras de escritorio con interfaces gráficas sofisticadas, las personas utilizaban sistemas basados en textos que eran simplemente terminales conectadas físicamente a una computadora central. Una vez que las redes estuvieran disponibles, las personas necesitaban acceder en forma remota a los sistemas informáticos de la misma manera en que lo hacían con las terminales conectadas en forma directa.

 © DGAPA-PAPIME

Telnet se desarrolló para satisfacer esta necesidad. Telnet se remonta a principios de la década de los setenta y se encuentra entre los servicios y protocolos de capa de aplicación más antiguo dentro del grupo TCP/IP. Telnet proporciona un método estándar de emulación de dispositivos de terminal basados en texto en la red de datos. El protocolo y el software del cliente que implementa el protocolo comúnmente se definen como Telnet.

Y como consecuencia, una conexión que utiliza Telnet se llama Sesión o conexión de terminal virtual (VTY). En lugar de utilizar un dispositivo físico para conectar al servidor, Telnet utiliza software para crear un dispositivo virtual que proporciona las mismas funciones que una sesión terminal con acceso a la Interfaz de línea de comandos (CLI) del servidor.

Para admitir conexiones al cliente Telnet, el servidor ejecuta un servicio llamado daemon de Telnet. Se establece una conexión de terminal virtual desde un dispositivo final utilizando una aplicación del cliente Telnet. La mayoría de los sistemas operativos incluye un cliente de Telnet de la capa de aplicación.

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

Telnet es un protocolo cliente-servidor y especifica cómo se establece y se termina una sesión VTY. Además proporciona la sintaxis y el orden de los comandos utilizados para iniciar la sesión Telnet, como así también los comandos de control que pueden ejecutarse durante una sesión. Cada comando Telnet consiste en por lo menos dos bytes. El primer byte es un carácter especial denominado Interpretar como comando (IAC). Como su nombre lo indica, el IAC define el byte siguiente como un comando en lugar de un texto.

Algunos de los comandos del protocolo Telnet de muestra son:

- Are You There (AYT): Permite al usuario solicitar que aparezca algo en la pantalla del terminal para indiciar que la sesión VTY está activa.

- Erase Line (EL): Elimina todo el texto de la línea actual.

- Interrupt Process (IP): Suspende, interrumpe, aborta o termina el proceso al cual se conectó la terminal virtual. Por ejemplo, si un usuario inició un programa en el servidor Telnet por medio de VTY, puede enviar un comando IP para detener el programa.

Aunque el protocolo Telnet admite autenticación de usuario, no admite el transporte de datos encriptados.

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

 © DGAPA-PAPIME

9.4 SNMP.

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Existen tres versiones, sin embargo, las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales.

La última versión SNMPv3 posee algunos cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados;
- Agentes;
- Sistemas administradores de red (NMS's).

Un dispositivo administrado en este caso es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

9.5 FTP.

FTP (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos) El protocolo de transferencia de archivos (FTP) es otro protocolo de la capa de aplicación comúnmente utilizado. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y se utiliza para cargar y descargar archivos desde un servidor que ejecuta el daemon FTP (FTPd).

© DGAPA-PAPIME

Para transferir los archivos en forma exitosa, el FTP requiere de dos conexiones entre cliente y servidor: una para comandos y respuestas, otra para la transferencia real de archivos.

El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor.

El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo.

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

9.4 Bibliografía y Mesografía

Mark A. Dye, Rick McDonald y Antoon W.Rufi
Aspectos Básicos de networking. Guía de estudio de CCNA Exploration
2008, Pearson Educación S.A
Cisco Press, Madrid España

Rick Graziani, Allan Johnson
Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration.
2008, Pearson Educación S.A
Cisco Press, Madrid España

Apuntes de Clase de Redes de Datos.
M.C. Ma. Jaquelina López Barrientos
Facultad de Ingeniería, UNAM
2008, México D.F

http://132.248.183.220/tutorial/
http://www.wikipedia.org/
http://www.geocities.com/jcredesii/REDES2-73.htm
http://mx.geocities.com/experimental_h/dr_01.html
http://www.monografias.com/trabajos-pdf/enrutamiento-redes-datos/enrutamiento-redes-datos.pdf