



**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

A LOS ASISTENTES A LOS CURSOS

Las autoridades de la Facultad de Ingeniería, por conducto del jefe de la División de Educación Continua, otorgan una constancia de asistencia a quienes cumplan con los requisitos establecidos para cada curso.

El control de asistencia se llevará a cabo a través de la persona que le entregó las notas. Las inasistencias serán computadas por las autoridades de la División, con el fin de entregarle constancia solamente a los alumnos que tengan un mínimo de 80% de asistencias.

Pedimos a los asistentes recoger su constancia el día de la clausura. Estas se retendrán por el período de un año, pasado este tiempo la DECFI no se hará responsable de este documento.

Se recomienda a los asistentes participar activamente con sus ideas y experiencias, pues los cursos que ofrece la División están planeados para que los profesores expongan una tesis, pero sobre todo, para que coordinen las opiniones de todos los interesados, constituyendo verdaderos seminarios.

Es muy importante que todos los asistentes llenen y entreguen su hoja de inscripción al inicio del curso, información que servirá para integrar un directorio de asistentes, que se entregará oportunamente.

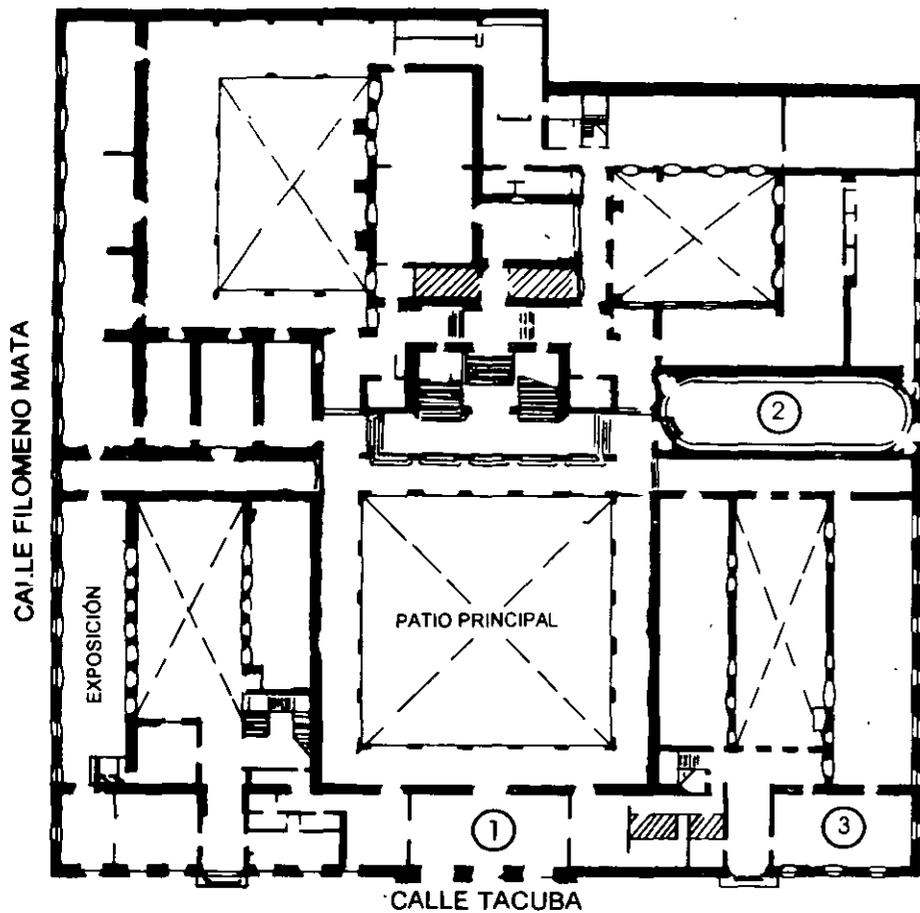
Con el objeto de mejorar los servicios que la División de Educación Continua ofrece, al final del curso deberán entregar la evaluación a través de un cuestionario diseñado para emitir juicios anónimos.

Se recomienda llenar dicha evaluación conforme los profesores impartan sus clases, a efecto de no llenar en la última sesión las evaluaciones y con esto sean más fehacientes sus apreciaciones.

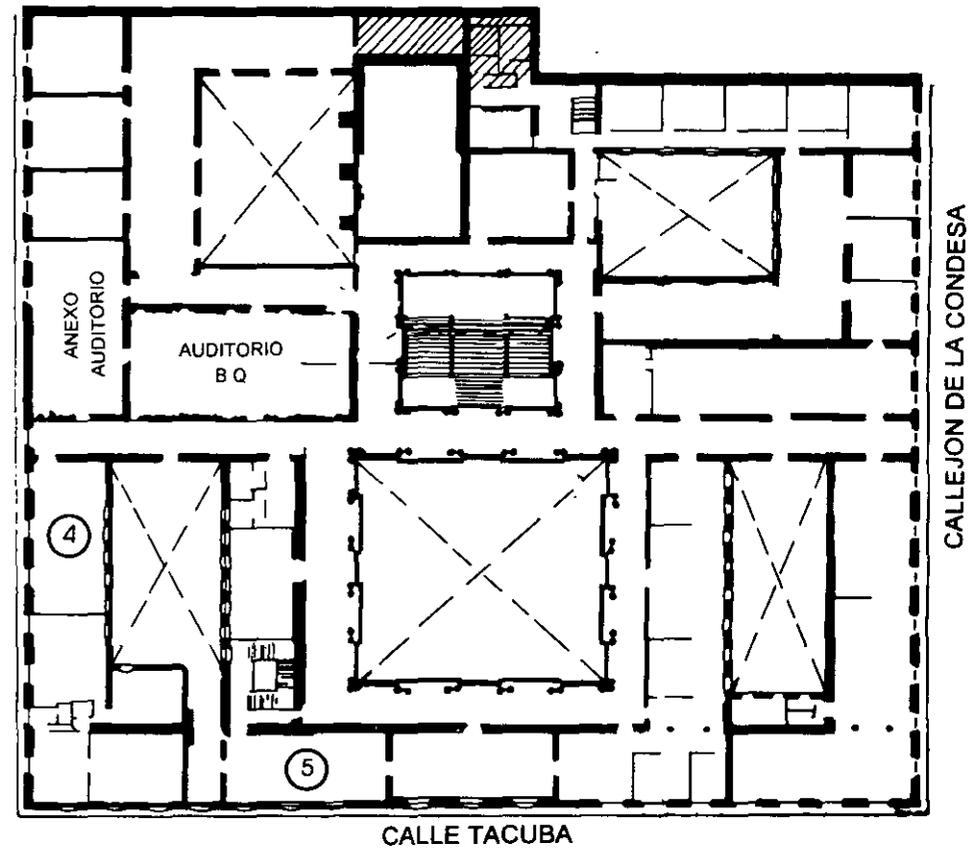
Atentamente

División de Educación Continua.

PALACIO DE MINERIA

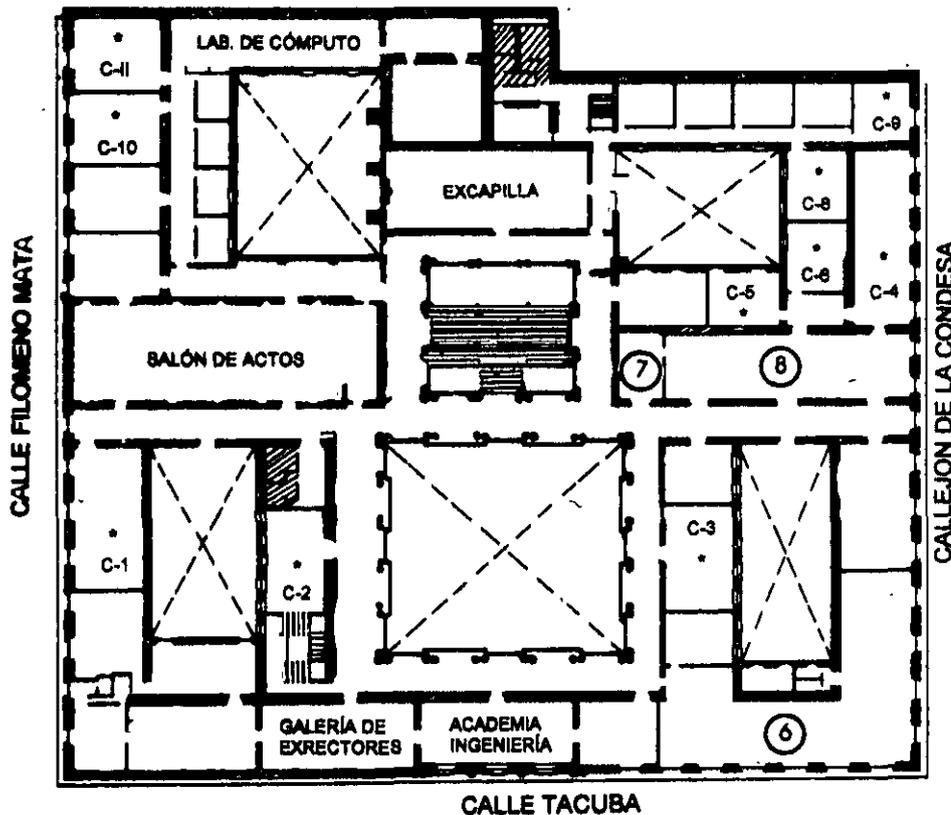


PLANTA BAJA



MEZZANINNE

PALACIO DE MINERÍA



GUÍA DE LOCALIZACIÓN

1. ACCESO
2. BIBLIOTECA HISTÓRICA
3. LIBRERÍA UNAM
4. CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN "ING. BRUNO MASCANZONI"
5. PROGRAMA DE APOYO A LA TITULACIÓN
6. OFICINAS GENERALES
7. ENTREGA DE MATERIAL Y CONTROL DE ASISTENCIA
8. SALA DE DESCANSO

SANITARIOS

* AULAS

1er. PISO



DIVISIÓN DE EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA U.N.A.M.
CURSOS ABIERTOS

DIVISIÓN DE EDUCACIÓN CONTINUA





**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

Diplomado en redes WAN

**Redes de Computadoras
(CA109)**

Apuntes

Versión 1.0 23/02/1998

Ing. Marco Antonio López Meléndez

Parte 1

Diplomado en redes WAN

Redes de Computadoras
(CA109)

Apuntes

Versión 1.0 23/02/1998

Ing. Marco Antonio López Meléndez

Parte 1

Prefacio

Introducción:

Las redes de computadoras han tenido un desarrollo muy importante en los últimos años. El nuevo mercado se ha enfocado hacia las telecomunicaciones y las redes de datos, es por ello que se debe contar con personal altamente capacitado para dar soporte a la infraestructura de red y proporcionar soluciones integrales a los problemas de comunicación que se presentan hoy en día.

Propósito:

Este documento tiene como finalidad proporcionar las bases necesarias para la comprensión de los términos de las redes de computadoras.

Dirigido a:

Ingenieros en computación, Licenciados en informática y área afines interesados en las redes de computadoras.

Continúa en la siguiente página.

Prefacio *(continuación)*

Documentos

- Relacionados** Networking Standars. A guide to OSI, ISDN, LAN and MAN Standars.
Stallings, William
Ed. Addison Wesley
- Ethernet Networks
Held, Gilbert
Ed. Addison Wesley
- Networking the Enterprise.
Baker, Richard H.
Ed. Mc Graw Hill
- Redes de Computadoras. Protocolos, Normas e Interfaces.
Black Uyles
Ed. Macrobit
- Implementación de Redes de Area Local.
Bronson, Purdy.
Techonology Training S. de R.L. de C.V.

1 Introducción

1.1 Historia de las redes

Necesidad de las redes

Las redes surgen de la necesidad de compartir recursos de alto costo entre varias personas. En los inicios de las computadoras, los recursos eran de un costo altísimo, el poder de cómputo era uno de los mas valiosos y mas costosos. En los centros de investigación se hacia necesario que todos los investigadores tuvieran acceso a este tipo de recursos y que estos recursos fueran distribuidos en forma tal que no se tuviese un desperdicio de tiempo de procesamiento.

Nacimiento de las redes

Las primeras redes de computadoras que se crearon, eran del tipo centralizado, es decir, un procesador central, el cual tenia el poder de cómputo y las terminales que le enviaban las tareas a realizar al procesador. Estas redes exigían que la conexión se realizara punto a punto.

El desarrollo de la tecnología permitió tener redes que comunicaban computadoras en sitios distantes, este avance obligo a crear protocolos de comunicación entre las computadoras. Estos protocolos eran propietarios de los fabricantes de las maquinas. Aquí es donde se comienza a ver la necesidad de crear de protocolos estándares para comunicar maquinas y redes de diferentes fabricantes y de diferentes tipos.

Propósito:

Este documento tiene como finalidad proporcionar las bases necesarias para la comprensión de los términos de las redes de computadoras.

Continúa en la siguiente página.

1.1 Historia de las redes *(Continuación)*

Historia

En 1973, la Agencia de Investigaciones avanzadas de la Defensa de los Estados Unidos (DARPA) inicio un programa para investigar las técnicas y las tecnologías para la interconexión de redes de diversos tipos. El objetivo era desarrollar protocolos de comunicación los cuales pueden permitir a redes de computadoras comunicarse en forma transparente a través de múltiples redes. Este proyecto fue llamado Internetting project, y el sistema de redes que emergió de estas investigaciones fue conocido como Internet.

El sistema de protocolos desarrollados en el transcurso de esta investigación, dieron forma a lo que después se conocería como la suite del protocolo TCP/IP.

En 1986, la National Science Foundation (NSF) de los E. U. inicio el desarrollo de la NSFNET, la cual provee un servicio de comunicación muy importante para la Internet.

La NASA y el Departamento de Energía de los E.U. contribuyeron con otra parte del canal principal de Internet con la NSINET y ESNET respectivamente. En Europa también hay una gran parte del canal principal de Internet, esta red es conocida como NORDUNET.

Actualmente Internet enlaza computadoras de Universidades, Oficinas Gubernamentales, Instituciones Públicas y Privadas, Centros de investigación, etc.

Durante el curso de la evolución de Internet, particularmente después de 1989, el sistema de Internet comenzó a integrar el soporte para otras suites de protocolos en su estructura de red básica. Se puso énfasis en una red multi-protocolo y en particular en la integración de los protocolos de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) dentro de la arquitectura.

En los década de los 80 se crearon cerca de 100 aplicaciones publicas y comerciales de protocolos de la suite TCP/IP . Durante los comienzos de 1990 también se crearon aplicaciones del protocolo OSI.

1.2 Objetivos de las Redes

Definición de una Red

Una red de computadoras, es un conjunto de computadoras conectadas entre sí, a través de medios de comunicación (líneas telefónicas, cable coaxial, fibra óptica y microondas); que cumplen con ciertos objetivos. Ya que cada red precisa de un estudio completo para determinarlos y esto dependerá de las necesidades del usuario, empresa o compañía.

Lineamientos para dar confiabilidad a una Red

- ◆ **Compartición de Recursos.**- Significa en hacer que todos los programas, información y equipos estén disponibles en cualquier computadora de la red, eso sin importar la ubicación física, tanto del recurso como del usuario.
- ◆ **Confiabilidad.**- Esto quiere decir que la red nos va a dar alternativas múltiples ya sea que un archivo puede duplicarse en dos o tres máquinas, de modo que si una no esta disponible puede tener acceso a otra.
- ◆ **Ahorro de recursos.**- Con la implementación de una red se va a ahorrar dinero, ya que al tener varias computadoras en red se puede compartir una impresora y satisfacer las necesidades del usuario, esto sin tener una impresora para cada computadora. Aquí se puede emplear el dicho de "una para todos y todos para una".
- ◆ **Medio de comunicación.**- Determinar si el medio de comunicación es el adecuado para la transmisión de datos a gran escala
- ◆ **Seguridad.**- Hoy día algo muy importante en lo que se refiere al manejo y manipulación de la información ya que se manejan grandes B.D. y que con la gran Red de Redes (Internet) todos podemos acceder a dicha información por lo tanto se debe tener un total cuidado en su manejo.

2 Clasificación de las Redes

Introducción

Hoy día en la actualidad el desarrollo de la tecnología se esta dando en forma continua, existen numerosas opciones de estructura al planear una red de datos. Por lo que existen diferentes tipos de redes , su clasificación se da por el tipo de propietario y también por su extensión geográfica.

2.1 Clasificación por propietario

Redes Privadas

Son las más comunes, normalmente pertenecen a universidades, bancos y empresas tanto públicas como privadas. Su característica es de que sólo un grupo reducido de personas tienen acceso a la red (los propietarios, los socios, empleados o estudiantes).

Redes Comerciales

Rentan sus servicios a personas interesadas en tener acceso a la información de la red. En este tipo de redes pueden pertenecer revistas científicas, agencias de noticias y otros grupos que deseen vender sus productos.

Redes Públicas

Son administradas generalmente por el gobierno en países subdesarrollados y por grandes consorcios en países capitalistas. La infraestructura que se da para éstas redes es por medio de la red telefónica, ofreciendo sus servicios a cualquier organización que se suscriba a la red.

Existen tres tipos de clasificación geográfica, WAN (Wide Area Network), MAN (Metropolitan Area Network) y LAN (Local Area Network). Sin embargo, este tipo de clasificación no tiene una definición específica, se basa en concepciones geográficas.

2.2 Clasificación por extensión geográfica

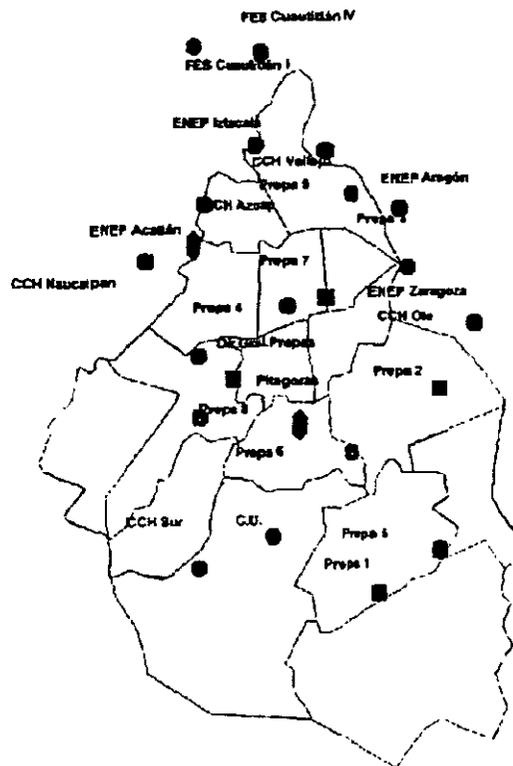
Existen tres tipos de clasificación geográfica, WAN (Wide Area Network), MAN (Metropolitan Area Network) y LAN (Local Area Network). Sin embargo, este tipo de clasificación no tiene una definición específica, se basa en concepciones geográficas.

Redes de Area Metropolitana

Las redes de Área Metropolitana MAN (Metropolitan Area Networks). Son redes híbridas, es decir, redes que conectan PC's, mini y macrocomputadoras. Se diferencian de las redes WAN ya que son equipos tan sofisticados y por lo tanto no transmiten a distancias muy grandes.

Un ejemplo de este tipo de red es como lo muestra la figura 1, donde se tienen conectadas a la red las diferentes dependencias de la UNAM dentro del área metropolitana. Aquí se muestra la comunicación entre los diferentes campus dentro de una misma región utilizando enlaces de microondas y de RDI punto a punto. Este es el medio para la comunicación entre dichas dependencias.

Red Metropolitana de las diversas dependencias de la UNAM.



Continúa en la siguiente página.

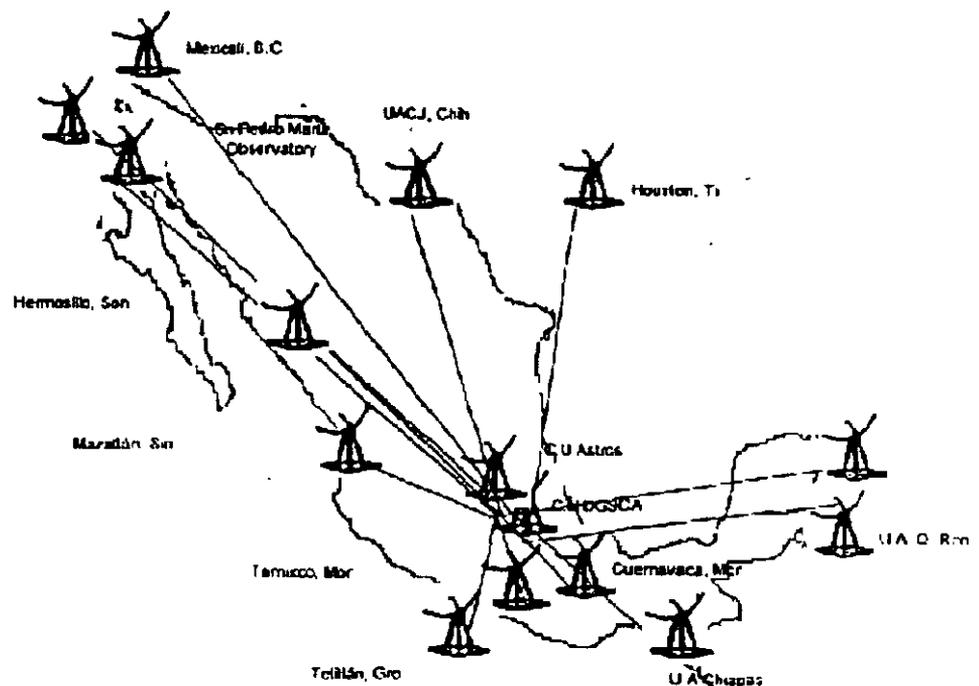
2.2 Clasificación por extensión geográfica (Continuación)

Redes de Area Amplia

Este tipo de redes surge entre 1960 y 1970. Los científicos e ingenieros idearon maneras de construir redes que conectaran varias computadoras a través de grandes distancias geográficas, llamadas *Redes de área amplia* (Wide Area Networks, WAN) o redes de trayectos largos (long-haul networks). Este tipo de tecnología difiere de un conjunto de líneas de transmisión desarticuladas ya que incluyen una computadora adicional con propósitos especiales en cada sitio que se conecta a las líneas de transmisión y mantiene la comunicación independiente de las computadoras que utilizan la WAN.

Para poder comprender como puede ser útil una WAN, podemos poner de ejemplo la propia UNAM, en donde para la comunicación entre los diferentes campus en regiones alejadas del país se utilizan enlaces vía satélite cuya capacidad de transmisión es pequeña y permite la comunicación en lugares en donde por la ubicación geográfica no existen otros medios de comunicación. Tal es el caso del enlace entre la estación "Puerto Morelos" del Instituto de Ciencias del Mar y Limnología en el estado de Quintana Roo, del enlace con el "Observatorio Astronómico Nacional" a cargo del Instituto de Astronomía y otras más, esto se puede apreciar mejor observando la 0

Red de Area Amplia con enlaces satelitales con diferentes dependencias en el interior de la República



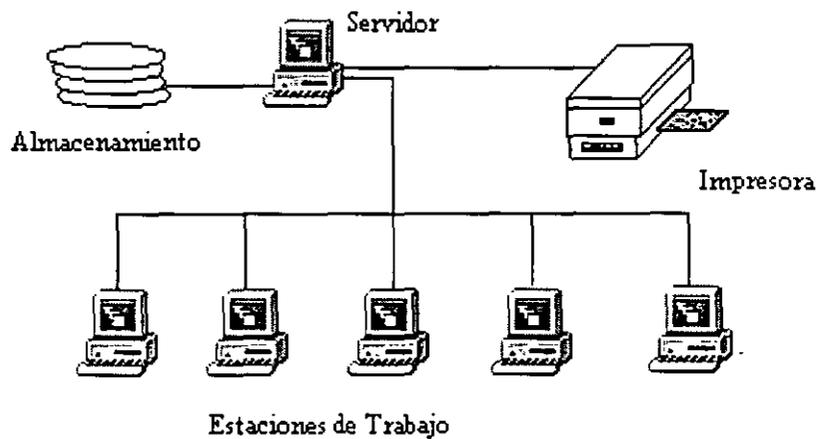
Continúa en la siguiente página.

2.2 Clasificación por extensión geográfica (Continuación)

Redes de Area Local

La necesidad de mejorar la comunicación telefónica hace que surja una tecnología que hoy día es muy importante para cualquier empresa que quiera estar a la vanguardia de las comunicaciones y es la Red de Area Local (Local Area Network). Se le llama así ya que se usa en distancias cortas para conectar las computadoras, la longitud que debe de tener es por no más de 3Km de cable, dichas computadoras interoperan y permiten al usuario compartir recursos. Ver 0. El aumentar la distancia de una LAN puede dar como resultado un funcionamiento deficiente.

Ejemplo de una Red de Area Local



Continúa en la siguiente página.

2.2 Clasificación por extensión geográfica (Continuación)

Historia de las redes de Area Local

El trabajo más importante sobre LAN's para muchos fue el realizado por Xerox Corporation en el Centro de Desarrollo de Palo Alto (PARC) a finales de la década de 1970 y comienzo de 1980.

En PARC, se concibieron y desarrollaron, hasta el punto de obtener un producto comercial, un conjunto de estándares y protocolos llamados Ethernet. Casi al mismo tiempo, usuarios trabajando independientemente en Datapoint Corporation desarrollaron un estándar llamado ARCNet.

Más tarde IBM desarrolló una de las tres tecnologías de red más utilizadas actualmente, Token Ring.

En cada definición de LAN se mezclaban tipos específicos de cable de cobre, conectores específicos, una configuración física y ciertas funciones de software. Pero como el gobierno y la industria exigían flexibilidad, se amplió el conjunto de especificaciones para cada tipo de red y así incluir diferentes tipos de cables, configuraciones y protocolos.

Hoy día se pueden mezclar un conjunto de hardware y software para crear una red personalizada y aún estar dentro de las especificaciones de red soportadas por productos de diferentes compañías.

Características de las LAN

- ◆ Medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipos; independientemente del lugar físico donde se encuentre el usuario o el dispositivo.
 - ◆ Velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo.
 - ◆ Distancia entre ordenadores relativamente corta, como ya se había mencionado anteriormente es de aproximadamente 3Km.
 - ◆ Utilización de cables de conexión
 - ◆ Sistema de detección y corrección de errores de transmisión
 - ◆ Flexibilidad ya que el usuario administra y controla su propio sistema
 - ◆ Comunicación directa del usuario con sus compañeros de trabajo, reemplazando el teléfono.
-

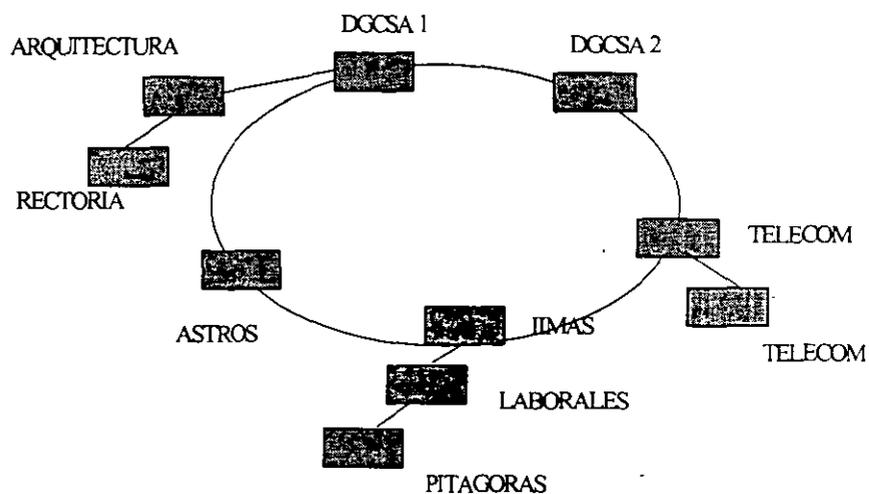
Continúa en la siguiente página.

2.2 Clasificación por extensión geográfica (Continuación)

RedUnam

La 0 nos ilustra un ejemplo verdadero de lo que puede ser una conexión de Redes locales en forma general. En esta figura se muestra a la red UNAM como un conjunto de redes de área local, en donde se observan ruteadores que se encuentran dentro del anillo (Backbone) así como aquellos que no están directamente conectados a este pero que son considerados importantes dentro de la red. Cada uno de éstos contiene las LAN's de las diferentes facultades, así como de algunas dependencias que tienen sus instalaciones dentro del Campus de Ciudad Universitaria y que en su mayoría están conectadas a las ruteadores vía fibra óptica. Estas redes utilizan las topologías más empleadas que son variantes de Ethernet.

**Anillo central
de la Red
UNAM**



2.3 Clasificación por topología

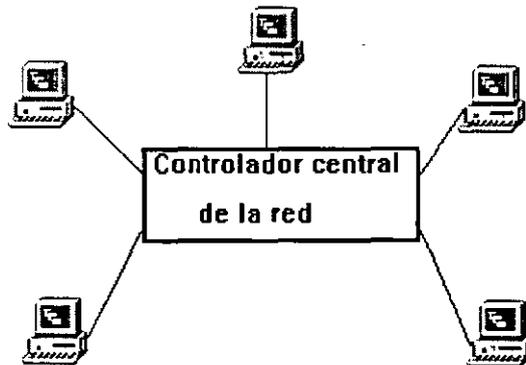
Topología

La topología es el ordenamiento de la estructura que consta de las rutas e interruptores, que proveen las comunicaciones interconectando nodos de la red.

Topología estrella

Una de las principales razones de su empleo es histórica. La topología estrella consiste de un elemento de nodo central, al cual se le conectan todos los dispositivos de comunicación de datos. Cuando se quiere una comunicación entre los dispositivos, el servidor central pone los interruptores adecuados, pareciendo ser entre los mismos un enlace punto a punto. La red tipo estrella se utilizó a lo largo de los años 70's por que resultó fácil de controlar, su software no es complicado y su flujo de tráfico no es sencillo emana del núcleo de la estrella, que es el nodo central, hacia el nodo en particular.

Topología Estrella



Continúa en la siguiente página.

2.3 Clasificación por topología (continuación)

Topología Anillo

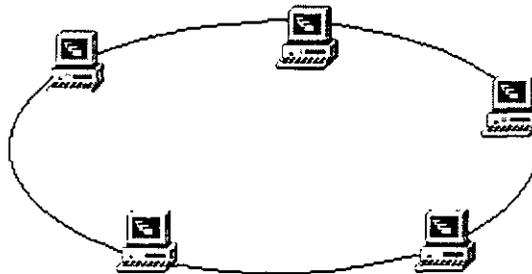
En la topología anillo se enlazan repetidores punto a punto, hasta formar entre ellos un círculo imaginario y cada uno de ellos se conectan los dispositivos, el flujo se hace entre cada enlace de los repetidores y de estos a los dispositivos.

El sistema anillo consiste de un número de repetidores, en el que cada repetidor se conecta a otros dos con un enlace unidireccional hasta que se forma una ruta cerrada. Los datos se transmiten secuencialmente, bit a bit, y cada repetidor los regenera y los retransmite.

Para que el sistema se comporte como una red de comunicaciones, requiere tres funciones: inserción del mensaje, recepción del mensaje y el borrado del mensaje. Para la inserción del mensaje en el canal de comunicaciones y transmisión, se encarga el repetidor. En la recepción del mensaje, como la dirección del destinatario, el repetidor verifica si le corresponde, si es afirmativo lo apropia de lo contrario lo retransmite. Con respecto al borrado del mensaje se tiene dos criterios: uno es que el destinatario después de copiarlo se encargue de borrarlo y el segundo consiste en que el transmisor después de dar una vuelta lo borre, de esta manera se puede hacer que varias estaciones puedan copiar el mensaje. Fig.6

El más grande beneficio de LAN's con topología anillo es que son a base de enlaces de comunicación punto a punto. También representa un beneficio que cada repetidor regenere y retransmite cada bit ya que se logra un mayor grado de seguridad de transmisión correctamente. Por último, en ciertas condiciones se alcanzan tasas altas de *throughput* (datos procesados efectivos), son bastante raros los embotellamientos.

Topología Anillo



Problemas de la Topología de Anillo

Los problemas potenciales que presenta son: vulnerabilidad del cable, falla del repetidor y un estudio más detallado al agregar nuevos repetidores. La vulnerabilidad del cable se presenta cuando hay una ruptura de algún enlace lo que provoca que se caiga el sistema. Cada componente sólo ha de llevar a cabo una serie de tareas muy sencillas: Aceptar los datos, enviarlos al nodo conectado al anillo o retransmitirlos al próximo componente del mismo.

Con respecto a la falla del repetidor, sucede cuando los datos no son transmitidos correctamente y por tanto, también ocasiona una caída del sistema. Agregar nuevos repetidores es problemático porque necesita un buen estudio de los repetidores que están juntos donde se quiere agregar.

Continúa en la siguiente página

2.3 Clasificación por topología (continuación)

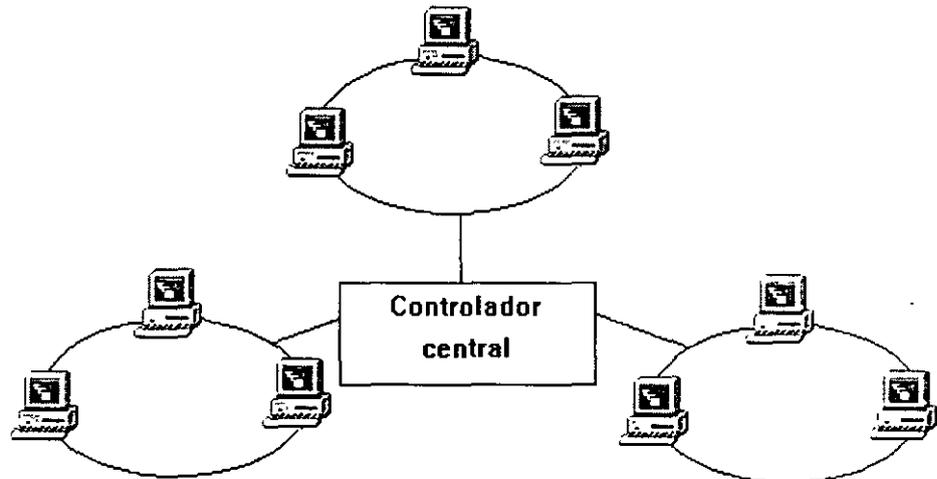
Topología

Anillo-Estrella

Una modificación a la topología anillo es la combinación anillo-estrella. Consiste básicamente en tener concentrados todos los enlaces, permitiendo tener interconexión de repetidores. Esto permite que cuando existe una falla de algún cable sea más fácil localizarlo y después repararlo, además en ese momento se puede utilizar otros enlaces que se tenga a los dos repetidores donde se encuentra la falla. Finalmente en esta arquitectura es más fácil agregar repetidores.

Topología

Anillo - Estrella



Continúa en la siguiente página.

2.3 Clasificación por topología (*continuación*)

Topología Bus

Es caracterizada por el uso de un medio de transmisión múltiple acceso. Los dispositivos comparten el medio y solo un dispositivo puede transmitir a la vez.

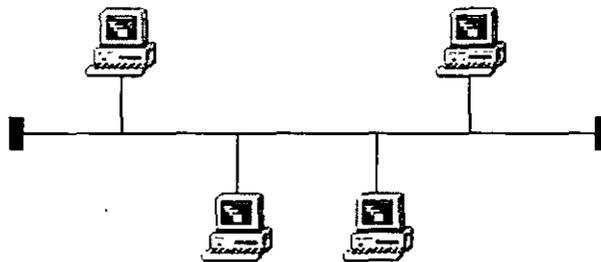
Es relativamente fácil controlar el flujo de tráfico entre los distintos nodos, ya que el bus permite que todas las estaciones reciban todas las transmisiones, es decir, una estación puede difundir, la información a todas las demás.

Dado que varios elementos comparten el mismo canal o trayectoria de datos, solo un elemento puede transmitir su información a la vez, usualmente en forma de paquete de datos, conteniendo éste, su información de acceso a la terminal de trabajo, los demás nodos reciben la información, pero solo el nodo direccionado accesa la información.

Esta topología permite que si un nodo falla el resto continúe operando. La principal limitación de una topología de este tipo es que existe un solo canal de comunicaciones para todos los dispositivos de la red. En consecuencia si el canal de comunicaciones falla, toda la red deja de funcionar.

Algunos fabricantes proporcionan canales completamente redundantes por si falla el canal principal, y otros ofrecen computadoras que permiten rodear un nodo en caso de que falle. Otro inconveniente de esta configuración estriba en la dificultad de aislar las averías de los componentes individuales conectados al bus, la falta de puntos de concentración complica la resolución de este tipo de problemas.

Topología Bus

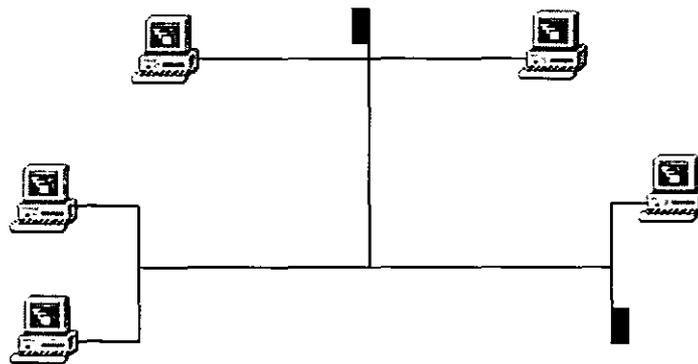


2.3 Clasificación por topología (continuación)

Topología Bus-Arbol

En la topología bus (la bus es un caso especial de la de árbol, con sólo un tronco y sin ramificaciones). También jerárquica (más extendidas). El software que controla la red es relativamente simple, y la topología proporciona un punto de concentración de las tareas de control de errores.

Topología Bus-Arbol



3 Protocolos de Comunicación de Alto Nivel

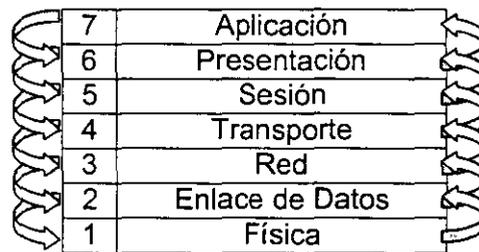
Protocolo

La forma en la cual dos partes de la red se comunican es llamada protocolo, lo cual asegura que cada una de las partes de la comunicación entienda a la otra sin ambigüedad. Un protocolo puede especificar la forma en que los datos son codificados, como puede ser identificado el comienzo y el fin de un mensaje, como las direcciones de los puntos origen y destino son mostradas, y las acciones a tomar si se encuentran errores durante la transmisión. Debe existir un protocolo definido para conectar dos niveles adyacentes, pero la estructura completa de una red puede consistir de muchas especificaciones diferentes.

ISO

La Organización Internacional para Estandarización (ISO, International Standard Organisation) desarrolló un modelo de referencia para la estandarización de los protocolos de red. El modelo es conocido como el modelo de referencia para Interconexión de Sistemas Abiertos, (OSI, Open System Interconnection). OSI es un modelo de siete capas.

Modelo OSI



El modelo OSI sólo se ha podido implantar en algunos sistemas experimentales debido al alto costo que representa su implementación.

Por ejemplo, la capa de red (Capa 3), tendrá especificaciones de protocolo para la capa de enlace de datos (capa 2) y para la capa de transporte (Capa 4). Esto es, a la capa 3 no le interesan las especificaciones para la capa 1 o para la capa 5, dado que esas capas no forman parte del área de interés de la capa. Esto da como consecuencia una flexibilidad considerable cuando las especificaciones son cambiadas o se agregan nuevas opciones.

3.1 Generalidades del Modelo OSI

La capa Física

La capa física esta encargada de la sincronización de los bits y de la identificación de un elemento como un uno o un cero. La unidad de datos de este protocolo es el Bit.

Describe las especificaciones mecánicas y eléctricas para la estructura del cableado. define como serán convertidos los bits en corriente eléctrica, pulsos luminosos o cualquier otra forma física. Determina el método por el cual las ráfagas de bits son enviadas a través de la red.

Proporciona los servicios de enlace que están asociados con la adquisición, mantenimiento y desconexión de circuitos físicos que conforman la ruta de conexión de la comunicación. Maneja tanto la interfaz como los requerimientos procedurales del medio de conexión. Es similar a la interfaz DCE-DTE.

Protocolos Típicos

- ◆ Familia RS-232.
 - ◆ Familia RS-449
 - ◆ Interfaz CCITT X.25
 - ◆ Interfaz CCITT X.21
 - ◆ Serie de Recomendaciones CCITT V
 - ◆ Serie de Recomendaciones CCITT X
 - ◆ IEEE 802.X para redes de área local
-

Ejemplos

Algunas de las especificaciones de medios físicos más utilizadas es el cableado de cobre. En los estándares de cableado de cobre en redes Ethernet existen dos tendencias básicas: cableado coaxial y cable UTP (Unshielded Twisted Pair). El cableado coaxial tiene básicamente dos variantes: el cable coaxial delgado y el cable coaxial grueso

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI *(Continuación)*

Capa de Enlace de Datos

Es la responsable de hacer que el enlace físico sea confiable. Esta encargada de comenzar y terminar los enlaces, además de detectar y controlar los errores. El trabajo del comité IEEE 802.3 ha subdividido esta capa en dos subcapas.

Subcapas

La capa que sirve como interfaz con la capa física es llamada capa de Control de Acceso al Medio (MAC) y la capa que sirve de interfaz con la capa de transporte es llamada capa de Control Lógico de Enlace.

La capa de control lógico de enlace (LLC) es responsable de ensamblar y particionar los frames, agregando direcciones origen y destino, facilidades para el control y detección de errores en el receptor. Los Puentes (Bridges) funcionan en esta capa. LLC es la capa responsable de controlar el intercambio de datos entre usuarios que se están comunicando a través de la capa de Control de Acceso al Medio.

Funciones

Con excepción de la capa física, los servicios y protocolos proporcionados por la capa de enlace deben de ser familiares a aquellos que están en la industria de la comunicación de datos. Los servicios de la capa de enlace están relacionados con el intercambio confiable de datos a través de un enlace punto a punto o multipunto que ha sido establecido en la capa física. Los protocolos de la capa de enlace de datos manejan el establecimiento, control y terminación de la conexión lógica. Controla el flujo de datos del usuario, supervisa la recuperación de errores y condiciones anormales, mantiene la sincronización de los bloques o frames y caracteres.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI *(Continuación)*

Capa de Red

Proporciona aquellos servicios asociados con el traslado de los datos de los usuarios a través de una red constituida por enlaces encadenados, teniendo muchas rutas disponibles entre los puntos. Estos servicios incluyen ruteo, switcheo, secuenciación de datos, control de flujo y recuperación de errores.

Funciones

Es responsable de establecer y monitorear las conexiones entre redes de área local. También se realiza el control y selección de las rutas lógicas y conexiones entre usuarios de puntos finales en una red. Un ejemplo sería un circuito virtual en una red pública de datos

Ejemplos

La capa de paquetes del CCITT X.25 es el mejor protocolo de capa de red para redes de switcheo de paquetes. X.21 es usado para redes de switcheo de circuitos. El Departamento de Defensa de E.U. ha desarrollado un protocolo de internet conocido como IP. Otros ejemplos de protocolos de red incluyen el CCITT Q.931 y el protocolo ISO 8473 no orientado a conexión, después veremos la diferencia entre un servicio orientado a conexión y uno no orientado a conexión.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Transporte

La capa de transporte es la capa mas alta asociada con el movimiento de datos a través de la red. Esta capa provee un mecanismo universal transparente para ser usado por las capas mas altas que representa a los usuarios de los servicios de comunicación. De la capa de Transporte se espera la optimización del uso de los recursos disponibles.

Funciones

Los protocolos de transporte son responsables de la integridad del intercambio de datos y deben de ser el puente conector entre los servicios proporcionados por las capas inferiores y los requeridos por las capas superiores. Se han desarrollado numerosas clases de protocolos de transporte desde algunas muy simples hasta otras muy complejas. Las capas de transporte simples pueden ser utilizadas cuando la red provee un servicio confiable y de calidad. Un protocolo de transporte complejo es usado cuando los servicios de las capa inferior es incapaz de proporcionar el nivel de servicio requerido. La complejidad es necesaria debido a que esta capa duplica los mecanismos de recuperación que deben haber sido proporcionados por las capas inferiores.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Sesión

Una sesión enlaza dos procesos de aplicación en una relación cooperativa durante cierto tiempo. La capa de sesión proporciona un servicio administrativo que maneja el establecimiento y liberación de una conexión entre dos entidades de presentación. Las sesiones son establecidas cuando un proceso de aplicación pide acceso a otro proceso de aplicación.

Funciones

Cuando una sesión es establecida, los servicios de control dialogan y supervisan el intercambio de datos actual. El propósito de esta capa es proporcionar el control sobre la comunicación entre las aplicaciones. Esta asume que la conexión física es confiable y es controlada por las capas inferiores. Una simple sesión puede mantener varias conexiones de transporte o muchas sesiones consecutivas pueden ser mantenidas en una conexión de transporte única. Actualmente los protocolos de sesión incluyen el ISO 8327, el CCITT X.25, ECMA 75 y el CCITT T.62 el cual esta orientado a servicios de Teletex.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de

Presentación Esta capa permite a una aplicación interpretar en forma adecuada la información transferida. Esta capa esta involucrada con la traducción, transformación, formato y sintaxis de la información. Esas funciones son requeridas para adaptar las características de manejo de la información de un proceso de aplicación a otro.

Funciones

Esta capa es la responsable de presentar los datos a aplicaciones diferentes en un formato que ambos puedan reconocer. También controla características tales como cifrado y compresión de datos. Un ejemplo de la función de esta capa es la de convertir datos ASCII, usados por la mayoría de las PCs y el sistema de códigos EBCDIC usado en las mainframes IBM.

Estándares

La ISO realizo una selección internacional de estándares de presentación, conocido como DIS 8823. La representación sintáctica de datos ha sido definida en DIS 8824 y 8825. La CCITT ha descrito el protocolo de presentación para manejo de mensajes en X.409 y para Telex en X.61.

Ejemplos

Algunos ejemplos de las acciones que se realizan en esta capa, serian, la traducción de códigos, estructuración de los datos para el despliegue en pantalla, control de formato y protocolos de terminales virtuales.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Aplicación

Incluye una parte de la administración de la red y tareas de aplicación general, tales como transferencia de archivos. Aunque esta es la capa superior de la arquitectura del modelo OSI, la capa de aplicación no es la casa de las aplicaciones. Esta es simplemente la ventana a través de la cual las aplicaciones obtienen el acceso a los servicios proporcionados por la arquitectura de comunicaciones.

Funciones

Esta capa proporciona servicios de comunicación que son más directamente comprensibles al usuario. Estas incluyen identificación de procesos cooperativos, autenticación del comunicante, verificación de autoridad, determinación de los recursos disponibles y acuerdo de sintaxis.

La capa de aplicación puede ser visualizada como una conexión de elementos de usuario que son específicos al proceso de aplicación; un elemento de aplicación específica tiene funciones como transferencia de archivos, intercambio de datos de negocio, o operaciones de terminales virtuales y un elemento común constituido de funciones generales.

Relación del Modelo OSI con Otros estándares

Capas OSI	Sistemas Apple	Sistemas Banyan	DEC DECNET	IBM SNA	Redes Microsoft	Novel Netware	TCP/IP	Xerox XNS
Aplicación	Programas de aplicación y protocolos para la transferencia de archivos							
Presentación	Apple Talk Filling Protocol	Remote Procedural Calls	Administración de redes y aplicaciones de red	Servicios de transacción Presentación de servicios	Server Message Block (SMB)	Protocolos nucleos de Netware	Protocolos de Aplicación específica	Interacción de procesos y control
Sesión	Protocolo de sesión Apple Talk	Remote Procedure Calls	Sesión	Control de Flujo de Datos	NetBios	NetBios	Telnet, FTP, SNMTP, etc.	interacción de procesos y control
Transporte	Protocolo de Transacciones Apple Talk (ATP)	Comunicación interprocesos VINES	Comunicaciones finales	Control de Transmisión	NetBEUI	SPX	TCP	SSP
RED	Protocolo de envío de datagramas (DDP)	Protocolo de Internet VINES	Ruteo	Control de Ruta	NetBEUI	IPX	IP	IDP
Enlace de Datos	Tarjetas de Interfaz de Red. Ethernet, Token-Ring, etc. Controladores de Tarjetas ODI, NDIS, etc							
Física	Medio de transmisión Par tensado, Coaxial, Fibra optica, Microondas, etc							

3.2 TCP/IP

Descripción

La suite de protocolos permite a computadoras de todos los tamaños, de diferentes proveedores, corriendo sistemas operativos totalmente diferentes comunicarse entre si. TCP/IP comenzó a finales de los 60's como un proyecto de investigación financiado por el gobierno de E. U.

TCP/IP es realmente un sistema abierto en el cual la definición de la suite de protocolos y muchas de sus implementaciones están disponibles al público con un pequeño o nulo cargo. También le da forma a lo que se le llama World Wide Internet o Internet.

Capas de TCP/IP

Aplicación	Telnet, ftp, e-mail, etc.
Transporte	TCP, UDP
Red	IP, ICMP, IGMP
Enlace	Controlador del dispositivo y tarjeta interfaz.

Capa de Enlace

Algunas veces es llamada también capa de enlace de datos o la capa de interfaz de red. Normalmente incluye el controlador del dispositivo en el sistema operativo y la correspondiente interfaz de red en la computadora. Juntos, manejan todos los detalles de la interfaz física con el cable (o cualquiera que sea el tipo de medio que este siendo usado)

Capa de Red

También conocida como capa de internet, maneja el movimiento de paquetes a través de la red. Por ejemplo, el ruteo de paquetes es realizado aquí. IP (Internet Protocol), ICMP (Internet Control Message Protocol) y IGMP (internet Group Management Protocol) proporcionan la capa de red en la suite TCP/IP.

Continúa en la siguiente página

3.2 TCP/IP (Continuación)

Capa de Transporte

La capa de transporte proporciona un flujo de datos entre dos computadoras. En la suite del protocolo TCP/IP hay dos protocolos de transporte totalmente diferentes: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

TCP proporciona un flujo confiable de datos entre dos hosts. Está relacionado con cosas tales como la división de datos de una aplicación en trozos de tamaño apropiado a la capa de red adyacente, y proporciona mecanismos de control para la recepción y envío de paquetes, configura los tiempos de fin de vida de un paquete, etc. Dado que este flujo de datos confiable, la capa de aplicación puede ignorar todos estos detalles.

UDP por otro lado, proporciona un servicio mucho más simple a la capa de aplicación. Este solo manda paquetes de datos llamados datagramas desde un host a otro, pero no hay garantía de que el datagrama llegue al otro host. Cualquier implantación de confiabilidad debe ser agregada por la capa de aplicación.

Capa de Aplicación

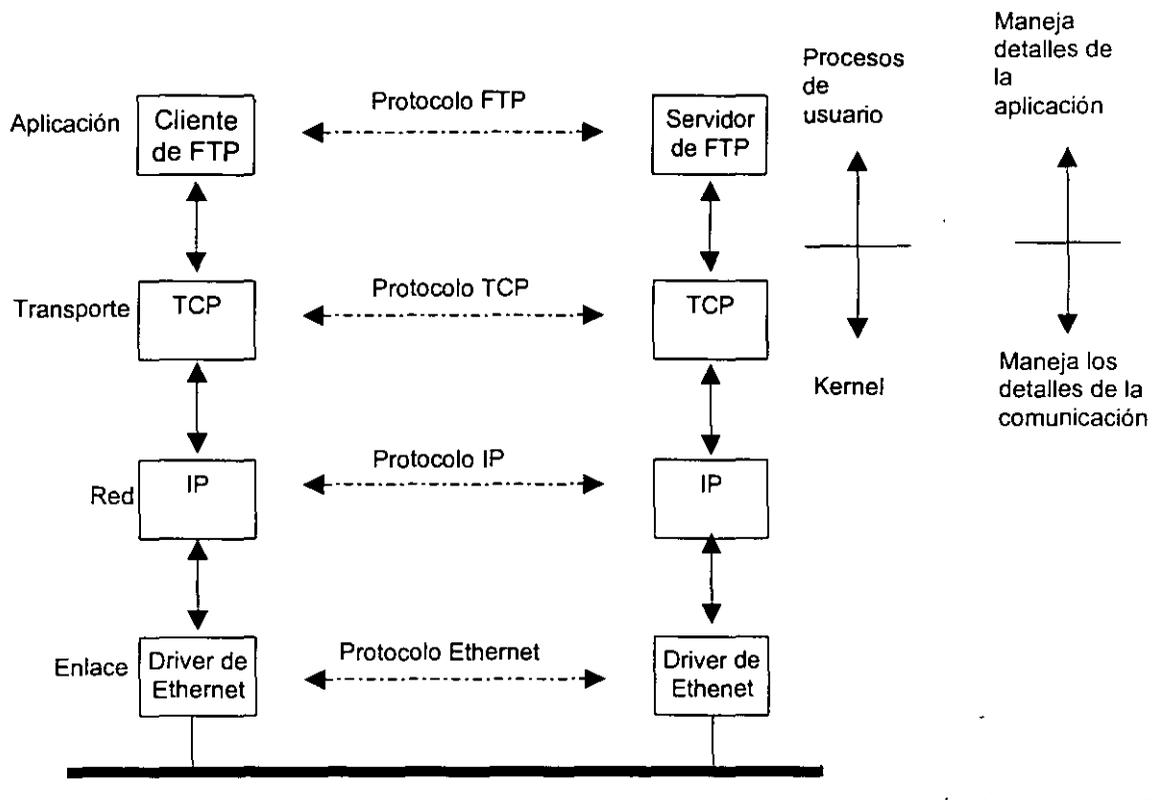
Esta capa es la encargada de manejar los detalles de la aplicación en particular. Hay muchas aplicaciones comunes de TCP/IP que al menos cada implementación proporciona:

- ◆ Telnet para sesiones remotas
 - ◆ FTP. Protocolo de Transferencia de Archivos. (File Transfer Protocol).
 - ◆ SMTP. Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol) para correo electrónico.
 - ◆ SNMP, Protocolo de Administración de Redes Simples. (Simple Network Management Protocol).
-

Continúa en la siguiente página

3.2 TCP/IP (Continuación)

Interacción entre capas.



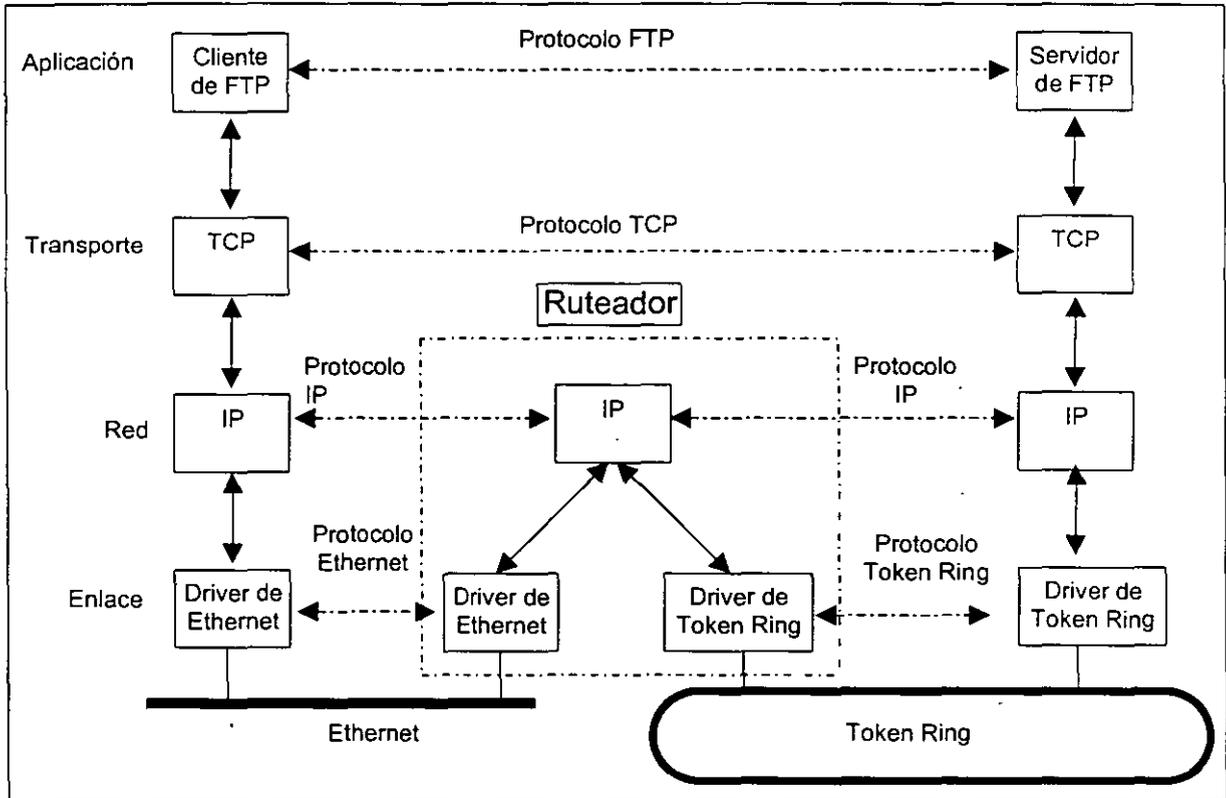
Si tenemos dos hosts en una red de área local (LAN), tal como ethernet, ambos corriendo FTP, la interacción de protocolos se ve como en la figura anterior. Aquí se nota que la capa de aplicación solo se encarga de los detalles propios de la aplicación, no se encarga de ver los detalles de la transmisión.

Aunque la capa de transporte se conecta con la capa de red, lógicamente, cada capa se comunica con su correspondiente en el otro extremo de la comunicación.

Aunque en la figura solo aparece un protocolo por capa, la realidad es que pueden existir varios protocolos para la misma capa. La principal razón que dio origen a la creación de este tipo de protocolos, fue la de interconectar muchas redes entre sí, sin que se perdiera el control sobre la comunicación.

3.2 TCP/IP (Continuación)

Interacción entre capas.



Hay una diferencia crítica entre la capa superior de la figura anterior y las tres capas inferiores. La capa de aplicación está interesada solo por los detalles de la aplicación y no con el movimiento de datos a través de la red. Las capas inferiores no saben nada de la aplicación pero manejan todos los detalles de la comunicación.



**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

Diplomado en redes

CA - 109

Complemento

Versión 1.0 23/02/1998

Ing. Marco Antonio López Meléndez

3 Protocolos de Comunicación de Alto Nivel

Protocolo

La forma en la cual dos partes de la red se comunican es llamada protocolo, lo cual asegura que cada una de las partes de la comunicación entienda a la otra sin ambigüedad. Un protocolo puede especificar la forma en que los datos son codificados, como puede ser identificado el comienzo y el fin de un mensaje, como las direcciones de los puntos origen y destino son mostradas, y las acciones a tomar si se encuentran errores durante la transmisión. Debe existir un protocolo definido para conectar dos niveles adyacentes, pero la estructura completa de una red puede consistir de muchas especificaciones diferentes.

ISO

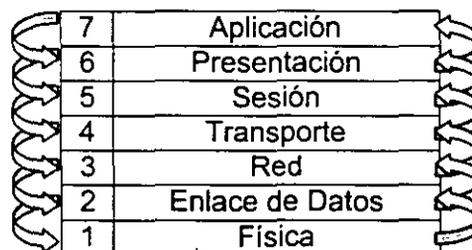
La Organización Internacional para Estandarización (ISO, International Standard Organisation) desarrolló un modelo de referencia para la estandarización de los protocolos de red. El modelo es conocido como el modelo de referencia para Interconexión de Sistemas Abiertos, (OSI, Open System Interconnection). OSI es un modelo de siete capas.

OSI y TCP/IP

Estrictamente hablando, el uso práctico de OSI en la comunicación real y aplicada es limitado. En un principio se pensó que suplantaría el uso de TCP/IP y que sería la panacea para todos los problemas de comunicación. Se invirtió mucho esfuerzo y tiempo en la elaboración de los estándares que componen a OSI. Mientras tanto, TCP/IP demostró con hechos que era una arquitectura que podía responder a las necesidades reales. Un ejemplo de lo anterior es la red INTERNET, que basada en TCP/IP, atiende a más de 30 millones de usuarios en más de 146 países.

¿En qué radica entonces la importancia de OSI?, en que es una arquitectura sumamente completa, esta es su principal ventaja, pero también su principal obstáculo, ya que es difícil y costosa de implantar.

Modelo OSI



Por ejemplo, la capa de red (Capa 3), tendrá especificaciones de protocolo para la capa de enlace de datos (capa 2) y para la capa de transporte (Capa 4). Esto es, a la capa 3 no le interesan las especificaciones para la capa 1 o para la capa 5, dado que esas capas no forman parte del área de interés de la capa. Esto da como consecuencia una flexibilidad considerable cuando las especificaciones son cambiadas o se agregan nuevas opciones.

3.1 Generalidades del Modelo OSI

La capa Física

La capa física esta encargada de la sincronización de los bits y de la identificación de un elemento como un uno o un cero. La unidad de datos de este protocolo es el Bit.

Describe las especificaciones mecánicas y eléctricas para la estructura del cableado. define como serán convertidos los bits en corriente eléctrica, pulsos luminosos o cualquier otra forma física. Determina el método por el cual las ráfagas de bits son enviadas a través de la red.

Proporciona los servicios de enlace que están asociados con la adquisición, mantenimiento y desconexión de circuitos físicos que conforman la ruta de conexión de la comunicación. Maneja tanto la interfaz como los requerimientos procedurales del medio de conexión. Es similar a la interfaz DCE-DTE.

Protocolos Típicos

- ◆ Familia RS-232.
 - ◆ Familia RS-449
 - ◆ Interfaz CCITT X.25
 - ◆ Interfaz CCITT X.21
 - ◆ Serie de Recomendaciones CCITT V
 - ◆ Serie de Recomendaciones CCITT X
 - ◆ IEEE 802.X para redes de área local
-

Ejemplos

Algunas de las especificaciones de medios físicos más utilizadas es el cableado de cobre. En los estándares de cableado de cobre en redes Ethernet existen dos tendencias básicas: cableado coaxial y cable UTP (Unshielded Twisted Pair). El cableado coaxial tiene básicamente dos variantes: el cable coaxial delgado y el cable coaxial grueso

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI *(Continuación)*

Capa de Enlace de Datos

Es la responsable de hacer que el enlace físico sea confiable. Esta encargada de comenzar y terminar los enlaces, además de detectar y controlar los errores. El trabajo del comité IEEE 802.3 ha subdividido esta capa en dos subcapas.

Subcapas

La capa que sirve como interfaz con la capa física es llamada capa de Control de Acceso al Medio (MAC) y la capa que sirve de interfaz con la capa de transporte es llamada capa de Control Lógico de Enlace.

La capa de control lógico de enlace (LLC) es responsable de ensamblar y particionar los frames, agregando direcciones origen y destino, facilidades para el control y detección de errores en el receptor. Los Puentes (Bridges) funcionan en esta capa. LLC es la capa responsable de controlar el intercambio de datos entre usuarios que se están comunicando a través de la capa de Control de Acceso al Medio.

Funciones

Con excepción de la capa física, los servicios y protocolos proporcionados por la capa de enlace deben de ser familiares a aquellos que están en la industria de la comunicación de datos. Los servicios de la capa de enlace están relacionados con el intercambio confiable de datos a través de un enlace punto a punto o multipunto que ha sido establecido en la capa física. Los protocolos de la capa de enlace de datos manejan el establecimiento, control y terminación de la conexión lógica. Controla el flujo de datos del usuario, supervisa la recuperación de errores y condiciones anormales, mantiene la sincronización de los bloques o frames y caracteres.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Red

Proporciona aquellos servicios asociados con el traslado de los datos de los usuarios a través de una red constituida por enlaces encadenados, teniendo muchas rutas disponibles entre los puntos. Estos servicios incluyen ruteo, switcheo, secuenciación de datos, control de flujo y recuperación de errores.

Funciones

Es responsable de establecer y monitorear las conexiones entre redes de área local. También se realiza el control y selección de las rutas lógicas y conexiones entre usuarios de puntos finales en una red. Un ejemplo sería un circuito virtual en una red pública de datos

Ejemplos

Los capa de paquetes del CCITT X.25 es el mejor protocolo de capa de red para redes de switcheo de paquetes. X.21 es usado para redes de switcheo de circuitos. El Departamento de Defensa de E.U. ha desarrollado un protocolo de internet conocido como IP. Otros ejemplos de protocolos de red incluyen el CCITT Q.931 y el protocolo ISO 8473 no orientado a conexión, después veremos la diferencia entre un servicio orientado a conexión y uno no orientado a conexión.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Transporte

La capa de transporte es la capa mas alta asociada con el movimiento de datos a través de la red. Esta capa provee un mecanismo universal transparente para ser usado por las capas mas altas que representa a los usuarios de los servicios de comunicación. De la capa de Transporte se espera la optimización del uso de los recursos disponibles.

Funciones

Los protocolos de transporte son responsables de la integridad del intercambio de datos y deben de ser el puente conector entre los servicios proporcionados por las capas inferiores y los requeridos por las capas superiores. Se han desarrollado numerosas clases de protocolos de transporte desde algunas muy simples hasta otras muy complejas. Las capas de transporte simples pueden ser utilizadas cuando la red provee un servicio confiable y de calidad. Un protocolo de transporte complejo es usado cuando los servicios de las capa inferior es incapaz de proporcionar el nivel de servicio requerido. La complejidad es necesaria debido a que esta capa duplica los mecanismos de recuperación que deben haber sido proporcionados por las capas inferiores.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Sesión

Una sesión enlaza dos procesos de aplicación en una relación cooperativa durante cierto tiempo. La capa de sesión proporciona un servicio administrativo que maneja el establecimiento y liberación de una conexión entre dos entidades de presentación. Las sesiones son establecidas cuando un proceso de aplicación pide acceso a otro proceso de aplicación.

Funciones

Cuando una sesión es establecida, los servicios de control dialogan y supervisan el intercambio de datos actual. El propósito de esta capa es proporcionar el control sobre la comunicación entre las aplicaciones. Esta asume que la conexión física es confiable y es controlada por las capas inferiores. Una simple sesión puede mantener varias conexiones de transporte o muchas sesiones consecutivas pueden ser mantenidas en una conexión de transporte única. Actualmente los protocolos de sesión incluyen el ISO 8327, el CCITT X.25, ECMA 75 y el CCITT T.62 el cual esta orientado a servicios de Teletex.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Presentación Esta capa permite a una aplicación interpretar en forma adecuada la información transferida. Esta capa esta involucrada con la traducción, transformación, formato y sintaxis de la información. Esas funciones son requeridas para adaptar las características de manejo de la información de un proceso de aplicación a otro.

Funciones Esta capa es la responsable de presentar los datos a aplicaciones diferentes en un formato que ambos puedan reconocer. También controla características tales como cifrado y compresión de datos. Un ejemplo de la función de esta capa es la de convertir datos ASCII, usados por la mayoría de las PCs y el sistema de códigos EBCDIC usado en las mainframes IBM.

Estándares La ISO realizo una selección internacional de estándares de presentación, conocido como DIS 8823. La representación sintáctica de datos ha sido definida en DIS 8824 y 8825. La CCITT ha descrito el protocolo de presentación para manejo de mensajes en X.409 y para Telex en X.61.

Ejemplos Algunos ejemplos de las acciones que se realizan en esta capa, serian, la traducción de códigos, estructuración de los datos para el despliegue en pantalla, control de formato y protocolos de terminales virtuales.

Continúa en la siguiente página.

3.1 Generalidades del Modelo OSI (Continuación)

Capa de Aplicación

Incluye una parte de la administración de la red y tareas de aplicación general, tales como transferencia de archivos. Aunque esta es la capa superior de la arquitectura del modelo OSI, la capa de aplicación no es la casa de las aplicaciones. Esta es simplemente la ventana a través de la cual las aplicaciones obtienen el acceso a los servicios proporcionados por la arquitectura de comunicaciones.

Funciones

Esta capa proporciona servicios de comunicación que son más directamente comprensibles al usuario. Estas incluyen identificación de procesos cooperativos, autenticación del comunicante, verificación de autoridad, determinación de los recursos disponibles y acuerdo de sintaxis.

La capa de aplicación puede ser visualizada como una conexión de elementos de usuario que son específicos al proceso de aplicación; un elemento de aplicación específica tiene funciones como transferencia de archivos, intercambio de datos de negocio, o operaciones de terminales virtuales y un elemento común constituido de funciones generales.

Relación del Modelo OSI con Otros estándares

Capas OSI	Sistemas Apple	Sistemas Banyan	DEC DECNET	IBM SNA	Redes Microsoft	Novel Netware	TCP/IP	Xerox XNS
Aplicación	Programas de aplicación y protocolos para la transferencia de archivos							
Presentación	Apple Talk Filling Protocol	Remote Procedural Calls	Administración de redes y aplicaciones de red	Servicios de transacción Presentación de servicios	Server Message Block (SMB)	Protocolos nucleos de Netware	Protocolos de Aplicación específica.	Interacción de procesos y control.
Sesión	Protocolo de sesión Apple Talk	Remote Procedure Calls	Sesion	Control de Flujo de Datos	NetBios	NetBios	Telnet, FTP, SNMTP, etc.	Interacción de procesos y control
Transporte	Protocolo de Transacciones Apple Talk (ATP)	Comunicación interprocesos VINES	Comunicaciones finales	Control de Transmisión	NetBEUI	SPX	TCP	SSP
RED	Protocolo de envío de datagramas (DDP)	Protocolo de Internet VINES	Ruteo	Control de Ruta	NetBEUI	IPX	IP	IDP
Enlace de Datos	Tarjetas de Interfaz de Red. Ethernet, Token-Ring, etc. Controladores de Tarjetas ODI, NDIS, etc.							
Física	Medio de transmisión Par tensado, Coaxial, Fibra óptica, Microondas, etc.							

3.2 TCP/IP

Descripción

La suite de protocolos permite a computadoras de todos los tamaños, de diferentes proveedores, corriendo sistemas operativos totalmente diferentes comunicarse entre si. TCP/IP comenzó a finales de los 60's como un proyecto de investigación financiado por el gobierno de E. U.

TCP/IP es realmente un sistema abierto en el cual la definición de la suite de protocolos y muchas de sus implementaciones están disponibles al público con un pequeño o nulo cargo. También le da forma a lo que se le llama World Wide Internet o Internet.

Capas de TCP/IP

Aplicación	Telnet, ftp, e-mail, etc.
Transporte	TCP, UDP
Red	IP, ICMP, IGMP
Enlace	Controlador del dispositivo y tarjeta interfaz.

Capa de Enlace

Algunas veces es llamada también capa de enlace de datos o la capa de interfaz de red. Normalmente incluye el controlador del dispositivo en el sistema operativo y la correspondiente interfaz de red en la computadora. Juntos, manejan todos los detalles de la interfaz física con el cable (o cualquiera que sea el tipo de medio que este siendo usado)

Capa de Red

También conocida como capa de internet, maneja el movimiento de paquetes a través de la red. Por ejemplo, el ruteo de paquetes es realizado aquí. IP (Internet Protocol), ICMP (Internet Control Message Protocol) y IGMP (internet Group Management Protocol) proporcionan la capa de red en la suite TCP/IP.

Continúa en la siguiente página

3.2 TCP/IP (Continuación)

Capa de Transporte

La capa de transporte proporciona un flujo de datos entre dos computadoras. En la suite del protocolo TCP/IP hay dos protocolos de transporte totalmente diferentes: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

TCP proporciona un flujo confiable de datos entre dos hosts. Esta relacionado con cosas tales como la división de datos de una aplicación en trozos de tamaño apropiado a la capa de red adyacente, y proporciona mecanismos de control para la recepción y envío de paquetes, configura los tiempos de fin de vida de un paquete, etc. Dado que este flujo de datos confiable, la capa de aplicación puede ignorar todos estos detalles.

UDP por otro lado, proporciona un servicio mucho mas simple a la capa de aplicación. Este solo manda paquetes de datos llamados datagramas desde un host a otro, pero no hay garantía de que el datagrama llegue al otro host. Cualquier implantación de confiabilidad debe ser agregada por la capa de aplicación.

Capa de Aplicación

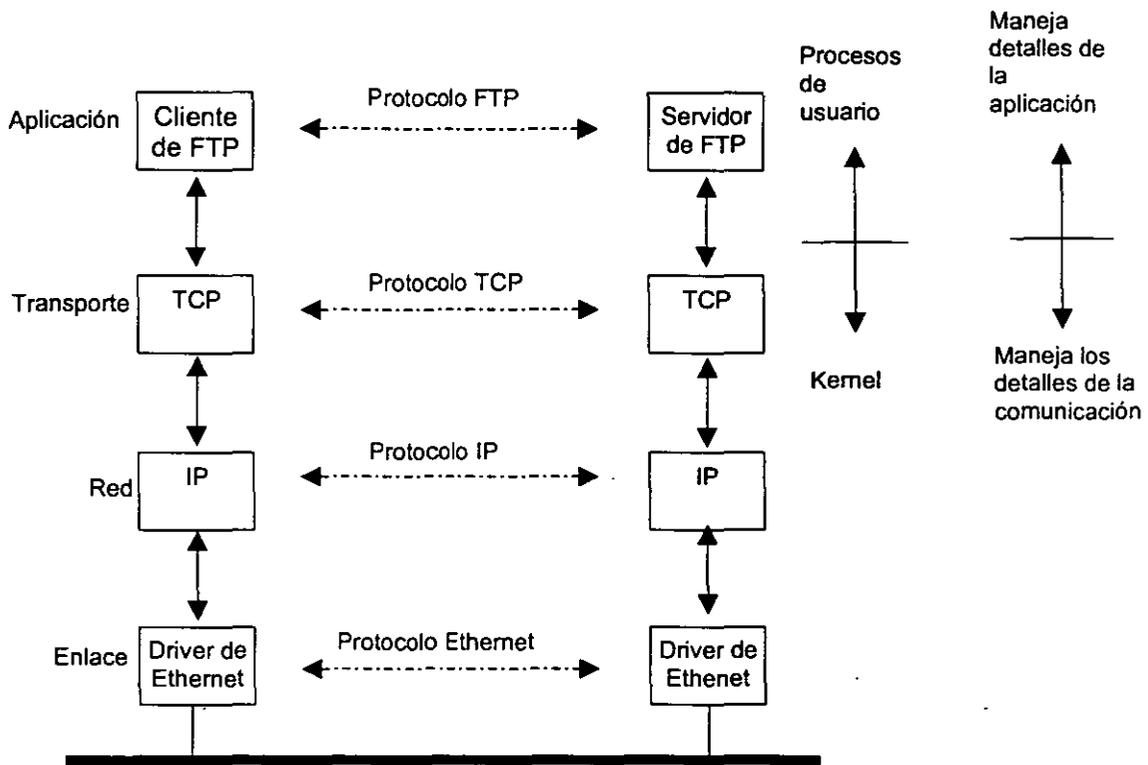
Esta capa es la encargada de manejar los detalles de la aplicación en particular. Hay muchas aplicaciones comunes de TCP/IP que al menos cada implementación proporciona:

- ◆ Telnet para sesiones remotas
 - ◆ FTP. Protocolo de Transferencia de Archivos. (File Transfer Protocol).
 - ◆ SMTP. Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol) para correo electrónico.
 - ◆ SNMP, Protocolo de Administración de Redes Simples. (Simple Network Management Protocol).
-

Continúa en la siguiente página

3.2 TCP/IP (Continuación)

Interacción entre capas.



Si tenemos dos hosts en una red de área local (LAN), tal como ethernet, ambos corriendo FTP, la interacción de protocolos se ve como en la figura anterior. Aquí se nota que la capa de aplicación solo se encarga de los detalles propios de la aplicación, no se encarga de ver los detalles de la transmisión.

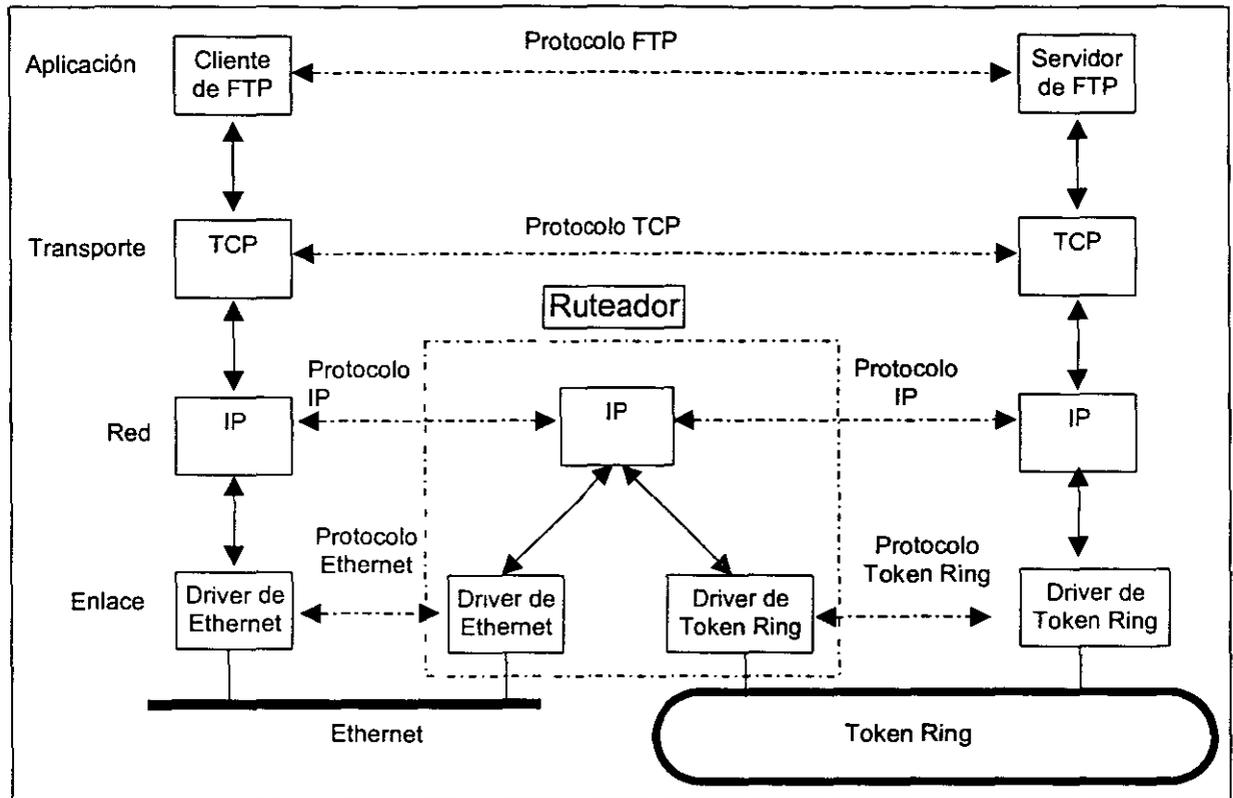
Aunque la capa de transporte se conecta con la capa de red, lógicamente, cada capa se comunica con su correspondiente en el otro extremo de la comunicación.

Aunque en la figura solo aparece un protocolo por capa, la realidad es que pueden existir varios protocolos para la misma capa. La principal razón que dio origen a la creación de este tipo de protocolos, fue la de interconectar muchas redes entre sí, sin que se perdiera el control sobre la comunicación.

Continúa en la siguiente página

3.2 TCP/IP (Continuación)

Interacción entre capas.



Hay una diferencia crítica entre la capa superior de la figura anterior y las tres capas inferiores. La capa de aplicación está interesada solo por los detalles de la aplicación y no con el movimiento de datos a través de la red. Las capas inferiores no saben nada de la aplicación pero manejan todos los detalles de la comunicación.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI

Capa de Aplicación

Función

La capa de aplicación es la mas superior de todas dentro del modelo OSI. Es la que se encuentra mas cerca de las aplicaciones del usuario, y por lo tanto, es la que les proporciona servicio.

Respecto a otras arquitecturas

Difícilmente encontraremos en otra arquitectura un equivalente a la capa de aplicación, sin embargo, sus protocolos pueden implantarse como aplicaciones sobre otra arquitectura, fuera del estándar, y como parte de la labor del programador de aplicaciones.

Conceptos Básicos

Application Process (AP) Un componente dentro de un sistema abierto. Es una representación abstracta de los elementos de un sistema abierto, que realiza cierto procesamiento para una aplicación en específico. En otras palabras un proceso.

Application Entity(AE). Representa al AP dentro de OSI. Da al AP la posibilidad de comunicarse dentro de un sistema OSI.

Application Service Element (ASE). Parte de un AE, que da un conjunto de capacidades específicas al AP dentro de OSI. Por ejemplo, hay AE para tener capacidades de transferir archivos, para enviar y recibir correo electrónico. etc. Esto no tiene relación alguna con la forma de estructurar estas aplicaciones dentro de TCP/IP(Internet).Un ASE puede comunicarse con otro ASE del mismo tipo a través de **APDUs (Application Protocol Data Units)**

Common Application Service Element (CASE): Es un ASE que da servicios a gran variedad de aplicaciones. esto es porque da servicios tan básicos que la mayor parte de los AP los utilizan. Por ejemplo: para establecer comunicación entre dos aplicaciones se utiliza un CASE llamado ACSE.

Specific Application Service Element(SASE). Es un ASE que da servicios a un conjunto limitado de aplicaciones. Generalmente sus servicios son mas especializados, por ejemplo, transferencia de archivos (FTAM), transferencia de trabajos (JTM), correo electrónico (X.400),etc.

User Element (UE) Parte de un AE. Representa el AP al AE, es específico a la aplicación.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

ASE

Podemos ver a los ASE's como las subrutinas que proporcionan un conjunto de servicios común a varias aplicaciones, en este caso, todos los servicios que proporcionan están relacionados con la comunicación a través de una red OSI. La comunicación hacia la capa inferior se realiza a través de puntos de acceso (Access Points) que en este caso se denominan Presentation Service Access Point. (PSAPs).

ACSE

El primer ASE que analizaremos es un **CASE**, su nombre es **ACSE: Association Control Service Element**. La definición de los servicios que presta se encuentra en CCITT X.217 o ISO 8649. La especificación de los protocolos que utiliza se encuentra en CCITT X.227 o ISO 8650.

La función de ACSE es la de soportar la asociación entre aplicaciones, como esta es una función muy común, se trata de un CASE.

Consta de cuatro servicios:

- A-ASSOCIATE Crea una asociación entre aplicaciones.
- A-RELEASE Libera una asociación entre aplicaciones.
- A-ABORT Aborta una asociación entre aplicaciones.
- A-P-ABORT Aborta una asociación entre aplicaciones.

La diferencia entre A-RELEASE y A-ABORT es que A-RELEASE no libera las asociaciones entre las capas inferiores, mientras que A-ABORT termina las asociaciones entre las capas de aplicación, presentación y sesión.

La diferencia entre A-ABORT y A-P-ABORT es que la segunda es iniciada por la capa de presentación, mientras que la primera por el usuario (persona o programa).

Asociaciones

Una asociación entre aplicaciones es una descripción detallada de una relación cooperativa entre dos entidades de aplicación (AE) a través del uso de los servicios de la capa de presentación dentro de un contexto de aplicación. Un contexto de aplicación es un conjunto de elementos de servicios (ASE's) e información relacionada utilizada para la asociación entre aplicaciones.

Al igual que con los otros ASES, no analizaremos aquí las primitivas, unidades de protocolo, parámetros, ni la máquina de estados de ACSE, tan solo conoceremos sus funciones. Para mayor referencia deberá consultarse la bibliografía.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

RTSE

Debido a que es necesario contar con un mecanismo para la transmisión confiable de las unidades de protocolo de la capa de aplicación (APDUs), se implanto RTSE (Reliable Transfer Service Element). Este protocolo además permite recuperarse de situaciones de falla en las comunicaciones o en los sistemas finales. También permite la negociación del tamaño de las unidades de protocolo, la segmentación de las unidades, y el establecimiento de puntos de chequeo para verificar el envío de unidades segmentadas o no segmentadas. La definición de los servicios que proporciona RTSE se encuentra en CCITT X.218 o en ISO 9066-1, la especificación de los protocolos que utiliza se encuentra en CCITT X.208 o en ISO 9066-2.

RTSE proporciona siete servicios:

- RT-OPEN
- RT-TRANSFER
- RT-TURN-PLEASE
- RT-TURN-GIVE
- RT-P-ABORT
- RT-U-ABORT
- RT-CLOSE

Al efectuarse un **RT-OPEN**, se negocia:

Tamaño de los puntos de chequeo. Máxima cantidad de datos a enviar entre puntos de sincronización, o bien, no se utilizan puntos de sincronización.

Tamaño de la ventana: Máxima cantidad de puntos de sincronización que pueden estar pendientes, antes de que la transmisión de datos se interrumpa.

Tipo de dialogo: Dos vías o monólogo

Turno inicial: Acuerdo en que RTSE tiene el turno inicial, es decir el permiso para hablar.

RT-TURN-PLEASE y RT-TURN-GIVE solicitan y dan el turno para hablar.

RT-U-ABORT y RT-P-ABORT difieren en que el primero es iniciado por el usuario, mientras que el segundo por el ASE que proporcione el servicio a RTSE, o bien la capa de presentación.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

ROSE

A través de este ASE se da soporte al procesamiento interactivo de aplicaciones distribuidas. La definición de los servicios que proporciona se encuentra en CCITT X.219 o ISO 9072-1. y la especificación del protocolo se encuentra en CCITT X.229 o ISO 9072-2.

ROSE (Remote Operations Service Element) no tiene capacidades de transmisión, se auxilia de otros ASES para realizar esto. Casi todos sus parámetros pasan directamente a los ASES que ROSE utiliza para controlar la comunicación. así ROSE únicamente define un mecanismo para invocar una acción en un AE determinado y recibir información referente al resultado de esta acción. Soporta dos formas de operación, sincrónica y asincrónica, dependiendo si el AE que invoca la operación puede o no seguir invocando operaciones a pesar de no recibir los últimos resultados.

Los servicios que proporciona ROSE son:

RO-INVOKE
RO-RESULT
RO-ERROR
RO-REJECT-U
RO-REJECT-P

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

CCR

CCR (Commitment, concurrency and Recovery) describe las acciones necesarias para administrar la actividad entre mas de una aplicación. La mayoría de sus funciones están relacionadas con la transferencia y actualización de elementos en bases de datos (registros, campos).

La idea básica detrás de CCR es la de estados consistentes para las aplicaciones o datos involucrados en una actividad. Esto garantiza que los sistemas y datos afectados son correctos y que cualquier copia duplicada contiene los mismos valores.

CCR asume que aunque los sistemas se encuentran distribuidos, existe un centralizador que controla la actividad entre las aplicaciones y/o las bases de datos. Con el fin de evitar deadlocks cuando se ejerce el control sobre una base de datos, es preferible utilizar un commit de dos fases. CCR esta descrito en ISO 8649 e ISO 8650, básicamente opera como sigue:

Fase 1: El superior determina que subordinados se involucraran en la actividad, e informa a cada subordinado de las acciones. El subordinado acepta o niega estas acciones.

Fase 2: El superior ordena el commit o libera los recursos a su estado inicial.

Los servicios que proporciona CCR son:

- C-BEGIN
- C-READY
- C-COMMIT
- C-PREPARE
- C-REFUSE
- C-ROLLBACK
- C-RESTART

C-BEGIN Es lanzado por el iniciador, para que se comience una acción atómica. No se confirma

C-READY Es lanzado por una de las partes (no iniciador), cuando esta listo para dar commit o para dar rollback. No necesita confirmación.

C-COMMIT Es lanzado por el iniciador para que se ejecute el commit. Necesita confirmación

C-PREPARE Lanzado por el iniciador y superior para determinar si un subordinado esta listo para dar commit.

C-REFUSE Lanzado por el que responde, como una respuesta al C-READY. No necesita confirmación.

C-ROLLBACK. Lanzado por el iniciador para revertir la acción y restablecer el estado inicial antes del commit.

C-RESTART Lanzado por el iniciador o participante para iniciar los procesos de recuperación.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

VT

El concepto central en el SASE Virtual Terminal es aislar las terminales de las aplicaciones. De esta manera, diferentes terminales pueden acceder diferentes aplicaciones corriendo en diferentes sistemas. VT logra esto a través de una entidad VT simulando una terminal real y negociando las características operativas con la otra entidad. Es tarea de los VTs resolver diferencias e incompatibilidades entre la terminal y la aplicación.

Podemos entender el funcionamiento de VT a través de un modelo de objetos descrito en ISO 9040 e ISO9041. El estándar VT está basado en un modelo genérico de comunicación de terminales (CCA Conceptual Communication Area). La CCA es una estructura abstracta compartida que representa el ambiente de la terminal. Contiene al dispositivo virtual que es mapeado a la terminal real de un lado, e interacciona con las aplicaciones por el otro. Los usuarios de VT (el subsistema de terminales y la aplicación) se comunican entre sí a través de la CCA. La CCA se extiende entre los dos sistemas distribuidos a través del protocolo VT que se utiliza entre las entidades VT.

La CCA contiene un modelo que representa el teclado, pantalla y otros dispositivos de entrada/salida. El modelo es una colección de objetos de datos abstractos. Las aplicaciones hacen uso de este modelo utilizando las primitivas VT en vez de comandos específicos a las terminales. La CCA contiene estructura de datos que incluyen objetos de despliegue, objetos de control, objetos de dispositivo.

Todos los datos que se despliegan o se ingresan son transferidos por el objeto de despliegue (Display Object). El objeto de despliegue está distribuido entre los dos sistemas, y no hay comunicación directa entre la aplicación y la terminal.

Los objetos de dispositivo (Device Objects) sirven para realizar la función de mapeo hacia los dispositivos reales. Los objetos de dispositivo y sus mapeos no son estandarizados, pero se incluyen en el modelo porque su operación es afectada por los parámetros de VT, y es controlada por los objetos de control.

Los objetos de control (Control Objects) reflejan la asignación de tokens, derechos de acceso, y otros datos de control. Puede haber muchos objetos de control, entre los que se incluyen: control local del eco y control de interrupciones.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Aplicación (continuación)

Servicios de VT

Los servicios de VT sirven para:

Establecer, controlar y finalizar una asociación entre dos usuarios de VT.

Negociar un conjunto consistente de parámetros para el modelo CCA. La negociación toma lugar en el momento del establecimiento de la asociación o durante la transmisión.

Tener una manera de transferir datos independientemente de la representación local y características de la terminal real.

Controlar la integridad de la transferencia de datos a través de la administración del diálogo.

Los servicios que proporciona VT son:

VT-ASSOCIATE
VT-RELEASE
VT-U-ABORT
VT-P-ABORT
VT-DELIVER
VT-ACK-RECEIPT
VT-GIVE-TOKENS
VT-DATA
VT-START-NEG
VT-END-NEG
VT-NEG-INVITE
VT-NEG-OFFER
VT-NEG-ACCEPT
VT-NEG-REJECT
VT-BREAK
VT-SWITCH-PROFILE

Esto es lo que respecta a la etapa de aplicación, una vez mas. debemos recordar que la estudiamos principalmente como un ejemplo didáctico. ya que en la practica casi nunca se utilizara. Sin embargo, da una buena idea de los conceptos que se deben tomar en cuenta cuando se diseña una aplicación que trabaje en red

Continúa en la siguiente página

3.3 Detalles del Modelo OSI (continuación)

Capa de Presentación

Relación con otras capas

La capa de presentación es la capa 6 en el modelo OSI. Proporciona servicios a la capa de aplicación a través de sus PSAPs (Presentation Service Access Point), y hace uso de los servicios de la capa 5 (sesión) a través de los SSAPS (Session Service Access Point).

Para que una comunicación pueda llevarse a cabo, es necesario que ambas partes sean capaces de comprender los mensajes que se intercambian. La capa de presentación tiene el objetivo de asegurar que la información que se intercambia entre los participantes de una comunicación no sea ambigua, sino que conserve su significado.

Los problemas que resuelve la capa de presentación

La raíz del problema que la capa de presentación resuelve se encuentra en que cada computadora puede tener diferentes maneras de representar la misma información. En el caso más sencillo, la representación de los caracteres puede ser un problema, ya que no existe un código único (además de ASCII existe el EBCDIC). Si la información se transmitiera y fuera recibida tal cual por una computadora que utilizara un código diferente al que la envió, de nada serviría el trabajo de todas las capas inferiores, recordemos que aquí estamos hablando de información, no de datos. La información tiene un significado y una estructura que no deberá perderse cuando se transmite.

Otra causa de problemas es la forma de representación de los números enteros, números de punto flotante, y aun el ordenamiento de los bytes dentro de una palabra (Una palabra es un conjunto de bytes que varía en tamaño según la computadora de que se trate), o el ordenamiento de los bits dentro de un byte (big endian o little endian).

Debe notarse que para cada conexión establecida entre entidades de presentación (al igual que en la capa de aplicación, existen entidades que conforman a la capa), hubo antes una negociación, en donde se especificaron las representaciones de datos a utilizar. La representación común que se utiliza en la conexión puede o puede no ser la misma que la representación interna que utilice cada sistema final. Por lo tanto la capa de presentación tal vez tenga que hacer alguna transformación en la representación de los datos interna a la que se utiliza en la transmisión y viceversa.

Algunas veces, a pesar de que la representación interna de los datos en los sistemas finales es la misma, se utiliza una representación diferente para la transmisión, ya que puede compactarse o encriptarse la información (Notar entonces que estas funciones estarían dentro de la capa de presentación).

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

Conceptos Básicos

Sintaxis Abstracta: Una descripción de alto nivel (es decir no a nivel de unos y ceros, sino de una notación) para la definición de tipos y estructuras de datos.

Sintaxis de Transferencia: La representación en bits que se utiliza para transferir los datos entre sistemas

Administración de contexto: Para la identificación y control ordenado de múltiples sintaxis en una conexión

Sintaxis de Representación

Aquí se debe definir:

La estructura de los datos (registros, arreglos, etc.)

Los tipos de los datos (entero, real, etc.)

Reglas de codificación (Como serán representados, ya en bits los datos)

Recordando las funciones de la capa de aplicación, entre ellas no se incluye ninguna que tenga que ver con la representación de los datos, precisamente la capa de presentación es la que se encarga de esto. Así pues, la capa de aplicación envía a la capa de presentación los datos representados con una sintaxis abstracta que es independiente de la forma en que esto se codifique en bits. Mas adelante veremos ASN. 1 que es precisamente una notación para esta sintaxis abstracta.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

Servicios que proporciona

Los servicios que proporciona la capa de presentación pueden agruparse en dos:

Servicios de sesión:

Todos los servicios de la capa de sesión para la estructuración de diálogos pasan a través de la capa de presentación, ya que el modelo no permite brincar entre capas.

Servicios de selección de sintaxis:

La selección de sintaxis es una negociación que se lleva a cabo en dos niveles. Por una parte las entidades de aplicación pasan a través de parámetros a la capa de presentación las sintaxis abstractas que desean utilizar, esto debe ser confirmado por las entidades de aplicación del otro lado de la comunicación. Además de esta negociación, en el nivel de presentación, las entidades de presentación llegan a un acuerdo en lo que toca a la sintaxis de transferencia que se utilizara. La combinación entre una sintaxis abstracta y la sintaxis de transferencia que se utilizara se denomina contexto de presentación. Una conexión entre entidades de presentación puede manejar mas de un contexto, esto es porque una sola aplicación (User Element) puede estar conformada por varios ASES, cada uno usando sintaxis abstractas diferentes.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

Servicios Los servicios que proporcionan son:

P-CONNECT
P-ALTER CONTEXT
P-DATA
P-EXPEDITED DATA
P-TYPED DATA
P-CAPABILITY DATA
P-TOKEN GIVE
P-TOKEN PLEASE
P-CONTROL GIVE
P-SYNC MINOR
P-SYNC MAJOR
P-RE SYNCHRONIZE
P-P-EXCEPTION REPORT
P-U-EXCEPCION REPORT
P-ACTIVITY START
P-ACTIVITY RESUME
P-ACTIVITY INTERRUPT
P-ACTIVITY DISCARD
P-ACTIVITY END
P-RELEASE
P-U-ABORT
P-P-ABORT

Muchas de estas primitivas simplemente mapean los servicios de la capa de sesión hacia la capa de aplicación, y prácticamente la capa de presentación no realiza función alguna a partir de que las recibe.

Hemos hablado en este tema y en el anterior de los servicios o primitivas y de una descripción breve de las funciones de las dos capas superiores. Sin embargo, no se ha aclarado el papel de las unidades de protocolo de cada una de estas capas. Recordemos que las entidades de la capa de aplicación intercambian mensajes a través de unidades de protocolo denominadas APDU. De igual manera las entidades de la capa de presentación intercambian mensajes a través de unidades de protocolo denominadas PPDU. Las unidades de protocolo son las que realizan el intercambio de información entre entidades. Las primitivas, entonces, causan que una capa trabaje, parte procesando los parámetros que se le pasan a través de ella y parte intercambiando mensajes entre las entidades equivalentes en la otra computadora. Por lo tanto, a veces no hay una equivalencia exacta entre unidades de protocolo y primitivas, ya que una primitiva puede desatar mensajes en unidades de protocolo de formato diferente. o bien, una sola unidad de protocolo puede transmitir la información que necesitan varias primitivas.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

ASN

Debido a que las unidades de protocolo deben contener la representación de los datos, deberá existir una manera de describir la estructura de las mismas. Para esto fue creado ASN 1. ASN 1 está definido en CCITT X.208 o ISO 8824. ASN 1 permite construir un conjunto de tipos de datos estructurados a partir de un grupo de elementos de datos básico, de manera semejante a como se hace con un lenguaje de programación. Por otra parte, la representación en bits de los datos se da en base a las Basic Encoding Rules (BER). BER está descrito en X.209 o ISO 8825. Los datos representados con BER constan de tres partes: un identificador especificando el tipo de dato, un campo identificando la longitud del dato, y un campo para el valor del dato.

Tipos de datos de ASN

BOOLEAN
INTEGER
ENUMERATED
REAL
BIT STRING
OCTET STRING
NULL
Numeric String
Printable String
String
Generalized Time and UTC Time

Constructores en ASN

SEQUENCE
SEQUENCE OF
SET
SET OF
TAGGED
CHOICE
ANY

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

Ejemplo de lo que se puede hacer con ASN

```
ROSEapdus: =CHOICE{
[1] IMPLICIT INVOKE
[2] IMPLICIT RESULT
[3] IMPLICIT ERR
[4] IMPLICIT REJECT
}
```

```
RESULT:= SEQUENCE{
InvokeID    INTEGER
SEQUENCE{
OPERATION
result     ANY}
OPTIONAL}
```

Esta es la definición de la estructura del APDU que utiliza el protocolo ROSE, y el formato de uno de los posibles contenidos.

Hay que notar los números entre corchetes o tags, que sirven para distinguir una estructura bidimensional en un flujo unidimensional de bits. es decir para distinguir un dato del otro. La palabra implicit sirve para indicar que en la transferencia de datos, no viajaran las definiciones de estos tipos. porque cada CASE ROSE ya sabe de que tipo de datos se trata, dependiendo del orden en que se encuentre. También deberá notarse como a partir de tipos básicos pueden construirse datos complejos.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Presentación (continuación)

BER

Los datos codificados son de la forma:

Identificador, Longitud, Contenido

Identificador

Bits	8			7	6	5	4	3	2	1
	Clase	Universal,	de	Primitivo/		Código				de
	Aplicación,	de Contexto		Constructor		identificación				de tipo.

Identificador de tipo

Son valores hexadecimales, por ejemplo, 0x01 para Booleano, 0x02 para entero, etc. El Bit 8 especifica en que contexto será valido el tipo definido, si para todas las aplicaciones, una aplicación en específico o en un dato en específico.

Longitud

La longitud es definida en un byte para aquellas longitudes menores a 128, se distinguen porque comienzan con 0, para aquellas mayores en el primer byte se guarda cuantos bytes ocupara la longitud, y en los demás la longitud en si.

Representación de datos

El contenido de los datos se guarda de acuerdo a un estándar, los booleanos son codificados con todos 0 para falso, y verdadero es cualquier otro valor. Los enteros son guardados con complemento a dos.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI (continuación)

Capa de Sesión

Función

La comunicación entre computadoras, al igual que la comunicación humana, tiene cierta estructura, y debe llevarse a cabo de forma ordenada. La capa de sesión hace esto posible proporcionando servicios a la capa de presentación y mejorando los de la capa de transporte.

Conceptos básicos

Activities. Cuando conversan dos personas, generalmente lo hacen en base a tópicos definidos, por ejemplo, en un principio podrían hablar de la situación económica del país, después de las condiciones de seguridad en la ciudad, etc, estos tópicos se definen como activities.

Tipo de Comunicación. Generalmente, las personas hablan en un modo half duplex, es decir, primero una y luego la otra. En el caso de las aplicaciones, estas pueden comunicarse en modo half duplex, simplex o full duplex. La negociación para llegar a un acuerdo en cuanto a esto, que se lleva a cabo en el momento de establecer una comunicación, es responsabilidad de la capa de sesión.

Puntos de sincronía Cuándo se habla con una persona para explicarle algo, a menudo se utilizan puntos de sincronización con las siguientes palabras "Hasta aquí hay alguna duda?", si la respuesta es afirmativa se puede seguir adelante, si no habrá que regresar a retransmitir algunos conceptos. De igual manera las aplicaciones manejan puntos de sincronización. Esto es diferente a la sincronización que se maneja en las capas inferiores, ya que estas solo verifican el envío correcto de la información, mientras que aquí lo que se esta asegurando es el procesamiento de la misma (Una persona puede oír mas no entender).

Tipos de Servicios

Los servicios especializados de la capa de sesión caen dentro de las siguientes categorías:

- Administración de las interacciones
- Sincronización de la conexión
- Administración de actividades
- Reporte de excepciones.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Sesión (continuación)

Administra- ción de interacciones

Permite a las entidades de presentación controlar explícitamente quien tiene el turno para realizar ciertas funciones de control. Permite el intercambio voluntario del turno. Se permite una interacción full duplex, half duplex o simplex.

Sincroniza- ción de la conexión

La sincronización de la conexión permite a las entidades de presentación definir e identificar puntos de sincronización que pueden numerarse dentro del flujo de datos, regresar la conexión a un punto definido o acordar regresar a un punto de re- sincronización.

Conexiones

La capa de sesión proporciona a la capa de presentación el servicio de establecimiento de conexiones a nivel sesión. Una conexión de nivel presentación se mapea a una conexión de nivel sesión no se multiplexan las conexiones de sesión a las conexiones de transporte, sin embargo, una conexión de sesión puede utilizar una conexión de transporte que se encuentre disponible (es decir ya fue liberada por otra entidad de sesión), si es que le es útil. A su vez, la capa de sesión solicita a la capa de transporte la apertura y liberación de una conexión, y el transporte de datos normales y expeditos.

Servicios

S-CONNECT
S-DATA
S-EXPEDITED DATA
S-TYPED DATA
S-CAPABILITY DATA
S-TOKEN GIVE
S-TOKEN PLEASE
S-CONTROL GIVE
S-SYNC MINOR
S-SYNC MAJOR
S - RESYNCHRONIZE
S-P-EXCEPTION REPORT
S-U-EXCEPTION REPORT
S-ACTIVITY START
S-ACTIVITY RESUME
S-ACTIVITY INTERRUPT
S-ACTIVITY DISCARD
S-ACTIVITY END
S-RELEASE
S-U-ABORT
S -P-ABORT

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Sesión (continuación)

Descripción de los servicios de conexión

S-CONNECT establece una conexión de sesión, entre sus parámetros incluye la dirección de capa de sesión con la que establecerá comunicación y la del que inicia, asimismo incluye la calidad de servicio solicitada, este parámetro se pasa a la capa de transporte.

S-DATA se mapea casi directamente con P-DATA, pero a diferencia de esta, solo es válida si la entidad de la capa de sesión tiene el turno para enviar datos (recordemos que precisamente este control de turno es una de las funciones de la capa de sesión).

S-RELEASE permite una terminación ordenada de la conexión, sin pérdida de datos, a diferencia de S-UABORT y S-P-ABORT. Notar la letra P, que significa que el proveedor de servicios de la capa de sesión, en este caso la capa de transporte, es el que indica que la comunicación debe abortarse.

S-P-Exception Report o S-U-Exception report, indican la presencia de una condición de error, que sin embargo no es tan grave como para abortar la comunicación. Las condiciones de error pueden corregirse a través de la resincronización, aborto, interrupción de la actividad o liberar el token.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Sesión (continuación)

Tokens de Sincronía

Hemos mencionado que la comunicación ordenada es el objetivo de la capa de sesión. Y para eso hace uso de los tokens. Existen cuatro tipos de tokens. El token DATA que permite al usuario de la capa de sesión utilizar la primitiva S-DATA no quedan sujetas a este control la S-TYPED DATA o S-EXPEDITED DATA. El token RELEASE que permite al usuario utilizar la primitiva S-RELEASE. El token SYNCHRONIZE MINOR permite al usuario de la capa de sesión utilizar la primitiva S-SYNC MINOR (por supuesto si en la fase inicial de la conexión se realizaron las negociaciones necesarias para que se utilizaran puntos de sincronía). El token MAJOR ACTIVITY que controla que usuario de la capa de sesión tiene el derecho de utilizar S-SYNC MAJOR o cualquiera de las peticiones S-ACTIVITY (al igual que con la sincronización menor, estas se pueden utilizar si fueron negociadas con éxito en la fase inicial de la comunicación). S-TOKEN GIVE y S-TOKEN PLEASE dan y solicitan los tokens que se hayan pasado como parámetro a la primitiva.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Sesión (continuación)

Re- sincronía

Como ya mencionamos, la capa de sesión es capaz de regresar la transmisión de datos a un estado determinado a través de puntos de sincronía. Estos puntos dividen el flujo de datos en unidades lógicas. Los puntos de sincronía menor (S-SYNC Minor) pueden requerir o no confirmación, y no interrumpen el flujo de información. Por otra parte, los puntos de sincronía mayor (S-SYNC Major) siempre requieren confirmación y detienen el flujo de información mientras esta no se reciba

A través de la primitiva S-RESYNCHRONIZE podemos valer de los puntos de sincronización para llegar a un estado determinado de la comunicación. Esta primitiva tiene como parámetro el tipo de resincronización que se solicita, es decir si esta implicaran el abandono, recomienzo o comienzo en un estado dentro de una determinada actividad. Además se pasa como parámetro el punto de sincronización que se utilizara, como quedaran los tokens (es decir, después de la resincronización, quien tiene permiso de hacer que cosa) y un espacio para datos.

Tipos de Re-sincronía

Abandon: Es decir solicita la resincronización de la transmisión a través del salto a un punto de sincronización mayor a cualquiera que hasta el momento se haya utilizado, abortando cualquier comunicación que en ese momento se este llevando a cabo. (Por ejemplo, si se estaban haciendo una serie de reservación es para vuelos de avión con escalas, y de pronto se decidiera cancelar el viaje por completo).

Restart: Es decir regresar ambas partes regresaran de común acuerdo a un punto de sincronización, este no puede ser anterior que el ultima punto de sincronización mayor. Cabe notar que se necesitara retransmitir todo lo que había pasado después, pero esto no es responsabilidad de la capa de sesión, sino de las entidades de aplicación que se estén comunicando.

Reset: Es decir colocar el valor numérico del punto de sincronización en algún valor de común acuerdo

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Sesión (continuación)

Activities

La capa de sesión permite estructurar un dialogo en base a actividades. Las actividades son un conjunto de transmisiones relacionadas, que componen una unidad lógica que puede interrumpirse y después reanudarse.

Las primitivas S-ACTIVITY START, S-ACTIVITY RESUME, S-ACTIVITY INTERRUPT, S-ACTIVITY DISCARD, S-ACTIVITY END permiten comenzar, reiniciar, interrumpir, descartar (terminar de manera anormal) y terminar con una actividad. A través del uso de actividades, se acorta el tiempo de establecimiento de conexiones, ya que se pueden reutilizar las conexiones de transporte.

Relación entre las primitivas

SERVICIO	PRIMITIVA APLICACION	PRIMITIVA PRESENTACION	PRIMITIVA SESION
Establecimiento de conexión	A-ASSOCIATE	P-CONNECT	S-CONNECT
Liberación de conexión	A-RELEASE	P-RELEASE	S-RELEASE
Inicio de transacción	C-BEGIN	P-SYNC MINOR	S-SYNC MINOR
Rollback	C-ROLLBACK	P-RESYNC	S-RESYNC
Commit	C-COMMIT	P-SYNC MAJOR	S-SYNC MAJOR
Transferencia de datos (no asegurada)		P-DATA	S-DATA
Comienzo de actividad		P-ACTIVITY START	S-ACTIVITY START

Comentario

A partir de este momento comenzaremos a analizar las capas inferiores del modelo OSI. Tienen una filosofía completamente diferente, ya que están mas orientadas a la comunicación de los datos y no tanto a la organización lógica de los mismos. También, en diversas arquitecturas de red, se encontraran implantadas de manera diferente. Así como en los temas anteriores mostramos ejemplos de la implantación de estas capas en el modelo OSI, de aquí en adelante nos centraremos mas sobre TCP/IP, ya que se ha convertido en la arquitectura de red más exitosa.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI (continuación)

Capa de Transporte

Función

La capa de transporte trabaja en los puntos finales de la transmisión, es decir en el receptor y en el transmisor. Su objetivo es proporcionar un servicio a través del cual puedan enviarse cadenas de bits a través de una infraestructura de red, con la calidad de servicio que el usuario requiera (capa de sesión o programa de aplicación en el caso de TCP/IP) sin importar la calidad características que la red tenga.

La capa de transporte puede proporcionar servicios orientados a conexión (connection oriented) o sin conexión (connectionless), y como ya se mencionó, proporciona el nivel de servicio que el usuario requiera e indique a través del parámetro QOS (calidad de servicio).

Servicios Orientados a Conexión

Establecimiento de conexiones: A través de este servicio, las entidades de la capa de sesión, que se identifican a través de sus direcciones (TSAPs) pueden pedir a la capa de transporte que establezca una conexión entre ellas con un cierto nivel de servicio. Puede solicitarse más de una conexión entre las mismas direcciones.

Durante la fase de establecimiento de conexión, la capa de transporte se encarga de mapear las direcciones de la capa de transporte a direcciones de la capa de red, obtener una conexión de capa de red que satisfaga los requerimientos de la capa de sesión, tomando en cuenta la calidad y costo de los servicios. Además de decidir si deberá multiplexar o dividir el flujo de datos entre las conexiones de nivel red. La capa de transporte deberá también determinar la unidad de transmisión máxima (en algunas ocasiones deberá realizar segmentación y reensamblaje)

Transferencia de datos: Permite el intercambio de datos en modo full-duplex. La transferencia de datos se lleva a cabo de acuerdo a la calidad de servicio solicitada, y comprende transferencias de mensajes de longitud arbitraria, y transferencia de mensajes expeditos de longitud limitada (no sujetos a mecanismos de control de flujo). Puede realizar secuenciación de los mensajes (para poder después identificar el orden de estos dentro de una transmisión). Segmentación, concatenación, multiplexación o división del flujo de datos. En caso de que la transmisión de datos no pueda mantener el nivel de servicio solicitado, la conexión termina y las entidades de sesión son informadas

Desconexión: Permite la liberación de una conexión entre dos entidades de sesión a solicitud de cualquiera de estas. Las entidades de la capa de sesión son informadas de esta situación.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Servicios

La funciones de la capa de transporte están definidas en CCITT X.214 o ISO 8072, y las primitivas son las siguientes:

T-CONNECT
T-DATA
T-EXPEDITED DATA
T-DISCONNECT

La especificación de los protocolos de la capa de transporte de OSI están definidos en CCITT X.224 o ISO 8073.

Relación con la capa de Red

El trabajo de la capa de transporte es mas o menos intenso dependiendo de la confiabilidad de la infraestructura de red y de la calidad de servicio solicitada por el usuario de la capa de transporte. Si el servicio solicitado implicaba que se tuviera un transporte de datos perfecto, y la red es muy propensa a producir errores en la transmisión, se tendrán que realizar más actividades que si la red fuera confiable. Lo inverso también se aplica. Por esto, de acuerdo a las circunstancias, será adecuado o no el que la capa de Transporte utilice ciertos mecanismos, y de acuerdo a la implementación (es decir ya un producto utilizable, no solo un estándar) podrán incluirse algunas funcionalidades.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Tipos de Capas de Red

Clasificación	Tasa de Transmisión y Errores	Tipo físico de red.
Tipo A	Tasa aceptable de errores residuales (no detectados). Tasa aceptable de errores detectados.	Línea Dedicada confiable o red de conmutación de paquetes confiable
Tipo B	Tasa aceptable de errores residuales(No detectados), tasa no aceptable de errores detectados.	Red de conmutación de paquetes no confiable
Tipo C	Tasas no aceptables de errores detectados y no detectados	Red no orientada a conexión.

Tipos de Capas de Transporte

El nivel más básico de funcionalidad lo proporciona la clase 0 de protocolos de transporte, y el más complejo la clase 4, de hecho esta clase se ha derivado del protocolo TCP que se analizará mas adelante.

Clase	Nombre	Tipo de Red	Características
0	Clase Simple	A	No multiplexa, No se Recupera de Errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
1	Clase de recuperación básica de errores	B	No multiplexa, se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
2	Clase de Multiplexaje	A	Multiplexa, no se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
3	Clase de Multiplexaje y recuperación de errores	B	Multiplexa, se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
4	Clase de detección y recuperación de errores.	C	Multiplexa, divide la conexión de transporte entre muchas conexiones de red, permite el uso de redes no orientadas a conexión, recuperación de errores reportados por la capa de red, detección y corrección de errores no reportados por la capa de red.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

TCP

Funciones

El protocolo TCP descansa sobre IP en la arquitectura de red TCP/IP y a través de él se especifican los formatos de los datos y acuses de recibo que las dos computadoras (transmisora y receptora) intercambiarán con el fin de lograr una transferencia confiable, así como los procedimientos a través de los cuales las computadoras aseguran que los datos llegan correctamente. El protocolo no incluye la definición de las interfaces exactas que las aplicaciones utilizarán para solicitar los servicios de TCP ya que esto dependerá de las características del equipo y sistema operativo sobre las que se implante. TCP no define tampoco ninguna característica para el medio de transmisión que utilizara, y por lo tanto, este protocolo podrá implementarse de tal manera que utilice líneas telefónicas, enlaces de red de área local, satelitales, etc.

Puertos

Para definir el punto final de una comunicación, TCP utiliza el concepto de puerto (TSAP en OSI). A cada puerto se le asigna un número, que junto con la dirección de IP de una computadora (también conocida como dirección Internet o dirección de la capa de red), permiten definir el punto de acceso a determinada aplicación, por ejemplo se podría decir que el servidor de ftp de la DCAA se encuentra en (132.248.27.10,21).

Podemos pensar que TCP va colocando los segmentos (unidades de transmisión de TCP) en una cola a medida que van llegando, y que hay una cola para cada conexión. Una conexión está definida por dos puntos finales, por ejemplo si mi computadora con dirección 132.248.10.1 se quiere comunicar con el servidor de ftp mencionado antes, tal vez utilizando el puerto 1038: existiría una conexión definida por lo siguiente: (132.248.10.1, 1038) (132.248.27.10,21) con su cola correspondiente.

Extendiendo más este concepto, si otro usuario quiere comunicarse al mismo servidor a través de su computadora (132.248.67.3) y número de puerto 988, existiría otra conexión definida por (132.248.67.3,988) (132.248.27.10,21), que también tendría esta cola para que el software de TCP fuera colocando los segmentos que llegaran.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Formato de un segmento TCP

0	4	10	16	24	31
SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	RESERVED	CODEBITS	WINDOW		
CHECKSUM			URGENT POINTER		
OPTIONS(SI HAY)				PADDING	
DATA					
...					

Al principio del mismo encontramos los puertos de origen y destino, después viene el número de secuencia que identifica este segmento, mas adelante el número de secuencia que se espera (es decir, este número es para el control de la comunicación en el sentido inverso). Después encontramos un campo HLEN que especifica el tamaño del header en múltiplos de 32 bits, el campo de ventana indica cuantos bytes se pueden recibir. El campo de checksum sirve para verificar la exactitud de la información.

El campo CODE BITS se compone de 6 bits, cada uno con un significado. Hablando específicamente del bit número 6, este indica que los datos deberán transmitirse en modo urgente, es decir, ignorando los mecanismos de control de flujo. Esto es importante cuando se desea transmitir comandos que aborten o interrumpan al programa en el otro extremo. En este caso el campo URGENT POINTER tiene significado, e indica en donde acaban los datos urgentes.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Tamaño de segmento

Un aspecto importante en TCP es la determinación del tamaño máximo de segmento. El tamaño máximo de segmento deberá negociarse al inicio de la conexión, y de esto dependerá en mucho la eficiencia de la transmisión de datos. Cuando se escoge un tamaño máximo de segmento demasiado pequeño no se aprovecha al máximo la capacidad de transmisión de la red, si por otra parte, este es demasiado grande, la transmisión se vera afectada por el tiempo que consumirá a la capa de red la segmentación de estos en paquetes que se ajusten al MTU (Unidad máxima de transferencia para el enlace de red correspondiente). No existe un mecanismo estándar para encontrar el tamaño máximo de segmento mas conveniente.

Checksum

El campo de CHECKSUM sirve para verificar la integridad de los datos y el header de TCP. Se obtiene al realizar el complemento a uno de la suma en complemento a uno de todos los campos del segmento de TCP. Para realizar esta suma, se antepone al segmento de TCP un pseudoheader, también se asume que el campo de CHECKSUM es 0, y se agregan los bits necesarios para que su numero(es decir el numero de bits en el segmento y en el pseudoheader) sea un múltiplo de 16 bits.

Acuses de Recibo

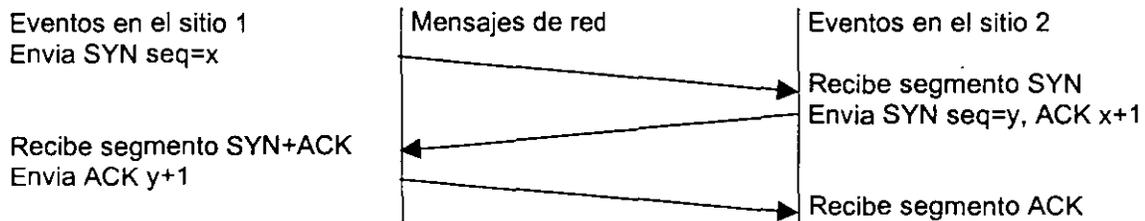
Debe quedar claro que los acuses de recibo (acknowledges) no se refieren a los segmentos, sino a los bytes. Cada acknowledge, indica el siguiente byte que se espera recibir. Este acknowledge refleja, dentro del flujo de bytes que se transmitió, cuales son los bytes que el receptor ha podido reensamblar en un flujo continuo. Por ejemplo, si el emisor ya ha transmitido 5000 bytes después del numero 5000, pero por alguna razón el receptor solo ha podido captar del byte 5500 en adelante (el primer segmento se ha retrasado), el campo de acknowledge seguirá reflejando el valor 5001. TCP deberá decidir si retransmitir todos los paquetes o solo el primero. Esto es una decisión complicada, ya que no tiene manera de saber cuales son los paquetes que han llegado correctamente.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Inicio de conexión

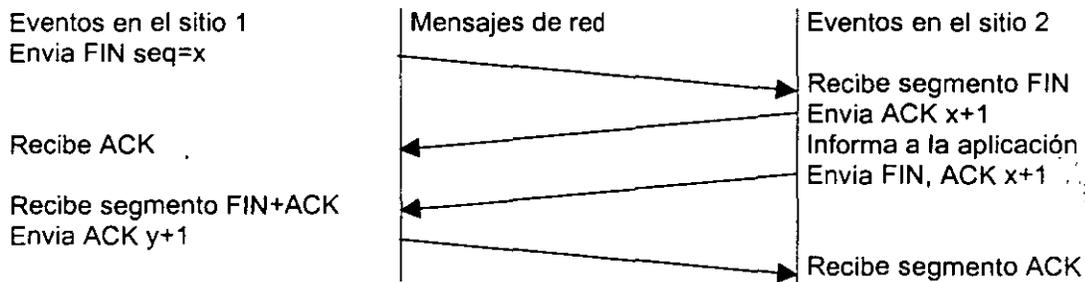
A través del uso de los bits en el campo CODE BITS se pueden enviar estas señales de sincronización (bit 2) y acknowledge (bit 5)



Es muy importante notar que al finalizar el proceso de conexión, ambas partes ya acordaron los números de secuencia iniciales que utilizarán en sus transmisiones. Los números de secuencia no pueden ser siempre 1 al inicio, ya que esto podría acarrear problemas en cuanto existieran condiciones de error en los equipos.

Cierre de conexión

El proceso de cerrar una conexión de TCP involucra el envío de un segmento con el bit FIN encendido (este bit forma parte del campo CODE BITS). El receptor envía un acuse de recibo del FIN e informa al programa de aplicación de su lado que no hay más datos disponibles. Una vez que la conexión se encuentra cerrada, TCP no acepta más datos de esa dirección. Mientras tanto, pueden seguir transmitiéndose datos en la dirección contraria, hasta que la conexión se cierre en ese sentido.



Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Puertos Comunes

Ya que TCP es la capa superior en la arquitectura TCP, sirve para proporcionar direcciones a través de las cuales podremos acceder a las diferentes aplicaciones que corren sobre este protocolo. Los servidores WWW, SMTP, FTP, Telnet, etc. generalmente se encuentran en puertos bien conocidos, de tal manera que las aplicaciones cliente pueden localizarlos con facilidad. Por otra parte, los puertos a través de los cuales estas aplicaciones cliente se comuniquen no son realmente importantes (los servidores no van a buscar a los clientes sino viceversa) En la siguiente tabla encontraremos algunos de los números de puerto asignados por default a las aplicaciones mas comunes.

Número decimal	Nombre aplicación	Nombre en UNIX	Descripción
0			Reservado
1	TCPMUX	-	Multiplexor TCP
5	RJE	-	Remote Job Entry
7	ECHO	echo	Echo
20	FTP-DATA	ftp-data	File Transfer Protocol (datos)
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Terminal Connection
119	NNTP	nntp	USENET News Transfer Protocol

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

UDP

Funciones

Este protocolo proporciona los servicios de la capa de transporte, sus servicios, a diferencia de los de TCP no son orientados a conexión (connection less). A través de UDP, la comunicación ya no solo se define en base a direcciones de computadoras, sino de aplicaciones dentro de estas computadoras. Esta funcionalidad también la proporciona TCP a través de los puertos y conexiones, sin embargo, la forma en que este mecanismo trabaja en UDP es diferente.

El concepto de conexión no es utilizado en UDP, sino que los puertos se pueden visualizar como áreas de memoria en donde existen colas de mensajes. Los mensajes se encolan a medida que van llegando, y los procesos los toman.

UDP representa el mecanismo principal a través del cual, los programas de aplicación envían datagramas (o paquetes de datos) a otros programas de aplicación.

UDP no garantiza ningún nivel de servicio, no ordena los mensajes, no cuenta con mecanismos de control de flujo, mecanismos contra la duplicación ni contra la pérdida de mensajes. Simplemente, sirve para que las aplicaciones tengan puntos de entrada a un servicio de transferencia de datos a través de la red, ya que las capas inferiores no proporcionan el esquema de direccionamiento necesario para llevar esto a cabo.

Formato de mensajes de UDP

Al igual que las de TCP, las unidades de protocolo de UDP se dividen en dos partes: encabezado o header y un área de datos.

El campo UDP Source port es opcional, el campo UDP MESSAGE LENGTH indica la longitud en bytes del header y el área de datos, aunque el campo de CHECKSUM es opcional, es altamente recomendable que las aplicaciones lo utilicen, ya que es la única manera de garantizar que los datos sean correctos. Se obtiene mediante un mecanismo igual que el utilizado para obtener el CHECKSUM en TCP.

0	16	31
UDP SOURCE PORT	UDP DESTINATION PORT	
UDP MESSAGE LENGTH	UDP CHECKSUM	
DATA		
...		

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Transporte (continuación)

Puertos conocidos de UDP Al igual que lo que sucede con segmento de datos de TCP, el paquete de datos de UDP es encapsulado dentro de un paquete IP, y este a su vez en un frame.

Número decimal	Nombre aplicación	Nombre en UNIX	Descripción
0			Reservado
7	ECHO	echo	Echo
37	TIME	time	Time
67	BOOTPS	bootps	Bootstrap protocol server
68	BOOTPC	bootpc	Bootstrap protocol client
111	SUNRPC	sunrpc	Sun Microsystem RPC

3.3 Detalles del Modelo OSI (continuación)

Capa de Red

Función

La capa de red se encarga del enrutamiento, conmutación e intercambio de información entre redes, con el fin de proporcionar un camino entre los puntos finales (de red) en una transmisión de datos. El objetivo es proporcionar un servicio de transferencia de datos que sea uniforme, independientemente de las redes físicas que se utilicen para llevar esto a cabo.

La capa de red opera sobre múltiples redes reales, estas redes pueden ser de tecnología diferente (Redes de Area Local Redes X.25, ISDN, etc.). En la terminología de OSI estas redes son llamadas Subredes (subnetworks).

La capa de red puede proporcionar servicios de dos tipos: Los orientados a conexión y los connectionless.

Servicios utilizados por la ISO

ISO nunca se puso de acuerdo en que esquema utilizar, y se adoptaron los dos, para los servicios orientados conexión generalmente se utiliza X.25 de CCITT, y para los servicios sin conexión se utiliza CLNP ISO 8473. Dentro de la arquitectura de TCP/IP, IP es un protocolo connectionless.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Servicios**Orientados a
Conexión
(Connection-
oriented)**

En los servicios son orientados a conexión(en base a circuitos virtuales), se tienen tres fases en la transmisión de datos entre dos entidades de la capa de red, en la primera se establece la conexión, después se pueden intercambiar datos, y al final se libera la conexión.

Esto es similar al sistema telefónico. El sistema telefónico es informado por el usuario del destino que se desea alcanzar (discando el número), después de esto, se establece un camino entre el usuario que llama y el teléfono que se disco, generalmente reservando recursos de cierto tipo, que permanecerán asignados por toda la duración de la llamada, después de que la llamada es aceptada. se puede conversar. Un servicio orientado a conexión tiene las siguientes características:

- (a) La red garantiza que todos los paquetes serán enviados en orden, sin pérdida o duplicación, si ocurre algo que no lo permita, la red desconectara a las entidades en comunicación.
- (b) Se establece un camino único para el flujo de datos, y todos los datos fluyen a través de el, si algo sucede que no permita seguir utilizando este camino, la red desconecta a las entidades en comunicación.
- (c) La red garantiza cierta capacidad de transmisión (ancho de banda) para las entidades que se comunican, si no la utilizan, el recurso se desperdicia.
- (d) Si la red se satura, se rechaza cualquier intento de establecer una conexión (como en las compañías telefónicas).

**Servicios no
orientados a
conexión.
(connection-
less)**

Si los servicios son connectionless(en base a datagramas), la capa de red transmite hacia la red real un paquete de datos, que incluye la dirección a la que deberá enviarse. La red deberá hacer su mejor esfuerzo para enviar los datos, pero hay probabilidades de que los datos se pierdan, se dañen o sean duplicados.

Asimismo, cada paquete es enrutado independientemente, y la red no garantiza que estos llegaran en orden a su destino. El modelo connectionless es similar al servicio postal.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Pros de servicios orientados a conexión

Las redes son utilizadas de manera primordial para transferir archivos y para acceder a sistemas remotos a través de emulación de terminal. Estas aplicaciones requieren que los paquetes permanezcan ordenados, y no toleran la pérdida de paquetes. Esto es complejo, y es mejor que este servicio se encuentre en la red, lejos de los sistemas que se desean comunicar.

Los servicios orientados a conexión permiten que los enrutadores sean más rápidos, ya que las decisiones complejas se realizan al inicio de la comunicación, después bastará con que el enrutador busque en una tabla el camino que deberá seguir el paquete de datos.

Es mejor rechazar conexiones que afectar la capacidad de transmisión sobre las que ya están establecidas.

Es mejor para la capa de transporte, que la capa de red defina un camino único para toda la conexión, ya que así la capa de transporte podrá determinar el tamaño de segmento que sea más eficiente, también será más sencillo determinar los niveles de retransmisión que deberán adoptarse por la pérdida de un acuse de recibo, ya que se conocerá el tiempo de viaje de cada paquete.

Una capa de red orientada a conexión, elimina la necesidad de que la capa de transporte sea compleja.

Pros de los servicios no orientados a conexión

La mayoría de las redes orientadas a conexión están construidas de tal manera que si algo falla durante la transmisión, el circuito se interrumpe inmediatamente, tal vez, sin posibilidad de que se recuperen los paquetes que en ese momento se encontraban en tránsito. Por lo tanto, en lugar de evitar esfuerzos para la capa de transporte, los duplica.

Muchas aplicaciones no requieren que los paquetes sean enviados en orden. En particular, la transmisión de voz, en donde un pequeño porcentaje de paquetes perdidos no afecta la calidad del sonido. También, la transferencia de archivos puede ser implantada en base a un protocolo no secuencial, que sería más adecuado para redes de alta velocidad.

El tráfico en una red no es uniforme, es decir, hay momentos en los que se transmiten datos de manera masiva, y hay otros en los que no existe nada. Es mejor tener una división estadística de los recursos que apartar para que se desperdicien.

Es mejor que la capacidad de transmisión se degrade, que no permitir el acceso mas que a algunos pocos usuarios afortunados.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

X. 25

Función

X.25 es un conjunto de protocolos incorporados en una red de switcheo de paquetes. La red de switcheo de paquetes esta hecha de servicios de switcheo que originalmente fueron establecidos para conectar terminales remotas a sistemas host de mainframes.

Una red de switcheo de paquetes X.25 utiliza switches, circuitos y rutas disponibles para proporcionar la mejor ruta en cualquier momento. Dado que estos componentes cambian rápidamente dependiendo de las necesidades y de la disponibilidad, son representadas por nubes. Las nubes indican una situación cambiante o que no existe un conjunto estándar de circuitos.

Las primeras redes X.25 usaban líneas telefónicas para transmitir los datos. Este fue un medio no confiable que tenía demasiados errores, por lo que X.25 incorporó un chequeo excesivo de errores. Debido a todo el chequeo de errores y retransmisión, X.25 puede parecer lenta.

X.25 fue adoptado por ISO con el numero 8208, este estándar no especifica como construir una red que proporcione un servicio orientado a conexión, sino la manera de interaccionar con una. Especifica la interfaz entre un host o nodo final (conocido en X.25 como DTE) y un enrutador (conocido en X.25 como DCE)

X.25 especifica los tres niveles, red, enlace de datos y físico, pero ahora solo atenderemos el nivel superior o de red.

Conexiones con X.25

Al establecer una conexión, X.25 le asigna un numero, que se denomina Numero de Circuito Virtual, este numero solo tiene significado entre el DTE y el DCE locales. X.25 solo especifica lo que sucede entre el DTE y el DCE locales.

Una llamada puede ser iniciada por cualquiera de las partes (SVC Switched Virtual Circuit), o inclusive, encontrarse disponible de manera permanente(PVC Permanent Virtual Circuit).

Cada paquete de datos contendrá dentro de su encabezado, el numero de circuito virtual al que pertenece, en lugar de las direcciones fuente y destino completas, esto disminuye la cantidad de datos que se intercambian, y la velocidad a la que los enrutadores pueden tomar sus decisiones.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

**Formato del
identificador
de circuito
virtual**

Los identificadores de circuito virtual son de una longitud de 12 bits, y se componen de dos partes, el grupo al que pertenece este circuito virtual, y el número de circuito virtual en sí. De esta manera, se puede reservar el grupo 0 para los paquetes de control, otro grupo para los circuitos permanentes otro más para las llamadas recibidas y uno más para las llamadas de salida. Esto es muy útil ya que evita posibles choques en el uso de los números de circuito virtual (por ejemplo si se desea establecer una llamada en el mismo momento en que se recibe una).

**Estableci-
miento de
llamadas**

Si un DTE A quisiera comunicarse con el DTE B, el DTEA deberá escoger un número de circuito virtual de salida que no se encuentre en uso. Entonces, mandará un paquete de solicitud de llamada.

A través de un mecanismo no definido, el DCE A informará al DCE B que el DTE A desea comunicarse con el DTE B. El DCE B escoge un número de circuito virtual que no este en uso por el DTE B. Debido a que ambas partes pueden escoger el mismo estándar para agrupar las llamadas de entrada y de salida, el número que se escoge para el circuito virtual del lado B casi nunca será el mismo que del lado A. El paquete que recibe el DTE B puede ser diferente al que envió el DTE A en los campos de identificador de circuito virtual (por lo que ya se menciono) y en el tamaño de paquete en el campo facilities. Si el DTE B acepta la llamada, manda un paquete indicándolo al DCE B. El número de llamada aceptado será el número recibido por B. Entonces el DCE B se comunicará de alguna manera no especificada con el DCE A, el cual a su vez notifica al DTE A que la llamada ha sido aceptada

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Transmisión de datos

Una vez que la llamada se ha establecido, la transferencia de datos es full duplex. Los paquetes de datos pueden ser en dos formatos, en uno los números de secuencia son de 3 bits, y en otro es de 7 bits. El uso de uno u otro no puede ser cambiado a la mitad de una llamada. El bit Q se puede utilizar para cualquier fin. El bit M (more) sirve para transmitir paquetes mas largos que el máximo permitido por el enlace DTE/DCE. El DTE parte el paquete en pedazos del tamaño máximo permisible y les coloca el bit M, excepto al ultimo.

El bit D determina si el acuse de recibo fue enviado por el DCE o el DTE destino. Cada paquete tiene un numero de secuencia. Mediante un procedimiento de acuse de recibo similar al que se vio para TCP, X.25 puede controlar el flujo de datos. solo que aquí es en base a paquetes no a bytes, y el tamaño de la ventana es fijo.

En el momento en que se contrata el servicio, (recordemos que el protocolo X.25 permite conectarse a una red publica), se pueden especificar ciertas características por ejemplo, si el tamaño de ventana será fijo para todas las llamadas o puede negociarse, si el tamaño de los paquetes es fijo o puede negociarse, si se puede negociar la tasa de transmisión, eliminar las llamadas de entrada o de salida, etc.

Liberación de la conexión

El mecanismo para liberar una conexión es a través de un clear request originado por un DTE hacia su DCE. El DCE informa al DCE del otro extremo y a su vez al DTE del otro extremo, si esto es aceptado, la secuencia se presenta en el sentido contrario.

Cuando se detecta un problema en la conexión (alguno de los enlaces se ha caído o bien, la sincronización entre el DTE y el DCE se ha perdido), X.25 puede mandar un clear request o un reset (que coloca los números de secuencia en 0), no tan común es que la comunicación se restablezca sin problemas.

Los paquetes de interrupción, no están sujetos al flujo de datos, y son enviados inmediatamente a su destino, sin embargo. no puede enviarse otro hasta que se haya recibido el acuse de recibo del anterior.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Diferencias de operación entre connection oriented y connectionless

La implementación del servicio de red orientado a datagramas es más complicada que su contraparte orientada a circuitos virtuales. Como un ejemplo de esto, podemos mencionar el caso de la fragmentación de los paquetes (recordemos que estos deberán ser de un tamaño máximo acorde al medio de transmisión). En el caso de X.25, simplemente se marcaba cada paquete con un bit M, el cual indicaba que seguían más paquetes. En cambio, en un servicio orientado a datagramas, esto no es suficiente ya que los paquetes no se reciben en orden. También deberá pensarse en el mecanismo que la capa de red deberá seguir para reensamblar estos paquetes, lo cual es costoso en recursos de memoria y procesador.

Estrategia de estudio de los servicios connectionless

Analizaremos los servicios connectionless con respecto a tres áreas:

- (a) Que características y como son proporcionados los servicios connectionless, especificando el formato de las unidades de protocolo.
 - (b) Como los nodos finales saben si deberán utilizar un enrutador o no para comunicarse con otro nodo, y como llegan a saber en donde se encuentra ese enrutador.
 - (c) Los algoritmos de enrutamiento que utilizan los enrutadores para definir el camino que seguirán los datagramas.
-

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Esquema de Direcciones

Para poder entender mas a fondo que características y como son proporcionados los servicios de la capa de red, deberemos analizar la estructura de direccionamiento y las características que deben tener las direcciones en este nivel. Nos enfocaremos a los esquemas utilizados en IP.

En la vida diaria, estamos acostumbrados a utilizar direcciones jerárquicas, por ejemplo, cuando enviamos una carta, especificamos el país, la ciudad, la colonia, la calle y el numero dentro de esa calle al cual la carta deberá llegar. esto es una estructura jerárquica. La complejidad de un sistema de asignación de nombres de calles que garantizara un nombre único a nivel mundial seria inmensa. Por lo anterior, al especificar en que país, ciudad y colonia se encuentra una calle, reducimos el problema a que el responsable de los nombres de calles dentro de una colonia asigne nombres únicos.

Con las redes de computadoras sucede algo similar. En primer lugar, las direcciones deberán ser únicas en la región de influencia de la red, si hablamos de la Internet esto es a nivel mundial. Por otra parte, el trabajo de un centro que designara las direcciones únicas seria enorme. Por eso se designan centros regionales que tienen la capacidad de definir una parte de la dirección jerárquica. Si definimos cuatro niveles en la estructura jerárquica, una dirección ejemplo se vería como 132.248.27.10, en donde cada uno de los puntos, representa una jerarquía. Cabe mencionar que por ejemplo, las direcciones de la capa de enlace de datos no son jerárquicas, ya que, como sabemos, esta capa tiene el objeto de suministrar conectividad entre puntos contiguos, típicamente estos puntos contiguos existen dentro de la misma subred.

Clases de direcciones IP

Clase A	0	7 Bits Identificación de red	24 Bits Identificación de host
Clase B	1 0	14 Bits Identificación de red	16 Bits Identificación de host
Clase C	1 1 0	21 Bits Identificación de red	8 Bits Identificación de host
Clase D	1 1 1 0	28 Bits Dirección multicast de grupo	
Clase E	1 1 1 1 0	27 Bits (reservados para futuro uso)	

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Direcciones especiales

Existen números con significado especial cuando se utilizan dentro de una dirección, por ejemplo, el número 0 representa "este" y el número 1 "todos". Por ejemplo la dirección 132.248.255.255 es un broadcast hacia la red 132.248, la 132.248.27.255 es un broadcast hacia la subred 132.248.27., la 0.0.0.0 se utiliza cuando el host no conoce su dirección y desea solicitarla. Otra dirección especial es la 127.x.x.x. que representa un loopback.

Además existen las direcciones clase D o de multicast, es decir, especifican la dirección de mas de una maquina, estas se distinguen porque comienzan con 1110.

Definición de IP

Se encuentra definido en el RFC 791 (Como contraparte, en OSI el protocolo CLNP esta definido como "Protocol for Providing the Connectionless-mode Network Service" en ISO 8473), también veremos la forma en que la red reporta errores en ICMP, esto se encuentra en el RFC 792 (Como contraparte, en OSI esto se encuentra en el documento 8473). El formato de los paquetes de datos de IP es muy similar al del CLNP.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Paquete de IP

La dirección fuente y destino es de 32 bits. La longitud del header se especifica en el campo HLEN, esta se expresa en múltiplos de 32 bits.

0	4	8	16	19	24	31	
VERS		HLEN		SERVICE TYPE		TOTAL LENGTH	
IDENTIFICATION				FLAGS		FRAGMENT OFFSET	
TIME TO LIVE			PROTOCOL		HEADER CHECKSUM		
SOURCE IP ADDRESS							
DESTINATION IP ADDRESS							
IP OPTIONS (SI HAY)						PADDING	
DATOS							
...							

El campo total length contiene la longitud del header mas el campo de datos, su nombre puede llevar a confusiones, pues si el paquete se fragmenta, el campo expresara la longitud del fragmento, no del paquete antes de partirse.

El cheksum se obtiene con un procedimiento de suma de palabras de 16 bits en complemento a 1, y después tomando el complemento a 1 del resultado. Este solo se aplica sobre el header.

El campo tiempo de vida, sirve para evitar que paquetes viejos sigan circulando por la red, con lo que se podría causar que existieran al mismo tiempo dos paquetes diferentes con el mismo numero de secuencia. Esto se expresa en segundos. Debido a la dificultad que existe en calcular el tiempo de viaje de un paquete, generalmente este campo es utilizado mas como un contador de saltos.

El bit de "permite fragmentación" o DF, especifica si el paquete puede fragmentarse en el camino.

El identificador del paquete viene en el campo identificación, esto sirve para saber que fragmentos pertenecen a un paquete original.

El campo fragment offset sirve para saber en que parte del paquete original cae determinado fragmento.

El bit MF indica si a este fragmento le siguen otros.

El campo Version especifica la versión de TCP/IP que se esta utilizando.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Paquete de IP

(Continuación) El campo protocolo especifica que protocolo esta utilizando el área de datos del paquete, por ejemplo TCP UDP, ICMP, etc.

El campo Type of Service es de un byte, y se compone de 3 bits de prioridad y tres bits que definen si lo que se desea es poco retardo (bit D), buena capacidad de transferencia (bit T), o confiabilidad (bit R). Depende del enrutador como tratar a los paquetes dependiendo de estos bits.

El campo de opciones puede especificar si se desea guardar la ruta que ha atravesado el paquete, especificarle una ruta, etc.

Ruteo

El conocimiento entre vecinos, es decir, como un nodo sabe cuales son sus vecinos es el segundo problema que analizaremos. Podemos decir que el problema es diferente, dependiendo de la localización del nodo, ya sea en una LAN o en un enlace punto a punto.

Si el nodo se encuentra en un enlace punto a punto, el problema se limita a que el enrutador que se encuentra del otro extremo del enlace, de a conocer y conozca el mismo, la dirección del nodo que tiene unido por esa interfaz. Posiblemente, el enrutador tenga varios enlaces punto a punto. En el caso de IP este problema es resuelto desde el momento de la configuración del enrutador, ya que se le configuran las tablas necesarias para que conozca la dirección de red y la mascara de cada una de sus interfaces. El enrutador entonces, puede darlas a conocer.

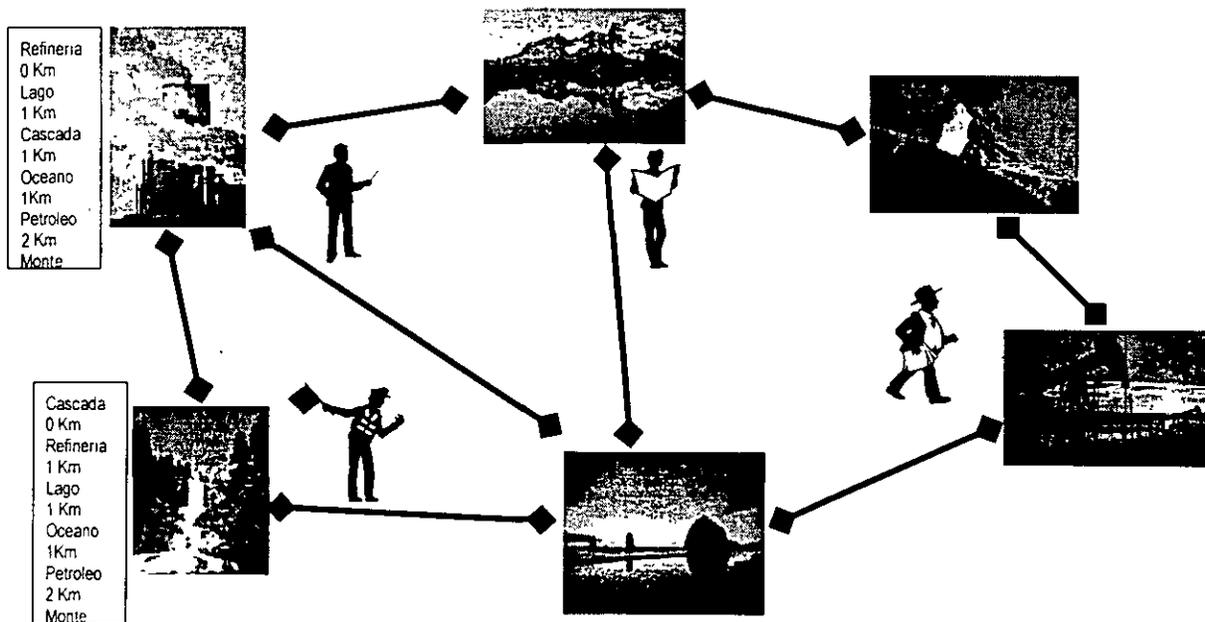
Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Algoritmo de Enrutamiento de Estado de Enlace

También conocido como "Bellman-Ford" puede ser entendido a través de la siguiente analogía:

Una persona se encuentra en un pueblo que también es una intersección de caminos, su trabajo es colocar avisos en esta intersección, estos avisos deberán contener el nombre de cada pueblo y la distancia que falta para llegar a él. Puede comenzar colocando un letrero con el nombre de esta intersección indicando que faltan 0 km. Entonces, puede continuar midiendo la distancia que existe entre este pueblo y sus vecinos inmediatos, anotando además la información que se encuentra en los letreros de ese pueblo. Después de un rato, y si en cada pueblo había una persona dedicada a la misma labor, contara con un conjunto de letreros que indicaran las distancias a cada pueblo, y la dirección en la que se encuentra (aquella en donde hayamos visto que suma la distancia mas corta).



Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Algoritmo de estado de enlace para computadoras

El algoritmo para una red de computadoras va como sigue:

- 1) Cada ruteador es configurado con su propio ID
- 2) Cada ruteador es configurado, de tal manera que a cada enlace le corresponda un numero, o costo de enlace.
- 3) Cada ruteador, comienza con un vector de distancias de valor 0 para el mismo, y un valor de infinito para cualquier otro destino.
- 4) Cada ruteador transmite su vector de distancias a cada vecino, siempre que la información cambie.
- 5) Cada ruteador salva el vector de distancias mas reciente que haya recibido de cada uno de sus vecinos.
- 6) Cada ruteador calcula su propio vector de distancias, minimizando el costo a cada destino, a través del examen del costo hacia ese destino que haya sido reportado por cada vecino, agregandole el costo del enlace hacia ese vecino.
- 7) Los siguientes eventos causan un recalcuho del vector de distancias:
 - Recibir de un vecino, un vector de distancias diferente.
 - Descubrir que el enlace a un vecino se ha caído.

El algoritmo de vector distancia sufre de un tiempo de convergencia muy largo, es decir, una vez que existe un cambio en la topología de la red, este cambio puede tardar mucho tiempo en ser reportado a todos los puntos. Existen diversas maneras de solucionar este problema a través de "parches" al algoritmo, sin embargo, existe una alternativa en el uso de otro algoritmo diferente.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Algoritmo de Estado de Enlace

1. Cada ruteador es responsable de encontrar a sus vecinos y aprender sus nombres. Este punto puede ser resuelto facilmente en los enlaces punto a punto, transmitiendo un paquete especial a través de cada enlace. En IP, los ruteadores se configuran con las direcciones de las interfaces.
2. Cada ruteador construye un paquete conocido como "link state packet" o LSP, que contiene una lista de los nombres y costo de llegar a cada vecino. El LSP se genera periódicamente o cuando el costo de un enlace ha cambiado, o el enlace se ha caído.
3. El LSP, de alguna manera, es transmitido a todos los otros ruteadores, cada ruteador guarda el LSP mas reciente de cada ruteador.

La diseminación de los paquetes LSP no puede depender del enrutamiento, ya que precisamente este depende de los LSP deberá adoptarse un mecanismo de distribución que no dependa del enrutamiento, esto es, deberán transmitirse a cada vecino siguiendo las condiciones que se muestran a continuación. El numero de secuencia (que junto con el campo age sirve para que el ruteador que lo recibe sepa si es el mas reciente) deberá ser lo suficientemente grande como para que nunca se llegue al maximo excepto en los casos de enrutadores que trabajen mal. El campo age es colocado al máximo en el momento de que se genera, y cada enrutador deberá decrementarlo en 1 cuando pasa a través de el, y seguirlo decrementando mientras lo mantiene en memoria.

Cuando un enrutador recibe un LSP, deberá determinar si debe ser retransmitido (esto en el caso de que sea un LSP mas reciente y diferente al que tiene guardado) por algunos de sus enlaces(excepto a través del cual se recibió). Los LSP no son encolados inmediatamente, sino que son marcados, para el momento en que el enlace a través del cual se enviaran se encuentre disponible. Además para cada LSP debe de generarse un acuse de recibo(que se marcara para enviarse como los anteriores)

4. Cada ruteador, conociendo la topología de la red, calcula las rutas hacia cada destino. Una vez que el ruteador tiene un conjunto completo de LSPs, conoce la topología de la red, y puede calcular las rutas a los diversos ruteadores. Para organizar esta información se tienen varias bases de datos:
 - La base de datos de estados de enlaces, que consiste del LSP mas reciente de cada ruteador.
 - PATH. que consiste de tripletes (ID, costo, dirección). Cada triplete representa la mejor ruta a cada destino.
 - TENT, tiene la misma estructura que PATH, sin embargo, estas son rutas tentativas, una vez que se determina que una ruta dentro de TENT es la mejor posible, se mueve a PATH
 - La base de datos que el ruteador utiliza para enviar los paquetes por el mejor camino, que es simplemente la base PATH sin el campo de costo.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Algoritmo de Dijkstra

1. Se comienza con el ruteador actual, esta será la raíz del árbol. En la base PATH se coloca (ID,O,O)

2. Para cada nodo N en PATH, se examina el LSP de N. Para cada vecino M de N, se agrega el costo del enlace desde la raíz hasta N. Si M no está en PATH o TENT con un costo mejor, se agrega el triplete (M, costo, dirección hacia N) al TENT.

3. Si TENT se encuentra vacío, se termina el algoritmo, de otra manera se encuentra el triplete con menor costo de TENT y se mueve a PATH, se sigue al paso 2.

Los dos algoritmos (Vector de distancias y estado de enlaces) pueden ser mejorados si se permite que exista más de un camino hacia un destino determinado, de esta manera el tráfico puede dividirse haciendo un mejor uso de la red. Entonces los distintos caminos pueden elegirse utilizando un método round robin, al azar o dependiente de la carga de los enlaces.

Esto nos lleva a otro aspecto que no hemos tocado, el costo del enlace deberá variar dependiendo del tráfico en el mismo o deberá ser un número fijo, mas aun, este deberá ser encontrado por el ruteador, o deberá ser configurado por un humano?. No existe mucho a este respecto, y las opiniones son encontradas (para mayor referencia ver la bibliografía).

El ruteador enviara un paquete de datos por un camino determinado dependiendo de sus tablas, y de la dirección destino del paquete. En el caso de IP, el enrutador deberá comparar la dirección destino del paquete, con cada una de las direcciones destino en sus tablas, esta comparación deberá de chequear lo mas posible, es decir, el número de 1s en una mascara contigua deberá ser el mayor con un resultado positivo.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

RIP

Se encuentra definido en el RFC 1058, sin embargo, este fue escrito después de que RIP ya estaba ampliamente difundido. RIP está basado en el algoritmo de estado de enlace.

La porción del paquete que comienza con address family identifier y que termina con metric, puede aparecer hasta 25 veces dentro de un solo paquete, lo que significa que se pueden reportar 25 destinos dentro de un solo paquete.

El campo command sirve para distinguir peticiones de respuestas. Las peticiones pueden ser de un destino específico o generales. Las respuestas contienen los pares, (destino, costo).

Las respuestas pueden enviarse periódicamente, generalmente cada 30 segundos. Las respuestas pueden enviarse como resultado de una petición. Las respuestas pueden enviarse cuando la información cambie.

El campo versión es igual a 1. El campo Address Family Identifier es igual a 2 para IP. No hay posibilidad de transmitir una máscara. El campo metric tiene un valor máximo de 16, tiene una longitud de 32 bits únicamente con el fin de que el paquete contenga un múltiplo de 4 bytes.

OSPF

La especificación está disponible públicamente, por lo que varios fabricantes pueden implantarlo.

Se puede lograr enrutamiento en base a tipo de servicio, es decir, no solo la dirección destino, sino el tipo de servicio requerido por el paquete es determinante.

Se puede lograr el balanceo de cargas. Si existen muchas rutas hacia el mismo destino. OSPF puede distribuir el tráfico de manera equitativa.

Para hacer las redes más fáciles de administrar, permite dividir las áreas independientes, en donde cada área no conoce la topología de la otra.

Son autenticados todos los intercambios de información entre ruteadores, de tal manera que no será posible que un ruteador no autorizado envíe información (RIP puede causar errores de seguridad)

Cuando se trabaja en una LAN, un ruteador designado es el que se encarga de mantener la información.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Red (continuación)

Campo TYPE

Tipo	Significado
1	Hello(para probar si se puede llegar a un destino)
2	Database description (topology)
3	Link Status Request
4	Link status update
5	Link status acknowledgment

Mensajes de OSPF

OSPF envía mensajes HELLO periódicamente, para establecer y probar la accesibilidad de un vecino . El formato del mensaje hello se muestra en la figura 22. El campo NETWORK MASK contiene la mascara para la red a través de la cual se enviara el mensaje. El campo DEAD TIMER da el tiempo en segundos, después del cual el vecino se considera muerto. El campo HELLO INTER da el intervalo normal en segundos entre mensajes de hello que se muestra a continuación.

CHECKSUM		DATE	
TIME			
TIMESTAMP		LOCAL ENTRY	# HOSTS
DELAY 1		OFFSET 1	
DELAY 2		OFFSET 2	
....			
DELAY N		OFFSET N	

Para intercambiar mensajes de descripción de las bases de datos de OSPF, se utiliza un paquete como el que se muestra a continuación

VERSION (1)	TYPE	MESSAGE LENGTH
SOURCE GATEWAY IP ADDRESS		
AREA ID		
CHECKSUM	AUTHENTICATION TYPE	
AUTHENTICATION (octetos 0-3)		
AUTHENTICATION (octetos 4-7)		

Continúa en la siguiente página

3.3 Detalles del Modelo OSI (continuación)

Capa de Enlace de Datos

Función e

Historia

El propósito de la capa de enlace de datos es organizar los datos de las capas superiores en bloques de bits llamados frames, para la transmisión ordenada y control de errores.

La capa de enlace de datos fue concebida sobre la base ya establecida de estándares en los protocolos llamados de línea o de enlace (line protocols o link protocols). Los primeros protocolos de línea trabajaban en base a caracteres, ASCII o EBCDIC que se insertaban en el flujo de datos, indicando el principio o fin de estructuras de control. Un ejemplo de los protocolos de este tipo es el Binary Synchronous Control o BSC.

Más tarde, los protocolos evolucionaron, de tal manera que ya no eran necesarios los caracteres especiales para la delimitación y control de los mensajes, estos protocolos se denominan "orientados a bits". El más difundido de estos protocolos es el HDLC, que de una u otra manera aparece en todos los estándares de OSI para enlace de datos. Por ejemplo, X.25 en su capa 2 maneja el LAPB, ISDN utiliza el LAPD, y las redes de área local LLC.

Como ya mencionamos, la capa de enlace de datos está involucrada en la transmisión de datos a través de las líneas de comunicación, y con la detección y opcionalmente corrección de cualquier error que pudiera ocurrir. Puede proporcionar servicios orientados a conexión o sin conexión a la capa de red.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Enlace de Datos *(continuación)*

Servicios orientados a conexión

Cuando la capa de enlace de datos proporciona servicios orientados a conexión, debe de cumplir lo siguiente:

- Proporcionar las funciones necesarias para establecer, mantener y liberar conexiones de enlace de datos entre entidades de la capa de red.
 - Las unidades de transmisión se transfieran en orden y correctamente.
 - Señalar a la capa de red los errores irre recuperables que hayan ocurrido en la transmisión, a través de la desconexión del enlace.
-

Servicios no orientados a conexión

Cuando la capa de enlace de datos proporciona servicios sin conexión (p.ej. LLC tipo I en las LAN), simplemente esta encargada de transmitir frames, uno a la vez, sin recuperación de errores. Cualquier frame corrompido se descarta, y no se reportan frames perdidos al transmisor.

Definición de la capa de enlace de datos

La definición de la capa de enlace de datos se encuentra en CCITT X.212 o ISO 8886, a continuación veremos la estructura general de HDLC, después veremos dos de los principales estándares derivados de HDLC: LAPB para X.25 y LLC para las redes LAN. El primer caso nos presentara una implantación de protocolo de enlace de datos para líneas punto a punto, mientras que el segundo, para medios compartidos.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Enlace de Datos (continuación)

HDLC

Delimitación de Frames

En HDLC las unidades de transmisión se denominan frames. Cada frame es delimitado con una bandera de 8 bits, 01111110. El problema que podría ocurrir si en los datos se incluyera este patrón de bits se soluciona, insertando un 0 por cada 5 bits seguidos si se trata de datos.

Descripción del Frame HDLC

El campo de dirección es de 8 bits en LAPB o LAPD y de 16 bits en LLC. El campo de control indica el tipo de frame que se envía, y si se está utilizando un servicio orientado a conexiones, este indica el número de secuencia del frame (que puede ser de 1 o 2 bytes). El campo de información contiene los datos a transmitir (las unidades de protocolo de las capas superiores). El campo de checksum se obtiene por el método de redundancia cíclica, y sirve para asegurar que los frames llegan correctamente.

Modos de trabajo de HDLC

Aquí es necesario hacer un paréntesis para aclarar que HDLC puede trabajar en tres modos, pero principalmente en el modo maestro-esclavo y el modo equilibrado. En el primero o NRM (Normal Response Mode) existe el concepto de una estación maestro o primaria que puede mandar comandos a la estación esclava o secundaria, la cual solo puede enviar frames en respuesta a comandos. En el segundo o ABM (Asynchronous Balanced Mode), cada estación es equivalente y puede comunicarse de manera simétrica.

Tipos de Frame

Podemos encontrar tres tipos de frame en base al contenido del campo de control:

- Frames numerados que contienen información que se transmite cuando se está utilizando un servicio orientado a conexiones.
- Frames de supervisión, que son utilizados con un servicio orientado a conexiones para el control de errores y de flujo.
- Frames no numerados, utilizados para el establecimiento de una conexión, o para la transferencia de datos sin conexión.

Continúa en la siguiente página

3.3 Detalles del Modelo OSI Capa de Enlace de Datos (continuación)

LLC

Proyecto 802

El proyecto 802 de la IEEE es el que mas ha aportado al desarrollo de las especificaciones para redes de área local. Para una LAN generalmente hablamos de un medio de transmisión compartido. Así, deberá existir un mecanismo para que las diversas estaciones que se encuentran conectadas a este medio, puedan utilizarlo sin mayores complicaciones y sin entrar en conflicto con las demás. Podemos decir, entonces, que deberá haber un Medium Access Control (MAC), que junto con el LLC (Logical Link Control) cumplirá las labores necesarias en la capa 2 para que la transmisión pueda llevarse a cabo en una LAN. El estándar LLC se encuentra en 802.2 o ISO 8802-2.

Estándares más importantes para acceso al medio

IEEE 802.3 o ISO 8802-3 denominado CSMA/CD o ETHERNET ,
IEEE 802.4 o ISO 8802-4 denominado token bus
IEEE 802.5 o ISO 8802-5 denominado token ring

El formato de LLC esta dentro de la estructura de MAC (acceso al medio). Juntos definen el formato de un frame en una LAN. Existen dos campos, cada uno de un byte, para el direccionamiento.

El DSAP (Destination Service AccessPoint) es la dirección de la entidad de red que maneja los datos del frame. El primer bit indica si es una dirección individual o de grupo.

El SSAP (Source Service Access Point) indica la dirección de la entidad de red que envía los datos contenidos en el frame. El primer bit sirve para distinguir entre un comando y una respuesta.

En IEEE 802.2 se definen tres opciones para el LLC:

LLC tipo 1. Servicio sin conexión no confirmado
LLC tipo 2 Servicio orientado a conexiones similar a LAPB
LLC tipo 3 Servicio sin conexión confirmado.

Generalmente en redes CSMA/CD se utiliza el tipo 1, y el tipo 2 en redes token ring.

En LLC tipo 1 solo hay dos primitivas: DI-Data request y DI-Data indication. Los frames de HDLC que se utilizan son UI, XID y TEST. En el caso de las LAN, la estructura de LLC va dentro de la estructura de acceso al medio. Esta estructura sirve para que varias computadoras puedan compartir un solo medio de transmisión, sin que exista conflicto entre ellas.

Antes ya vimos que dentro de la capa de red, existían maquinas encargadas del enrutamiento de la información a través de una red de redes. Estos elementos se denominan enrutadores