

Arquitectura de Redes y Comunicaciones

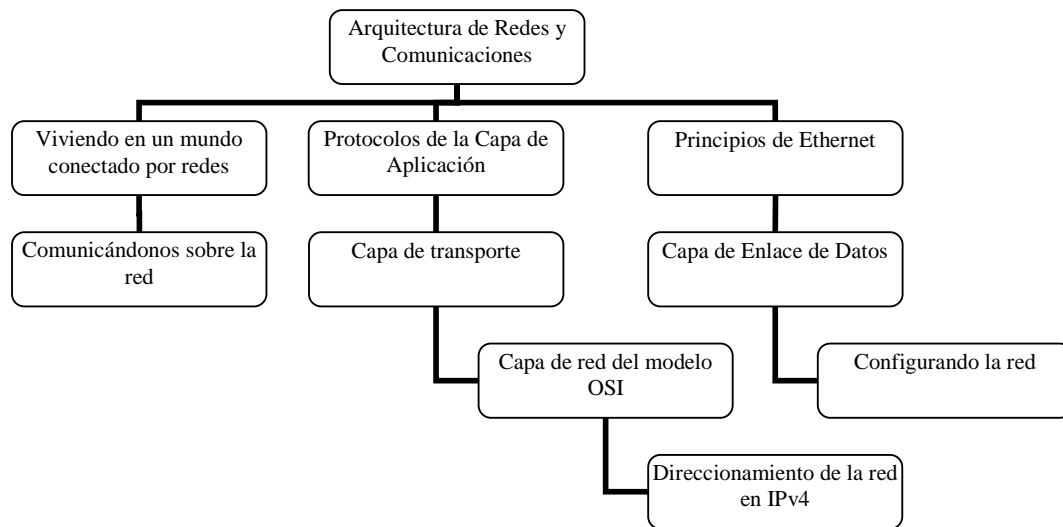
Índice

Presentación	5
Red de contenidos	6
Sesiones de aprendizaje	
SEMANA 1 : Viviendo en un mundo conectado por redes	7
SEMANA 2 : Comunicándonos sobre la red	23
SEMANA 3 : Protocolos y funciones de la capa de Aplicación – Parte I	43
SEMANA 4 : Protocolos y funciones de la capa de Aplicación – Parte II	57
SEMANA 5 : Capa de Transporte	69
SEMANA 6 : Capa de red del Modelo OSI	85
SEMANA 7 : Examen Parcial	
SEMANA 8 : Direccionamiento de red en IPv4	97
SEMANA 9 : Capa de Enlace de Datos	109
SEMANA 10 : Capa Física del Modelo OSI	115
SEMANA 11 : Principios básicos del Modelo Ethernet – Parte I	127
SEMANA 12 : Principios básicos del Modelo Ethernet – Parte II	139
SEMANA 13 : Planeando la red – Parte I	147
SEMANA 14 : Planeando la red – Parte II	155
SEMANA 15 : Configurando y examinando la red – Parte I	163
SEMANA 16 : Configurando y examinando la red – Parte I	171
SEMANA 17 : Examen Final	

Presentación

Este curso proporciona a los alumnos las habilidades necesarias para tener éxito en la instalación y configuración de redes. También ayuda a los estudiantes a desarrollar las habilidades necesarias para cumplir con el trabajo y responsabilidades de los técnicos de red, los administradores de red, y los ingenieros de redes. Proporciona conceptos teóricos relativos a las tecnologías actuales de las redes a profundidad, así como mucho trabajo práctico para la instalación de las redes y el uso de Internet.

Red de contenidos





Viviendo en un mundo conectado por redes

TEMA

Viviendo en un mundo conectado por redes

OBJETIVOS ESPECÍFICOS

- Comprender como la tecnología actual afecta nuestro modo de vivir
- Comprender la conexión física para comunicar una computadora a Internet
- Identificar los elementos de un computador

CONTENIDOS

- Viviendo en un mundo conectado por redes
- ¿Qué es la comunicación?
- Comunicación sobre redes
- La arquitectura de Internet

ACTIVIDADES

- Actividad de medios interactivos
- Uso del Packet Tracer

1. Viviendo en un mundo Conectado por redes:

Ahora estamos en un punto de inflexión crítico en el uso de la tecnología para ampliar y potenciar nuestra red humana. La globalización de la Internet se ha logrado más rápido de lo que nadie podría haber imaginado. La manera en que las relaciones sociales, comerciales, políticas se producen está cambiando rápidamente para mantenerse al día con la evolución de esta red mundial. En la próxima fase de nuestro desarrollo, gente innovadora utilizará la Internet como un punto de partida para crear nuevos productos y servicios específicamente diseñados para aprovechar las capacidades de la red.

Este capítulo presenta la plataforma de redes de datos sobre la cual nuestras relaciones sociales y de negocios dependen cada vez más. El elemento que sienta las bases para el estudio de los servicios, las tecnologías, y las cuestiones encontradas por los profesionales de la red, ya sea para diseñar, crear y mantener la red moderna.

1.1 Redes de Apoyo a la manera en que vivimos

Entre todos los elementos imprescindibles para la existencia humana, la necesidad de interactuar con otros elementos es de vital importancia. La comunicación es casi tan importante para nosotros como nuestra necesidad en el aire, el agua, los alimentos y la vivienda.

Los métodos que utilizamos para compartir ideas e información están en constante cambio y evolución. Desde la imprenta a la televisión, cada nuevo desarrollo ha mejorado y aumentado nuestra comunicación.

En un inicio las redes de datos se limitaron a intercambiar caracteres entre los sistemas informáticos conectados. Actualmente las redes han evolucionado para transportar voz, video, texto, gráficos entre los muchos tipos diferentes de dispositivos. Distintas formas de comunicación, anteriormente separadas han convergido en una plataforma común. Esta plataforma ofrece acceso a una amplia gama de alternativas y nuevos métodos de comunicación que permiten a las personas interactuar directamente con los demás casi instantáneamente.

El carácter inmediato de las comunicaciones a través de Internet alienta a la formación de comunidades a nivel mundial. Estas comunidades fomentan la interacción social que es independiente de la ubicación o de la zona horaria.

La comunidad mundial

La tecnología es tal vez el más importante agente de cambio en el mundo de hoy, ya que contribuye a crear un mundo en el que las fronteras nacionales, las distancias geográficas, y las limitaciones físicas se vuelven menos relevantes, y presentan cada vez menos obstáculos. La creación de comunidades en línea para el intercambio de ideas y de la información tiene el potencial de aumentar la productividad de oportunidades en todo el mundo. A medida que la Internet conecta a la gente, y promueve la comunicación sin restricciones, se presenta como la plataforma de

apoyo a la gestión de las empresas, para hacer frente a situaciones de emergencia, y para informar a las personas, y para apoyar la educación, la ciencia, y el gobierno.

Es increíble lo rápido que la Internet se convirtió en una parte integral de nuestra rutina diaria. La compleja interconexión de los dispositivos electrónicos y medios de comunicación que conforman la red es transparente para los millones de usuarios que hacen un valioso y personal parte uso de la red.

Redes de datos que alguna vez solo sirvieron para el transporte de la información de empresa a empresa se han re-encaminado para mejorar la calidad de vida de las personas en todo el mundo. En el curso de un día, los recursos disponibles a través de Internet puede ayudarle a:

- Decidir como vestirse de acuerdo a la situación meteorológica actual.
- Encontrar la ruta menos congestionada hasta su destino.
- Verificar su saldo bancario y pagar las facturas por vía electrónica.
- Recibir y enviar e-mails.
- Hacer una llamada telefónica, desde un café Internet durante el almuerzo.
- Obtener información sobre la salud y el asesoramiento de expertos en nutrición de todo el mundo.
- Descargar nuevas recetas y técnicas de cocina para crear una espectacular cena.
- Publicar y compartir tus fotografías y videos caseros con el mundo entero.

1.2 Herramientas de Comunicación Populares

La existencia y la amplia adopción de Internet ha abierto nuevas formas de comunicación.

Mensajería instantánea

La mensajería instantánea (IM) es una forma de comunicación en tiempo real entre dos o más personas sobre la base de texto escrito. El texto se transmite a través de computadoras conectadas más bien a una red interna o privada sobre una red pública, como Internet. Desarrollado a partir de Internet Relay Chat (IRC), mensajería instantánea también incorpora características tales como transferencia de archivos, voz, video y comunicación. Al igual que el correo electrónico, los mensajes instantáneos envían un registro por escrito de la comunicación. Sin embargo, mientras que la transmisión de mensajes de e-mail se puede retrasar en algunas ocasiones, los mensajes instantáneos se reciben de inmediato. A esta forma de comunicación se le denomina comunicación en tiempo real.

Weblogs (blogs)

Weblogs (blogs) son páginas web que son fáciles de actualizar y editar. A diferencia de los sitios web comerciales, que son creados por profesionales expertos en comunicación, los blogs le dan a cualquier persona un medio para comunicar sus pensamientos a un público mundial, sin conocimientos técnicos de diseño web. Hay blogs en casi todos los temas que se puedan pensar.

Wikis

Los wikis son páginas web que grupos de personas pueden editar y ver juntos. Considerando que un blog es algo de una sola persona, un diario personal, un wiki es hecho por un grupo de creación. Al igual que los blogs, los wikis se pueden crear en

etapas, y por cualquier persona, sin el patrocinio de una importante empresa comercial. Hay un wiki público, llamada Wikipedia, que se está convirtiendo en una fuente completa de información. Las organizaciones privadas y los particulares también pueden construir sus propias wikis para capturar colección de conocimientos sobre un tema en particular. Muchas empresas utilizan los wikis como herramienta de colaboración interna.

Podcasting

Podcasting es un medio basado en audio que originalmente permitió a la gente grabar audio y convertirlo para su uso con los iPods (un pequeño dispositivo portátil para la reproducción de audio fabricados por Apple). La capacidad de grabar audio y guardarlo en un archivo de computador no es nueva. Sin embargo, el podcasting permite a la gente entregar sus grabaciones a una amplia audiencia. El archivo de audio se sitúa en un sitio web (o blog o wiki) donde otros puedan descargarlo y reproducir la grabación en sus computadores, portátiles, y los iPods.

Herramientas de Colaboración

Las herramientas de colaboración dan a la gente la oportunidad de trabajar juntos en documentos compartidos, sin las limitaciones de la ubicación o de la zona horaria. Los individuos conectados a un sistema compartido pueden hacer uso de la palabra los unos a los otros, compartir textos y gráficos, y editar documentos juntos. Con herramientas de colaboración siempre disponible, las organizaciones pueden moverse rápidamente para compartir información y conseguir sus objetivos. La amplia distribución de las redes de datos significa que la gente en lugares remotos puede contribuir en igualdad de condiciones con las personas en el corazón de los grandes centros de población.

1.3 Las redes apoyan la manera en que aprendemos

La comunicación, colaboración y compromiso son pilares fundamentales de la educación. Las instituciones están continuamente tratando de mejorar estos procesos para maximizar la difusión de los conocimientos.

Los cursos emitidos utilizando la red o recursos de Internet suelen tener experiencias de aprendizaje en línea o e-learning.

La disponibilidad de cursos del tipo e-learning ha multiplicado los recursos disponibles a los estudiantes. Los métodos de aprendizaje tradicionales proporcionan principalmente dos fuentes de las que el estudiante puede obtener información: el libro de texto y el instructor. Estas dos fuentes son limitadas, tanto en el formato y el momento de la presentación. Por el contrario, los cursos en línea pueden contener voz, datos y vídeo, y están disponibles a los estudiantes en cualquier momento y desde cualquier lugar. Los estudiantes pueden seguir los enlaces y referencias a los diferentes expertos en el tema a fin de mejorar su experiencia de aprendizaje. Grupos de discusión en línea y tableros de mensajes permiten a un estudiante colaborar con el instructor, con otros estudiantes en la clase, o incluso con otros estudiantes de todo el mundo.

El acceso a la alta calidad de la enseñanza ya no está restringido a los estudiantes que viven en las inmediaciones en donde la instrucción está siendo entregada. La enseñanza a distancia ha eliminado las barreras geográficas y mejorado la oportunidad de los estudiantes.

El Cisco Networking Academy Program, que ofrece este curso, es un ejemplo de una experiencia de aprendizaje en línea a nivel mundial. El instructor ofrece un programa de estudios preliminares y establece un calendario para completar el contenido de los cursos. La Academia programa, complementa los conocimientos de los instructores con un plan de estudios interactivo que ofrece muchas formas de experiencias de aprendizaje. El programa ofrece textos, gráficos, animaciones, y un entorno de simulación de redes herramienta llamada Packet Tracer. Packet Tracer proporciona una manera de construir representaciones virtuales de las redes y de emular muchas de las funciones de los dispositivos de red.

Los estudiantes pueden comunicarse con el instructor y compañeros de clase mediante herramientas en línea, como el correo electrónico, boletín y foros de debate, salas de chat y mensajería instantánea.

Además de los beneficios para el estudiante, las redes han mejorado la gestión y administración de los cursos también. Algunas de estas funciones incluyen la inscripción en línea, la evaluación y el proceso de entrega de libros.

1.4 Las redes apoyan la manera en que trabajamos

Al principio, las redes de datos se han utilizado internamente por las empresas para registrar y gestionar la información financiera, la información de los clientes, los empleados y los sistemas de nómina de pagos. Estas redes empresariales han evolucionado para permitir la transmisión de muchos tipos diferentes de los servicios de información, incluyendo el correo electrónico, vídeo, mensajería y telefonía.

Las Intranets, son redes privadas para el uso de una sola empresa, permiten a las empresas comunicarse y realizar transacciones a nivel mundial entre los empleados y sucursales. Las empresas pueden desarrollar extranets, o internetworks ampliadas, para proporcionar a los proveedores, y clientes un acceso limitado a datos de las empresas para comprobar el estado de sus pedidos, de inventario y de partes listas.

1.2 El proceso de la comunicación

1.2.1 ¿Que es la comunicación?

La comunicación en nuestra vida cotidiana tiene muchas formas y tiene lugar en muchos entornos. Tenemos expectativas diferentes en función de si estamos chateando a través de Internet o participar en una entrevista de trabajo. Cada situación tiene su correspondiente comportamiento y estilo.

El establecimiento de las Normas

Antes de empezar a comunicarse entre sí, se deben establecer las normas o acuerdos que rigen la conversación. Estas reglas, o protocolos, se deben seguir a fin de que el mensaje que se emitió con éxito sea comprendido.

Los elementos que rigen el éxito de la comunicación humana son los siguientes:

- Un identificador para el remitente y el receptor
- Acordar el método de comunicación (cara a cara, teléfono, carta, la fotografía)
- Lenguaje común y la gramática
- La velocidad y el calendario de las entregas
- Confirmación o acuse de recibos

Las reglas de la comunicación pueden variar según el contexto. Si un mensaje transmite un concepto o hecho importante, es necesaria la confirmación de que el mensaje ha sido recibido y comprendido.

1.2.2 Calidad de las Comunicaciones

Factores internos

Los factores internos que interfieren con la comunicación de red están relacionados con la naturaleza del propio mensaje.

Los diferentes tipos de mensajes pueden variar en complejidad e importancia. Los mensajes claros y concisos suelen ser más fáciles de comprender que los mensajes complejos. Comunicaciones más importantes requieren más cuidado para asegurar que sean entregados y comprendidos por el destinatario.

Los factores internos que afectan el éxito de la comunicación a través de la red incluyen:

- El tamaño del mensaje
- La complejidad del mensaje
- La importancia del mensaje

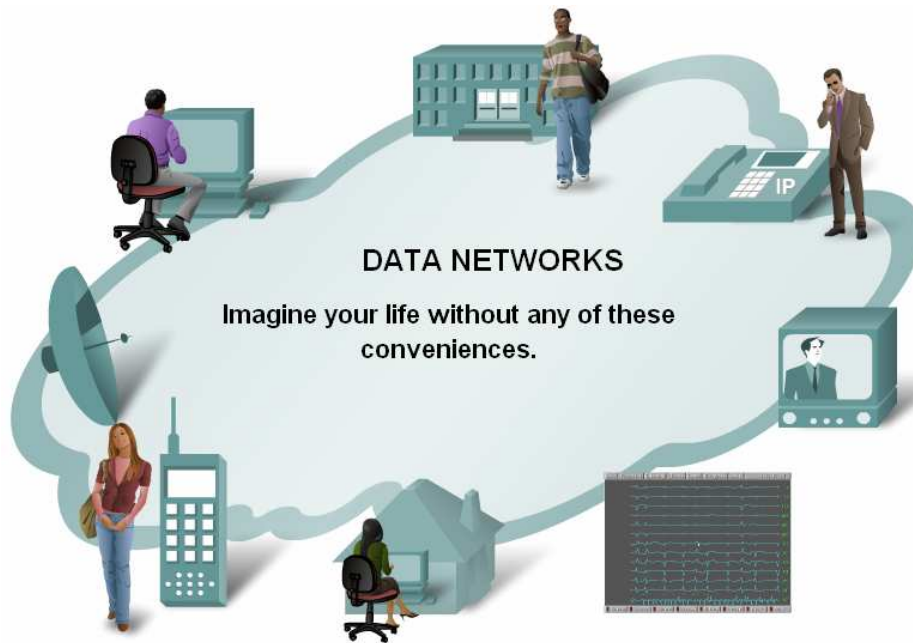
Los mensajes de gran tamaño pueden ser interrumpidos o retrasados en diferentes puntos dentro de la red. Un mensaje con una baja prioridad o importancia podría ser eliminado si la red se sobrecarga.

1.3.1 Comunicación sobre Redes

Ser capaz de comunicar fehacientemente a cualquiera, en cualquier lugar, es cada vez más importante para nuestra vida personal y de negocios. Con el fin de apoyar la entrega inmediata de los millones de mensajes intercambiados entre personas de todo el mundo, nos apoyamos en una red de redes interconectadas. Estos datos o redes de información varían en tamaño y capacidades, pero todas las redes tienen cuatro elementos básicos en común:

- Normas o acuerdos que rigen cómo se envían los mensajes, instrucciones, como son recibidos e interpretados.
- Los mensajes o las unidades de información que viajan de un dispositivo a otro.
- El medio que puede transportar los mensajes de un dispositivo a otro.
- Los dispositivos de la red que intercambian los mensajes entre sí.

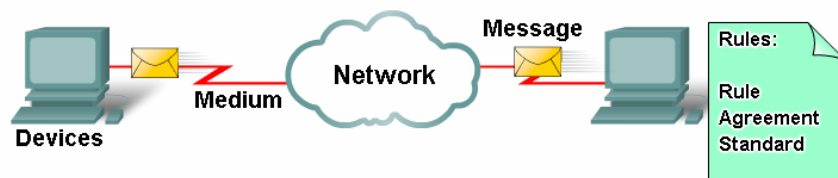
La normalización de los distintos elementos de la red permite a los equipos y dispositivos creados por distintas empresas trabajar juntos. Expertos en diversas tecnologías pueden aportar sus mejores ideas sobre cómo desarrollar una red eficiente, sin tener en cuenta la marca o fabricante del equipo.



This course covers how data networks support the human network.

1.3.2 Los elementos de una red:

El diagrama muestra los elementos típicos de una red, incluidos los dispositivos, los medios de comunicación, y los servicios, unidos por normas, que trabajan juntos para enviar mensajes. Usamos la palabra mensajes como un término que incluye las páginas web, correo electrónico, mensajes instantáneos, llamadas telefónicas, y otras formas de comunicación a través de Internet. En este curso, vamos a aprender acerca de una gran variedad de mensajes, los dispositivos, los medios de comunicación, y los servicios que permiten la transmisión de los mensajes. También vamos a aprender acerca de las reglas, o protocolos, que estén relacionados con estos elementos de la red.



Four elements of a network:

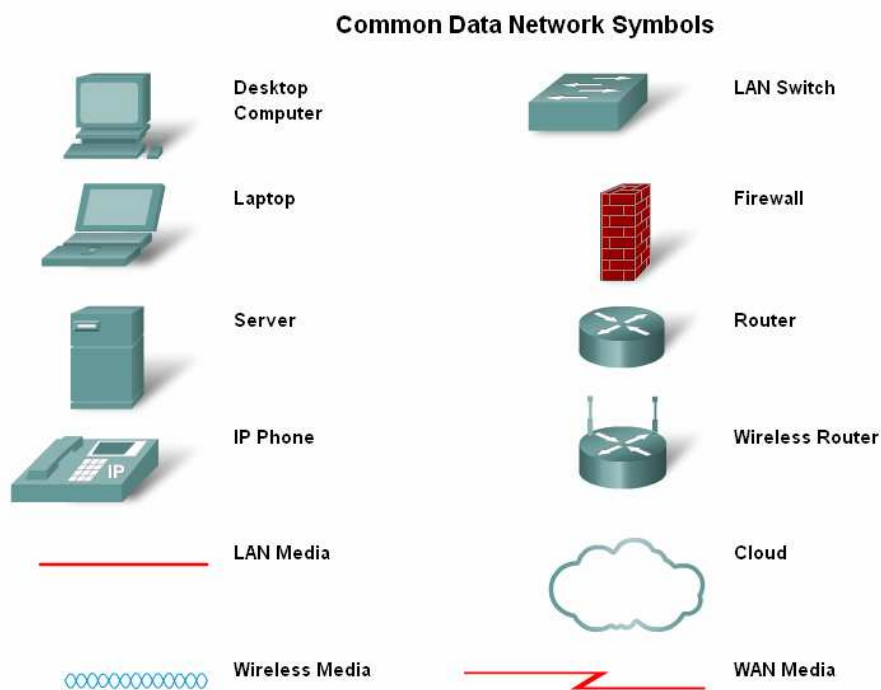
- Rules
- Medium
- Messages
- Devices

En este curso, se discutirán numerosos dispositivos de red. La Red es un tema muy orientado a los gráficos, y los iconos se usan comúnmente para representar los dispositivos de redes. En la parte izquierda del diagrama se muestran algunos

dispositivos comunes que a menudo originan los mensajes que componen nuestra comunicación. Por ejemplo, distintos tipos de computadoras (PC y portátiles), los servidores y los teléfonos IP. En las redes de área local son estos dispositivos suelen estar conectados por medios de comunicación de la LAN (por cable o de manera inalámbrica).

La parte derecha de la figura muestra algunos de los más comunes de los dispositivos intermedios, utilizados para dirigir y gestionar mensajes a través de la red, así como otros símbolos de red comunes. También se muestran símbolos genéricos para:

- Switch - el dispositivo más común para la interconexión de redes de área local
- Firewall proporciona seguridad a las redes
- Router - ayuda a dirigir los mensajes que viajan a través de una red
- Router inalámbrico - un tipo específico de router que se encuentran frecuentemente en las redes del hogar.
- Cloud - usado para resumir a un conjunto de dispositivos de red, cuyas características pueden no ser importantes para la discusión del momento.
- Serial Link - una forma de interconexión WAN, representado por el rayo en forma de línea.



Para que una red pueda funcionar, los dispositivos deben estar interconectados. Las conexiones de red pueden darse por cable o de manera inalámbrica. En las conexiones por cable, o bien el medio es el cobre, que transporta señales eléctricas, o de fibra óptica, que transporta las señales de luz. En conexiones inalámbricas, el medio es la atmósfera de la Tierra, o en el espacio, y las señales son las microondas. Incluye los cables de cobre, como el telefónico de cable de par trenzado, cable coaxial, o lo que se conoce comúnmente como par trenzado Categoría 5 no apantallado (UTP).

En el caso de las fibras ópticas, lo que tenemos son delgados filamentos de vidrio o de plástico que llevan las señales de luz, son otras formas de redes o medios de comunicación.

Los medios inalámbricos, son medios de comunicación que pueden incluir en la casa, la conexión inalámbrica entre un router inalámbrico y un computador con una tarjeta de red inalámbrica, la conexión inalámbrica terrestre entre dos estaciones terrestres, o de la comunicación entre los dispositivos que en la Tierra y los satélites.

Los seres humanos a menudo envían y reciben una gran variedad de mensajes utilizando múltiples aplicaciones informáticas; estas aplicaciones requieren los servicios prestados por la red. Algunos de estos servicios incluyen la World Wide Web, correo electrónico, mensajería instantánea y la telefonía IP. Los protocolos son las reglas que usan los dispositivos de red para comunicarse entre sí. El estándar de la industria en la creación de redes de hoy es un conjunto de protocolos llamado TCP / IP (Transmission Control Protocol / Internet Protocol). TCP / IP se utiliza en redes domésticas y empresariales, además de ser el principal protocolo de Internet.

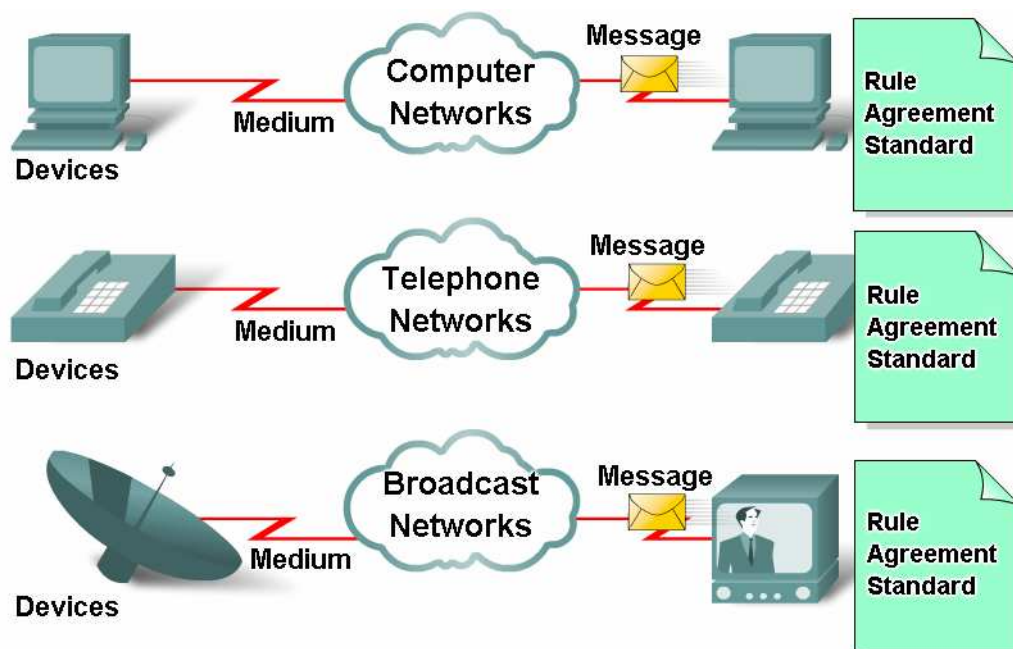
1.3.3 Redes convergentes

Múltiples servicios - múltiples redes

El teléfono tradicional, la radio, la televisión, la computadora y las redes de datos de cada individuo tienen sus propias versiones de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para transmitir sus señales. Además, cada servicio tiene su propio conjunto de reglas y normas para garantizar el éxito de la transmisión de su señal a través de un medio específico.

Redes convergentes

Los avances tecnológicos están permitiendo la consolidación de estas tecnologías de redes dispares bajo una sola plataforma - una plataforma que se define como una red convergente. El flujo de voz, vídeo, datos que viaja sobre la misma red elimina la necesidad de crear y mantener redes separadas. En una red convergente existen todavía muchos puntos de contacto y muchos dispositivos especializados - por ejemplo, computadores personales, teléfonos, televisores, asistentes personales, pero todos ellos trabajan con una sola infraestructura de red común.



Multiple services are running on multiple networks.

Las redes de información inteligentes

El papel de la red está evolucionando. La plataforma de comunicaciones inteligentes del mañana ofrecerá mucho más servicios que solo la conectividad básica y el acceso a las aplicaciones. La convergencia de los diferentes tipos de redes de comunicaciones en una sola plataforma representa la primera etapa en la construcción de la red de información inteligente. En la actualidad estamos en esta fase de la evolución de la red. La siguiente fase será la de consolidar no sólo los diferentes tipos de mensajes en una única red, sino también la unificación de las aplicaciones que generan, transmiten, y aseguran la transmisión de los mensajes. No sólo se busca que la voz y el video se transmitan por la misma red, los dispositivos que realizan la conmutación telefónica y efectúan la radiodifusión de vídeo seguirán la misma ruta que los dispositivos que envían simples mensajes a través de la red. La plataforma de comunicaciones resultante proporcionará funcionalidad de alta calidad a un costo reducido.

Planificación para el Futuro

La rápida expansión de Internet explica el ritmo acelerado al que están ocurriendo los nuevos y apasionantes desarrollos de programas de red convergente. Esta expansión ha creado un público más amplio y una mayor base de consumidores por cualquier tipo de mensaje, producto o servicio que pueda ser entregado. La mecánica y procesos que impulsan este crecimiento explosivo han dado lugar a una arquitectura de red que se requiere que sea a la vez resistente y escalable. Como elemento clave de apoyo a la plataforma de la tecnología para vivir, aprender, trabajar y jugar en la red humana, la arquitectura de red de Internet debe adaptarse constantemente a los cambios y a las necesidades de un servicio de alta calidad y seguridad.

1.4 La Arquitectura de Internet

1.4.1 La Arquitectura de la red

Las redes deben apoyar una amplia gama de aplicaciones y servicios, así como apoyar muchos tipos diferentes de infraestructuras físicas. El término arquitectura de la red, en este contexto, se refiere a las tecnologías que sirven de apoyo a la infraestructura, los servicios programados y los protocolos que mueven los mensajes a través de esta infraestructura. Como Internet, y las redes en general evolucionan, se descubre que existen cuatro características básicas que toda arquitectura necesitan con el fin de satisfacer las expectativas del usuario: tolerancia a fallos, escalabilidad, calidad de servicio, y la seguridad.

La tolerancia de fallas

El hecho de que Internet este siempre disponible para los millones de usuarios que dependen de ella requiere de una arquitectura de red que se ha diseñado y construido para ser tolerantes a errores. El concepto de tolerancia a fallos de red limita la posibilidad de que un fallo de hardware o software se de y si este se da, que la red se pueda recuperar rápidamente. Estas redes dependen de los enlaces o rutas redundantes, entre la fuente y el destino de un mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes puedan ser enrutados al instante entre los usuarios de cualquiera de los extremos.

Escalabilidad

Una red escalable puede crecer rápidamente para apoyar a nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio que se entrega a los usuarios existentes. Miles de nuevos usuarios se conectan a Internet cada semana. La capacidad de la red de apoyar a estas nuevas interconexiones depende de una concepción jerárquica en capas subyacentes de la infraestructura de la arquitectura física y lógica.

Calidad de Servicio (QoS)

La Internet actualmente proporciona un nivel aceptable de tolerancia a fallos y escalabilidad para sus usuarios. Sin embargo, las nuevas aplicaciones a disposición de los usuarios generan mayores expectativas por la calidad de los servicios entregados. Las transmisiones de voz y video en directo exigen un nivel alto de calidad de la transmisión y la certeza de una transmisión ininterrumpida. Las redes tradicionales de voz y de video están diseñadas para apoyar a un solo tipo de transmisión, y por lo tanto son capaces de producir un nivel aceptable de calidad. Los nuevos requisitos para apoyar esta calidad de los servicios convergentes sobre una red están cambiando la forma en que las arquitecturas de red se están diseñando y aplicando.

Seguridad

La Internet ha evolucionado de ser una internetwork estrictamente controlada por las organizaciones gubernamentales y orientada a la educación hacia una red que permite servir como medio de transmisión de comunicaciones personales y de negocios. Como resultado de ello, las necesidades de seguridad de la red han cambiado. La seguridad y la privacidad de las comunicaciones requieren altos estándares para ofrecer seguridad a los interlocutores del proceso de comunicación. Como resultado de ello, muchos esfuerzos se están dedicando a

esta área de investigación y desarrollo. Entre tanto, muchas herramientas y procedimientos se están aplicando para luchar contra fallas de seguridad inherentes en la arquitectura de red.

1.4.2 La arquitectura de una red, tolerancia a fallas

La Internet, en un inicio, fue el resultado de la investigación financiada por el Departamento de Defensa (DoD) de los Estados Unidos. Su principal objetivo era el de tener un medio de comunicación que pudiera soportar la destrucción de numerosos sitios y servicios de transmisión sin que esto logre interrumpir el servicio.

Redes orientadas a la conexión de Circuitos

Para comprender el reto que los investigadores de Departamento de Defensa tuvo que enfrentar, es necesario examinar como trabajaban los sistemas basados en los teléfonos de esa época. Cuando una persona hace una llamada mediante un teléfono tradicional, la palabra en primer lugar pasa por un proceso de configuración, luego se requiere que se de la identificación total entre la persona y el teléfono para que se efectúe una conmutación de circuitos entre ellos. Un camino temporal, o circuito, se crea a través de los diversos lugares a cambio de su uso mientras dure la llamada telefónica. Si algún vínculo o dispositivo que participan en el circuito de falla, la llamada se cae. Para restablecer el enlace, debe hacerse una nueva convocatoria debe hacerse, y crearse un nuevo circuito entre la fuente y el teléfono de destino. Este tipo de red orientado a la conexión se denomina una red de conmutación de circuitos.

Redes orientadas a la conmutación de paquetes

En la búsqueda de una tecnología de red que pudiera soportar la pérdida de una cantidad significativa de sus datos, los primeros diseñadores de Internet evaluaron la posibilidad de trabajar con redes de conmutación de paquetes. La premisa de este tipo de redes es que un mismo mensaje puede ser dividido en varios bloques. Los bloques individuales que contienen información indican tanto su punto de origen y su destino final. Para este fin se hace uso de unidades de mensajes llamados paquetes. Estos paquetes pueden ser enviados a través de la red a lo largo de varios senderos, y pueden ser reensamblados al llegar a su destino.

Utilizando Paquetes

Los dispositivos dentro de la propia red no son conscientes del contenido de los paquetes individuales, sólo es visible la dirección del destino final y el siguiente dispositivo en el camino a ese destino. No se construyen circuitos reservados entre el remitente y el receptor. Cada paquete es enviado de manera independiente de una ubicación a otra. En cada punto de llegada, un router tomara una decisión sobre que a que lugar se enviara el paquete en el camino hacia su destino final. Si un camino utilizado anteriormente ya no está disponible, la función de enrutamiento dinámico puede elegir la mejor ruta disponible. Debido a que los mensajes se envían en paquetes, en vez de un único mensaje completo, los pocos paquetes que se pueden perder cuando hay un fallo pueden ser retransmitidos al destino a lo largo de un camino diferente. En muchos casos, el equipo final o de destino no es consciente de que se halla producido un fallo o error.

Conmutación de paquetes - Redes no orientadas a conexión

Los investigadores del Departamento de Defensa se dieron cuenta de que una red de conmutación de paquetes sin conexión tenía las características necesarias para proporcionar un sistema de tolerancia a fallos en la arquitectura de la red. La necesidad de un único circuito reservado de extremo a extremo no existe en una red de conmutación de paquetes. Cualquier parte de un mensaje se puede enviar a través de la red utilizando cualquier ruta disponible. Los paquetes contienen partes de los mensajes de los diferentes hosts de la red que pueden viajar al mismo tiempo. Con esto el problema de los circuitos ociosos o subutilizados se elimina completamente, todos los recursos disponibles se pueden utilizar en cualquier momento para efectuar la entrega de los paquetes a su destino final. Al proporcionar un método para utilizar dinámicamente rutas redundantes, sin intervención por parte del usuario, la Internet se ha convertido en una red con tolerancia a fallos y un muy escalable método de comunicaciones.

Redes Orientadas a la conexión

Aunque la conmutación de paquetes sin conexión satisfizo las necesidades del Departamento de Defensa, y continúa siendo la principal infraestructura de Internet para el día de hoy, hay algunos beneficios en un sistema orientado a la conexión, como es el caso de la conmutación de circuitos utilizado por el sistema telefónico. Este sistema permite garantizar al 100% la comunicación entre 2 equipos cuando tengan necesidad de comunicarse, por otro lado al tener que separarse un canal común entre los dos equipos es factible de facturación por tiempo de uso. Esta es una característica de los sistemas de telecomunicación actuales.

1.5 Tendencias en las Tecnologías de Networking

La convergencia de los diferentes medios de comunicación en una única plataforma de red está fomentando el crecimiento exponencial de las capacidades de red.

Sin embargo hay tres grandes tendencias que están contribuyendo a la forma futura de las complejas redes de información:

- Número cada vez mayor de usuarios móviles
- Proliferación de los dispositivos de red capaz
- Ampliar la gama de servicios

Autoevaluación

1. Identificar las principales tendencias en las tecnologías de Networking actuales.
2. ¿Cuáles son las maneras de proporcionar seguridad a las redes?
3. Identificar cuales son los elementos que garantizan que una red sea escalable.
4. Identificar las ventajas de trabajar con una red de paquetes conmutados.
5. Identificar las ventajas de trabajar con una red de circuitos conmutados.
6. ¿Qué significa que trabajemos con una red orientada a conexión?
7. Identificar las características que debe tener toda red para garantizar un servicio correcto y adecuado.

Para recordar

Los métodos que utilizamos para compartir ideas e información están en constante cambio y evolución. Desde la imprenta a la televisión, cada nuevo desarrollo ha mejorado y aumentado nuestra comunicación.

La tecnología es tal vez el más importante agente de cambio en el mundo de hoy, ya que contribuye a crear un mundo en el que las fronteras nacionales, las distancias geográficas, y las limitaciones físicas se vuelven menos relevantes, y presentan cada vez menos obstáculos. La creación de comunidades en línea para el intercambio de ideas y de la información tiene el potencial de aumentar la productividad de oportunidades en todo el mundo.

Las herramientas de colaboración dan a la gente la oportunidad de trabajar juntos en documentos compartidos, sin las limitaciones de la ubicación o de la zona horaria.

La comunicación, colaboración y compromiso son pilares fundamentales de la educación. Las instituciones están continuamente tratando de mejorar estos procesos para maximizar la difusión de los conocimientos.

Ser capaz de comunicar fehacientemente a cualquiera, en cualquier lugar, es cada vez más importante para nuestra vida personal y de negocios. Con el fin de apoyar la entrega inmediata de los millones de mensajes intercambiados entre personas de todo el mundo, nos apoyamos en una red de redes interconectadas.

Para que una red pueda funcionar, los dispositivos deben estar interconectados. Las conexiones de red pueden darse por cable o de manera inalámbrica. En las conexiones por cable, o bien el medio es el cobre, que transporta señales eléctricas, o de fibra óptica, que transporta las señales de luz. En conexiones inalámbricas, el medio es la atmósfera de la Tierra, o en el espacio, y las señales son las microondas. Incluye los cables de cobre, como el telefónico de cable de par trenzado, cable coaxial, o lo que se conoce comúnmente como par trenzado Categoría 5 no apantallado (UTP).



Comunicándonos sobre la red

TEMA

- Comunicándonos sobre la red

OBJETIVOS ESPECÍFICOS

- Identificar los elementos de la comunicación
- Describir la plataforma de comunicación de la red de datos
- Identificar los tipos de redes
- Entender los modelos de red basados en capas

CONTENIDOS

- Comunicándonos sobre la red
- La plataforma para la comunicación
- LAN, WAN y Redes
- Las reglas que gobiernan las comunicaciones
- Usando un modelo basado en capas
-

ACTIVIDADES

- Actividad de laboratorio electrónico:

2. Comunicándonos sobre la red

Más y más, las redes nos permiten estar conectados. La gente se comunica en línea alrededor de todo el mundo. A medida que nuestra red humana sigue aumentando, la plataforma que la une y la apoya también debe crecer.

En este curso, nos centramos en estos aspectos de la red de información:

- Los dispositivos que componen la red
- Los medios de comunicación que conectan a los dispositivos
- Los mensajes que se transportan a través de la red
- Normas y procesos que rigen la red de comunicaciones
- Herramientas y comandos para la construcción y mantenimiento de las redes

Un elemento central para el estudio de las redes es el uso de modelos aceptados de manera general que describen las funciones de la red. Estos modelos proporcionan un marco para la comprensión actual de las redes y facilitan el desarrollo de nuevas tecnologías para apoyar las futuras necesidades de comunicación.

Dentro de este curso, utilizamos estos modelos, así como herramientas destinadas a analizar y simular la funcionalidad de las redes. Dos de las herramientas que le permitirán crear e interactuar con redes simuladas son Packet Tracer 4,1 software y Wireshark analizador de protocolos de red.

2.1 La plataforma para la comunicación

2.1.1 Los elementos de la comunicación

La comunicación comienza con un mensaje, o información, que deberá ser enviado desde un individuo o dispositivo a otro. Las personas intercambian ideas utilizando diferentes métodos de comunicación.

Todos estos métodos tienen tres elementos en común.

- El primero de estos elementos es el mensaje fuente, o remitente. Mensajes fuentes son las personas, o los dispositivos electrónicos, que deben enviar un mensaje a otras personas o dispositivos.
- El segundo elemento de la comunicación es el destino o receptor, del mensaje. El destino recibe el mensaje y lo interpreta.
- Un tercer elemento, llamado canal, consta de los medios de comunicación que ofrece la vía sobre la que el mensaje puede viajar desde el origen al destino.

Consideremos, por ejemplo, el deseo de comunicarse mediante palabras, imágenes y sonidos. Cada uno de estos mensajes pueden ser enviados a través de una red de información pero primero deben ser convertidos en dígitos binarios, o bits. Estos bits se codifican en una señal que puede ser transmitida por el medio que se considere oportuno. En las redes de computadoras, los medios de comunicación son por lo general medios cableados, o medios inalámbricos.

El término red en este curso se referirá a las redes de datos o redes de información capaces de transportar muchos tipos diferentes de información, incluidos los datos informáticos, interactivos de voz, vídeo, y productos de entretenimiento.

2.1.2 Comunicando los mensajes

En teoría, solo un flujo de datos puede enviarse a través de una red desde un equipo origen a un equipo destino bajo la forma de una masa continua de bits. Si los mensajes fueran efectivamente transmitidos de esta manera, significaría que ningún otro dispositivo sería capaz de enviar o recibir mensajes en la misma red al mismo tiempo que esta transferencia de datos este en marcha. Por lo tanto el envío de grandes flujos de datos originaría grandes retrasos. Además, si un enlace de la infraestructura de la red de interconexión fallara durante la transmisión, el mensaje completo se perdería.

Un mejor enfoque consiste en dividir los datos en partes más manejables y pequeñas piezas para enviarlas a través de la red. Esta división del flujo de datos en partes más pequeñas se llama segmentación. La segmentación de los mensajes tiene dos ventajas principales.

En primer lugar, mediante el envío de pequeñas piezas individuales desde el origen al destino, muchas conversaciones pueden ser efectuadas en la red. El proceso utilizado para enviar simultáneamente los paquetes de datos se llama multiplexado. En segundo lugar, la segmentación puede incrementar la fiabilidad de la red de comunicaciones, pues las piezas separadas de cada mensaje no tienen que viajar por el mismo camino a través de la red desde el origen al destino. Si un enlace se convierte en un camino congestionado con tráfico de datos, las piezas individuales del mensaje puede ser dirigidos a un destino utilizando vías alternas. Si algunas partes del mensaje no llegan al destino, sólo estas partes faltantes serán retransmitidas.

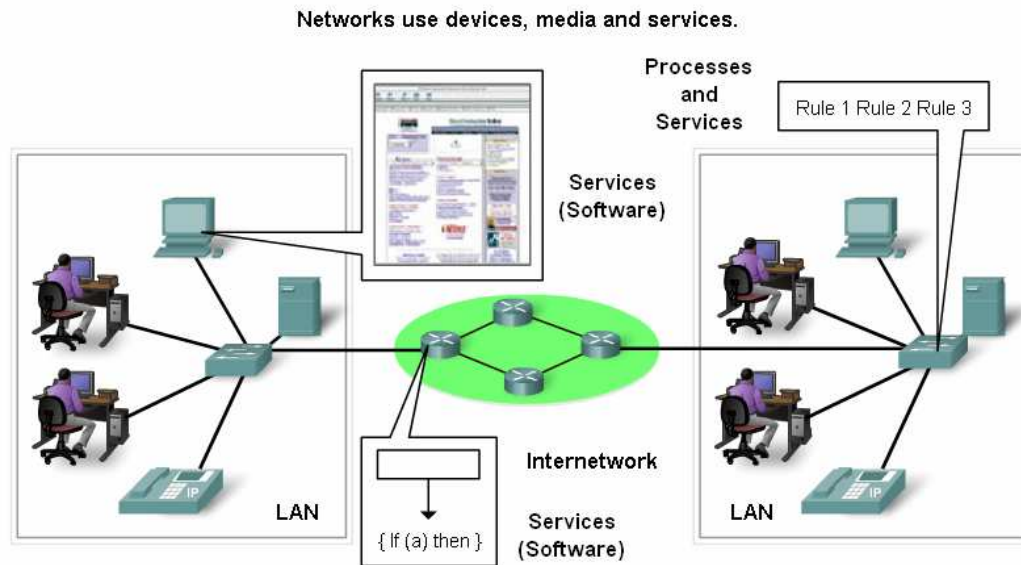
La desventaja de usar la segmentación y la multiplexación al transmitir mensajes a través de una red es el nivel de complejidad que se añade al proceso. Imagínese si tuviera que enviar una carta de 100 páginas, pero que cada página se enviara en un sobre independiente. El proceso de tratamiento, el etiquetado, envío, recepción y apertura de la totalidad de cien sobres consumiría mucho mas tiempo tanto para el remitente y el destinatario, que enviar las 100 paginas en un solo sobre.

En la red de comunicaciones varios tipos de dispositivos participan en el proceso de garantizar que los mensajes lleguen a su destino.

2.1.3 Componentes de la red

La ruta que toma un mensaje desde el origen al destino puede ser tan simple como un único cable de conexión de un computador a otro o tan complejo como una red que se extiende por todo el mundo, literalmente. Esta infraestructura de red es la plataforma que apoya nuestra red humana. Proporciona el canal estable y fiable sobre los que se dan nuestras comunicaciones.

Los dispositivos y los medios de comunicación son los elementos físicos o el hardware de la red. El hardware es a menudo el elemento visible que compone la plataforma de red, como una portátil, un PC, un interruptor, o el cableado utilizado para conectar los dispositivos. Puede ocurrir que algunos de los componentes puedan no ser tan visibles. En el caso de los medios de comunicación inalámbrica, los mensajes se transmiten a través del aire utilizando invisibles ondas de radio o señales infrarrojas. Los servicios y procesos son proporcionados por los programas de comunicación, a los que se les denomina de manera general software de red, que se ejecuta en los dispositivos de red. Un servicio de red proporciona información en respuesta a una petición. Los servicios incluyen muchas de las aplicaciones de red que la gente usa todos los días, como el correo electrónico y los servicios de hosting para el alojamiento web. Los procesos son menos obvios, pero son fundamentales para el funcionamiento de las redes.



2.1.4 Dispositivos finales y su rol en la red

Los dispositivos de red con los que la gente está más familiarizada son llamados dispositivos finales. Estos dispositivos forman la interfase entre el ser humano y la red subyacente de la red de comunicaciones. Algunos ejemplos de dispositivos finales son los siguientes:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Móviles, dispositivos de mano (como lectores de código de barras inalámbrico, PDA)

En el contexto de una red, los dispositivos finales se denominan hosts. Un hosts es la fuente o el destino de un mensaje transmitido a través de la red. Con el fin de distinguir uno de otro hosts, cada host en una red se identifica por una dirección. Cuando un host inicia un proceso de comunicaciones, utiliza la dirección destino del hosts para especificar donde será enviado el mensaje.

En las redes modernas, un host puede actuar como un cliente, un servidor, o ambos. El software instalado en el hosts determinara en buena medida que papel es el que desempeña en la red.

Los servidores son las máquinas que tienen instalado el software que les permite proporcionar la información y los servicios, como el correo electrónico o páginas web, a otras máquinas de la red.

Los clientes son aquellos equipos que tienen instalado el software que les permite solicitar y mostrar la información obtenida desde el servidor.

2.1.5 Dispositivos intermedios y su rol en la red

Además de los dispositivos finales con los que las personas están familiarizadas, las redes se basan en equipos intermediarios para proporcionar conectividad, estos equipos trabajan entre bastidores para asegurar que los flujos de datos a través de la red puedan llegar a sus destinos. Estos dispositivos conectan a los hosts individuales

a la red y pueden conectar múltiples redes individuales para formar una internetwork. Ejemplos de dispositivos intermediarios son los siguientes:

- Dispositivos de Acceso de Red (Hubs, switches, puntos de acceso inalámbricos)
- Dispositivos de Interred (routers)
- Servidores de Comunicación y módems
- Dispositivos de seguridad (firewalls)

La gestión de los datos conforme fluyen a través de la red es también un papel de los dispositivos intermediarios. Estos dispositivos utilizan la dirección de destino del host, junto con la información acerca de la interconexión de las redes, a fin de determinar el camino que deben tomar los mensajes a través de la red. Los procesos ejecutándose en los dispositivos intermediarios de red deben realizar estas funciones:

- Regenerar y retransmitir señales de datos
- Mantener información acerca de las redes que existen a través de la red y la internetwork.
 - Notificar a otros dispositivos de comunicación sobre los errores y fallos de envío de los datos.
- Redireccionar los datos a lo largo de las vías alternas cuando hay un enlace caído.
- Clasificar y enviar mensajes de acuerdo a las prioridades definidas por el QoS.
- Permitir o negar el flujo de datos, en base a las opciones de seguridad.

2.1.6 El medio de transporte de la red

La comunicación a través de una red se realiza sobre un medio. El medio proporciona el canal sobre los que el mensaje viaja desde el origen al destino.

Las redes modernas utilizan principalmente tres tipos de medios de comunicación para interconectar dispositivos y proporcionan la vía sobre la que se pueden transmitir los datos. Estos medios de comunicación son los siguientes:

- Cables metálicos dentro de cables.
- Las fibras de vidrio o de plástico (cable de fibra óptica)
- Las transmisiones inalámbrica.

El tipo de codificación que se aplicara sobre la señal varia dependiendo del tipo de medio. En los cables metálicos, los datos son codificados en impulsos eléctricos que coincidan con patrones específicos. En la fibra óptica la transmisión depende de los pulsos de luz, ya sea dentro de los rangos de la luz visible o las luces infrarrojas. En las transmisiones inalámbricas, los patrones de las ondas electromagnéticas representan los distintos valores de los bits.

Los criterios para la elección de una red de comunicación son los siguientes:

- La distancia que los medios de comunicación pueden transmitir con éxito una señal.
- La cantidad de datos y la velocidad a la que debe transmitirse.
- El costo de los medios de comunicación y la instalación.

2.2. LAN, WAN y Redes

2.2.1 Redes de área local (LANs)

La infraestructura de las redes puede variar mucho en términos de:

- El tamaño del área cubierta

- El número de usuarios conectados
- El número y el tipo de servicios disponibles

Una red pequeña normalmente se extiende por una sola zona geográfica, proporcionando servicios y aplicaciones a las personas que forman parte de una organización común, como una sola empresa, la escuela o la región. Este tipo de red se denomina una red de área local (LAN). Una LAN suele ser administrado por una sola organización. El control administrativo que rige la seguridad y las políticas de control de acceso se aplican en el ámbito de la red.

2.2.2 Redes de Área Extensa (WAN)

Cuando una empresa u organización tiene sucursales que están separados por grandes distancias geográficas, puede que sea necesario usar un proveedor de servicios de telecomunicaciones (ISP) para interconectar las redes de área local en los diferentes lugares. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden extenderse a grandes distancias. Tradicionalmente, las empresas de telecomunicaciones se encargaban de las comunicaciones de voz y datos sobre redes alejadas. Sin embargo actualmente, estos son los proveedores que ofrecen los servicios de redes convergentes de información a sus suscriptores.

Estas organizaciones por lo general rentan las conexiones de los servicios de telecomunicaciones a través de una red de proveedores. Estas redes que unen las redes de área local en lugares geográficamente separados se denominan redes de área extensa (WAN). A pesar de que el cliente mantiene la totalidad de las políticas y la administración de la LAN en ambos extremos de la conexión, las políticas asignadas en el enlace rentado por el proveedor de servicios de comunicaciones de red son controladas por el ISP. Las redes WAN utilizan dispositivos de red diseñados específicamente para hacer las interconexiones entre redes de área local. Debido a la alta importancia que tienen estos dispositivos para la red, la configuración, instalación y mantenimiento de estos dispositivos son habilidades que forman parte del equipo de soporte de la empresa.

Las redes LAN y WAN son muy útiles para las distintas organizaciones. Se encargan de conectar a los usuarios dentro de la organización, permiten muchas formas de comunicación incluyendo el intercambio de mensajes de correo electrónico, la capacitación dentro de la empresa, y otros recursos compartidos.

2.2.3 La Internet – Red de Redes

Aunque es muy beneficioso el uso de una red LAN o WAN, la mayoría de nosotros se debe comunicar con los recursos de una red fuera de nuestra organización local. Ejemplos de este tipo de comunicaciones son:

- Enviando un e-mail a un amigo en otro país.
- Acceder a las noticias o los productos ofrecidos en un sitio web.
- Obtener un archivo de la computadora de un vecino.
- Utilizar la mensajería instantánea para comunicarse con un familiar en otra ciudad.

Internetwork

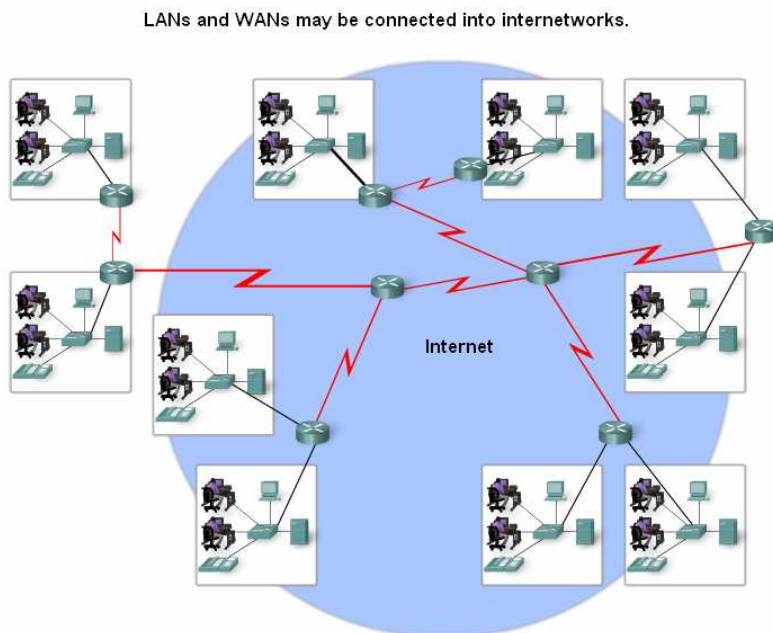
Una red mundial de redes interconectadas (internetworks), permite que se puedan cubrir estas necesidades de la comunicación humana. Algunas de estas redes de interconexión son propiedad de las grandes organizaciones públicas y privadas, tales como los organismos públicos o empresas industriales, y están reservados para su

uso exclusivo. Sin embargo la más conocida y ampliamente utilizada red de acceso público es la Internet.

La Internet se forma por la interconexión de las redes pertenecientes a los proveedores de servicios de Internet (ISP). Estas redes se conectan entre sí para facilitar el acceso de millones de usuarios alrededor del mundo. Garantizar una comunicación eficaz a través de esta variada infraestructura de red requiere de la aplicación coherente y de reconocidas tecnologías y protocolos de red, así como la cooperación de muchos organismos de la administración de la red.

Intranet

El término intranet se utiliza a menudo para referirse a una conexión privada de LAN y WAN que pertenece a una organización, y está diseñado para ser accesible sólo por los miembros de la organización, empleados, u otros con autorización respectiva.



2.2.4 Símbolos para representar las redes

Cuando se desean representar a los dispositivos de la red y se desea visualizar el proceso de transmisión de la información, es útil hacer uso de símbolos visuales y gráficos de la red. Para este fin se utilizan un conjunto común de símbolos para representar los diferentes dispositivos de red y medios de comunicación. La habilidad de reconocer la lógica de las representaciones de los componentes físicos de las redes es fundamental para ser capaz de visualizar a la organización y funcionamiento de una red.

A lo largo de este curso y de los laboratorios, usted aprenderá cómo estos dispositivos funcionan y cómo realizar las tareas básicas de configuración de estos dispositivos. Además de estas representaciones, también se utiliza terminología especializada cuando se habla de cómo cada uno de estos medios de comunicación se conectan entre sí.

Los términos importantes a recordar son:

Tarjeta de interfaz de red:

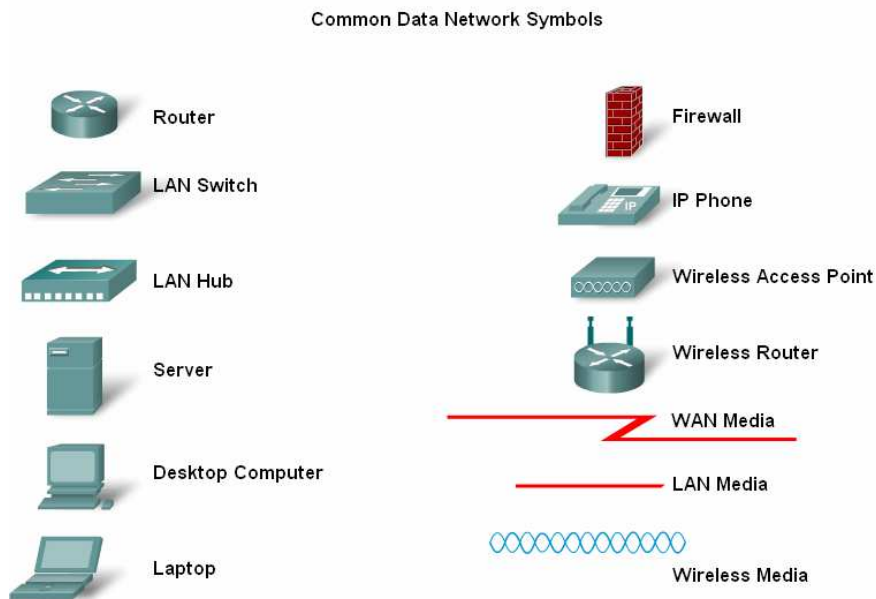
Un NIC, o adaptador de LAN, proporciona la conexión física a la red en el PC u otro dispositivo de conexión.

Puerto Físico:

Un conector o salida de un dispositivo de red, donde los cables de comunicación se conectan al host u otro dispositivo de red.

Interfase:

Puertos especializados en dispositivo de interconexión que se conectan a las redes individuales. Dado que los routers se utilizan para interconectar a las redes, los puertos de un router hacen referencia a las interfaces de red.



2.3.1 Las reglas que gobiernan las comunicaciones

Todas las comunicaciones, ya sea cara a cara o a través de una red, se rigen por normas preestablecidas denominadas protocolos. Estos protocolos son específicos para cada sistema de comunicación. Esto ocurre así también en nuestra comunicación personal, las normas que utilizamos para efectuar una llamada telefónica, no son necesariamente las mismas que utilizamos para la utilización de otros medios, tales como el envío de una carta.

Piense en la cantidad de diferentes protocolos o normas que rigen todos los diferentes métodos de comunicación que existen en el mundo de hoy.

La comunicación exitosa entre las máquinas de distintas redes requiere de la interacción de muchos protocolos diferentes. Un grupo de protocolos interrelacionados necesarios para llevar a cabo una función de comunicación se denomina una suite de protocolos. Estos protocolos se implementan en software y hardware y se cargan en cada dispositivo de red o host.

Una de las mejores maneras de visualizar la forma en que todos estos protocolos interactúan entre sí es verlo como una pila. Una pila de protocolos muestra como los protocolos individuales se ubican dentro de la suite de protocolos.

Los protocolos son vistos como una jerarquía de niveles, teniendo que los niveles más altos brindan servicios a las capas inferiores. Las capas inferiores de la pila se ocupan de mover datos a través de la red y prestan sus servicios a las capas superiores, que se centran en el contenido del mensaje enviado y en la interfaz del usuario.

El uso de capas para describir la comunicación frontal

Por ejemplo, considerar la posibilidad de dos personas comunicarse cara a cara. Podemos utilizar tres capas para describir esta actividad. En la capa inferior, la capa física, tenemos dos personas, cada una con una voz que puede pronunciar las palabras en voz alta. En la segunda capa, la capa de reglas, tenemos un acuerdo de hablar en un lenguaje común. En la capa superior, la capa de contenido, hablamos realmente de las palabras es decir el contenido de la comunicación. Quien es testigos de esta conversación, en realidad no ve las "capas" flotando en el espacio. Es importante entender que el uso de capas es un modelo y, como tal, es un medio para dividir convenientemente una tarea compleja en partes y describir la manera en que funcionan.

2.3.2 Protocolos de red

En el nivel humano, algunas reglas de la comunicación son oficiales y otras son sobre-entendidas, o implícitas, y son asimiladas sobre la base de la costumbre y la práctica. Para que los equipos de una red se puedan comunicar con éxito, debe existir una suite de protocolos que permita describir como interaccionan entre si. La suite de protocolos de red deben describir procesos tales como:

- El formato o la estructura del mensaje.
- El proceso por el que los dispositivos de red intercambian información con otras redes.
- ¿Cómo y cuándo se pasaran mensajes de error entre los dispositivos de la red.
- La configuración y la terminación de los procesos de transferencia de datos

2.3.3 Suite de protocolos y estándares industriales

A menudo, muchos de los protocolos que comprenden una suite de protocolos referencia a su vez a otros protocolos o normas de la industria. Una norma es un proceso o protocolo, que ha sido apoyada por la industria de redes y ratificado por una organización de normalización, como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) o de la Internet Engineering Task Force (IETF).

El uso de las normas en la elaboración y aplicación de protocolos asegura que los productos de diferentes fabricantes pueden trabajar juntos para una comunicación eficaz. Si el protocolo no está rígidamente observada por un determinado fabricante, por un equipo o programa informático puede que no sea capaz de comunicarse con éxito con los productos fabricados por otros fabricantes. En las comunicaciones de datos, por ejemplo, si uno de los extremos de una conversación está usando un protocolo de una sola vía para regular la comunicación y el otro extremo esta usando un protocolo de comunicación de dos vías, con toda probabilidad entre esos dos equipos no se intercambiará información.

2.3.4 El proceso de interacción de los protocolos

Un ejemplo de la utilización de un protocolo conjunto en las comunicaciones en red es la interacción entre un servidor Web y un navegador Web. Esta interacción utiliza una serie de protocolos y normas en el proceso de intercambio de información entre ellos.

Los diferentes protocolos de colaboración utilizados permiten garantizar que los mensajes sean recibidos y comprendidos por ambas partes.

Ejemplos de estos protocolos tenemos:

Protocolo de aplicación:

El Protocolo de transferencia de hipertexto (HTTP) es un protocolo que rige la forma en que un servidor web y un cliente Web interactúan. El protocolo HTTP define el contenido y el formato de las peticiones y las respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente y el software de servidor web usan HTTP como parte de la solicitud. El protocolo HTTP se apoya en otros protocolos para controlar el proceso de transporte de los mensajes entre el cliente y el servidor.

Protocolo de transporte:

El Protocolo de Control de Transmisión (TCP) es el protocolo de transporte que gestiona las conversaciones individuales entre los servidores web y los clientes web. TCP divide el mensaje HTTP en piezas más pequeñas, llamadas segmentos, que se enviarán al cliente destino. También se encarga de controlar el tamaño y la velocidad a la que los mensajes se intercambian entre el servidor y el cliente.

Protocolos de Internetworking:

El más común protocolo de red es el Protocolo de Internet (IP). IP es el responsable de llevar los segmentos TCP, en el proceso de encapsulamiento de los paquetes, efectuar la asignación apropiada de las direcciones, y seleccionar el mejor camino a un host destino.

Protocolos de acceso a la red:

El protocolo de Acceso a la red describe dos funciones importantes, la función del enlace de los datos y la transmisión física de los medios de comunicación. Los protocolos de la capa de enlace de datos toman los paquetes de IP y les dan un formato para que se transmiten por los medios de comunicación. Las normas y protocolos de la capa física rigen la forma en que las señales son enviados a través de los medios de comunicación y la forma en que serán interpretados por los clientes. Los transceivers en la tarjeta de red implementan los estándares apropiados para el medio utilizado.

2.4 Usando un modelo basado en capas

2.4.1 Los beneficios de usar un modelo basado en capas

Para visualizar la interacción entre los distintos protocolos, es común utilizar un modelo de capas. Un modelo de capas describe el funcionamiento de cada uno de los protocolos dentro de cada capa, así como la interacción con las capas que están por encima y por debajo de ella.

Existen muchas ventajas al usar un modelo de capas para describir los protocolos de red.

- Ayuda en el diseño de protocolos, porque los protocolos que operan en una determinada capa definen la información que ellos utilizaran y la manera en que actuaran con respecto a los protocolos que se encuentran encima y por debajo.
- Fomenta la competencia porque los productos de diferentes proveedores pueden trabajar juntos.
- Proporciona un lenguaje común para describir las funciones y capacidades de las redes.

2.4.2 Los protocolos y los modelos referenciales

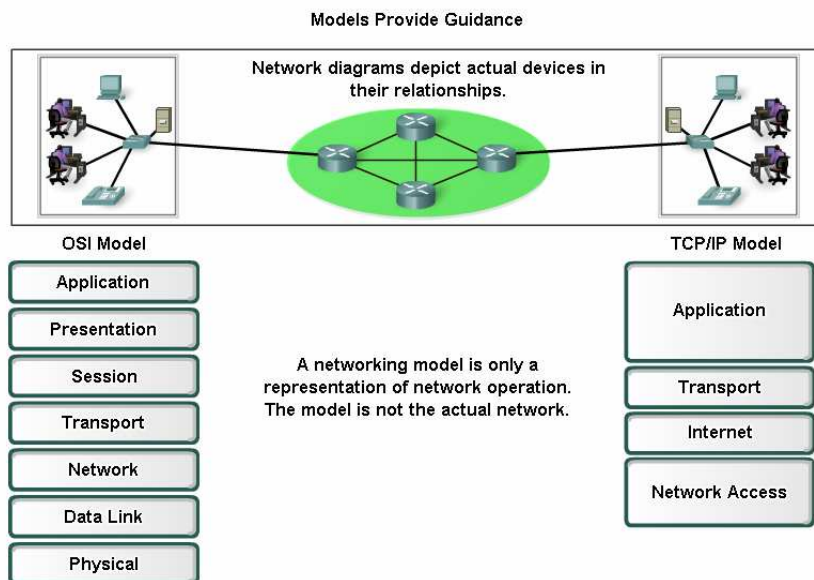
Hay dos tipos básicos de modelos de redes: modelos de protocolos y modelos de referenciales.

Un modelo de protocolo proporciona un modelo que se ajusta estrechamente a la estructura de un protocolo de una suite en particular. El modelo TCP / IP es un protocolo modelo, ya que describe las funciones que se producen en cada capa dentro de los protocolos de la suite TCP / IP.

Un modelo referencial proporciona un marco común para mantener la coherencia dentro de todos los tipos de protocolos de red y servicios. Un modelo referencial no está destinado a ser una aplicación particular que proporcione una explicación detallada de todos los servicios de una arquitectura de red. El propósito principal de un modelo de referencia es ayudar en la comprensión de las funciones y los procesos involucrados.

El modelo de Interconexión de sistemas abiertos (OSI) es el modelo referencial de internetwork mas conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento, y la resolución de problemas.

Aunque TCP / IP y OSI son los principales modelos utilizados cuando se habla de la funcionalidad de red, los diseñadores de protocolos de red, servicios o dispositivos pueden crear sus propios modelos para representar sus productos.



2.4.3 El modelo TCP/IP

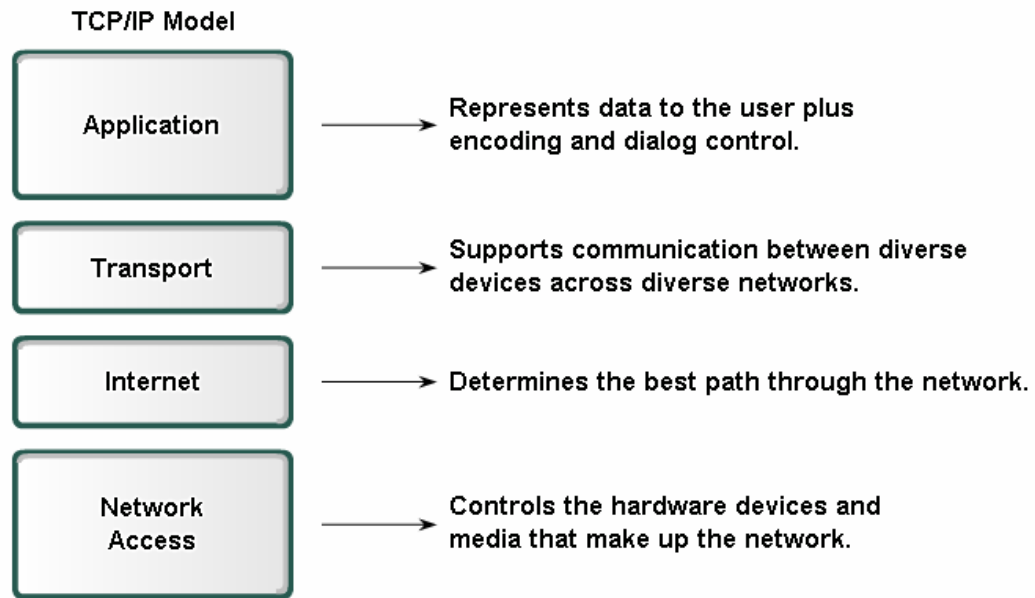
El primer modelo de protocolo para internetworks basado en capas fue creado a principios de 1970 y se conoce como el modelo de Internet.

Este modelo define cuatro capas que deben estar presentes para que las comunicaciones puedan tener éxito. La arquitectura de la suite del protocolo TCP / IP sigue la estructura de este modelo. Debido a esto, el modelo de Internet comúnmente se conoce como el modelo TCP / IP.

Algo importante es que el modelo TCP / IP es una norma abierta, por lo que no hay una empresa que tenga el control sobre las características del modelo. Las definiciones de la norma y las características de los protocolos TCP / IP se discuten en un foro público y se definen de manera públicamente en un conjunto de documentos

disponibles. Estos documentos se denominan solicitudes de comentarios (RFC). Ellos contienen las características oficiales de los protocolos de comunicaciones de datos. Los RFC también contienen los documentos técnicos y detalles organizacionales sobre la Internet, incluyendo las especificaciones técnicas y los documentos sobre las políticas elaborados por la Internet Engineering Task Force (IETF).

TCP/IP model



2.4.4 Unidad de datos de protocolo (PDU) y el encapsulamiento

Conforme las aplicaciones transmiten los datos hacia debajo de la pila de protocolos en su camino para ser transmitidos a través de la red de medios de comunicación, diversos protocolos le van añadiendo información en cada nivel. Esto es comúnmente conocido como el proceso de encapsulación.

La forma en que estos datos se van agregando en la data original forman una Unidad de Datos de Protocolo (PDU). Durante el encapsulamiento, cada capa encapsula la PDU que recibe de la capa superior, de acuerdo con el tipo de protocolo que se utilice. En cada etapa del proceso, un PDU tiene un nombre diferente para reflejar su nueva apariencia. Aunque no existe una fórmula universal para la designación de los PDUs, en este curso, los PDUs se nombran de acuerdo con los protocolos de la suite TCP/IP.

Datos:

El término general para identificar el PDU utilizado en la capa de Aplicación.

Segmento:

PDU de la capa de Transporte.

Paquete:

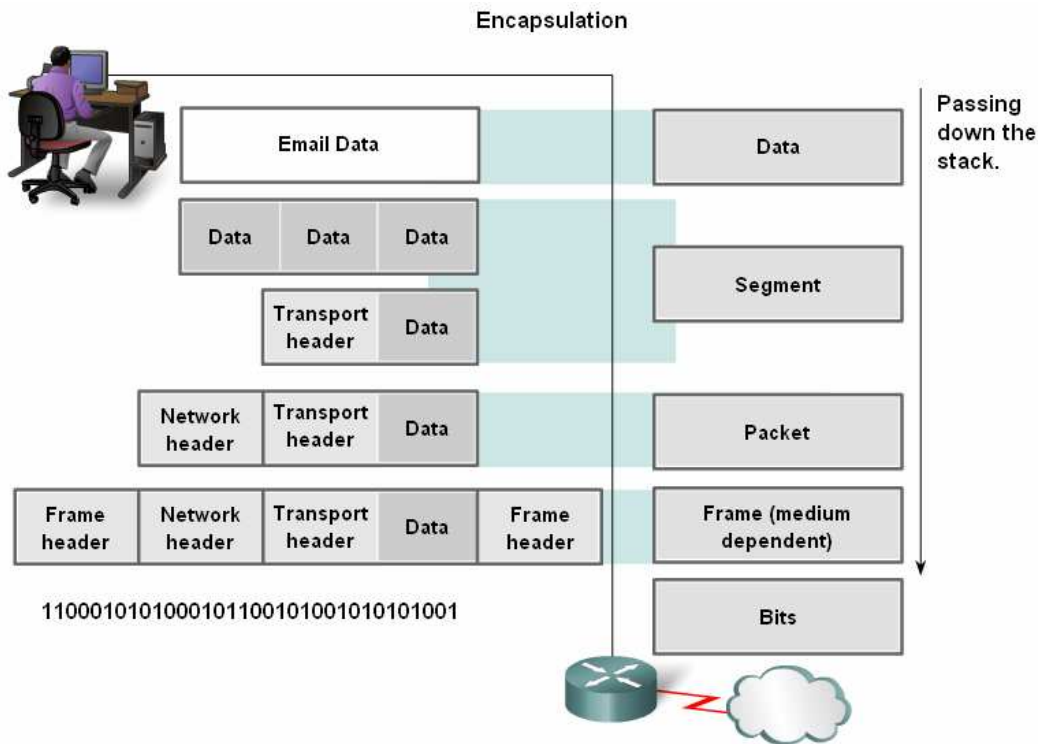
PDU de la capa de Internetwork.

Marco:

PDU de la capa de acceso a la red.

Bits:

El PDU utilizado cuando la data se transmite físicamente a través del medio.

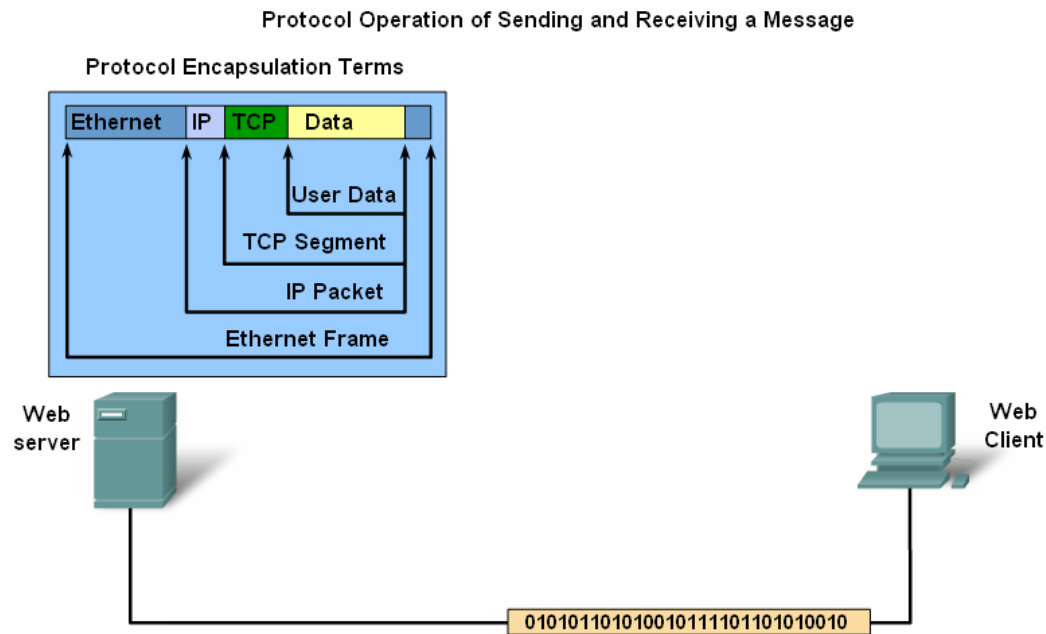


2.4.5 El proceso de recepción y transmisión

Al enviar un mensaje en la red, la pila de protocolos del host opera de arriba a abajo. En el ejemplo del servidor web, podemos usar el modelo TCP / IP para ilustrar el proceso de envío de una página HTML hacia un cliente.

El protocolo de la capa de aplicaciones, HTTP, comienza el proceso efectuando la entrega de la página web en formato HTML a la capa de transporte. Aquí los datos se dividen en segmentos TCP. A cada segmento TCP se le da una etiqueta, llamada cabecera, que contiene información sobre la aplicación que debe recibir el mensaje en el equipo destino. También contiene la información necesaria para que el proceso de destino pueda regresar los datos nuevamente a su formato original. La capa de transporte encapsula el código HTML de la página web dentro del segmento de datos y la envía a la capa de Internet, donde es implementado el protocolo IP. Aquí todo el segmento TCP se encapsula dentro de un paquete IP, que añade otra etiqueta, llamada la cabecera IP. El encabezado IP contiene la dirección del host origen y el destino, así como la información necesaria para entregar el paquete a su destino correspondiente.

Luego, el paquete IP se envía a la capa de acceso a la red, es decir al protocolo Ethernet en el que se encapsula dentro de un marco que contiene una cabecera y un campo final. Cada marco contiene una cabecera donde esta la dirección física origen y la dirección destino. La dirección física identifica a los hosts en la red local. El trailer (campo final del marco) contiene información para la comprobación de errores. Por último los bits se codifican en la capa Ethernet de los medios de comunicación por la tarjeta de red del servidor.



2.4.6 El modelo OSI

Al principio, el modelo OSI fue diseñado por la Organización Internacional de Normalización (ISO) para proporcionar un marco sobre el cual construir un conjunto de protocolos de sistemas abiertos. La visión era que estos protocolos se utilizarán para desarrollar una red internacional que sea completamente independiente de los sistemas de propiedad.

Lamentablemente, la velocidad a la que los protocolos de la suite TCP/IP basados en Internet fueron aprobados, y la rapidez con la que se popularizó, causó que el desarrollo de la suite del Protocolo OSI no se diera y finalmente languideciera. Aunque algunos de los protocolos desarrollados tomando en cuenta las especificaciones del modelo OSI son ampliamente utilizados en la actualidad, las siete capas del modelo OSI han hecho importantes contribuciones al desarrollo de otros protocolos y productos.

Como modelo de referencia, el modelo OSI ofrece una extensa lista de funciones y servicios que se pueden dar en cada capa. También describe la interacción de cada capa con las capas superiores y las que se encuentran directamente debajo de ella. Aunque el contenido de este curso se estructurará en torno a la Modelo OSI el foco de la discusión será el de los protocolos indicados en la suite TCP / IP.

Tenga en cuenta que mientras el modelo TCP / IP hace referencia a sus capas sólo por el nombre, las siete capas del modelo OSI son más a menudo referenciados por el número que por su nombre.



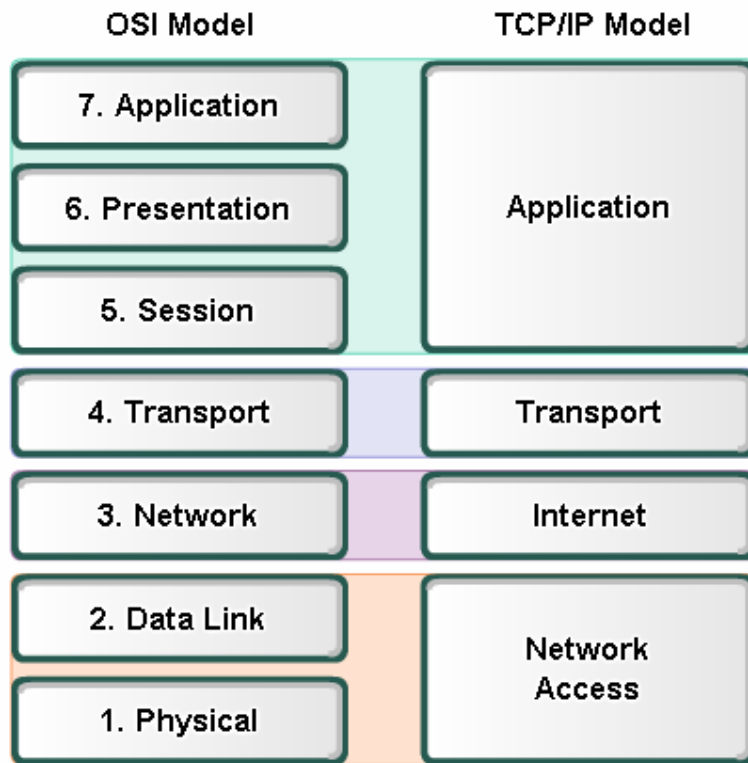
2.4.7 Comparación entre el modelo OSI y el modelo TCP/IP

Los protocolos que forman la suite TCP / IP pueden ser descritos en términos del modelo de referencia OSI. En el modelo OSI, la capa de acceso a la red y la capa de aplicación del modelo TCP / IP se dividen para describir funciones mucho más específicas que ocurren en estas capas.

En la Capa de acceso a la Red, el protocolo TCP / IP no especifica que protocolos se van a utilizar durante la transmisión por el medio físico, esta solo describe que los datos serán entregados desde la capa de Internet a la capa física. El modelo OSI en sus capas 1 y 2 explica los procedimientos necesarios para acceder a los medios de comunicación y como los medios físicos envían los datos a través de una red. Los paralelos claves entre los dos modelos de red se dan en las capas OSI 3 y 4.

La capa 3, conocida como la capa de red, se utiliza para analizar y documentar toda la variedad de procesos que se producen en todas las redes de datos y las maneras para enviar los mensajes a través de una internetwork. El Protocolo de Internet (IP) es el que se encarga de muchas de las funciones de la capa 3. La capa 4, equivale a la capa de transporte del modelo OSI, se utiliza a menudo para describir de manera general los servicios o funciones que gestionan las conversaciones individuales entre los host origen y destino. Estas funciones incluyen el reconocimiento, la recuperación de errores, y el envío secuencial de los segmentos. En esta capa, los protocolos: Protocolo de Control de Transmisión (TCP) y User Datagram Protocol (UDP) se encargan de proporcionar la funcionalidad necesaria. La capa de aplicación del protocolo TCP / IP incluye una serie de protocolos que proporcionan la funcionalidad específica para que se puedan desarrollar una gran variedad de aplicaciones de usuario final.

Las capas 5, 6 y 7 del modelo OSI se utilizan como referencia para que los desarrolladores de aplicaciones y proveedores de productos puedan ganar el acceso a la red.



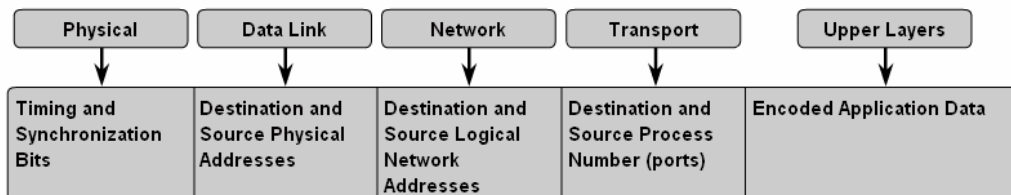
2.5 El direccionamiento de capa de red

2.5.1 Direccionamiento en la red:

El modelo OSI describe los procesos de codificación, el formato, la segmentación, y el proceso de encapsulamiento de los datos para su posterior transmisión a través de la red. Un flujo de datos que se envían desde la fuente a un destino se puede dividir en paquetes e intercalarlos con mensajes de otros hosts que viajan a otros destinos. Miles de millones de estas piezas de la información viajan a través de una red en un momento dado.

Existen varios tipos de direcciones que se deben incluir con éxito al momento de entregar los datos de una aplicación hacia otro equipo.

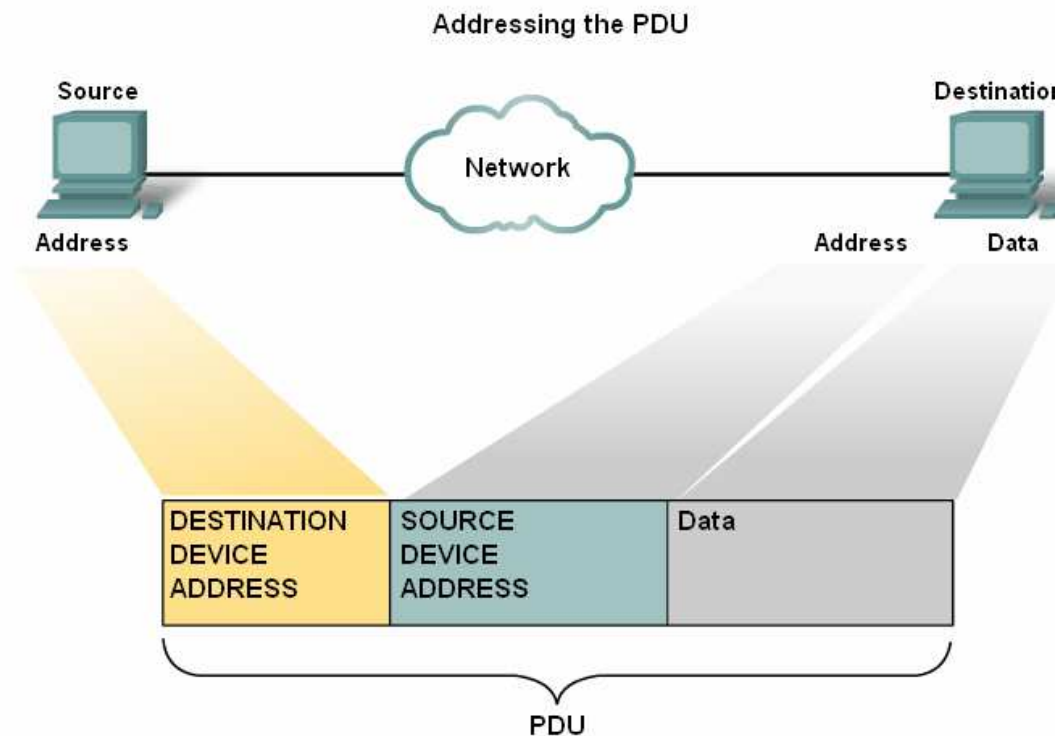
Utilizando el modelo OSI como guía, podremos estudiar los diferentes tipos de direcciones y los identificadores que son usadas en cada capa.



2.5.2 Llevando la data al dispositivo final

Durante el proceso de encapsulamiento, se van agregando una serie de identificadores a los datos a medida que estos van descendiendo por la pila de protocolos en el equipo origen. Así como hay múltiples capas de protocolos que preparan los datos para su transmisión a su destino, hay varias capas de direcciones que son agregadas para garantizar su entrega.

El primer identificador, la dirección física del hosts, esta contenida en la cabecera de la PDU de la Capa 2, llamada trama o marco. La capa 2, se encarga de la entrega de los mensajes en una única red local. La dirección de Nivel 2 es única en la red local y representantes a la dirección del dispositivo final de la capa física. En una red basada en Ethernet, a esta dirección se le llama la dirección MAC. Cuando dos dispositivos de la red local Ethernet deben comunicarse, las tramas que se intercambian entre ellos contienen la dirección destino y la dirección fuente de los hosts. Una vez que el marco es recibido por el host destino, la dirección del Nivel 2, elimina la información de direccionamiento pues los datos desencapsulados deben ser ahora trasladados hasta la pila de protocolos de la capa 3.



The Protocol Data Unit header contains device address fields.

2.5.3 Llevando la data a través de la red

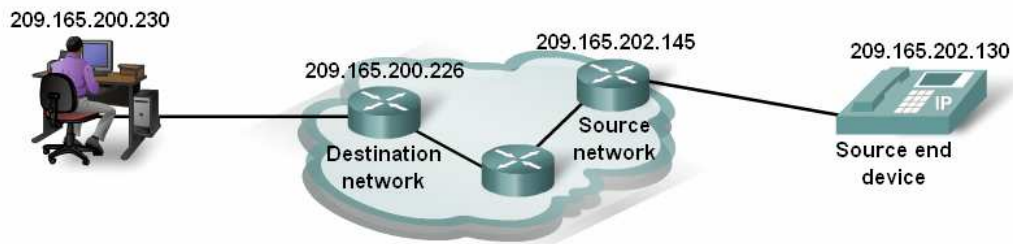
Los protocolos de capa 3 están diseñados principalmente para mover datos desde una red local a otra red local dentro de una internetwork. Mientras que la capa 2 solo se ocupa de la comunicación entre los dispositivos de una red local, en la capa 3 las direcciones deben incluir identificadores que permitan a los dispositivos de red intermediario poder ubicar equipos en diferentes redes. En la suite del protocolo TCP / IP, cada dirección IP de hosts contiene información acerca de la red donde se encuentra el host.

En la frontera de cada red local, un dispositivo intermedio de red, que suele ser un router, desencapsula la trama para leer la dirección de red destino contenido en la cabecera del paquete IP. Una vez que se determina la ruta, el router encapsula el paquete en un nuevo marco y lo envía en su camino hacia el dispositivo final. Cuando el marco llega a su destino final, el marco y la cabecera del paquete IP se eliminan y los datos son llevados hacia la capa 4.

Getting the Pieces to the Correct Network

Protocol Data Unit (PDU)				
Destination		Source		Data
Network Address	Device Address	Network Address	Device Address	

The Protocol Data Unit header also contains the network address.

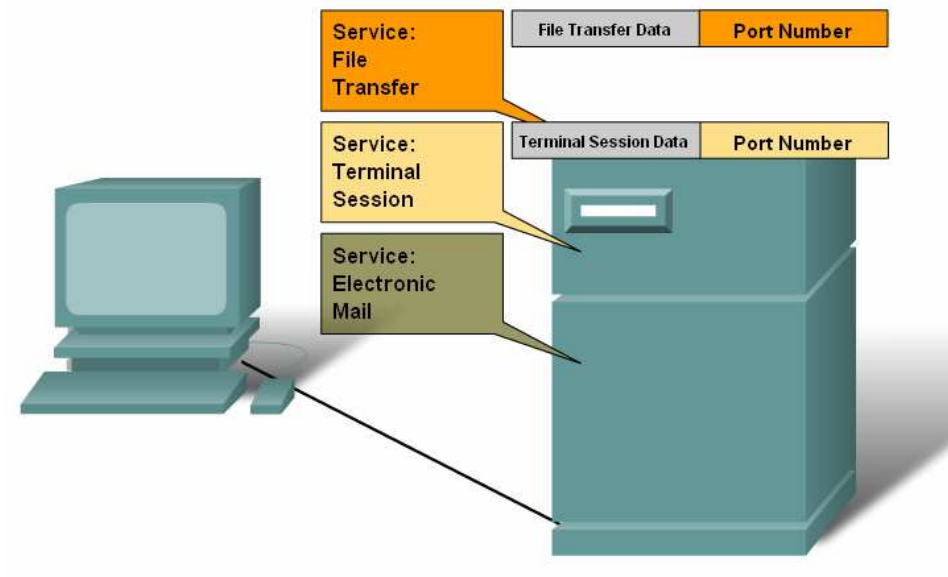


2.5.4 Llevando la data a la aplicación correcta

En la capa 4, la información que figura en el encabezado de la PDU no identifica a un destino de hosts o a una red destino. Lo que hace es identificar el proceso o servicio específico que se ejecuta en el dispositivo destino, donde se llevarán realmente los datos. Los servidores en Internet, pueden ejecutar varias aplicaciones de red simultáneamente. La capa 4 permite identificar y diferenciar estas aplicaciones. Los usuarios que utilizan una PC suelen tener un cliente de correo electrónico funcionando a la vez como un navegador web, un programa de mensajería instantánea, streaming media, y tal vez incluso un juego. Todos estos programas se ejecutan por separado, y son ejemplos de procesos individuales.

Ver una página web invoca al menos un proceso en la red. Al hacer clic en un hipervínculo se causa que un navegador web se comuniquen con un servidor web. Al mismo tiempo, a bajo nivel, un cliente de correo electrónico puede enviar y recibir correo electrónico, y un colega o amigo puede enviar un mensaje instantáneo. Todos estos programas envían sus datos a los equipos destino y estos llegan a la aplicación correcta.

Esto se debe a que cada uno de los procesos que se ejecutan en el hosts origen y el hosts destino que se están comunicando, utilizan un número de puerto como elemento identificador de la aplicación.



Autoevaluación

1. Identifique los elementos claves de la comunicación.
2. Brevemente defina el concepto de protocolo de redes. Defina su importancia
3. Identifique los elementos de hardware que forman parte de los medios de transmisión.
4. Defina el concepto de conmutación de paquetes y a qué se debe su complejidad.

Para recordar

La desventaja de usar la segmentación y la multiplexación al transmitir mensajes a través de una red es el nivel de complejidad que se añade al proceso.

Los dispositivos y los medios de comunicación son los elementos físicos o el hardware de la red. El hardware es a menudo el elemento visible que compone la plataforma de red, como una portátil, un PC, un interruptor, o el cableado utilizado para conectar los dispositivos.

La comunicación a través de una red se realiza sobre un medio. El medio proporciona el canal sobre los que el mensaje viaja desde el origen al destino.

Todas las comunicaciones, ya sea cara a cara o a través de una red, se rigen por normas preestablecidas denominadas protocolos. Estos protocolos son específicos para cada sistema de comunicación.



Protocolos y funciones de la capa de Aplicación – Parte I

TEMA

- Software de la capa de Aplicación
- El modelo Cliente servidor
- Aplicaciones Peer-to-peer

OBJETIVOS ESPECÍFICOS

- Describir como las funciones de las tres capas superiores del modelo OSI proporcionan servicios de red a las aplicaciones de los usuarios finales.
- Describir la manera en que los protocolos de la capa de Aplicación proporcionan los servicios solicitados por las capas superiores del modelo OSI..
- Definir como se usa la capa de aplicación como medio de comunicación a través de la red de información.

CONTENIDOS

- Aplicaciones – La interfase entre las redes
- Modelo OSI y TCP-IP
- El modelo Cliente-Servidor y Peer-to-Peer
- Protocolo DNS
- Servicio WEB y HTTP

3.1 Aplicaciones – La interfase entre las redes

3.1.1 Modelo OSI y TCP-IP

El modelo de referencia OSI (Interconexión de Sistemas Abiertos) es un modelo de capas, que sirve como una guía para el diseño de los protocolo de red. El modelo OSI divide el proceso de trabajo en red en siete capas lógicas, cada una de los cuales tiene sus propias características y funcionalidades a las que le son asignados determinados servicios y protocolos.

En este modelo, la información se pasa de una capa a la siguiente, partiendo de la capa de Aplicación del hosts transmisor, continuando con el envío hasta llegar a la capa física, pasando luego sobre el canal de comunicaciones hasta llegar al host destino.

La capa de aplicación, la capa siete, es la capa superior de los modelos OSI y TCP / IP. Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para la comunicación y la red subyacente sobre el que se transmiten nuestros mensajes. Los protocolos de la capa de aplicación se utilizan para el intercambio de datos entre programas que se ejecutan en el origen y el destino de los hosts. Hay muchos protocolos de la capa de aplicaciones y continuamente se van agregando nuevos desarrollos.

La Capa de Presentación

La capa de presentación tiene tres funciones principales:

Codificación y conversión de los datos de la capa de aplicaciones para garantizar que los datos del dispositivo fuente puedan ser interpretados por la aplicación adecuada en el dispositivo destino.

La compresión de los datos de una manera que puede ser descomprimido por el dispositivo de destino.

Cifrado de los datos para la transmisión y el descifrado de los mismos a partir de la recepción por parte del destinatario.

Las aplicaciones de la capa de Presentación no se encuentran asociadas a un protocolo en particular. Un ejemplo de estos son los estándares para gráficos y video. Algunos estándares para video muy populares incluyen el QuickTime and Motion Picture Experts Group (MPEG). QuickTime es una especificación para video y audio de Apple Computer, y MPEG es un estándar para compresión y codificación de video.

Entre los formatos conocidos de imágenes tenemos el Graphics Interchange Format (GIF), el Grupo Mixto de Expertos Fotográfico (JPEG), y Tagged Image File Format (TIFF). GIF y JPEG son normas de compresión y codificación de imágenes gráficas, y TIFF es un formato estándar para codificación de imágenes gráficas.

La Capa de Sesión

Como el nombre lo dice, la capa de sesión se encarga de crear y mantener diálogos entre el host origen y el host destino. La capa de sesión administra el intercambio de información para poder iniciar los diálogos, mantenerlos activos, y para poder reiniciar las sesiones que se interrumpen o inactivan durante un largo período de tiempo. La mayoría de las aplicaciones, como navegadores web o clientes de correo electrónico, incorporan la funcionalidad de las capas OSI 5, 6 y 7.

Los protocolos más conocidos de TCP / IP son los de la capa de aplicación pues son

los que permiten el intercambio de información entre los usuarios. Estos protocolos especifican el formato y la información necesaria para controlar muchas de las funciones comunes de comunicación en Internet. Entre estos protocolos TCP / IP tenemos:

Protocolo Servicio de Nombres de Dominio (DNS) se utiliza para resolver los nombres de Internet a direcciones IP.

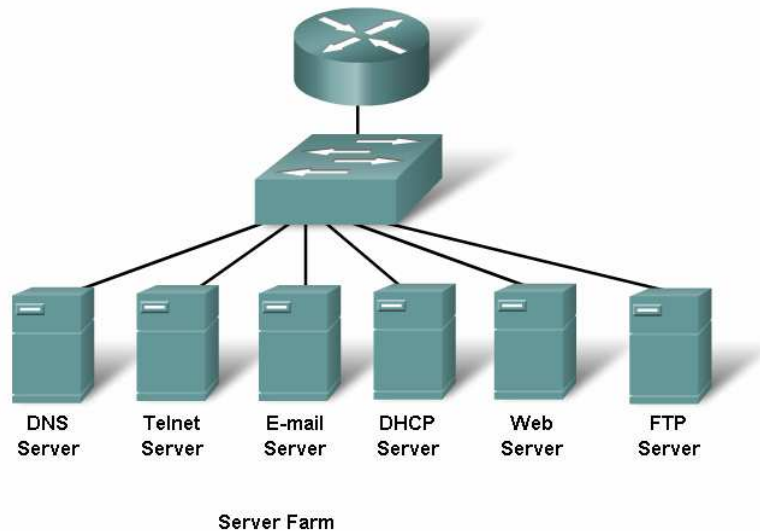
Protocolo de transferencia de hipertexto (HTTP) se utiliza para transferir los archivos que componen las páginas web de la World Wide Web.

Simple Mail Transfer Protocol (SMTP) se utiliza para la transferencia de mensajes de correo y los archivos adjuntos.

Telnet, un protocolo de emulación de terminal, se utiliza para proporcionar acceso remoto a servidores y dispositivos de redes.

Protocolo de transferencia de archivos (FTP) se utiliza para la transferencia interactiva de archivos entre sistemas.

Los protocolos de TCP / IP suite son generalmente definidos por solicitudes de comentarios o documentos RFC. La Internet Engineering Task Force mantiene las RFC como las normas oficiales para la suite TCP / IP.



3.1.2 Software de la capa de Aplicación

Las funciones asociadas a los protocolos de la capa de aplicación proporcionan a nuestra red humana la interface adecuada con la red de datos subyacente. Cuando abrimos un navegador web o una ventana de mensajería instantánea, una aplicación es ejecutada, y el programa se pone en la memoria del dispositivo en el que se ejecuta. Cada instancia de ejecución del programa cargado en un dispositivo se denomina un proceso.

Dentro de la capa de Aplicación, existen dos maneras en que los procesos o programas de software proporcionan el acceso a la red: mediante el uso de aplicaciones y servicios.

Red de las aplicaciones

Las aplicaciones son los programas de software utilizados por las personas para comunicarse a través de la red. Algunas aplicaciones de usuario final están en red, lo que significa que la aplicación de protocolos de la capa de aplicaciones y son capaces de comunicarse directamente con las capas inferiores de la pila de protocolos. E-mail

clientes y navegadores web, son ejemplos de este tipo de aplicaciones.

Servicios de nivel de aplicación

Otros programas pueden necesitar la asistencia de los servicios de la capa de aplicación para utilizar los recursos de la red, como transferencia de archivos o de impresión de red de spooling. Aunque transparente para el usuario, estos servicios son los programas que la interfaz con la red y preparar los datos para la transferencia. Los diferentes tipos de datos - si se trata de texto, gráficos, vídeo o - requieren diferentes servicios de red para asegurarse de que está bien preparado para llevar a cabo las funciones que ocurren en la parte inferior de las capas del modelo OSI. Cada aplicación o servicio de red utiliza protocolos que definen las normas y el formato que tendrán los datos. Sin protocolos, la red de datos no tendría un formato común ni una manera directa de tratar a los datos. Con el fin de comprender la función de los distintos servicios de red, es necesario familiarizarse con los protocolos que rigen su funcionamiento.

3.1.3 Aplicaciones de usuario, Servicios, y Protocolos de la capa de Aplicación

Como se mencionó anteriormente, la capa de aplicaciones utiliza protocolos que se encuentran dentro de las aplicaciones y servicios. Mientras que las aplicaciones permiten a las personas crear los mensajes, los protocolos de la capa de aplicación establecen los servicios que permitirán una comunicación con la interfaz de red.

En el modelo OSI, las aplicaciones que interactúan directamente con las personas se consideran que se encuentran en la parte superior de la pila.

Como todas las capas en el modelo OSI, la capa de aplicación se apoya en las funciones de las capas inferiores, a fin de poder completar el proceso de comunicación. Dentro de la capa de aplicación, los protocolos especifican qué mensajes se intercambian entre el origen y el destino de los hosts, la sintaxis de los comandos de control, el tipo y formato de los datos que se transmiten, y los métodos apropiados para la notificación y recuperación de errores.

3.1.4 Funciones de los protocolos de la capa de Aplicación

Los Protocolos de la capa de aplicación son utilizados tanto por el host origen y el host destino de los dispositivos de comunicación durante una sesión de comunicación. A fin de que la comunicación tenga éxito, los protocolos de la capa de aplicación utilizados en los hosts origen y destino deben coincidir.

Los protocolos establecen normas coherentes para el intercambio de datos entre las aplicaciones y los servicios ejecutados entre los dispositivos participantes.

Los protocolos especifican cómo los mensajes de datos deben estar estructurados y los tipos de mensajes que se envían entre el origen y el destino. Estos mensajes pueden ser las solicitudes de servicios, los reconocimientos, los mensajes de datos, mensajes de estado, o mensajes de error. Los Protocolos también definen los diálogos, asegurando que un mensaje enviado sea recibido por la aplicación esperada y que se invoque el servicio correcto se de la transferencia de los datos.

Muchos tipos diferentes de aplicaciones se comunican a través de las redes de datos. Por lo tanto, los servicios de capa de aplicación deben utilizar múltiples protocolos para proporcionar el rango deseado de experiencias de comunicación. Cada protocolo tiene un propósito específico y contiene las características requeridas para cumplir con ese propósito.

Las aplicaciones y los servicios también pueden utilizar varios protocolos en el transcurso de una sola conversación. Un protocolo puede especificar la forma de

establecer la conexión de red y otro describir el proceso para la transferencia de datos cuando el mensaje se pasa a la siguiente capa inferior.

3.2.1 El modelo Cliente-Servidor

Cuando la gente intenta acceder a la información de sus dispositivos, ya sea una PC, una portátil, PDA, teléfono celular, o algún otro dispositivo conectado a la red, los datos no pueden ser físicamente almacenados en su dispositivo. Si ese es el caso, debe presentarse una solicitud de acceso a la información sobre el dispositivo que contiene los datos.

El modelo cliente/servidor

En el modelo cliente / servidor, el dispositivo que solicita la información se llama un cliente y el dispositivo que da respuesta a la solicitud se llama un servidor. Los procesos Cliente y servidor se dan en la capa de aplicación. El cliente comienza el intercambio mediante la solicitud de datos del servidor, que responde con el envío de una o más secuencias de datos al cliente. Los Protocolos de la capa de aplicación describen el formato de las peticiones y respuestas entre clientes y servidores. Además de la transferencia de datos, este cambio también puede exigir información de control, tales como la autenticación de los usuarios y la identificación de un archivo de datos que se pretende transferir.

Un ejemplo de una red cliente / servidor es un entorno corporativo en el que los empleados de una empresa usan de servidor de correo electrónico para enviar, recibir y almacenar correo electrónico. El empleado utiliza su cliente de correo electrónico para emitir una solicitud al servidor de correo electrónico por cualquier correo no leído. El servidor responde enviando el e-mail solicitado al cliente.

Aunque este proceso se describe como que los datos fluyen desde el servidor al cliente, algunos datos siempre fluyen desde el cliente al servidor. El flujo de datos puede ser igual en ambas direcciones, o incluso puede ser mayor en la dirección que va desde el cliente al servidor. Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento. La transferencia de datos de un cliente a un servidor se le conoce como un proceso de carga de datos (upload) y de un servidor a un cliente como una descarga (download).

3.2.2 Servidores

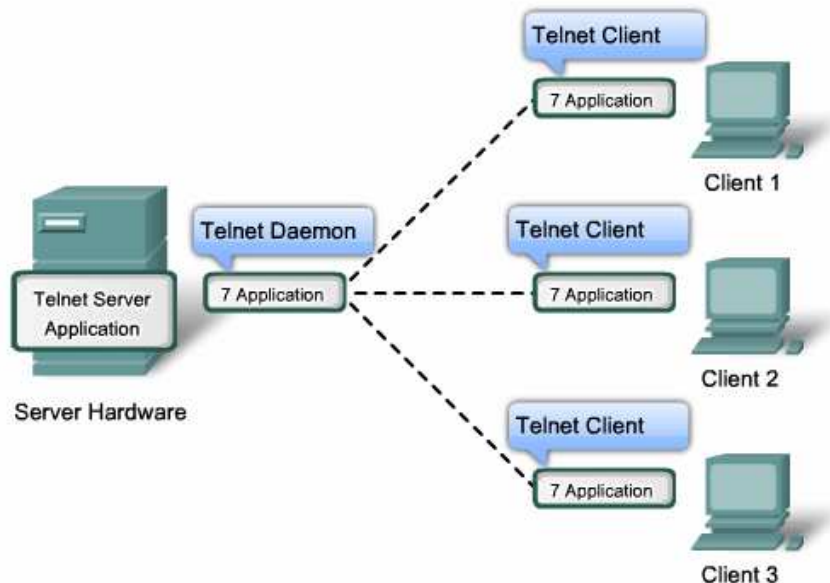
En un contexto general de redes, cualquier dispositivo que responde a las solicitudes de las aplicaciones cliente está funcionando como un servidor. Un servidor es un computador que por lo general contiene información que se comparte con muchos sistemas cliente. Por ejemplo, páginas web, documentos, bases de datos, imágenes, video y archivos de audio pueden ser almacenados en un servidor y entregados a la solicitud de los clientes. En otros casos, como una impresora de red, el servidor de impresión ofrece al cliente peticiones de impresión a la impresora especificada. Distintos tipos de aplicaciones de servidor pueden tener diferentes requerimientos para el acceso de los clientes. Algunos servidores pueden requerir la autenticación por parte del usuario para verificar si el usuario tiene permiso para acceder a los datos solicitados, o para usar una operación en particular. Tales servidores se basan en una lista central de las cuentas de usuario y de las autorizaciones o permisos, (tanto para el acceso a los datos y a las operaciones). Al utilizar un cliente FTP, por ejemplo, si usted solicita cargar los datos con el servidor FTP, puede que tenga permisos para escribir en su carpeta individual, pero no para leer otros archivos en el servidor. En una red cliente / servidor, el servidor ejecuta un servicio, o proceso, conocido como demonio (daemon). Al igual que la mayoría de los servicios, los demonios habitualmente se ejecutan en segundo plano y no se encuentran bajo el control

directo del usuario. Cuando un demonio escucha una petición de un cliente, intercambia una serie de mensajes con el cliente debido a que están programados para responder cada vez que el servidor recibe una solicitud sobre los servicios que presta.

3.2.3 Protocolos y Servicios de la Capa de Aplicación

Las aplicaciones pueden emplear diferentes servicios de la capa de aplicación, por lo tanto, lo que aparece para el usuario como una simple solicitud de una página web puede, de hecho, ascender a decenas de solicitudes individuales. Y para cada una de las peticiones, pueden ser ejecutados múltiples procesos. Por ejemplo, un cliente puede requerir varios procesos individuales para formular sólo una petición a un servidor.

Además, los servidores suelen tener varios clientes solicitando información al mismo tiempo. Por ejemplo, un servidor Telnet puede tener muchos clientes solicitando conexiones a la misma. Estas solicitudes individuales de los cliente debe ser tratados de manera simultánea y por separado de la red para tener éxito. La capa de aplicación procesa y otorga servicios con el fin de apoyar las funciones de las capas inferiores para gestionar con éxito las múltiples conversaciones.



3.2.4 Aplicaciones Peer-to-Peer (P2P)

El Modelo Peer-to-Peer

Además del modelo cliente / servidor en networking también hay un modelo peer-to-peer. Peer-to-peer puede ser entendido de dos formas distintas: diseño de redes de igual a igual y el diseño aplicaciones peer-to-peer (P2P). Ambas formas tienen características similares, pero en la práctica trabajan de maneras distintas.

Redes Peer-to-Peer

En una red peer-to-peer, dos o más computadores están conectados a través de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor

dedicado. Cada dispositivo final conectado (conocido como peer) bien puede funcionar como un servidor o un cliente. Un equipo puede asumir la función de servidor para una transacción al tiempo que actúa como un cliente para otra. Las funciones de cliente y servidor se establecen sobre la base de una solicitud.

Una simple red doméstica con dos computadoras conectadas para compartir una impresora es un ejemplo de una red peer-to-peer. Cada persona puede configurar su computador para compartir archivos, activar juegos en red, o compartir una conexión a Internet. Otro ejemplo de funcionalidad peer-to-peer red es la de dos computadores conectados a una gran red que utilizan un tipo de software para compartir recursos entre sí a través de la red.

A diferencia del modelo cliente / servidor, que utiliza servidores dedicados, una red peer-to-peer redes descentraliza los recursos de una red. En lugar de ubicar la información que se comparte en servidores especializados, la información puede estar ubicada en cualquier dispositivo conectado. La mayoría de los actuales sistemas operativos permiten compartir archivos e impresoras sin necesidad de software adicional. Debido a que las redes peer-to-peer por lo general no usan cuentas de usuario, permisos, o herramientas de monitoreo, se hace difícil hacer cumplir las políticas de acceso y seguridad en este tipo de redes. Las cuentas de usuario y derechos de acceso deben establecerse individualmente en cada host de la red.

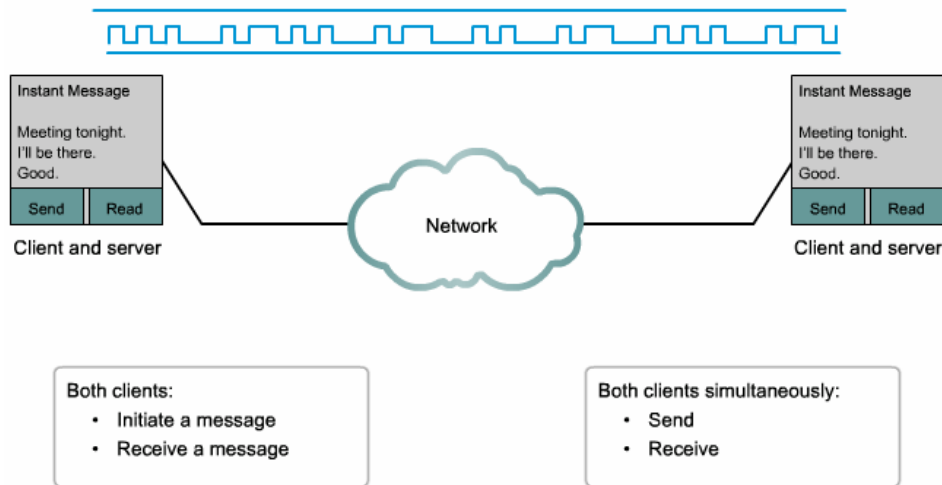
Aplicaciones Peer-to-Peer

Una aplicación peer-to-peer (P2P), a diferencia de una red punto-a-punto, permite que un dispositivo actúe como un cliente y un servidor en el mismo proceso de comunicación. En este modelo, cada cliente es un servidor y un servidor es un cliente. Ambos pueden iniciar la comunicación y se consideran iguales en el proceso de comunicación. Sin embargo, las aplicaciones peer-to-peer requieren que cada uno de los extremos del dispositivo proporcione una interfaz de usuario y ejecuten un servicio de apoyo. Cuando se ejecuta una aplicación peer-to-peer esta invoca las aplicaciones necesarias que sirvan como interfaz de usuario y los servicios que se ejecutaran en bajo nivel. Después de esto los dispositivos pueden comunicarse directamente.

Algunas aplicaciones P2P utilizan un sistema híbrido donde los recursos compartidos están distribuidos, pero los índices que apuntan a los recursos se almacenan en un directorio centralizado. En un sistema híbrido, cada uno de los equipos pares accede a un servidor que contiene los índices que le permitan obtener la ubicación de un recurso almacenado en otro peer. El servidor índice también puede ayudar a conectar dos hosts, pero una vez conectado, la comunicación tiene lugar entre los dos hosts, no necesitando luego que se comuniquen con el servidor índice.

Las aplicaciones peer-to-peer pueden ser utilizadas en redes peer-to-peer, cliente / servidor, y a través de Internet.

Peer-to-Peer Applications
Client and server in the same communication



3.3.1 Protocolo DNS

En las redes de datos, los dispositivos están etiquetados con sus direcciones IP, de manera que puedan participar en el envío y recepción de mensajes a través de la red. Sin embargo, a la mayoría de las personas les es muy difícil recordar direcciones numéricas. Por lo tanto, los nombres de dominio se crearon para convertir las direcciones numéricas en nombres reconocibles.

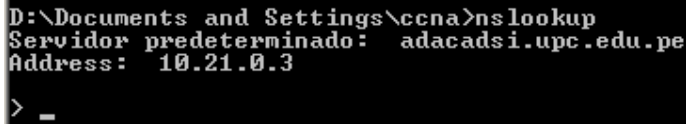
En Internet estos nombres de dominio, como por ejemplo www.cisco.com, son mucho más fáciles de recordar para el común de las personas que 198.133.219.25, que es la verdadera dirección numérica de este servidor. Además, si Cisco decide cambiar la dirección numérica, esto será transparente para el usuario, pues el nombre de dominio seguirá siendo www.cisco.com. La nueva dirección estará vinculada al actual nombre de dominio y la conectividad se mantendrá. Antiguamente cuando las redes eran pequeñas, era algo simple mantener la relación entre los nombres de dominio y las direcciones IP. Sin embargo, cuando las redes comenzaron a crecer y el número de dispositivos de red aumentó, este sistema manual se convirtió en algo impracticable. El sistema de nombres de dominio (DNS) se ha creado para resolver los nombres de dominio frente a las direcciones IP. El servicio DNS utiliza un conjunto de servidores distribuidos para resolver los nombres asociados con estas direcciones numéricas. El protocolo DNS define un servicio automatizado que relaciona los nombres de los recursos con la dirección de red numérica. Incluye el formato de las solicitudes, las respuestas, y los formatos de datos. El protocolo DNS utiliza un solo formato que se denomina mensaje. Este tipo de mensaje es usado para todos los tipos de consultas y respuestas de los clientes al servidor.

DNS es un servicio cliente / servidor, pero se distingue de los otros servicios cliente / servidor que estamos analizando. Pues los otros servicios usan un cliente que es una aplicación (como el navegador web, cliente de correo electrónico), en cambio el cliente DNS se ejecuta como un servicio. El cliente DNS, a veces se le llama "resolver" DNS, y apoya la resolución de nombres para nuestras otras aplicaciones de red y servicios que lo necesiten.

Al configurar un dispositivo de red, por lo general se ingresan una o varias direcciones del servidor DNS que el cliente puede utilizar para efectuar la resolución de nombres. Por lo general, el proveedor de servicios de Internet proporciona las direcciones de sus servidores DNS. Cuando un usuario pide conectarse a un dispositivo remoto usando

su nombre, el cliente DNS pregunta a uno de estos servidores de nombres para resolver el nombre y darle la dirección numérica.

Los sistemas operativos tienen una utilidad llamada nslookup, que permite que el usuario pueda realizar consultas a los servidores de nombres para resolver un determinado nombre de host. Esta utilidad también se puede utilizar para solucionar problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.



```
D:\Documents and Settings\ccna>nslookup
Servidor predeterminado:  adacads1.upc.edu.pe
Address:  10.21.0.3
> _
```

Un servidor DNS proporciona la resolución de nombres usando el proceso demonio, que es a menudo llamado el “named”.

El servidor DNS almacena distintos tipos de registros de recursos utilizados para resolver los nombres. Estos registros contienen el nombre, la dirección y el tipo de registro.

Algunos de estos tipos de registro son los siguientes:

A – define la dirección de un dispositivo final.

NS - un servidor de nombres con autoridad.

CNAME - el nombre canónico (o de Nombres de Dominio Totalmente Cualificado) de un alias; usado cuando múltiples servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.

MX - registro de intercambio de correo; mapea un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

Cuando un cliente hace una consulta, el servidor de nombres primero se remite a sus propios registros para ver si puede resolver el nombre. Si no es capaz de resolver el nombre con sus registros almacenados localmente, entra en contacto con otros servidores, a fin de resolver el nombre.

La solicitud puede ser pasada a lo largo de una serie de servidores, lo que puede tardar la resolución más tiempo y también consumir mas ancho de banda. Una vez que se encuentra una coincidencia, la consulta regresa al servidor solicitante original, y el servidor almacena temporalmente la dirección IP que coincide con el nombre en la memoria caché.

Si el mismo nombre le es solicitado una vez más, el primer servidor puede devolver la dirección utilizando el valor almacenado previamente en su caché. El Caché de DNS reduce tanto el trafico de la red al evitar la consulta de datos y el volumen de trabajo de los servidores de más alta jerarquía.

El servicio del Cliente DNS en Windows optimiza la resolución de nombres DNS mediante el almacenamiento de nombres que han sido resueltos previamente en la memoria. El comando ipconfig / displaydns muestra por pantalla todas las entradas de la caché de DNS en un equipo con Windows XP o Windows 2000.

DNS Message Format

DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers

Header	
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

El sistema de nombres de dominio utiliza un sistema jerárquico para crear una base de datos para proporcionar la resolución de nombres. La jerarquía parece un árbol invertido con la raíz en la parte superior y las ramas por debajo. En la parte superior de la jerarquía, los servidores raíz mantienen los registros sobre la forma de alcanzar el dominio de nivel superior de los servidores, los que a su vez tienen los registros que hacen referencia a los servidores de dominio de nivel secundario y así sucesivamente.

Los diferentes dominios de nivel superior representan ya sea el tipo de organización o el país de origen.

Ejemplos de dominios de nivel superior son:

AU – Australia

Co - Colombia

Com - una empresa o industria

JP - Japón

Org - una organización sin fines de lucro

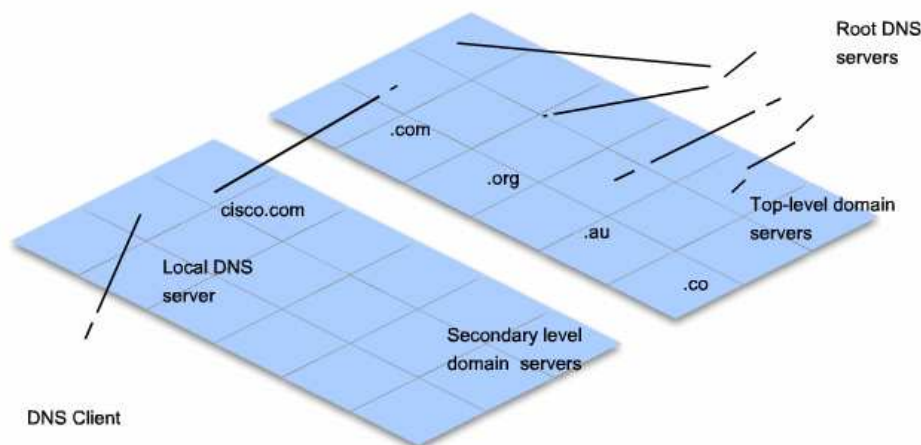
Después de los dominios de nivel superior están los de segundo nivel, y por debajo de ellos están otros dominios de nivel inferior.

Cada nombre de dominio es un camino a través de ese árbol invertido a partir de la raíz. Por ejemplo, como se muestra en la figura, el servidor raíz DNS puede no saber exactamente donde se encuentra el servidor de correo electrónico mail.cisco.com, pero mantiene un registro del dominio de nivel superior “com”. Del mismo modo, los

servidores del dominio "com" no podrán tener un registro para mail.cisco.com, pero tienen un récord del dominio "cisco.com". Los servidores en el dominio cisco.com tienen un registro (un registro MX para ser precisos) para mail.cisco.com.

El sistema de nombres de dominio se basa en esta jerarquía descentralizada de los servidores para almacenar y mantener estos registros de recursos. Los registros de recursos listan los nombres de dominio que el servidor puede resolver y otros servidores que también pueden efectuar las solicitudes. Si un servidor determinado tiene registros de recursos que corresponden a su mismo nivel en la jerarquía de dominios, se dice que es un servidor autorizado ("authoritative") para esos registros.

Por ejemplo, un servidor de nombres de dominio en cisco.netacad.net no sería autorizado para el registro mail.cisco.com porque este se encuentra en un dominio de mayor nivel, específicamente el nombre del servidor en el dominio cisco.com.



A hierarchy of DNS servers contains the resource records that match names with addresses.

3.3.2 Servicio WEB y HTTP

Cuando una dirección Web (o URL) se digita en un navegador web, el navegador establece una conexión con el servicio web ejecutándose en el servidor utilizado el protocolo HTTP. URL (Uniform Resource Locator) y URI (Uniform Resource Identifier) son los nombres que la mayoría de la gente asocia con las direcciones web. La URL <http://www.cisco.com/index.html> es un ejemplo de una URL que hace referencia a un recurso específico - una página web de nombre index.html en un servidor identificado como cisco.

Los navegadores Web son aplicaciones que nuestros clientes utilizan en los computadores para conectarse a la World Wide Web y dar acceso a los recursos almacenados en un servidor web. Como con la mayoría de los procesos de tipo servidor, el servidor web se ejecuta como un servicio de bajo nivel y hace que los diferentes tipos de archivos se encuentren disponibles.

Con el fin de acceder al contenido, los clientes web realizan conexiones al servidor para acceder a los recursos deseados. El servidor responde entregando los recursos y el navegador interpreta los datos y lo presenta al usuario.

Los navegadores pueden interpretar y presentar muchos tipos de datos, como texto plano o Lenguaje de hipertexto de marcas (HTML, el lenguaje en el que se construyen las páginas web). Otros tipos de datos, sin embargo, pueden requerir otros servicios o programas, por lo general, se les identifica como plug-ins o add-ons. Para ayudar al navegador a determinar qué tipo de archivo es el que recibe, el servidor especifica qué tipo de datos contiene el archivo.

Para entender mejor, la forma en que el navegador web y el cliente interactúan, podemos examinar la forma en que una página Web se abre en un navegador. Para este ejemplo, se utilizará la URL: <http://www.cisco.com/web-server.htm>.

En primer lugar, el navegador interpreta las tres partes de la URL:

1. Http (protocolo o esquema)
2. Www.cisco.com (el nombre del servidor)
3. Web-server.htm (el nombre de archivo solicitado)

El navegador entonces consulta con un servidor de nombres para convertir el nombre de dominio `www.cisco.com` en una dirección numérica, que luego es utilizada para conectarse con el servidor. Usando los requerimientos del protocolo HTTP, el navegador envía una solicitud GET al servidor y le pide el archivo `web-server.htm`. El servidor, a su vez, envía el código HTML de esta página web al navegador. Por último, el navegador descifra el código HTML y le da el formato correspondiente con el navegador.

El Protocolo de Transferencia de Hipertexto (HTTP), uno de los protocolos de la suite TCP / IP, se desarrolló originalmente para publicar y recuperar las páginas HTML y ahora es utilizado para distribuir, en sistemas de información colaborativos. HTTP se utiliza en todo el World Wide Web para la transferencia de datos y es uno de los protocolos de aplicación más utilizados.

EL protocolo HTTP especifica una petición / respuesta. Cuando un cliente, por lo general, un navegador web, envía un mensaje de petición a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar a la página web y también los tipos de mensajes el servidor usa para responder.

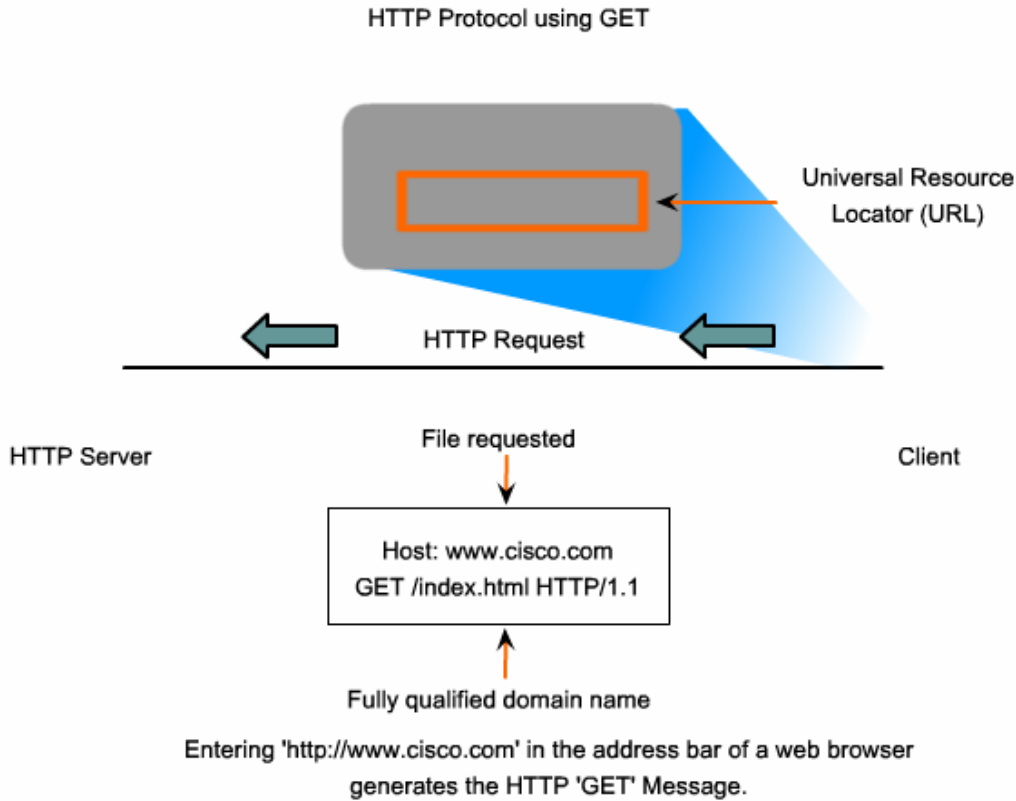
Los tres tipos de mensajes comunes son GET, POST, y PUT.

GET es un cliente de la solicitud de datos. Un navegador web envía el mensaje GET para solicitar páginas de un servidor web. Como se muestra en la figura, una vez que el servidor recibe la solicitud GET, responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje propio, el contenido del mensaje puede ser el archivo solicitado, un mensaje de error, o algún otro tipo de información.

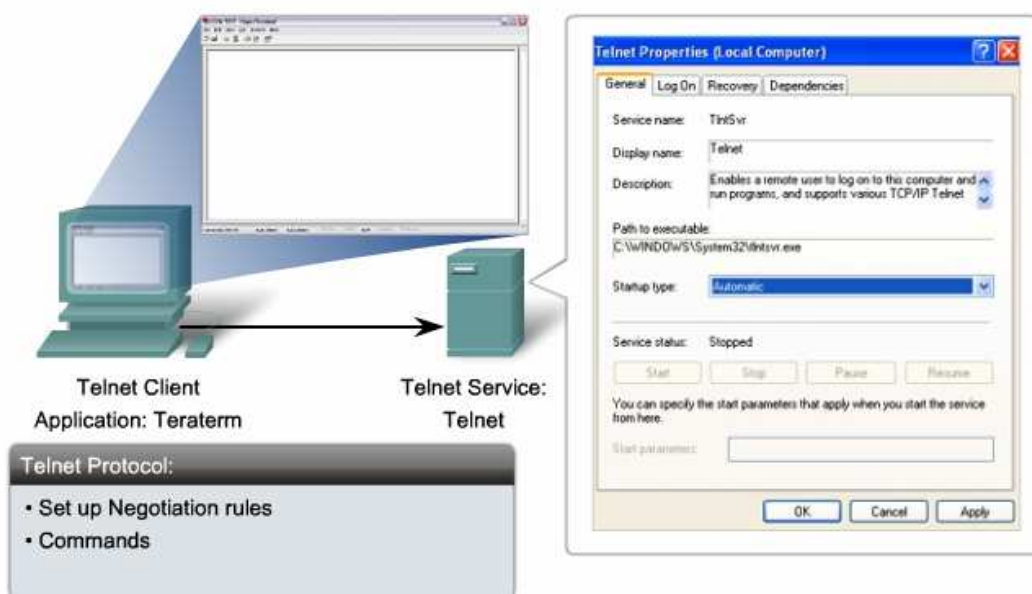
POST y PUT se utilizan para enviar mensajes para cargar los datos al servidor web. Por ejemplo, cuando el usuario introduce datos en un formulario incrustado en una página web, incluye los datos POST en el mensaje enviado al servidor. PUT sube recursos o archivos de contenido al servidor web.

Aunque es muy flexible, HTTP no es un protocolo seguro. Los mensajes POST usados para subir información al servidor se envían en formato texto que puede ser interceptado y leído. Del mismo modo, el servidor da sus respuestas, por lo general, también cifrar.

Para garantizar la comunicación a través de Internet, el Secure HTTP (HTTPS) es el protocolo utilizado para acceder o publicar la información del servidor web. HTTPS puede utilizar la autenticación y el cifrado de datos para garantizar los datos a medida que viajan entre el cliente y el servidor. HTTPS.



Telnet: Application, Service & Protocol



Autoevaluación

1. Identificar y definir las aplicaciones que podremos utilizar para tener acceso a la red Gnutella.
2. Mediante un diagrama identifique los protocolos del modelo TCP/IP
3. Identifique 4 características de las redes Peer-to-Peer.
4. ¿Cuál es la ventaja de una red cliente-servidor frente a una red peer-to-peer?

Para recordar

Las aplicaciones de la capa de Presentación no se encuentran asociadas a un protocolo en particular. Un ejemplo de estos son los estándares para gráficos y video. Algunos estándares para video muy populares incluyen el QuickTime and Motion Picture Experts Group (MPEG).

En el modelo OSI, las aplicaciones que interactúan directamente con las personas se consideran que se encuentran en la parte superior de la pila.

Los protocolos más conocidos de TCP / IP son los de la capa de aplicación pues son los que permiten el intercambio de información entre los usuarios.

En una red peer-to-peer, dos o más computadores están conectados a través de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado.



Protocolos y funciones de la capa de Aplicación – Parte II

TEMA

- Aplicaciones TCP/IP
- Servicios Peer-to-Peer

OBJETIVOS ESPECÍFICOS

- Describir la función de conocidas aplicaciones TCP / IP, como WWW y el correo electrónico, y de sus correspondientes protocolos (HTTP, DNS, SMB, DHCP, SMTP / POP, y Telnet).
- Describir los procesos de intercambio de archivos que utilizan las aplicaciones peer-to-peer y el protocolo Gnutella.

CONTENIDOS

- Servicios de correo y Protocolos SMTP/POP
- FTP
- DHCP
- Servicios para compartir archivos y protocolo SMB
- Servicios Peer-to-Peer y el Protocolo Gnutella
- Servicios Telnet

4.1. Servicios de correo y Protocolos SMTP/POP

El E-mail, el servicio de red más popular, ha revolucionado la forma que tienen las personas de comunicarse debido a su sencillez y rapidez. Sin embargo, para ejecutarse en un computador u otro dispositivo final, el correo electrónico requiere varias aplicaciones y servicios. Dos ejemplos de protocolos de la capa de aplicación son POP (Post Office Protocol) y Simple Mail Transfer Protocol (SMTP), que se muestra en la figura. Al igual que HTTP, estos procesos definen procesos cliente / servidor.

Cuando la gente compone mensajes de correo electrónico, normalmente utiliza una aplicación llamada Agente de Usuario de Correo (MUA), o cliente de correo electrónico. El MUA permite enviar los mensajes y luego coloca los mensajes recibidos en el buzón de correo del cliente, que son procesos distintos. Con el fin de recibir mensajes de correo electrónico de un servidor de correo electrónico, el cliente de correo electrónico puede utilizar el protocolo POP.

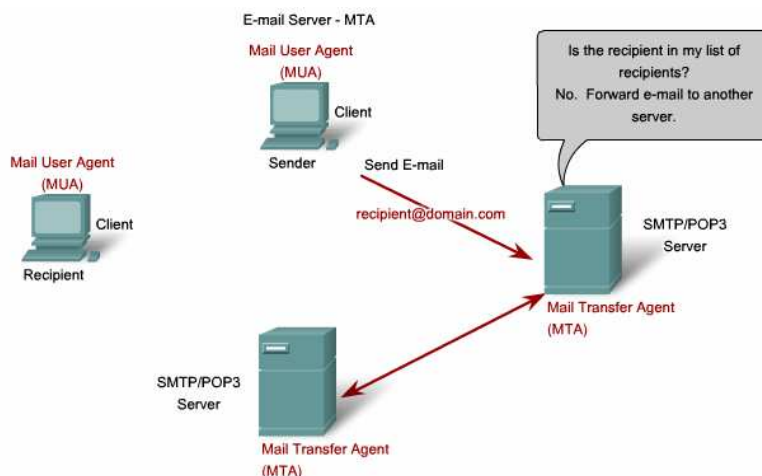
El envío de e-mail de un cliente, ya sea un servidor utiliza formato de mensajes y cadenas de mando definidas por el protocolo SMTP. Por lo general, un cliente de correo electrónico proporciona la funcionalidad de ambos protocolos dentro de una aplicación.

4.1.1 E-mail Server Processes - MTA and MDA

El servidor de correo electrónico opera dos procesos separados:

- Agente de Transferencia de Correo (MTA)
- Agente de entrega de correo (MDA)

El Agente de Transferencia de Correo (MTA) se utiliza para el proceso de enviar los e-mails. Como se muestra en la figura, el MTA recibe mensajes de los MUA o de otro MTA en otro servidor de correo electrónico. Usando como base la cabecera del mensaje, determina cómo se transmitirá el mensaje a su destino. Si el mail se dirige a un usuario cuyo buzón se encuentra en el servidor local, el correo se pasa a la MDA. Si el correo es para un usuario que no está en el servidor local, la MTA rutea el e-mail hacia el MTA en el servidor adecuado.



The Mail Transfer Agent process governs e-mail handling between servers and servers.

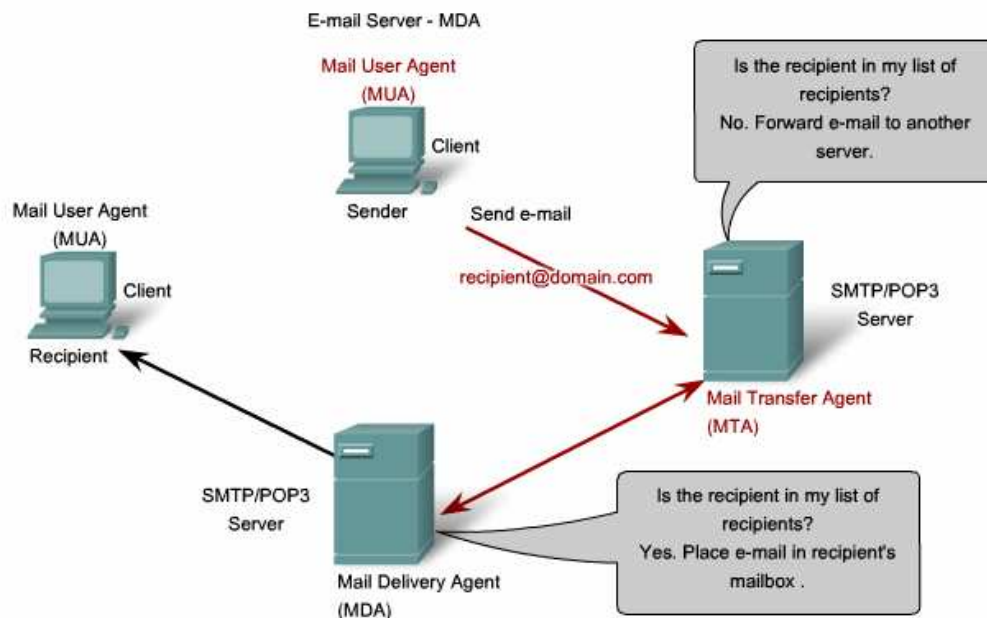
En la figura, vemos que el Agente de entrega de correo (MDA) acepta una parte del e-mail de un Agente de Transferencia de Correo (MTA) y realiza la entrega efectiva. El

MDA recibe todo el correo entrante del MTA y lo coloca en los buzones de correo de los usuarios. El MDA también puede resolver problemas de entrega final, tales como la detección de virus, filtrado de spam, y la manipulación del proceso de recepción-entrega. La mayoría de las comunicaciones por correo electrónico utilizan el MUA, MTA, MDA y aplicaciones. Sin embargo, hay otras alternativas para la entrega de correo electrónico.

Un cliente puede estar conectado a un sistema de correo electrónico corporativo, como el de IBM Lotus Notes, Novell Groupwise, o de Microsoft Exchange. Estos sistemas suelen tener su propio formato de correo electrónico interno, y sus clientes suelen comunicarse con el servidor de correo electrónico utilizando un protocolo propietario.

El servidor envía o recibe correo electrónico a través del gateway del producto, el cual realiza cualquier reformato que sea necesario. Si, por ejemplo, dos personas que trabajan para la misma compañía intercambian correo electrónico entre sí utilizando un protocolo propietario, sus mensajes permanecerán completamente dentro del sistema de correo electrónico de la empresa.

Como otra alternativa, los computadores que no cuentan con un MUA incluso podrían conectarse a un servicio de correo con un navegador web con el fin de recuperar y enviar mensajes de esta forma. Algunas computadoras pueden dirigir sus propios MTA y gestionar inter-dominios de correo electrónico.



The Mail Delivery Agent process governs delivery of e-mail between servers and clients.

Como se mencionó anteriormente, el correo electrónico puede utilizar los protocolos POP y SMTP (véase el gráfico para obtener una explicación de la forma en que trabaja cada uno de ellos). POP y POP3 (Post Office Protocol, versión 3) son protocolos de entrega de correo entrante.

Ellos envían correos electrónicos desde el servidor de correo al cliente (MUA). El servidor MDA escucha cuando un cliente se conecta a un servidor. Una vez que se establece una conexión, el servidor puede entregar el e-mail al cliente. El protocolo Simple Mail Transfer Protocol (SMTP), por otra parte, regula la transferencia del correo saliente del cliente hacia el servidor de e-mail. (MDA), así como el transporte del e-mail entre los servidores de e-mail (MTA). SMTP permite

enviar e-mails a través de redes de datos entre los diferentes tipos de software cliente y servidor y hace que el intercambio de correo electrónico se realice a través de Internet.

La estructura de los mensajes del protocolo SMTP utiliza un formato rígido de comandos y respuestas. Estos comandos apoyan a los procedimientos utilizados en SMTP, tales como la sesión de apertura, las transacciones de correo, reenvío de correo, verificación de nombres de buzón, la ampliación de las listas de correo, y la apertura y cierre de los intercambios de e-mail.

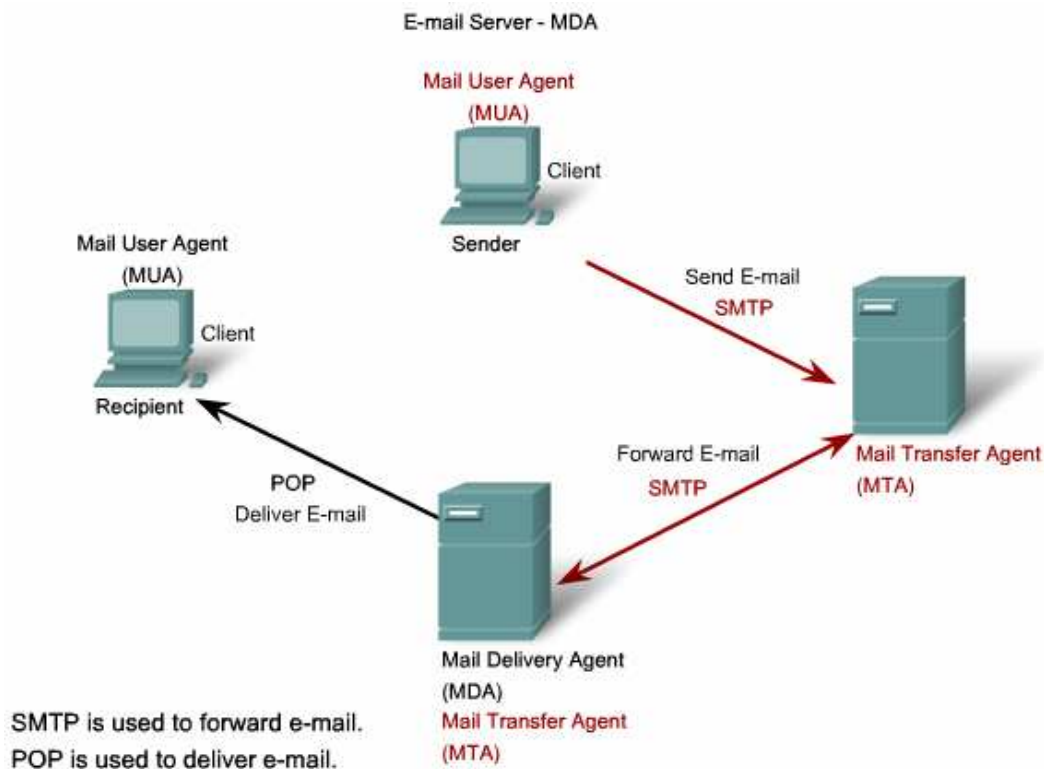
Algunos de los comandos especificados en el protocolo SMTP son:

HELO - SMTP identifica el proceso cliente con el proceso del servidor SMTP.
EHLO - Es una versión más reciente de HELO, que incluye extensiones de los servicios.

CORREO DE - Identifica el remitente

RCPT A - Identifica al destinatario

DATOS - Describe el cuerpo del mensaje



4.2 FTP

El Protocolo de transferencia de archivos (FTP) es otro protocolo de uso común de la capa de aplicación. FTP fue desarrollado para permitir la transferencia de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en un equipo que se utiliza para enviar y descargar los archivos desde un servidor FTP que esta ejecutando el demonio (FTPd).

Para poder transferir archivos, FTP requiere de dos conexiones entre el cliente y el servidor: una para los comandos y respuestas, el otro para la transferencia de los archivos.

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

El cliente establece la segunda conexión con el servidor en el puerto TCP 20. Esta conexión es para la transferencia neta de los archivos y se crea cada vez que hay una transferencia de archivos.

La transferencia de archivos puede ocurrir en cualquier dirección. El cliente puede descargar (pull) un archivo desde el servidor o, el cliente puede llevar (push) un archivo al servidor.

4.3 DHCP

El protocolo Dynamic Host Configuration Protocol (DHCP), es el servicio que permite a los dispositivos de una red obtener las direcciones IP y otra información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, puerta de enlace y otros parámetros de red IP.

DHCP permite a un host obtener una dirección IP dinámica cuando este se conecte a la red. El servidor DHCP será contactado y se le solicitará una dirección. El servidor DHCP elige una de manera aleatoria una dirección desde un rango de direcciones y las asigna ("renta") al hosts por un período determinado. En redes locales muy grandes, o en aquellas donde la población de usuarios cambia con frecuencia, se prefiere usar DHCP. Puede ser que usuarios nuevos lleguen con sus laptops y necesiten una conexión, o que se agreguen nuevos equipos que necesiten ser conectados. En lugar que sea el administrador de la red el que se encargue de asignar las direcciones IP para cada estación de trabajo, es más eficiente que estas direcciones sean asignadas automáticamente mediante DHCP. DHCP distribuye direcciones que no son asignados permanentemente a los hosts, sino sólo son arrendadas por un período de tiempo. Si el host se apaga o es retirado de la red, la dirección se devuelve al pool de direcciones para su reutilización. Esto es especialmente útil con los usuarios móviles que vienen y van en una red. Los usuarios pueden moverse libremente de un lugar a otro y volver a establecer conexiones de red de manera transparente. El host puede obtener una dirección IP una vez que se haya garantizado la conexión, ya sea a través de una LAN cableada o inalámbrica.

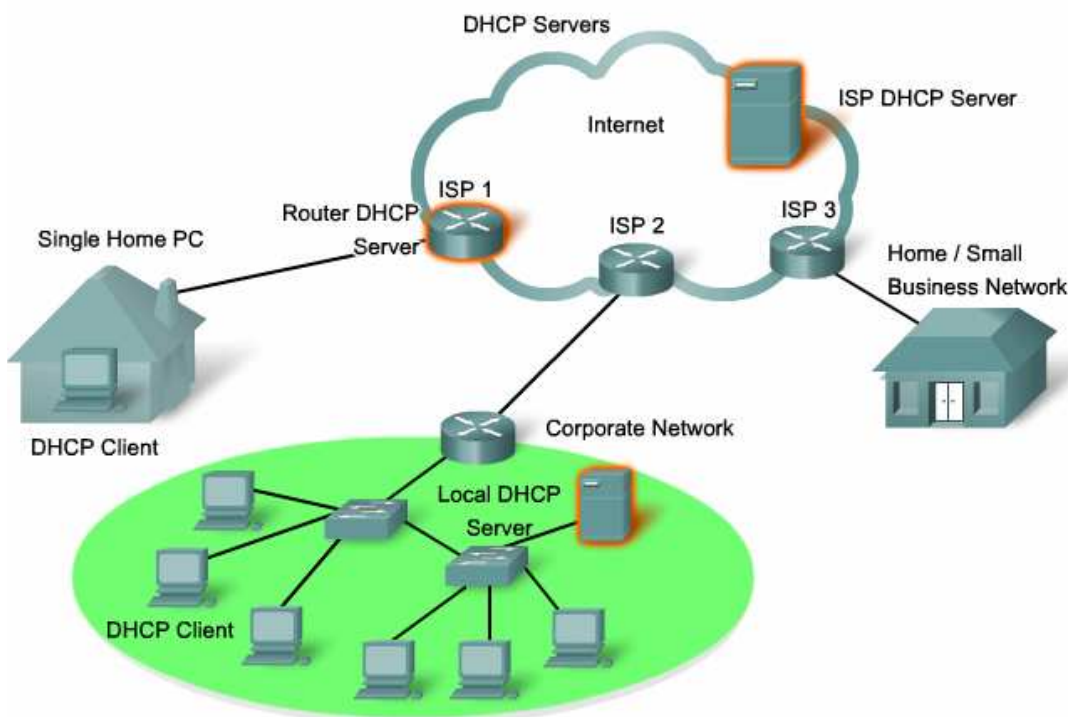
DHCP hace posible que usted pueda acceder a Internet haciendo uso de Puntos de Acceso inalámbricos en los aeropuertos o los cafés. Al entrar en el área, el cliente DHCP de su portátil entra en contacto con el servidor DHCP local a través de una conexión inalámbrica, y de esa manera el servidor DHCP asigna una dirección IP a su computadora portátil.

Distintos tipos de dispositivos pueden brindar el servicio de servidor DHCP, pues este es solamente un software que debe ser ejecutado. El servidor DHCP en la mayoría de redes medianas y grandes es por lo general un PC dedicado a ese fin.

En redes domésticas el servidor DHCP normalmente se encuentra en el proveedor de acceso a Internet y un host en la red de nuestra casa recibe su configuración IP directamente desde el proveedor de acceso a Internet.

DHCP puede suponer un riesgo de seguridad pues cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace que la seguridad física sea un factor importante al determinar si se usará una asignación dinámica o manual de las direcciones IP.

El direccionamiento dinámico y estático tiene su lugar en los diseños de red. Muchas redes usan ambos. En líneas generales DHCP se utiliza para asignar las direcciones a los hosts finales, y las direcciones estáticas se utilizan para asignarlas a dispositivos de red, tales como “gateways”, conmutadores, servidores e impresoras.

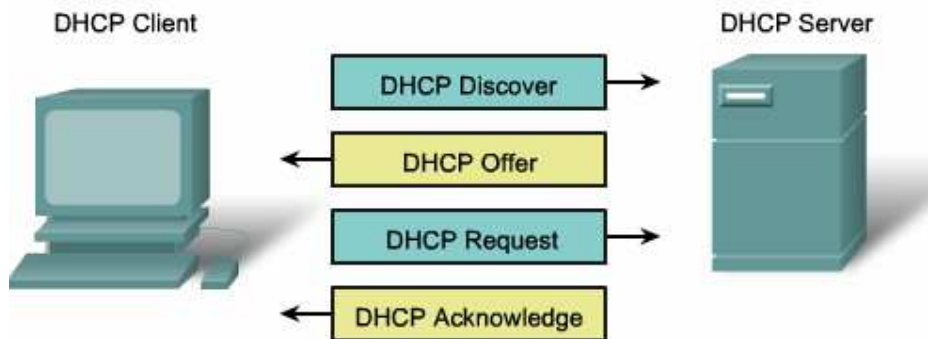


Sin DHCP, los usuarios tienen que ingresar manualmente la dirección IP, máscara de subred y otros parámetros de red para unirse a la red. El servidor DHCP mantiene un conjunto de direcciones IP y una dirección de arrendamiento a cualquier cliente DHCP habilitado cuando el cliente esté encendido. Dado que las direcciones IP son dinámicas (arrendado) no estático (permanente), las direcciones que ya no están siendo usadas se regresan automáticamente al pool de direcciones para su posterior reasignación. Cuando un dispositivo configurado con DHCP arranca o se conecta a la red, el cliente difunde un mensaje DHCP DISCOVER para tratar de ubicar a cualquier servidor DHCP que se encuentre en la red. El servidor DHCP responde con un DHCP OFFER, que es un mensaje que ofrece una dirección IP, la máscara de subred, servidor DNS, y la puerta de enlace por defecto, así como la duración de la entrega de las direcciones.

El cliente puede recibir múltiples paquetes DHCP OFFER si hay más de un servidor DHCP en la red local, por lo que debe elegir uno entre ellos, y transmitir un paquete DHCP REQUEST que identifica al servidor con el que va a trabajar.

Suponiendo que la dirección IP solicitada por el cliente, o la que ofrece el servidor, sigue siendo válida, el servidor DHCP le enviará un mensaje de ACK que reconoce la asignación de la dirección IP al cliente. Si la oferta ya no es válida - tal vez debido a un time-out o a la asignación de la IP a otro cliente entonces el servidor seleccionado va a responder con un mensaje DHCP NACK (Agradecimiento negado). Si el servidor envía un mensaje DHCP NACK, entonces el proceso de selección debe comenzar de nuevo con un nuevo mensaje DHCP DISCOVER.

Una vez que el cliente tiene el préstamo, este debe ser renovado antes que expire el contrato de arrendamiento a través de otro mensaje de solicitud DHCP. El servidor DHCP se asegura de que todas las direcciones IP sean únicas (una dirección IP no puede ser asignada a dos diferentes dispositivos de red al mismo tiempo). Usar DHCP permite a los administradores de red reconfigurar fácilmente las direcciones IP del cliente sin tener que hacer cambios manualmente a los mismos. La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a sus clientes que no requieren direcciones estáticas.

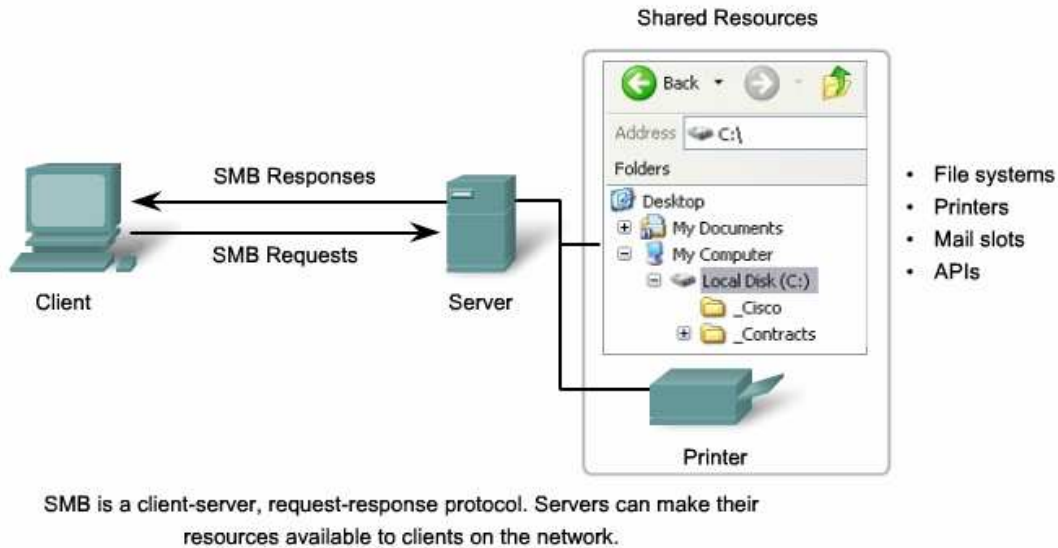


4.5 Servicios para compartir archivos y protocolo SMB

El Bloque de mensajes de servidor (SMB) es un protocolo cliente/servidor para el uso compartido de archivos. IBM desarrolló el protocolo Bloque de mensajes de servidor (SMB) a finales de 1980 para describir la estructura de los recursos compartidos de red, tales como directorios, archivos, impresoras y puertos serie. Se trata de un protocolo de petición-respuesta. A diferencia de los protocolos de uso compartido de archivos del tipo FTP, los clientes establecen una relación a largo plazo con los servidores. Una vez establecida la conexión, el cliente puede acceder a los recursos en el servidor como si el recurso fuera local.

El protocolo SMB para compartir archivos y servicios de impresión se han convertido en el pilar de la creación de redes Microsoft. Con la introducción de la serie de sistemas operativos Windows 2000, Microsoft cambió la estructura subyacente para el uso de SMB. En las versiones anteriores de los productos de Microsoft, los servicios SMB utilizaban un esquema non-TCP/IP para aplicar la resolución de nombres. A partir de Windows 2000, todos los productos de Microsoft utilizan nombres DNS. Esto permite que los protocolos TCP/IP apoyen directamente al protocolo SMB en la distribución de los recursos, tal como se muestra en la figura. LINUX y los sistemas operativos UNIX también proporcionan un método para compartir recursos con redes Microsoft utilizando una versión de SMB llamada SAMBA. Los sistemas operativos Macintosh de Apple también usan la distribución de los recursos utilizando el protocolo SMB.

File Sharing Using the SMB Protocol

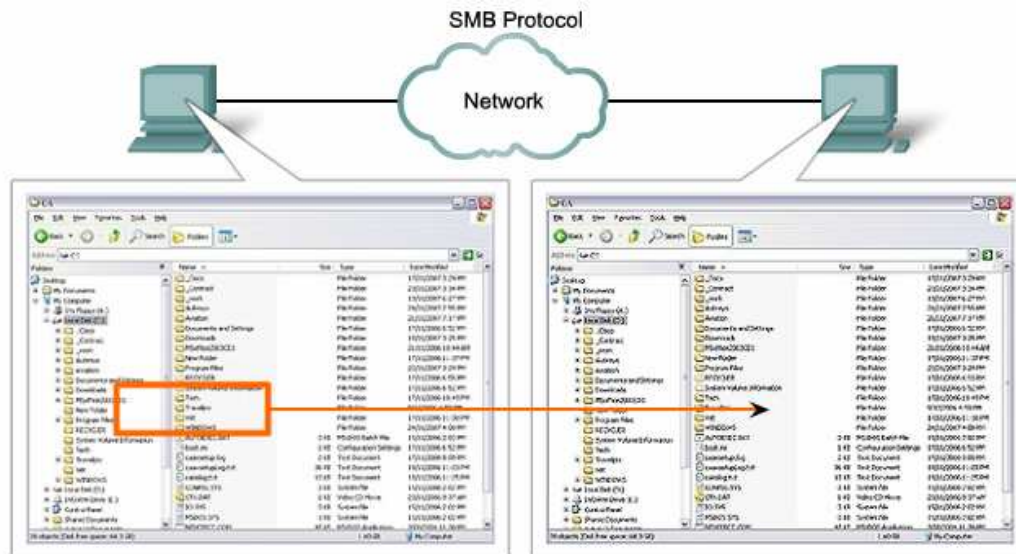


El protocolo SMB se describe la manera de acceder al sistema de archivos y cómo los clientes pueden hacer las peticiones a los archivos. También se describe el proceso interno de comunicación de SMB. Todos los mensajes SMB comparten un formato común. Este formato utiliza un encabezado de tamaño fijo seguido de una serie de parámetros de tamaño variable seguido de datos.

Los mensajes SMB pueden ser:

- Inicio, autenticar, y terminar los períodos de sesiones.
- Control de acceso a archivos e impresoras.
- Permitir a una aplicación enviar y recibir mensajes hacia o desde otro dispositivo.

El proceso de intercambio de archivos SMB se muestra en la figura.



A file may be copied from PC to PC with Windows Explorer using the SMB protocol.

4.6 Servicios Peer-to-Peer y el Protocolo Gnutella

Se ha visto que los protocolos FTP y SMB sirven para obtener archivos, ahora veremos otro protocolo de aplicación.

Compartir archivos a través de Internet se ha convertido en algo muy popular. Con aplicaciones P2P basados en el protocolo Gnutella, la gente puede compartir archivos guardados en el disco duro local y hacerlas disponibles para otros.

El software cliente Gnutella permite a los usuarios conectarse a la red de servicios Gnutella través de Internet, para localizar y acceder a los recursos compartidos por otros hosts que están ejecutando también el software Gnutella.

Muchas aplicaciones cliente están disponibles para acceder a la red Gnutella, incluyendo: BearShare, Gnucleus, LimeWire, Morpheus, WinMx y XoloX. Si bien el Foro de Desarrolladores Gnutella mantiene el protocolo base, los vendedores de aplicaciones suelen desarrollar extensiones para que el protocolo funcione mejor en sus aplicaciones.

Muchas aplicaciones P2P no utilizan una base de datos central para registrar todos los archivos disponibles en los hosts. En lugar de ello, cada dispositivo de red le comunica al otro qué archivos están disponibles en este momento y hace uso del protocolo Gnutella y sus servicios para que lo ayude en la localización de los recursos.

Cuando un usuario está conectado a un servicio de Gnutella, la aplicación cliente busca otros nodos Gnutella para conectarse. Estos nodos manejan las consultas y ubican las respuestas a las solicitudes. Ellos también gobiernan el control de los mensajes, que ayudan a descubrir este servicio en los demás nodos. El real proceso de transferencia de archivos por lo general depende del protocolo HTTP.

El protocolo Gnutella define cinco tipos de paquetes:

- Ping - para dispositivos
- Pong - como una respuesta a un ping
- Consulta - ubicación de archivos
- Consulta hit - como una respuesta a una pregunta
- Push - como la solicitud de descarga

4.7 Servicios Telnet

Mucho antes de que existieran las computadoras de escritorio con sofisticadas interfaces gráficas, la gente utilizaba los sistemas operativos basados en texto, que a menudo solo consistían en terminales de pantalla físicamente conectados a una computadora central. Una vez que aparecieron las redes, la gente necesitó una forma de acceder remotamente a los sistemas informáticos tal como si estuviera directamente conectada a ella.

El protocolo Telnet fue desarrollado para satisfacer esa necesidad. Telnet se remonta a principios de la década de 1970 y es uno de los protocolos más antiguos de la capa de aplicación de la suite TCP / IP. Telnet proporciona un método estándar de emulación de terminal basado en texto en los dispositivos de red de datos. Tanto el propio protocolo y el software cliente que implementa el protocolo se conocen comúnmente como Telnet.

Una conexión remota que usa Telnet se llama Terminal virtual (VTY). En vez de utilizar un dispositivo físico para conectarse con el servidor, Telnet utiliza el software para crear un dispositivo virtual que otorgue las mismas características de una sesión de terminal con el acceso a la interfaz de línea de comandos (CLI).

Para apoyar las conexiones de los clientes Telnet, el servidor ejecuta un servicio llamado el demonio Telnet. Una conexión del terminal virtual se establece desde un dispositivo que está ejecutando una aplicación cliente Telnet. La mayoría de los sistemas operativos incluyen un cliente Telnet. En una PC con Microsoft Windows, Telnet puede ejecutarse desde la línea de comandos. Otras aplicaciones que también usan clientes Telnet son HyperTerminal, Minicom, y TeraTerm.

Una vez que una conexión Telnet se establece, los usuarios autorizados pueden realizar cualquier función en el servidor remoto, como si estuvieran utilizando una línea de comandos servidor. Si se encuentra autorizado, pueden iniciar y detener los procesos, configurar el dispositivo, e incluso apagar el sistema. Telnet es un protocolo cliente/servidor que especifica la manera en que una sesión VTY se establece y es terminada. También proporciona la sintaxis y el orden de los comandos usados para iniciar el período de sesiones Telnet, así como para controlar los comandos que pueden emitirse durante un período de sesiones. Cada comando Telnet consiste de al menos dos bytes. El primer byte es un carácter especial llamado el "Interpretar como Comando" (CAI). Como su nombre lo indica, el CAI se define el siguiente byte como un comando en lugar de texto.

Algunos comandos de protocolo Telnet muestra son:

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

Borrar línea (EL) - Borra todo el texto de la línea actual.

Interrupción de Proceso (IP) - Suspende, interrumpe, aborta, o termine el proceso con el que el Terminal virtual está conectado. Por ejemplo, si un usuario inició un programa en el servidor Telnet a través de una sesión VTY, el mismo usuario puede enviar un comando IP para detener el programa.

Mientras que el protocolo Telnet soporta la autenticación de los usuarios, no permite transportar datos cifrados. Todos los datos intercambiados durante una sesión Telnet se transporta como texto plano a través de la red. Esto significa que los datos pueden ser interceptados y leídos.

Si la seguridad es una preocupación, el protocolo Secure Shell (SSH) ofrece un método alternativo y seguro para el acceso al servidor. SSH proporciona una infraestructura de mayor seguridad a los accesos remotos y a otros servicios de red. También proporciona autenticación más fuerte que Telnet y apoya el transporte de datos mediante el cifrado durante la sesión de trabajo. Como mejor práctica, la red siempre debería usar SSH en lugar de telnet, cuando sea posible. Más adelante en este curso, se utilizará Telnet y SSH para acceder y configurar los dispositivos en el laboratorio.

Autoevaluación

1. ¿Qué protocolo permite realizar el monitoreo remoto de los servidores?
2. Identifique 4 mensajes utilizados por el protocolo DHCP, describa sus funciones.
3. ¿Identifique las aplicaciones comerciales que permiten implementar el protocolo Telnet?
4. Identifique dos comandos usados por el protocolo Telnet.

Para recordar

- DHCP permite a un host obtener una dirección IP dinámica cuando este se conecte a la red. El servidor DHCP será contactado y se le solicitará una dirección. El servidor DHCP elige una de manera aleatoria una dirección desde un rango de direcciones y las asigna ("renta") al hosts por un período determinado.
- El Agente de Transferencia de Correo (MTA) se utiliza para el proceso de enviar los e-mails. Como se muestra en la figura, el MTA recibe mensajes de los MUA o de otro MTA en otro servidor de correo electrónico. El protocolo Simple Mail Transfer Protocol (SMTP), por otra parte, regula la transferencia del correo saliente del cliente hacia el servidor de e-mail. (MDA), así como el transporte del e-mail entre los servidores de e-mail (MTA).
- La estructura de los mensajes del protocolo SMTP utiliza un formato rígido de comandos y respuestas. Estos comandos apoyan a los procedimientos utilizados en SMTP, tales como la sesión de apertura, las transacciones de correo, reenvío de correo, verificación de nombres de buzón, la ampliación de las listas de correo, y la apertura y cierre de los intercambios de e-mail.



Capa de Transporte

TEMA

- Aplicaciones TCP/IP
- Servicios Peer-to-Peer

OBJETIVOS ESPECÍFICOS

- Explicar la utilidad de la capa de transporte.
- Identificar el rol de la capa de transporte y como ésta brinda la transferencia de data en el punto final de las aplicaciones.
- Describe el rol de los dos protocolos TCP/IP que usa la capa de transporte: TCP y UDP.
- Explicar las funciones principales de la capa transporte, seguridad, direccionamiento del puerto, y segmentación.
- Explicar cómo el TCP y UDP usan las principales funciones.

CONTENIDOS

- Servicios de correo y Protocolos SMTP/POP
- FTP
- DHCP
- Servicios para compartir archivos y protocolo SMB
- Servicios Peer-to-Peer y el Protocolo Gnutella
- Servicios Telnet

5.1.1 Propósito de la Capa de Transporte

La capa de transporte realiza la segmentación de la data y controla el reensamblado de estos fragmentos dentro de varios canales de comunicación. Sus responsabilidades primarias para lograr esto son:

- Rastrear la comunicación individual entre las aplicaciones en la computadora origen y destino.
- Segmentar la data y administrar cada fragmento.
- Reensamblar los segmentos dentro de los canales de cada aplicación.
- Identificar las diferentes aplicaciones

Rastrear conversaciones individuales

Cualquier computadora quizás tenga múltiples aplicaciones que están comunicándose a través de la red. Cada una de estas aplicaciones estará comunicándose con una o más aplicaciones en la computadora remota. La responsabilidad de la capa de transporte es mantener múltiples canales de comunicación entre estas aplicaciones.

Segmentación de la data

Como cada aplicación crea un canal de datos para ser enviado a la aplicación remota, esta data tiene que estar preparada para ser enviado a través del medio en fragmentos manejables. Los protocolos de la capa transporte brindan el servicio para segmentar esta data desde la capa de aplicación. Esto incluye el encapsulamiento requerido por cada fragmento de información. Cada fragmento de data de la aplicación requiere las cabeceras respectivas para ser incluido a la capa transporte y así indicar a que flujo de comunicación está siendo asociado.

Reensamblar los segmentos

La computadora que recibe, cada fragmento de data quizás este dirigido a la aplicación apropiada.

Adicionalmente, estos pedazos individuales de data tienen que ser reconstruidos completamente dentro del canal de data que es usado por la capa de aplicación. Los protocolos de la capa transporte describen como la información de la cabecera en la capa de transporte es usada para reensamblar estos fragmentos de data dentro del canal para ser pasado a la capa de aplicación.

Identifica las aplicaciones

Para poder pasar la data a la aplicación correcta, la capa de transporte tiene que identificar a la aplicación destino. Para lograr esto la capa de transporte asigna un identificador a cada aplicación. Los protocolos TCP/IP llaman a este identificador un número de puerto. Cada aplicación que necesite acceder a la red tiene asignado un único número de puerto en esta computadora. Este número de puerto es usado por la cabecera en la capa transporte para indicar que aplicación está asociada con los fragmentos de data.

La capa transporte es el enlace entre la capa aplicación y la capa más baja que es responsable de la transmisión en la red. Esta capa acepta la data desde conversaciones diferentes y lo envía a las capas más bajas como fragmentos administrables que pueden ser multiplexados eventualmente sobre el medio de comunicación.

Las aplicaciones no necesitan saber los detalles operacionales de la red que es usada. Las aplicaciones generan la data que es enviada desde una aplicación a otra, sin importarle el tipo de computadora destino, el tipo de medio por donde la data tiene que viajar, la ruta tomada por la data, la congestión en un enlace, o el tamaño de la red.

Adicionalmente, las capas más bajas no están conscientes si hay aplicaciones múltiples enviando data en la red. Su responsabilidad es enviar la data al dispositivo

correcto. La capa de transporte luego clasifica estos fragmentos antes de enviarlos a la aplicación correcta.

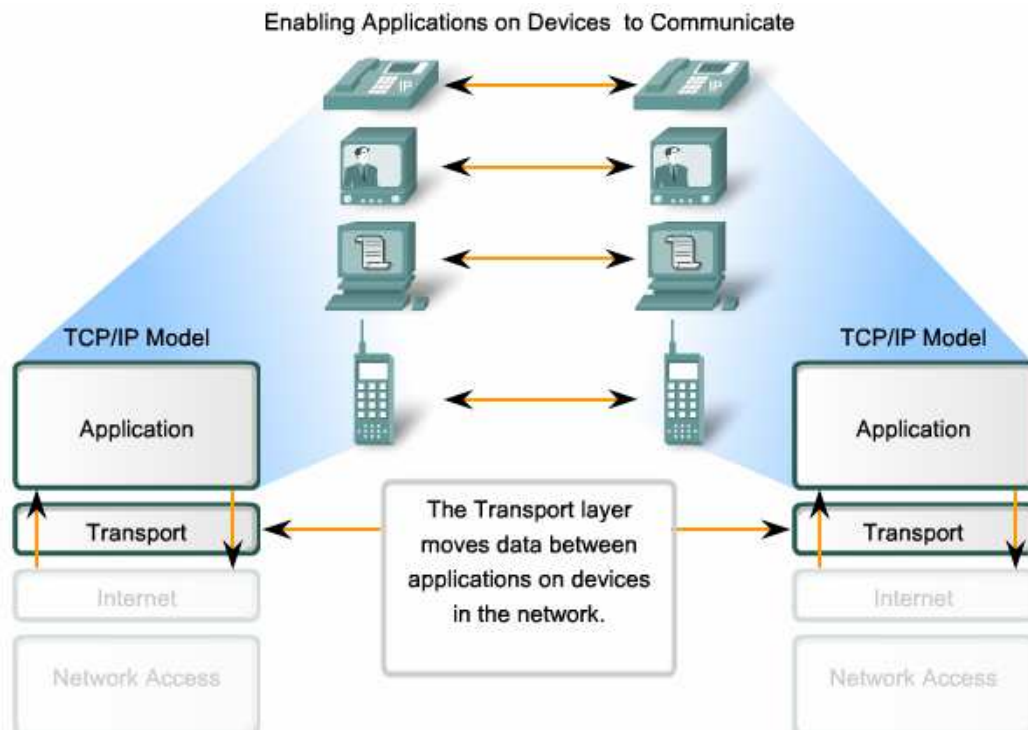
Modificación de los requerimientos de la Data

Debido a que diferentes aplicaciones tienen diferentes requerimientos, hay múltiples protocolos en la capa transporte. Para algunas aplicaciones, los fragmentos tienen que llegar en una secuencia específica para poder ser procesados de manera exitosa. En algunos casos, toda la data tiene que ser recibida por cualquiera para ser usado. En otros casos, la aplicación puede tolerar algunas pérdidas de data durante la transmisión sobre la red.

En la actualidad la convergencia de redes, obliga que diferentes aplicaciones con distintas necesidades de transporte estén comunicándose en la misma red. Los diferentes protocolos en la capa transporte tienen diferentes reglas permitiendo a los dispositivos intercambiar esta diversidad de data.

Algunos protocolos sólo brindan funciones básicas para la entrega eficiente de los fragmentos de data entre las aplicaciones apropiadas. Estos tipos de protocolos son muy usados para las aplicaciones cuya data es sensible a retrasos.

Otros protocolos de la capa transporte realizan procesos que brindan características adicionales, como brindar la entrega segura entre las aplicaciones. Mientras estas funciones adicionales brindan mayor robustez a la comunicación de la capa transporte entre las aplicaciones, también tienden a generar una mayor cantidad de demandas en la red.



Separar las comunicaciones múltiples

Imaginemos una computadora conectada a la red que está recibiendo y enviando simultáneamente e-mails y mensajes instantáneos, viendo sitios web, y contestando una llamada de voz IP. Cada una de estas aplicaciones está enviando y recibiendo data sobre la red al mismo tiempo, sin embargo, la data de la llamada telefónica no está dirigida al navegador web, y el texto del mensaje instantáneo no aparece en el e-mail.

Adicionalmente, los usuarios requieren que el e-mail o la página web sean recibidos completamente y presentados para que la información sea considerada útil. Los pequeños retardos son considerados aceptables para permitir que la información esté recibida y presentada completamente.

Ocasionalmente perder pequeñas partes de una conversación telefónica se puede considerado aceptable. Uno puede inferir la pérdida de audio del contexto de una conversación o preguntarle a la otra persona que repita lo que dijo. Esto es considerado preferible a los retardos que podrían resultar desde las redes que preguntan para administrar y reenviar los segmentos perdidos. En este ejemplo, el usuario –no la red- administra el reenvío o reemplazo de la información perdida.

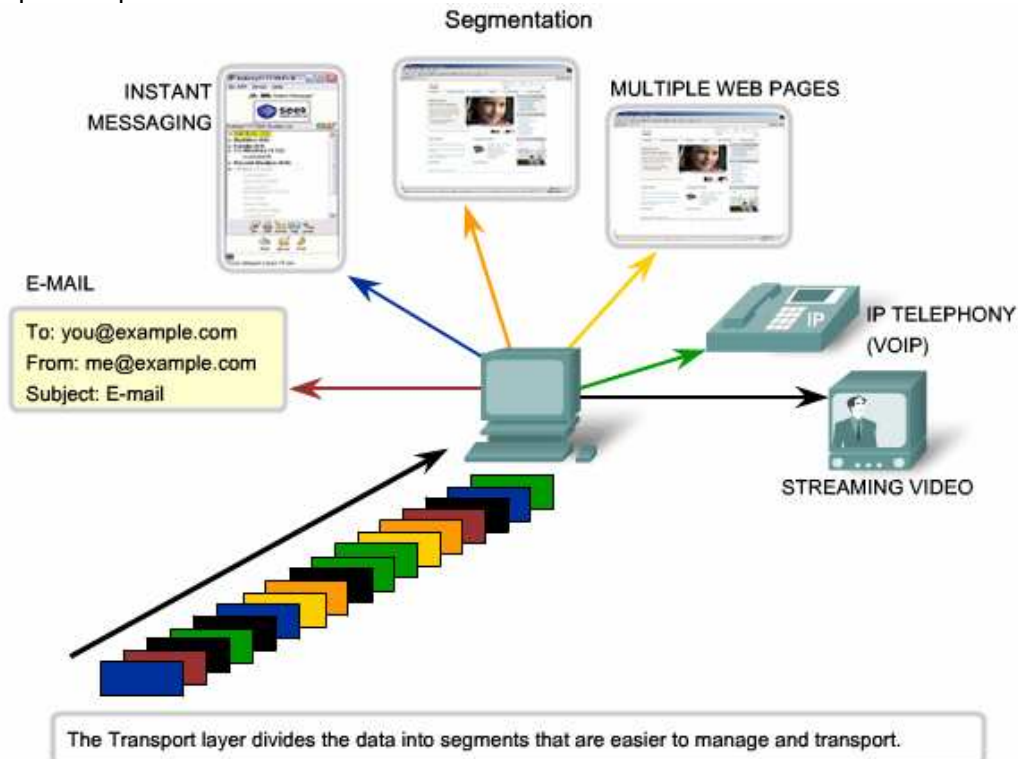
Como se explicó en los capítulos previos, enviar algún tipo de data un vídeo por ejemplo- a través de una red por un canal de comunicación podría prevenir que otras comunicaciones estén ocurriendo al mismo tiempo. También realiza la recuperación de error y la retransmisión de la data dañada.

Al dividir la data en pequeñas partes, y enviar esta partes desde el origen hacia el destino, permite que muchas comunicaciones diferentes puedan ser dadas (múltiplexado) en la misma red.

La segmentación de la data, de acuerdo con los protocolos de la capa transporte, brinda los medios para el envío y la recepción de la data cuando se ejecutan múltiples aplicaciones en una computadora. Sin segmentación, sólo una aplicación, podría recibir la data. Por ejemplo si se esta viendo un vídeo, no se podría recibir e-mails, chatear usando mensajes instantáneos, o ver páginas web mientras este viendo el vídeo.

En la capa de transporte, cada fragmento que fluye entre la aplicación origen y el destino origina una conversación.

Para identificar cada segmento de data, la capa transporte agrega a los fragmentos una cabecera que contienen data binaria. Esta cabecera contiene campos con una serie de bits. Este valor en esos campos permiten diferenciar que protocolos de la capa transporte van a realizar las diferentes funciones.



5.1.2 Controlando las conversaciones

La función primaria especificada por todos los protocolos de la capa transporte incluye:

Segmentación y reensamblado - La mayoría de redes tiene una limitación en la cantidad de data que pueden ser incluida en un solo paquete UDP. La capa de transporte divide la data de la aplicación dentro de bloques de data que son de un tamaño apropiado. En el destino, la capa transporte reensamblan la data antes que sea enviada a la aplicación destino o servicio.

Multiplexado de la conversación—Pueden haber muchas aplicaciones o servicios ejecutándose en cada computadora de la red. Cada una de estas aplicaciones o servicios está asignada a una dirección conocida como puerto. Es así como la capa de transporte puede determinar con que aplicación o servicio la data esta relacionada.

Adicionalmente para usar la información contenida en las cabeceras, para las funciones básicas de segmentación y reensamblado de data, algunos protocolos de la capa transporte brindan:

- Conversaciones orientadas a la conexión
- Entrega segura
- Ordenar la reconstrucción de data
- Control de flujo

Conversaciones orientadas a la conexión

La capa de transporte puede brindar una conexión orientada, al crear una sesión entre las aplicaciones. Estas conexiones preparan las aplicaciones para la comunicación con otras antes que cualquier información sea transmitida. Dentro de estas sesiones, la data para una comunicación entre las dos aplicaciones puede ser administrada de manera más cercana.

Entrega segura

Por muchas razones, es posible que un fragmento de data pueda estar corrupto, o dañado completamente, como estos fragmentos son transmitidos sobre la red. La capa de transporte puede entregar todos los fragmentos a su destino gracias al dispositivo origen que puede retransmitir cualquier data que se pierda.

Ordenar la entrega de la data

Debido a que las redes brindan múltiples rutas se pueden transmitir en diferentes momentos, y por lo tanto la data puede llegar en el orden incorrecto. Por medio de la numeración y secuencia de los segmentos, la capa de transporte puede brindar los segmentos en el orden apropiado.

Control de flujo

Las computadoras de las redes están limitadas por sus recursos, como la memoria o el ancho de banda. Cuando la capa transporte se percata que estos recursos se están saturando, algunos protocolos pueden solicitar que el flujo de datos se reduzca. Esto es hecho en la capa transporte regulando la cantidad de data que transmite la computadora al origen. El control de flujo puede prevenir la pérdida de segmentos en la red y evita la necesidad de retransmisión.

Como otros protocolos que serán discutidos en este capítulo, estos servicios serán explicados en mayor detalle.

5.1.3 Apoyando las comunicaciones confiables

Recuerde que la función primaria en la capa de transporte es administrar la data de la aplicación para lograr el diálogo entre las computadoras. Sin embargo, diferentes aplicaciones tienen requerimientos distintos para su data, y por consiguiente los diferentes protocolos de la capa transporte se han diseñado para satisfacer estos requerimientos.

Un protocolo de la capa de transporte puede implementar un método que brinda la seguridad en la entrega de la data. En términos de seguridad esto significa entregar cada fragmento de data que la computadora origen esté enviando al destino. En la capa de transporte las tres operaciones básicas para brindar la seguridad son:

- Seguimiento de la transmisión de data
- Reconocimiento de la data recibida
- Retransmisión de cualquier data que no esté reconocida

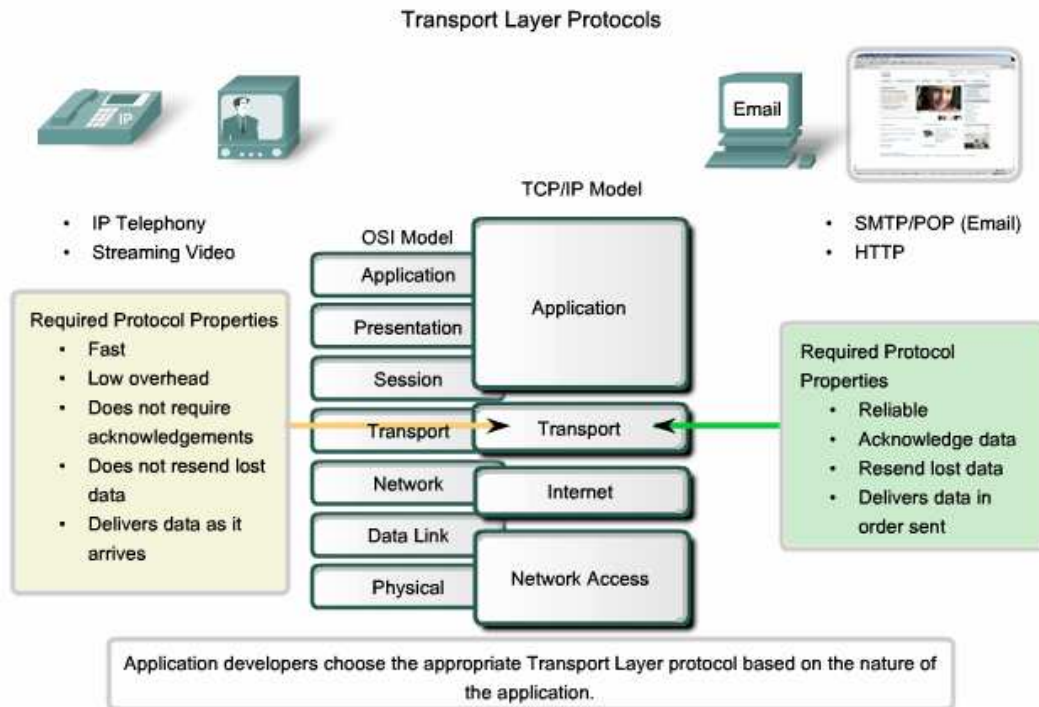
Esto requiere que los procesos de la capa de transporte y del origen y mantengan el rastreo de todos los fragmentos de data de cada conversación y la retransmisión de cualquier tipo de data que no haya sido reconocida por el destino. La capa de transporte tiene que rastrear la data que es recibida y reconocer la recepción de la data. Este proceso de seguridad sobrecarga los recursos de la red debido al reconocimiento, rastreo y retransmisión. Para soportar estas operaciones de seguridad, más datos de control son intercambiados entre las computadoras origen y destino. Este control de información está ubicado en la cabecera de la capa 4.

Esto crea un intercambio entre el valor de fiabilidad y la carga que se coloca en la red. Los diseñadores de aplicaciones tienen que escoger el tipo de protocolo de la capa de transporte adecuado para cumplir los requerimientos de sus aplicaciones. En la capa transporte, hay varios protocolos que especifican métodos para brindar seguridad, garantizar la entrega o hacer la entrega más rápida. En el contexto de red, hacer la entrega más rápida conlleva cierta inseguridad, porque no hay reconocimiento si la data es recibida en el destino.

Determinar las necesidades para la seguridad

Las aplicaciones, como la base de datos, páginas web, y e-mail, requieren que toda la data llegue a su destino, para lograr que la información sea útil. Cualquier pérdida de data puede causar una comunicación corrupta que estará incompleta o ilegible. Sin embargo, estas aplicaciones están diseñadas para usar los protocolos de la capa de transporte que brinden la seguridad. Adicionalmente la sobrecarga de la red es considerada como un requerimiento para estas aplicaciones.

Otras aplicaciones son más tolerantes a la pérdida de pequeñas cantidades de data. Por ejemplo, si uno o dos segmentos de un canal de video fallan, esto sólo generaría una interferencia momentánea en el canal. Esto quizás sería representado como una distorsión en la imagen y por lo tanto no sería una pérdida notable para el usuario.



5.1.4 UDP y TCP

Los dos protocolos más comunes de la capa transporte son el protocolo de control transmisión (TCP) y el protocolo de datagrama de usuario (UDP). Ambos protocolos administran la comunicación de múltiples aplicaciones.

Protocolo de datagrama de usuario (UDP)

UDP es un protocolo simple orientado a la desconexión, descrito en RFC 768. Este protocolo tiene la ventaja de brindar poca sobrecarga al envío de datos. Los fragmentos de comunicación en UDP son llamados datagramas. Estos datagramas son enviados con “el mínimo esfuerzo” por la capa de transporte.

Las aplicaciones que usan UDP incluyen:

Domain Name System (DNS)

Video Streaming

Voz sobre IP (VoIP)

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión, descrito en el RFC 793. TCP realiza una sobrecarga de tráfico para realizar funciones adicionales. Las funciones adicionales especificadas por TCP son: entregar la data de manera ordenada, segura, y realiza el control de flujo. Cada segmento TCP tiene 20 bytes de sobrecarga en el encapsulamiento de la cabecera de la capa de aplicación, frente a los 8 bytes de sobrecarga de UDP.

Las aplicaciones que usan TCP son:

- Navegador Web
- e-mail
- FTP

5.1.5 Direccionamiento de Puertos

Identificar la conversación

Considere el ejemplo anterior de las computadoras que simultáneamente reciben y envían e-mail, mensajes instantáneos, páginas web, y una llamada de VoIP.

Los protocolos TCP y UDP realizan sus servicios efectuando el seguimiento de las aplicaciones que se están comunicando. Para diferenciar los segmentos y datagramas de cada aplicación, ambos TCP y UDP, tienen campos que pueden identificar a estas aplicaciones. Estos identificadores únicos son los números de Puerto.

En la cabecera de cada segmento o datagrama, hay un puerto origen y destino. El número de puerto origen es el número asociado con la aplicación origen en la computadora local. El número de puerto destino es el número asociado con la aplicación destino en la computadora remota.

Los números de puerto son asignados de varias maneras, dependiendo de si el mensaje es una petición o una respuesta. Mientras los procesos del servidor tienen números de puertos estáticos asignados a ellos, los clientes seleccionan de manera dinámica el número de puerto para cada conversación.

Cuando una aplicación cliente envía una petición a la aplicación de un servidor, el puerto destino contiene en la cabecera el número de Puerto asignado para este servicio que se está ejecutando en la computadora remota. El software cliente tiene que saber que número de puerto está asociado con el proceso del servidor en la computadora remota. Este número de puerto destino está configurado, por defecto o manualmente. Por ejemplo, cuando un navegador web realiza una petición hacia el servidor web, el navegador usa TCP y el número de puerto 80 a menos que se especifique otro. Esto es porque el puerto 80 TCP es el puerto por defecto asignado a los servidores web.

El puerto origen en un segmento o en la cabecera del datagrama de una petición cliente es generado de manera aleatoria. Mientras no este en conflicto con otros puertos en uso por el sistema, el cliente puede escoger cualquier número de puerto. Este número de puerto actúa como una dirección de retorno para la petición de la aplicación. La capa transporte mantiene el rastreo de este puerto y la aplicación que inicializó la petición entonces cuando la respuesta es retornada, esta puede ser reenviada a la aplicación correcta. El número de puerto que solicita la aplicación es usado como el número de puerto destino en donde regresará la respuesta desde el servidor.

La combinación del número de puerto en la capa transporte y la dirección IP de la capa de red son asignados para identificar únicamente a la computadora. Esta combinación es llamada socket. Es muy posible que se utilicen estos términos de manera intercambiable. En el contexto de este curso, el término Socket está referido únicamente a la combinación de la dirección IP y el número de puerto.

Un socket par, consiste en la dirección y el número de puerto origen y destino, es también único e identifica la conversación entre dos computadoras.

Por ejemplo la petición HTTP de una página web está siendo enviada al servidor web (80) que ejecuta la computadora con la dirección IPv4 192.168.1.20 de la capa 3 debería ser destinado al socket 192.168.1.20:80.

Si el navegador web solicita la página web desde la computadora 192.168.100.48 y el número de puerto dinámico asignado al navegador web es 49152, el socket para la página web sería 192.168.100.48:49152.

La autoridad para asignar los números de Internet (IANA) asigna los números de puerto.

Existen diferentes tipos de números de puerto:

Los puertos bien conocidos (del número 0 a 1023)

Estos números están reservados para servicios y aplicaciones. Ellos son usados comúnmente por aplicaciones como HTTP (servidores web) POP3/SMTP (e-mail server) y Telnet. Por medio de la definición de estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones clientes pueden ser programadas para solicitar una conexión en estos puertos específicos y de esta manera ser asociadas al servicio.

Puertos registrados (del número 1024 a 49151)

Estos números de puerto son asignados a las aplicaciones o procesos del usuario. Estos procesos son aplicaciones individuales que un usuario ha escogido para instalar aplicaciones comunes que podrán recibir a estos puertos bien conocidos. Cuando no es usado por el recurso de un servidor, estos puertos quizás también sean usados dinámicamente por el cliente como el puerto origen.

Puertos privados o dinámicos (del número 49152 a 65535)

También conocido como puertos efímeros, estos usualmente se asignan dinámicamente por la aplicación cliente cuando inicializan una conexión. No es muy común para un cliente conectarse al servicio usando un puerto dinámico o privado.

Usar TCP y UDP

Algunas aplicaciones quizás usen ambos protocolo: TCP y UDP. Por ejemplo, la baja sobrecarga de UDP permite que los servidores DNS atiendan las peticiones de muchos clientes muy rápidamente. Algunas veces, sin embargo, el envío de la información solicitada requiera la seguridad de TCP. En este caso, el número de puerto 53 es usado por ambos protocolo con este servicio.

5.1.6 Segmentación y reensamblaje de paquetes

Algunas aplicaciones transmiten gran cantidad de data -en algunos casos, muchos gigabytes. No sería práctico enviar toda ésta data en un solo paquete grande. Un gran paquete de data podría tomar minutos u horas para ser enviada. Adicionalmente, si hubiese algún error, toda la información sería perdida o reenviada. Los dispositivos de red no tienen suficiente buffers de memoria para almacenar esta información mientras esté siendo recibida. Varios de los límites dependen de la tecnología de la red y las especificaciones del medio físico que está siendo usado para transmitir esta información.

Dividir la información de la aplicación dentro de fragmentos permite que la data sea transmitida dentro de los límites del medio y que la data de diferentes aplicaciones pueda ser multiplexada en el medio.

TCP y UDP intercambian diferentes segmentos

En TCP, cada cabecera de segmento contiene una secuencia numérica. Esta secuencia numérica permite a las funciones en la capa transporte de la computadora destino ensamblar los segmentos en el orden adecuado en el que fueron transmitidos.

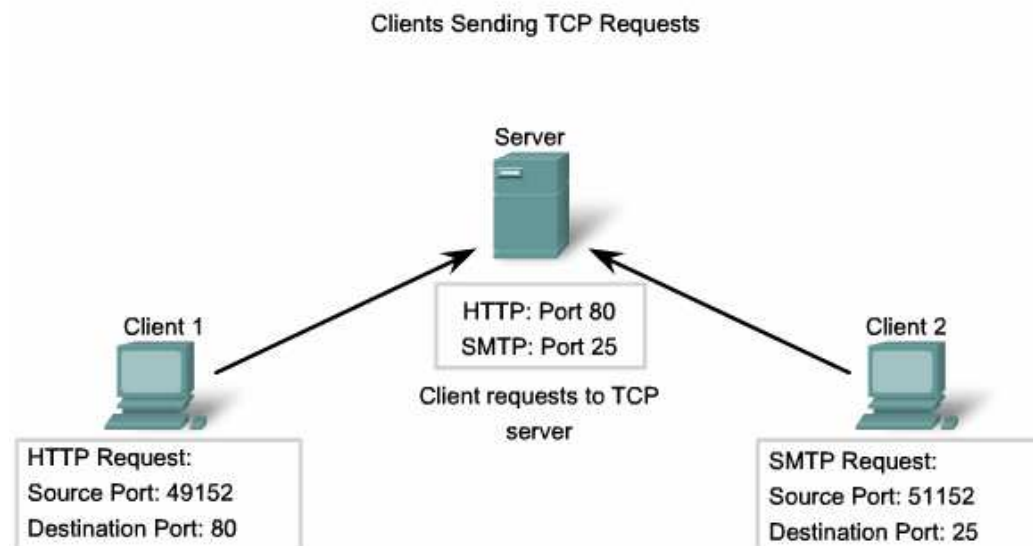
Aunque los servicios que usan UDP también rastrean las conversaciones entre las aplicaciones, ellos no se preocupan por el orden en que la información fue transmitida, o mantener la conexión. No hay secuencia numérica en la cabecera UDP. UDP es un simple diseño que genera poca sobrecarga a comparación de TCP, resultando esto en una transferencia de data mucho más rápida.

La información quizás llegue en un orden diferente del que fue transmitida por qué los diferentes paquetes quizás tomen rutas diferentes a través de la red. Una aplicación que use UDP debe tolerar el hecho que los datos pueden que no lleguen en el orden en que fueron enviados.

5.2.2. Procesos del servidor TCP

Cada proceso de una aplicación se ejecuta en el servidor y está configurado para usar un número de puerto por defecto, o manualmente asignado por un administrador. Un servidor individual no puede tener dos servicios asignados a un mismo número de puerto dentro de la misma capa de transporte. Si una computadora ejecuta la aplicación de un servidor web y una aplicación FTP no puede tener ambas ejecutándose y usando el mismo puerto (por ejemplo, TCP port 8080). Cuando está activa la aplicación de un servidor se le asigna un puerto específico, este puerto está considerado como “abierto” en el servidor. Esto significa que la capa de transporte acepta y procesa el direccionamiento de segmentos en este puerto. Cualquier petición entrante del cliente es direccionada al socket apropiado y la data enviada a la aplicación del servidor. Pueden haber muchos puertos abiertos simultáneamente en un servidor, cada aplicación activa un puerto en el servidor. Esto es común para un servidor que brinda más de un servicio, como un servidor web y un servidor FTP al mismo tiempo.

Una manera para brindar seguridad en un servidor es restringiendo el acceso únicamente a los puertos asociados con los servicios y las aplicaciones que deberían ser accesibles por peticiones autorizadas.



5.2.3 Conexión y término de sesiones TCP

Cuando dos computadoras se comunican usando TCP, se debe establecer una conexión antes de que la data pueda ser intercambiada. Antes que la comunicación este completada, las sesiones son cerradas y la conexión es terminada. Los mecanismos de conexión y sesión permite que se den las funciones de seguridad al TCP.

La computadora rastrea cada segmento de data dentro de una sesión e intercambia información acerca de que data se recibirá por cada computadora usando la información de la cabecera del TCP.

Cada conexión representa dos vías de comunicación, o sesiones. Para establecer la conexión, la computadora realiza el saludo de tres vías. Controla los bits en la cabecera TCP indicando el progreso y el status de la conexión. El saludo de tres vías, establece que el dispositivo destino este presente en la red

Verifica si el dispositivo destino tiene un servicio activo y si acepta peticiones en el número de puerto destino que el cliente intenta inicializar para establecer la sesión. Informa al dispositivo destino que el cliente origen intenta establecer una sesión de comunicación en ese número de puerto.

Los tres pasos para establecer una conexión TCP son:

1. El cliente que inicializa envía un segmento que contiene la secuencia del valor inicial (ISN), que sirve como petición al servidor para empezar una sesión de comunicación.
2. El servidor responden con un segmento que contiene un valor igual de reconocimiento a la secuencia recibida agregando 1, este incremento es propio del valor de sincronización secuencial. El valor es mayor al número secuencial porque el ACK es siempre el siguiente byte u octeto esperado. Este valor de reconocimiento permite al cliente relacionar el retorno de la respuesta al segmento original que este envió al servidor.
3. El cliente inicial responde con un valor igual de Acuse de recibo al valor secuencial recibido incrementando 1. Esto completa el proceso para establecer la conexión.

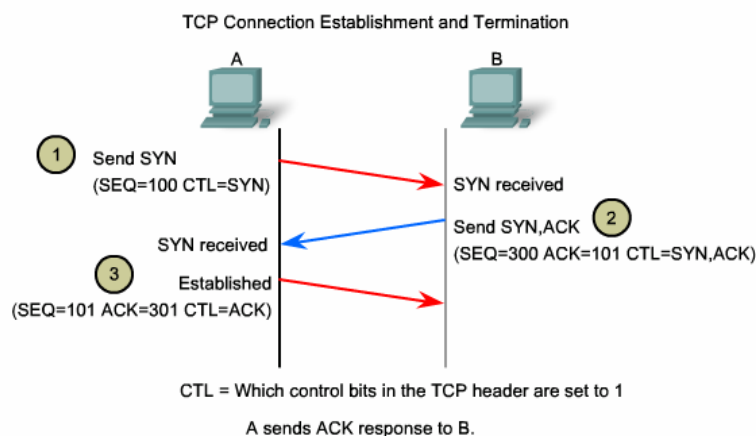
Para entender el proceso de saludo de tres vías, es importante ver lo que los host intercambian. Dentro de la cabecera del segmento TCP, existen seis campos de 1 bit que contienen el control de la información usada para administrar los procesos TCP.

Estos campos son:

- URG – Puntero de urgencia
- ACK – Acuse de recibo
- PSH – Función de Push
- RST – Reiniciar la conexión
- SYN – Sincronizar los numeros de secuencia (ISN)
- FIN - No mas data desde el equipo transmisor.

Estos campos están referidos como banderas (flags), porque el valor de estos campos es únicamente 1 bit, sin embargo, tienen dos valores: 1 o 0. Cuando el valor del bit esta en 1, indica el tipo de control de información que está contenido en el segmento.

Mediante un procedimiento de cuatro pasos, los indicadores son intercambiados para terminar la conexión TCP.



5.2.5 Termina de una conexión TCP

Para cerrar una conexión, se deberá habilitar la bandera de tipo FIN (final) en el segmento de la cabecera. Para finalizar cada sesión TCP de una vía, es usado un saludo de dos vías, consiste en el uso de un segmento FIN y ACK. Sin embargo, para terminar una conversación soportada por TCP, cuatro intercambios son necesarios para finalizar ambas sesiones.

1. Cuando el cliente no tiene más data para enviar por el canal, este envía un segmento con la bandera FIN habilitada.
2. El servidor envía un ACK para reconocer el recipiente del FIN ha terminado la sesión desde el cliente al servidor.
3. El servidor envía un FIN al cliente, para terminar la sesión del cliente.
4. El cliente responde como un ACK para reconocer el FIN desde el servidor.

Cuando el cliente no tiene más data para transferir, este habilita la bandera FIN en la cabecera de un segmento. Luego, el servidor termina la conexión con el envío de un segmento normal que contiene la data con la bandera ACK usando el número de reconocimiento, que confirma que toda la data ha sido recibida. Cuando todos los segmentos han sido reconocidos, la sesión es cerrada.

Las sesiones en las otras direcciones son cerradas usando el mismo proceso. El receptor indica que ya no hay más data para enviar habilitando la bandera FIN en la cabecera de un segmento enviada por el origen. El retorno de un acuse de recibo confirma que todos los bytes de data han sido recibidos y que la sesión está por cerrarse.

Es también posible terminar la conexión con el saludo de tres vías. Cuando el cliente no tiene más data para enviar, éste envía un FIN hacia el servidor. Si el servidor no tiene más data para enviar, éste puede responder con ambas banderas habilitadas en FIN y ACK, combinando estos dos pasos dentro de uno. El cliente responde con un ACK.

5.3 Administración de las sesiones TCP

5.3.1 Reensamblaje de los Segmentos TCP

Cuando los servicios envían data usando TCP, los segmentos quizás lleguen a su destino sin orden. Para que el mensaje original pueda ser entendido por el receptor, la data en estos segmentos es ensamblada dentro de la secuencia original. La secuencia numérica está signada en la cabecera de cada paquete para lograr este objetivo.

Durante el esquema de sesión, un número inicial de secuencia (ISN) es habilitada. Este número inicial de secuencia representa el valor inicial de los bytes para esta sesión que será transmitida y recepcionada en la aplicación. Como la data es transmitida durante la sesión, el número secuencial es incrementado por el número de bytes que van a ser transmitidos.

Este rastreo de data permite que cada segmento sea identificado de manera única y sea reconocido. Los segmentos perdidos pueden ser identificados.

La recepción del proceso TCP ubica la data desde un segmento dentro de un buffer receptor. Los segmentos son ubicados en el orden secuencial correcto y pasados a la capa de aplicación cuando éste es reensamblado. Cualquier de los segmentos que llegan con la secuencia numérica no continúa son mantenidos para ser procesados después. Entonces, cuando los segmentos que llegan con los bytes perdidos, estos segmentos son procesados.

Confirmar la recepción de los segmentos

Una de las funciones de TCP es estar seguro que cada segmento alcance el destino. El servicio TCP en la computadora destino reconoce la data que esta llegando de la aplicación origen.

La cabecera del segmento con el número secuencial y el número de reconocimiento son usados juntos para confirmar la recepción de todos los bytes de data contenidos en los segmentos. La secuencia numérica indica el número relativo de los bytes que han sido transmitidos en la sesión incluyendo los bytes del segmento TCP actual. TCP usa segmentos ACK que son regresados al equipo origen para indicar el siguiente byte en la sesión que el receptor espera recibir. Esto es llamado Acuse de recibo por expectativa.

Manejando la pérdida de segmentos

No importa que bien esté diseñada una red, la data perdida ocurrirá ocasionalmente. Sin embargo, TCP brindan métodos para administrar la pérdida de estos segmentos. Entre éstos está un mecanismo para retransmitir segmentos con datos no reconocidos.

Control de flujo

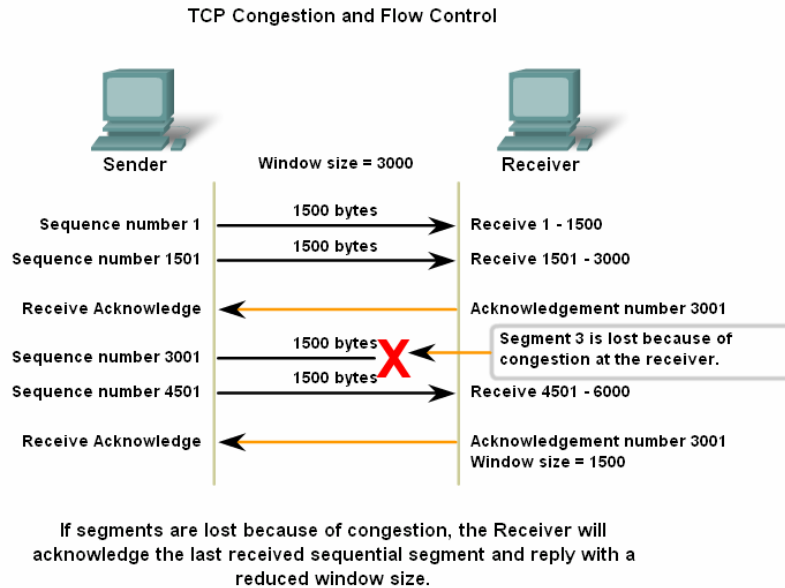
TCP también brindan mecanismos para controlar el flujo. El control de flujo ayuda a ganar confiabilidad en la transmisión de TCP ajustando la tasa de transmisión de los datos de manera efectiva entre los dos servicios en la sesión.

El campo del tamaño de ventana en la cabecera TCP especifica la cantidad de data que puede ser transmitida antes que un ACK sea recibido. El tamaño inicial de la ventana es determinado durante el inicio de la sesión del saludo de 3 vías.

Reducir el tamaño de ventana

Otra manera para controlar el flujo de data es modificar dinámicamente el tamaño de la ventana. Cuando un recurso de la red está sobrecargado, TCP puede reducir el tamaño de ventana que requiera los segmentos recibidos por un reconocimiento más frecuente. Esto retarda eficazmente la tasa de transmisión porque la fuente espera para que los datos sean reconocidos más frecuentemente.

El incremento y la disminución dinámica del tamaño de ventana es un proceso continuo en TCP, que determina el óptimo tamaño de ventana por cada sesión TCP. En redes altamente eficientes, el tamaño de ventana quizás sea muy grande porque la data no está siendo perdida. En redes donde la infraestructura subyacente está muy sobrecargada, el tamaño de ventana será pequeño.



5.4 Protocolo UDP

5.4.1 UDP: Baja carga vs Confiabilidad

UDP es un protocolo simple y brinda las funciones básicas de la capa transporte. Es mucho más bajo a la sobrecarga de TCP, porque este es un protocolo no orientado a la conexión y que no brindan los mecanismos sofisticados de retransmisión, secuencia ni control de flujo.

Esto no significa que las aplicaciones que usen UDP sean siempre inseguras. Esto simplemente significa que estas funciones no son provistas por la capa transporte y tienen que ser implementadas por la mismas aplicaciones si son requeridas.

Aunque la cantidad de tráfico UDP encontrada en una red es algunas veces relativamente bajo, los protocolos de la capa de Aplicación que usa UDP son:

- Domain Name System (DNS)
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Routing Information Protocol (RIP)
- Trivial File Transfer Protocol (TFTP)
- Online games

Algunas aplicaciones, como juegos en línea con VoIP, pueden tolerar alguna pérdida de data. Si usaran TCP, estos servicios podrían experimentar grandes retardos mientras TCP detecta la data perdida y la retransmite. Esto retardos degradarían más a la aplicación y la data perdida, algunas aplicaciones como DNS, simplemente repetirán la petición si ellas no recibieron una respuesta, y por eso no necesitan a TCP para garantizar el envío de mensajes.

La baja sobrecarga de UDP hace que están sea ideal para algunas aplicaciones.

Autoevaluación

1. Identifique los distintos tipos de segmentos TCP
2. ¿Por qué el protocolo UDP puede ser usado en algunos casos?
3. ¿Cómo efectúa el control de flujo el protocolo TCP?
4. Identificar los distintos pasos dados durante el saludo de tres vías

Para recordar

UDP y TCP son protocolos comunes de la capa transporte.

Los datagramas y los segmentos TCP tienen cabecera prefijadas que la data incluye con el número de puerto origen y destino. Estos números de puertos permiten que la data sea direccionada a la aplicación correcta que se ejecuta en la computadora destino.

TCP no envía ninguna data a la red hasta saber el destino está listo para recibirla. TCP entonces administra en flujo de la data y reenvía cualquier segmento de data que no ha sido reconocida como recepcionar en el destino. TCP usan mecanismos de saludo, temporizadores y reconocimientos, inunda ventana dinámica para lograr estas características de seguridad. Esta seguridad genera una sobrecarga en la red en otros términos muchas más cabeceras de segmentos y mayor tráfico entre el origen y destino que administra el transporte de la data.

Si la data de la aplicación necesita ser enviada a través de la red rápidamente, o si el ancho de banda no puede soportar sobrecargas de mensajes de control que estén siendo intercambiados en los sistemas origen y destino, UDP será el protocolo de la capa transporte preferido por los diseñadores. Porque UDP no rastrea o reconoce la recepción de datagramas en el destino -éste sólo pasa los datagramas recibidos a la capa de aplicación tal cual como llegaron -y no reenvía los datagramas perdidos. Sin embargo, esto no significa necesariamente que sea una comunicación insegura; quizás tengan mecanismos en los protocolos de la capa aplicación y servicios que procesen la pérdida o retardos de datagramas si la aplicación los requiere.



Capa de red del Modelo OSI

TEMA

- Capa de red del modelo OSI

OBJETIVOS ESPECÍFICOS

- Describir la función del protocolo IP.

Identificar las características del paquete IP, así como el control del proceso de fragmentación.

CONTENIDOS

- Capa de red del modelo OSI
- Rol de IPv4
- Características básicas de IPv4:
 - Independiente del medio
 - Encapsulando el PDU de la capa de Transporte

6. Capa de red del modelo OSI

6.1 IPv4

La capa de red, o la capa 3 del modelo OSI, brindan los servicios para intercambiar fragmentos individuales de data sobre la red entre los dispositivos finales. Para lograr éste transporte fin-a-fin, la capa 3 usa 4 procesos básicos:

- Direccionamiento
- Encapsulamiento
- Ruteo
- Desencapsulamiento

Direccionamiento

Primero, la capa de red tiene que brindar un mecanismo para garantizar el funcionamiento a estos dispositivos finales. Si los fragmentos individuales de la data son dirigidos hacia un dispositivo final, este dispositivo debe tener una única dirección. En una Red IPv4, cuando esta dirección es agregada al dispositivo, el dispositivo es luego referido como un host.

Encapsulamiento

Segundo, la capa de red tiene que brindar encapsulamiento. No solamente los dispositivos deben ser identificados con una dirección, los fragmentos individuales de la capa de red, también tienen que contener estas direcciones. Durante el proceso de encapsulamiento, la capa 3 recibe el PDU de la capa 4 y agrega la cabecera de la capa 3, o la etiqueta, para crear el PDU de la capa 3. Cuando nos referimos a la capa de red, nosotros llamamos a este paquete PDU. Cuando un paquete es creado, la cabecera de estar contenida, la cantidad de información, la dirección del host que esta enviando. Esta dirección es referida como la dirección destino. La cabecera de la capa 3 también contiene la dirección del host original. Esta dirección es llamada la dirección origen.

Antes que la capa de red complete en el proceso de encapsulamiento, el paquete es enviado abajo a la capa de enlace de datos para que sea preparada para la transportación sobre el medio.

Ruteo

Luego, la capa de red debe brindar los servicios para dirigir estos paquetes a su host destino. Los hosts origen y destino no siempre están conectados a la misma red. De hecho el paquete quizás tenga que viajar a través de muchas redes diferentes. Por delante del camino, cada paquete debe ser guiado a través de la red, cada paquete debe alcanzar el destino final. Los dispositivos intermedios que están conectados a las redes son llamados routers.

El rol de un Router es seleccionar las rutas por donde los paquetes son dirigidos a su destino, este proceso es conocido como routing.

Durante el ruteo a través de una internetwork, El paquete puede atravesar muchos dispositivos intermediarios. Cada ruta que un paquete toma para alcanzar el siguiente dispositivo es llamada un salto. Mientras el paquete es reenviado, su contenido (the Transport layer PDU), se mantiene intacta hasta que el host destino ha sido alcanzado.

Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la capa 3. El host examina la dirección destino para verificar que el paquete fue direccionado a este dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de red y la capa 4 PDU contenida en el paquete es enviada al servicio apropiado en la capa transporte.

A diferencia de la capa transporte (OSI Layer 4), que administra el transporte de la data entre los procesos que se ejecutan en cada host final, los protocolos de la capa de red especifican la estructura de los paquetes y el procesamiento usado para llevar la data de un host a otro host.

6.1.1 Capa de red – Comunicación de host a host

Protocolos de la capa de red

Los protocolos implementados en la capa de red son:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

El protocolo de Internet (IPv4 and IPv6) es el más ampliamente usado para llevar data en la capa 3 será el centro en este curso.

6.1.2 Rol de IPv4

Los servicios de la capa de red implementados por el protocolo TCP/IP son el protocolo de Internet (IP). Version 4 de (IPv4) es actualmente el más usado. Este es el único protocolo de la capa 3 usado para llevar la data del usuario sobre Internet y es el foco del curso CCNA. Por consiguiente, este será el ejemplo que nosotros usaremos para los protocolos de la capa de red en este curso.

IP versión 6 (IPv6) es diseñado e implementado en algunas áreas. El IPv6 funcionará a lo largo de IPv4 y lo puede reemplazar en el futuro. Los servicios previstos por IP, así como también la estructura de la cabecera del paquete y contenidos, están especificados por el protocolo IPv4 y el protocolo IPv6. Estos servicios y esta estructura del paquete se usan para encapsular a los segmentos UDP o TCP para su viaje a través de una internetwork.

Las características de cada protocolo son diferentes. El protocolo de Internet fue diseñado como protocolo con poca sobrecarga. Este brinda únicamente las funciones que son necesarias para enviar un paquete desde el origen al destino sobre sistemas de redes interconectados. El protocolo no fue diseñado para rastrear y administrar el flujo de data. Estas funciones son realizadas por otros protocolos que están en otras capas.

Características básicas de IPv4:

- Orientados a la desconexión - no existe una conexión establecida antes de enviar los paquetes de data.

- El mejor esfuerzo (inseguro) - no hay sobrecarga porque no se garantiza el envío de data.
- Independencia del medio – opera independientemente del medio para llevar la data.

6.1.3 No orientado a conexión

Servicio “Connectionless”

Un ejemplo de una comunicación orientada a la desconexión es el de enviarle una carta a alguien sin notificarle al receptor por adelantado. Como muestra la figura, el servicio de postal toma la carta y le envía al receptor. La comunicación orientada a la desconexión trabaja con el mismo principio. Los paquetes IPs son enviados sin notificar al host final que ellos están siendo enviados.

Los protocolos orientados a la conexión, como TCP, requieren que el control de data sea intercambiado para establecer una conexión.

Los paquetes orientados a la desconexión quizás envíen, sin embargo, la llegada de los paquetes en el destino estará fuera de secuencia. Si algún paquete está fuera de orden está perdido creará problemas para la aplicación que use la data, luego los servicios de la capa superior tendrán que resolver estos inconvenientes.

6.1.4 Mejor esfuerzo

El servicio de mejor esfuerzo (inseguro)

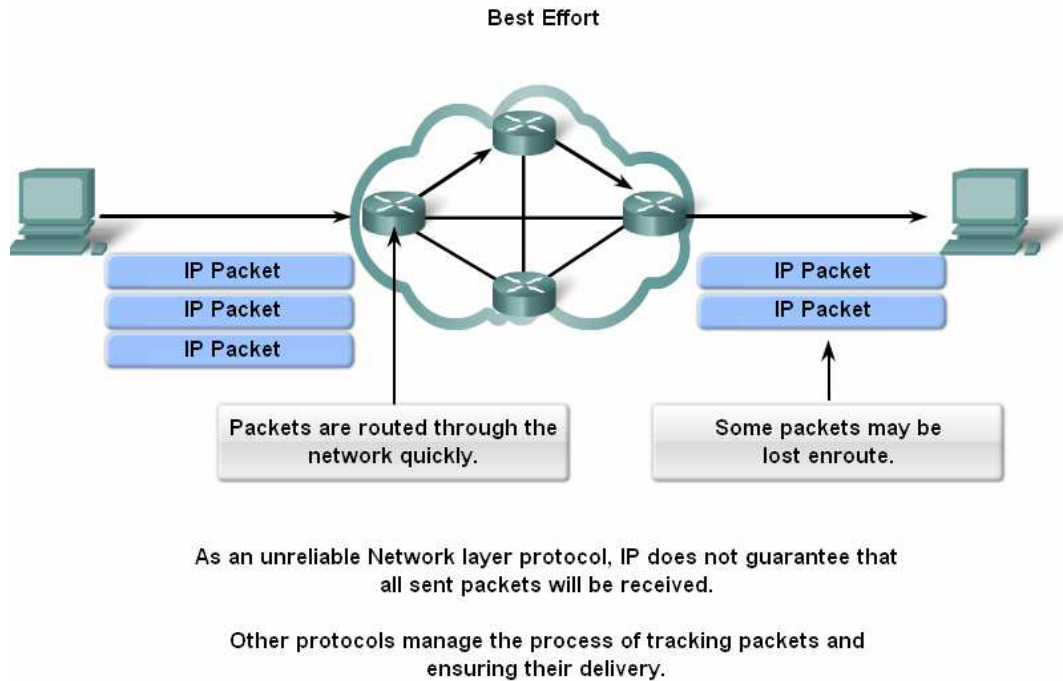
El protocolo IP no carga al servicio IP con la seguridad. Comparado aún protocolo seguro, la cabecera IP es muy pequeña. Transporta estas pequeñas cabeceras con poca sobrecarga. La poca sobrecarga significa menos retardo en la entrega. Esta característica es deseable para el protocolo de capa 3.

Es la misión de la capa 3 el transportar los paquetes entre los hosts mientras los ubica usando la menor sobrecarga que sea posible en la red.

La capa 3 no se preocupa y no es consciente del tipo de información que se contiene dentro de un paquete. Esta responsabilidad es función de las capas superiores. Las capas superiores pueden decidir si la comunicación entre los servicios necesita seguridad y si la comunicación puede tolerar los requerimientos de sobrecarga en la seguridad. IP es algunas veces referido como un protocolo inseguro. Inseguridad en este contexto no significa que IP trabaje algunas veces de manera apropiada o que no funcione bien otras veces. Inseguridad significa simplemente que IP no tiene la capacidad para administrar, y recuperar paquetes no entregados o corruptos.

Dado que los protocolos de otras capas pueden administrar la seguridad, a IP se le permite funcionar muy eficientemente en la capa de red. Si nosotros incluimos seguridad sobrecargaremos nuestro protocolo de capa 3, luego las comunicaciones que no requieren conexiones o seguridad no estarán agobiadas con el consumo de ancho de banda y los retardos producidos por estas sobrecargas. En la suite TCP/IP, la capa de transporte puede escoger TCP o UDP, basado en las necesidades de la comunicación. Al igual que con todo aislamiento brindado por los modelos de la red, dejan la decisión de fiabilidad para la capa de Transporte y hacen a IP más adaptable y complaciente para los diferentes tipos de comunicación

La cabecera de un paquete IP no incluye campos requeridos para la seguridad en entrega de data. No hay reconocimiento por los paquetes enviados. No hay control de error para la data y no hay ninguna forma de rastrear los paquetes, por consiguiente, no hay posibilidad para la retransmisión de paquetes.



6.1.5 Independiente del medio

Independencia del medio

La capa de red no le concierne las características del medio por donde los paquetes serán transportados. IPv4 e IPv6 opera independientemente del medio que lleva la data en las capas inferiores de la pila del protocolo. Cualquier paquete IP puede ser transmitido eléctricamente sobre el cable, como las señales ópticas sobre la fibra, o de manera inalámbrica como las señales de radio.

Esto es responsabilidad de la capa enlace de de datos del modelos para tomar un paquete IP y prepararlo para la transmisión sobre los medios de comunicación. Esto significa que el transporte de los paquetes IP no está limitado a ningún medio particular.

Hay, sin embargo, una característica mayor del medio que la capa de red considera: el tamaño máximo de PDU que cada medio puede transportar. Esta característica está referida como la unidad máxima de transmisión (MTU). Parte del control de la comunicación entre la capa de enlace de datos y la capa de red es establecer el máximo tamaño para el paquete. La capa de enlace de datos pasa el MTU hacia la capa de red. La capa de red luego determina qué tan grande debe crear el paquete.

En algunos casos, un dispositivo intermediario -usualmente un router- necesita dividir un paquete cuando se reenvían de un medio a otro medio con un MTU más pequeño. Este proceso es llamado fragmentar el paquete o fragmentación.

6.1.6 Encapsulando el PDU de la capa de Transporte

IPv4 encapsula, o empaqueta, el segmento de la capa transporte o el datagrama entonces la red puede entregar el paquete a su host destino.

El proceso de encapsular la data por capas permite que servicios diferentes puedan trabajar en distintas capas. Esto significa que los segmentos de la capa de transporte pueden ser fácilmente empaquetados por los protocolos existentes en la capa de red, como es IPv4 y IPv6 o por cualquier protocolo nuevo que quizás sea diseñado en el futuro.

Los routers pueden implementar estos diferentes protocolos de la capa de red para operar simultáneamente sobre la red hacia, y desde el mismo o diferentes hosts. El ruteo realizado por estos dispositivos intermediarios sólo consideran el contenido de la cabecera del paquete que encapsula el segmento.

En todos los casos, la porción de data de un paquete - que es, encapsulado como PDU en la capa transporte se mantiene igual durante los procesos de la capa de red.

6.1.7 El encabezado del paquete IP v4

El protocolo IPv4 define muchos campos diferentes en la cabecera del paquete. Estos campos contienen valores binarios que los servicios IPv4 hacen referencia mientras efectúan el envío de los paquetes a través de la red.

Consideraremos seis campos clave:

- Dirección IP origen
- Dirección IP Destino
- Time-to-Live (TTL) – Tiempo de Vida
- Type-of-Service (ToS) – Tipo de servicio
- Protocol
- Fragment Offset – Desplazamiento de Fragmento

Dirección destino IP

El campo de la dirección destino IP contiene el valor de 32-bits que representa la dirección destino en la capa de red del paquete destino.

Dirección origen IP

El campo de la dirección origen IP contiene el valor de 32-bits que representa la dirección origen en la capa de red del paquete origen.

Tiempo de vida

El tiempo de vida es un valor binario de 8-bits que indica el tiempo de vida de un paquete. El valor TTL es disminuido en uno cada vez que pasa por un router. (Esto es, cada salto). Cuando el valor se convierte en cero, el router descarta o arroja los paquetes y los elimina de la red. Estos mecanismos previenen que los paquetes se queden generando lazos cerrados de ruteo con el consiguiente consumo de ancho de banda.

Protocolo

Este valor de 8-bits binario indica el tipo de data que el paquete está llevando. El campo del protocolo permite a la capa de red pasar los datos al protocolo apropiado en la capa superior.

Un ejemplo de los siguientes valores:

01 ICMP

06 TCP

17 UDP

Tipo de servicio

El campo del tipo de servicio contiene 8-bits y son usados para determinar la prioridad de cada paquete. Este valor permite habilitar el mecanismo de calidad de servicio (QoS) que será aplicado a los paquetes con alta prioridad, como son el envío de data de voz por el teléfono. El router procesa los paquetes que pueden ser configurados para decidir que paquete es reenviado primero basado en el valor de tipo de servicio.

Fragment Offset

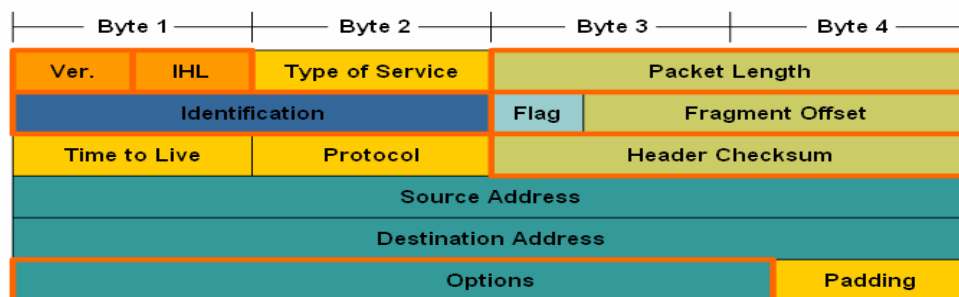
Como mencionamos anteriormente, un router quizás tenga que fragmentar un paquete cuando lo reenvíe de un medio a otro medio de tenga un MTU más pequeño. Cuando ocurre la fragmentación, el paquete IPv4 usa campo Fragment Offset y la bandera MF en la cabecera para reconstruir el paquete cuando este llegue a su host destino. El campo fragment offset identifica el orden en el cual es ubicado el paquete fragmentado en la reconstrucción.

Flag “Mas fragmentos”

La bandera para más fragmentos (MF) es un solo bit en el campo de la bandera usado con el Fragment Offset para la fragmentación y reconstrucción de los paquetes. Cuando el bit de la bandera “más fragmentos” está habilitado, esto significa que éste no es el último paquete del fragmento. Cuando un host receptor de un paquete que llega con el MF = 1, examina el Fragment Offset para ver dónde este fragmento está ubicado para la reconstrucción del paquete. Cuando el host receptor recibe un paquete con el MF = 0 y un valor sin cero en el fragmento offset, éste ubica el fragmento como la parte última en la reconstrucción del paquete. Un paquete desfragmentado tiene toda la información de la fragmentación en cero (MF = 0, fragment offset = 0).

Flag “No fragmentos”

La bandera no fragmentada es un solo (DF) en el campo Flag que indica que la fragmentación de un paquete no está permitida. Si el bit de la bandera no fragmentada está habilitado, luego la fragmentación en este paquete no está permitida. Si un router necesita fragmentar un paquete para permitirle pasar a la capa inferior (la capa enlace de datos), pero el bit DF está habilitado en 1, entonces el router descartará este paquete.



Otros campos de la cabecera IPv4

Revise cada campo en el gráfico para ver su propósito.

Versión:

Contiene el número de versión IP (4)

Longitud de la cabecera (Header Length IHL):

Especifica el tamaño de la cabecera del paquete.

Longitud del paquete:

Este campo nos brinda el tamaño entero del paquete incluyendo la cabecera y la data, en bytes.

Identificación:

Este campo es el principal usado para identificar a los fragmentos como únicos de un paquete original IP

Header Checksum

El campo checksum es usado para verificar errores en la cabecera del paquete.

Opciones

Hay provisión para campos adicionales en la cabecera IPv4 para brindar otros servicios que son usados raramente.

Paquete IP Típico:

La figura representa un paquete completo IP con los valores típicos en la cabecera

Ver = 4; IP version.

IHL = 5; tamaño de la cabecera en palabras de 32 bit (4 bytes). Esta cabecera es $5 \times 4 = 20$ bytes, el mínimo tamaño válido.

Longitud total = 472; tamaño del paquete (cabecera y data) es 472 bytes.

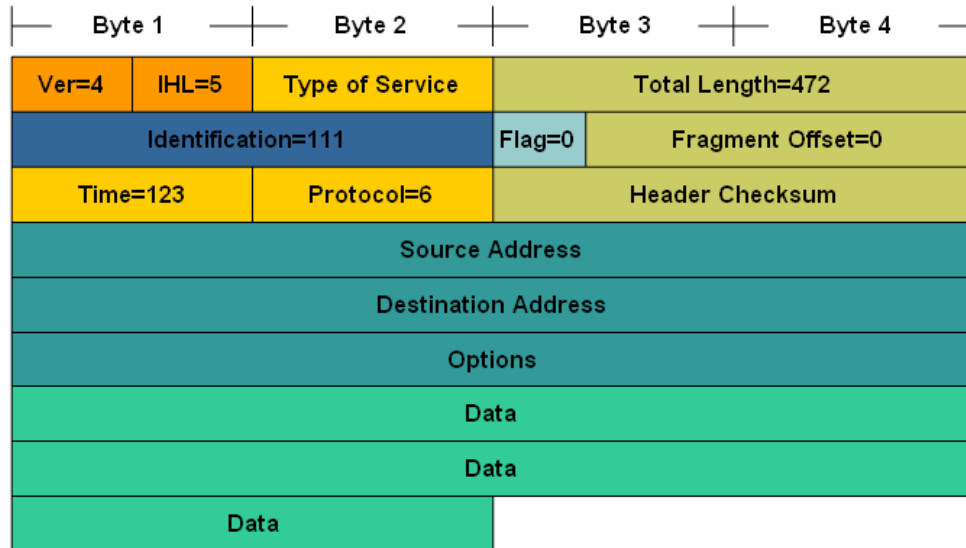
Identificación = 111; identificador original del paquete (Requerido si está más tarde fragmentado).

Bandera = 0; informa que el paquete pueden ser fragmentado si es requerido.

Fragmento Offset = 0; informa que este paquete no está fragmentado actualmente (no hay offset).

Tiempo de vida = 123; informa a la capa 3 procesar el tiempo en segundo antes del paquete sea descartado (disminuido por al menos 1 cada vez que un dispositivo procese el encabezado del paquete).

Protocolo = 6; informa que la data llevada por este paquete es un segmento TCP.



6.2.1 Redes –Separando hosts en grupos comunes

Uno de los roles mayores en la capa de red es brindar los mecanismos para el direccionamiento del host. Cuando el número de hosts en la red está creciendo, un es requerido un mayor planeamiento para administrar las direcciones de la red.

Dividir redes

En vez de tener a todos los hosts en todas partes conectados a una red global, es más práctico y administrable agrupar los hosts dentro de redes específicas. Históricamente, las redes basadas en IP tienen sus raíces en una red grande. Conforme esta única red crece, las redes grandes fueron separadas dentro de pequeñas redes que se fueron interconectando. Estas pequeñas redes algunas veces son llamadas subredes o subnets.

Red y subred son términos algunas veces usados intercambiamente para referirse a cualquier sistema de red que permita la comunicación común compartida de los protocolos del modelo del TCP/IP.

Conforme nuestras redes crecen, se convierten en redes muy grandes como para ser administradas en una sola red. En este punto, se hace necesario dividir nuestra red.

Las redes pueden ser agrupadas basadas en los siguientes factores:

- Ubicación geográfica
- Propósito
- Propiedad

6.2.2 ¿Por qué separar hosts en redes?

Rendimiento

Como mencionamos previamente, conforme las redes crecen presentan problemas debidos al incremento del tráfico de broadcast. Estos problemas pueden ser parcialmente aliviados dividiendo la red en redes más pequeñas.

Los principales inconvenientes con las redes grandes son:

- Degradación del rendimiento
- Cuestiones de seguridad
- Administración de las direcciones
- Mejorar el rendimiento

Grandes cantidades de hosts conectados a una única red lógica pueden producir mucho tráfico con el consiguiente problema del colapso de la red.

Autoevaluación

1. Identificar los campos del paquete IP que se encargan del proceso de control de la fragmentación IP.
2. Identificar algunas ventajas del protocolo IPv6 sobre IPv4
3. ¿Por qué se hace necesario dividir una red grande en redes lógicas pequeñas?
4. Identificar las características básicas del protocolo IPv4.

Para recordar

IP versión 6 (IPv6) es diseñado e implementado en algunas áreas. El IPv6 funcionará a lo largo de IPv4 y lo puede reemplazar en el futuro. Los servicios previstos por IP, así como también la estructura de la cabecera del paquete y contenidos, están especificados por el protocolo IPv4 y el protocolo IPv6. Estos servicios y esta estructura del paquete se usan para encapsular a los segmentos UDP o TCP para su viaje a través de una internetwork.

Primero, la capa de red tiene que brindar un mecanismo para garantizar el funcionamiento a estos dispositivos finales. Si los fragmentos individuales de la data son dirigidos hacia un dispositivo final, este dispositivo debe tener una única dirección.

Es la misión de la capa 3 el transportar los paquetes entre los hosts mientras los ubica usando la menor sobrecarga que sea posible en la red.

La capa de red no le concierne las características del medio por donde los paquetes serán transportados. IPv4 e IPv6 opera independientemente del medio que lleva la data en las capas inferiores de la pila del protocolo.



Direccionamiento de red en IPv4

TEMA

- Direccionamiento de red en IPv4

OBJETIVOS ESPECÍFICOS

- Describir la estructura de las direcciones de red IPv4
- Identificar los tipos de transmisión de datos

CONTENIDOS

- Direccionamiento IPv4
- Tipos de direcciones en IPv4
- Tipos de comunicación: Unicast, broadcast y multicast
- Direcciones IP Públicas y privadas

8. Direccionamiento IPv4

8.1 La anatomía de una direccion IPv4

Cada dispositivo en una red tiene que ser identificado como único. En la capa de red, los paquetes de comunicación necesitan ser identificados con las direcciones origen y destino de los 2 sistemas finales. Con IPv4, esto significa que cada paquete tiene una dirección origen de 32-bit y una dirección destino de 32-bit en la cabecera de la capa 3. Estas direcciones son usadas en la red de data como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para la interpretación de las direcciones. Para nosotros en la red de humanos, una cadena de 32 bits es difícil de interpretar y más aún difícil de recordar. Sin embargo, nosotros representamos las direcciones IPv4 usando el formato decimal.

Notación decimal

Los patrones ordinarios representados en las direcciones IPv4 son expresados como notación decimal y cada byte separado del patrón binario -, llamado un octeto, con un punto. Esto es llamado un octeto porque cada número decimal representa un byte o 8 bits.

Por ejemplo, la dirección:

10101100000100000000010000010100

Es expresada en notación decimal como:

172.16.4.20

Hay que tener presente que los dispositivos usan la lógica binaria. El formato de notación decimal es usado para hacer más fácil a los usuarios recordar las direcciones.

Campo de red y host

Por cada dirección IPv4, una parte de los bits representa la dirección de red. En la capa 3, nosotros definimos una red como un grupo de hosts que tienen los bits idénticos en la dirección de red.

Aunque todos los 32 bits son definidos en la dirección host IPv4, existe un número variable de bits que son identificados como el campo para la dirección de host. El número de bits usado en el campo del host determina el número de hosts que nosotros podemos tener dentro de la red.

Por ejemplo, si nosotros necesitamos tener como mínimo 200 hosts en una red particular, necesitamos usar los bits suficientes en el campo de host para poder representar como mínimo 200 diferentes bits.

Para asignar una dirección única a 200 hosts, nosotros deberíamos usar el último octeto. Con 8 bits, un total de 256 diferentes bits pueden ser representados. Esto significa que los primeros tres octetos representan el campo de red.

8.2 Tipos de direcciones en IPv4

Dentro del ramo de direcciones en cada red IPv4, nosotros tenemos tres tipos de direcciones:

Dirección de red - la dirección que hace referencia a la red.

Dirección de Broadcast - una dirección especial usada para enviar data a todos los hosts en la red.

Dirección de Host - la dirección asignada a los dispositivos finales en la red

Dirección de red

La dirección de red es una manera estándar para referirnos a la red. Por ejemplo, nosotros podemos referirnos a una red como "la red 10.0.0.0 " esto es mucho más conveniente y descriptivo para referirnos a la red, que usar un término como "la primera red." Todos los hosts en la red 10.0.0.0 tendrán los mismos bits de red.

Dentro de la dirección IPv4 de un rango de red, la dirección mínima es reservada para la dirección de red. Esta dirección tiene un 0 por cada host en el campo de host

Dirección de Broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación de todos los hosts en esa red. Para enviar data a todos los hosts en una red, un host puede enviar un solo paquete que es direccionado a la dirección de broadcast de la red.

La dirección de broadcast usan la dirección más alta en el rango de red. Esta es la dirección en donde los bits del campo host están todos en "1". Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. Esta dirección es también referida como directed broadcast.

Direcciones de Host

Como describimos previamente, cada dispositivo final requiere una dirección única para enviar un paquete al host. En las direcciones IPv4, nosotros asignamos los valores entre la dirección de red y la dirección de broadcast para los dispositivos en esa red.

Prefijos de red

Una pregunta importante es: ¿Cómo sabemos cuántos bits representa el campo de red y cuántos bits representa el campo de host? Cuando nosotros expresamos una dirección de red IPv4, agregamos la longitud del prefijo para la dirección de red. La longitud del prefijo es el número de bits en la dirección que nos da el campo de red. Por ejemplo, en 172.16.4.0 /24, la longitud del prefijo es /24 - esto nos dice que los primeros 24 bits son la dirección de red. Esto nos deja 8 bits, el último octeto es el campo de host. Después de este capítulo, aprenderemos más acerca de otras entidades que son usadas en el campo de red de una dirección IPv4 para los dispositivos de red. Esta es llamado la máscara de subred . La máscara de subred consta de 32 bits, y la dirección usa 1s y 0s para indicar cuántos bits son usados para el campo de red y cuántos bits son usados para el campo de host.

Las redes no siempre están diseñadas con un prefijo de /24. Dependiendo del número de hosts en la red, el prefijo asignado quizás sea diferente. Al tener un número

diferente de prefijo cambiará el rango de host y la dirección de broadcast para cada red.

Fíjese que las direcciones de red pueden ser las mismas, pero el campo de host y la dirección de broadcast son diferentes para cada longitud de prefijo. En esta figura se puede también ver el número de hosts que pueden ser direccionados en la red.

Using Different Prefixes for the 172.16.4.0 Network

Network	Network address	Host range	Broadcast address
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

SAME NETWORK ADDRESS
ALL PREFIXES

DIFFERENT BROADCAST
ADDRESS EACH PREFIX

8.2.1 Calculando la red, host y la dirección de broadcast

En este punto, usted puede preguntarse: ¿Cómo calculamos estas direcciones? Este proceso de cálculo requiere que nosotros veamos estas direcciones en binario.

En el ejemplo de las divisiones de red, nosotros necesitamos mirar el octeto de la dirección donde el prefijo divide el campo de la red y el campo del host. En todos estos ejemplos, el campo del host es el último octeto. Mientras esto es común, el prefijo puede también dividir cualquier octeto.

Para empezar a entender este proceso de determinar la dirección asignada, veamos algunos ejemplos que están debajo en binario.

Mire la figura para el ejemplo de la dirección asignada a la red 172.16.20.0 /25.

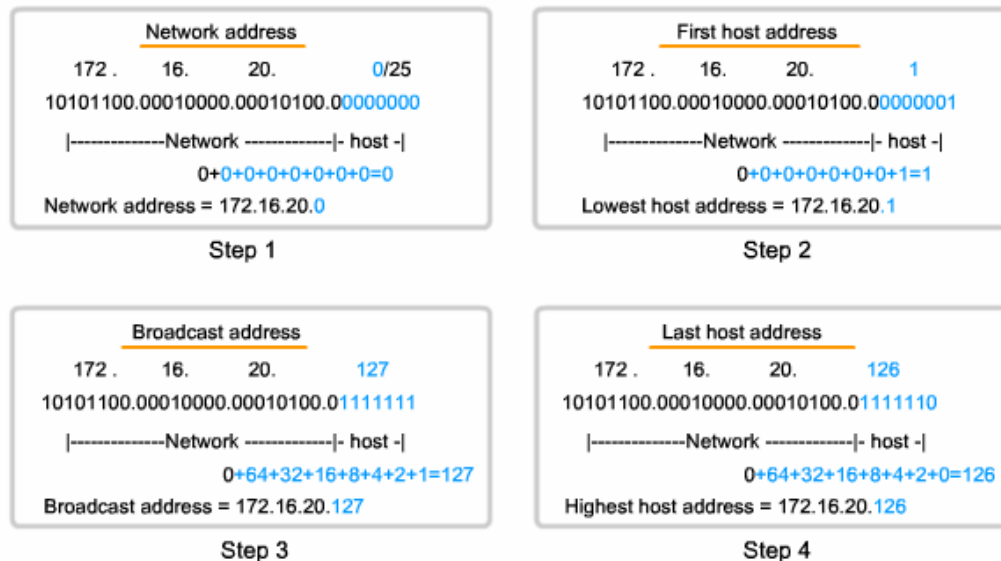
En el primer cuadro, nosotros vemos la representación de la dirección de red. Un prefijo de 25 bits, los últimos 7 bits son los bits para el host. Para representar la dirección de red, todos los bits del hosts estarán en '0'. Esto creará la dirección de red 172.16.20.0 /25.

En el segundo cuadro, vemos el cálculo de la dirección host más baja. Esto es siempre una dirección mayor que la dirección de red. Los últimos 7 bits del host se convierten a '1'. Con el bit más bajo de la dirección de host habilitado a 1, the de dirección más baja es 172.16.20.1.

El tercer cuadro muestra el cálculo para la dirección de broadcast de la red. Por consiguiente, todos los 7 bits del host usados en esta red están todos en '1s'. Del cálculo, nosotros tenemos el último octeto en 127. Esto nos da una dirección de broadcast 172.16.20.127.

El cuarto cuadro presenta el cálculo de la dirección de host más alta. La dirección de host más alta para la red es siempre una más baja que la de broadcast. Esto significa que el bit del host más bajo es '0' y todos los otros bits del host como '1s'. Como ves, esto hace que la dirección de host más alta en la red sea 172.16.20.126.

Assigning Addresses



A través de este ejemplo nosotros explicamos todos los octetos, por lo tanto solo necesitamos examinar el contenido del octeto dividido.

8.2.3 Tipos de comunicación: Unicast, broadcast y multicast

En una red IPv4, los hosts pueden comunicarse de 3 diferentes maneras:

Unicast:

El proceso de enviar un paquete desde un host a un host individual

Broadcast:

El proceso de enviar un paquete desde un host a todos los hosts en la red

Multicast:

El proceso de enviar un paquete desde un host a un grupo seleccionado de hosts

Estos tres tipos de comunicación son usados para propósitos diferentes en las redes de datos. En los 3 casos, la dirección IPv4 del host original es ubicada en la cabecera del paquete como la dirección origen.

Tráfico Unicast

La comunicación Unicast es usada por la comunicación normal host-a-host en ambas redes basadas en arquitectura cliente/servidor y peer-to-peer. Los paquetes Unicast usan la dirección host del dispositivo destino como la dirección destino y pueden ser ruteadas en una internetwork. Las transmisiones broadcast y multicast, sin embargo, usan direcciones especiales como la dirección destino. Usar estas direcciones especiales, como la broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast quizás esté limitado a la red local o ruteada a través de una internetwork.

En una red IPv4, la dirección unicast aplicada a un dispositivo final es referida como la dirección host. Para la comunicación unicast, las direcciones de host asignada a los

dos dispositivos finales son usadas como la dirección IPv4 fuente y destino. Durante el proceso de encapsulamiento, el host origen ubicado esta dirección en la cabecera del paquete unicast como la dirección host origen y la dirección IPv4 de la computadora destino en la cabecera del paquete como la dirección destino. La comunicación que usa un paquete unicast puede ser reenviada a través de una internetwork usando la misma dirección.

Transmisión de Broadcast

El tráfico broadcast es usado para enviar paquetes a todos los hosts en la red, para este fin el paquete hace uso de la dirección especial de broadcast. Cuando un host recibe un paquete con la dirección broadcast como destino, el host procesa el paquete como un paquete para una dirección unicast.

Las transmisiones broadcast son usadas para la ubicación de servicios/dispositivos especiales en donde la dirección no es conocida o cuando un host necesita brindar información a todos los hosts en la red.

Algunos ejemplos del uso de una transmisión broadcast son:

- Mapear las direcciones de las capas superiores a las direcciones de las capas inferiores.
- Solicitar una dirección.
- Intercambiar información de ruteo.

Cuando un host necesita información, el host envía una solicitud, llamada la consulta, para la dirección de broadcast. Todos los hosts en la red reciben y procesan esta consulta. Uno o más hosts con información solicitada responden típicamente usando unicast. Similarmente, cuando un host necesita enviar información a los hosts en una red, éste crea y envía un paquete broadcast con la información.

A diferencia de las transmisiones unicast, cuando los paquetes pueden ser ruteados a través de la internetwork, los paquetes de broadcast son usualmente restringidos a la red local. Esta restricción depende de la configuración del router que es usado en la red y el tipo de broadcast. Hay dos tipos de broadcasts: el broadcast dirigido y el broadcast limitado.

Broadcast dirigido

Un broadcast dirigido es enviado a todos los hosts en una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts en una red no-local. Por ejemplo, para un host fuera de la red la comunicación con los hosts dentro de la red 172.16.4.0 /24, la dirección destino del paquete sería 172.16.4.255

Broadcast limitado

El broadcast limitado es usado para la comunicación a los hosts en la red local. Estos paquetes usan la dirección IPv4 destino 255.255.255.255. Los Routers no reenvían este broadcast. Los paquetes direccionados a una dirección de broadcast limitada únicamente aparecerán en la red local. Por esta razón, una red IPv4 es también referida como un dominio broadcast. Los Routers forman el límite para dominio broadcast.

Como por ejemplo, un host dentro de la red 172.16.4.0 /24 enviará broadcast a todos los hosts dentro de esta red usando un paquete con la dirección destino 255.255.255.255.

Como se vio anteriormente, cuando un paquete es de tipo broadcast, ésta usando recursos de la red y también fuerza a cada host en la red a procesar este paquete. Sin embargo, el tráfico broadcast debería ser limitado debido a que afectará el rendimiento en la red por los dispositivos. Debido a que los routers separan los dominios de broadcast, subdividen las redes, y de esta manera podemos mejorar el rendimiento de la red.

Transmisión Multicast

La transmisión Multicast está diseñada para conservar el ancho de banda de las redes IPv4. Éste reduce el tráfico permitiendo que un host envíe un solo paquete a varios hosts seleccionados. Para alcanzar el destino de múltiples hosts se usa la comunicación unicast, pero en este caso un host origen necesitaría enviar un paquete individual direccionado a cada host. En cambio si usamos una transmisión multicast, el host origen puede enviar un solo paquete que alcance a miles de hosts destinos, que en este caso están agrupados bajo un grupo de multidifusión.

Algunos ejemplos de la transmisión multicast son:

- Distribución de audio y video
- Intercambio de información de Ruteo por los protocolos de ruteo
- Distribución de software

Clientes Multicast

Los Hosts que desean recibir data de tipo multicast en particular son llamados clientes multicast. Los clientes multicast usan servicios inicializados por un programa cliente para suscribirse al grupo multicast.

Cada grupo multicast es representado por una sola dirección destino multicast IPv4. Cuando un host IPv4 está suscrito a un grupo multicast, el host procesa los paquetes direccionados a esta dirección multicast así como los paquetes direccionados a la única dirección unicast ubicada. Como veremos, IPv4 tiene reservado un bloque especial para las direcciones multicast que va desde 224.0.0.0 a 239.255.255.255.

8.2.4 Direcciones IPv4 Reservadas

Expresado en formato decimal, el rango de dirección IPv4 es de 0.0.0.0 a 255.255.255.255. Como ya se vera, no todas estas direcciones pueden ser usadas como direcciones de host para la comunicación unicast. Existen una serie de restricciones que hay que tomar en cuenta.

Direcciones experimentales

Un bloque mayor de direcciones reservadas para propósitos especiales son las direcciones experimentales IPv4 que van desde el rango 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones están identificadas como reservadas para uso futuro (RFC 3330). Esto sugiere que podrían ser convertidos a direcciones utilizables. Actualmente, no pueden ser usados en redes de IPv4. Sin embargo, estas direcciones podrían servir para investigación o experimentación.

Direcciones Multicast

Como vimos previamente, otro bloque mayor de direcciones reservadas para propósitos especiales son las direcciones multicast IPv4 desde 224.0.0.0 a

239.255.255.255. Adicionalmente, el rango de direcciones multicast está subdividido dentro de diferentes tipos de direcciones: El enlace reservado de las direcciones locales y el ámbito global. Un tipo adicional de direcciones multicast es el ámbito administrativo, también llamadas direcciones de ámbito limitado.

Las direcciones multicast IPv4 224.0.0.0 a 239.255.255.255 están reservadas como direcciones de enlace local. Estas direcciones están siendo reservadas para su uso por parte de los grupos multicast en las redes locales. Los paquetes con estos destinos son siempre transmitidos con el valor de tiempo de vida (time-to-live TTL) en 1. Sin embargo, un router conectado a la red local nunca debería reenviarlos. Un uso típico de la dirección de enlace local está en los protocolos de ruteo que usan transmisiones multicast para intercambiar información de ruteo.

Las direcciones de ámbito global son 240.0.0.0 a 255.255.255.255. Estas direcciones es posible que sean usadas para transmitir data multicast a través de Internet. Por ejemplo, 224.0.1.1 ha sido reservada para el protocolo de tiempo de red (Network Time Protocol NTP) que permite sincronizar la hora en los relojes de los dispositivos de la red.

Direcciones de Host

Después de explicar sobre los rangos reservados para direcciones experimentales y direcciones multicast, nos queda un rango que abarca desde la dirección 0.0.0.0 a 223.255.255.255 que podría servir para los hosts IPv4. Sin embargo, dentro de este rango se encuentran muchas direcciones que ya están reservadas para propósitos especiales. Aunque previamente hemos cubierto algunas de estas direcciones, las direcciones reservadas más importantes serán discutidas en el siguiente capítulo:

Reserved IPv4 Address Ranges

Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	<ul style="list-style-type: none"> used for research or experimentation cannot currently be used for hosts in IPv4 networks 	240.0.0.0 to 255.255.255.254	1700 3330

8.2.5 Direcciones IP Públicas y privadas

Aunque la mayoría de direcciones de host IPv4 son direcciones públicas designadas para su uso en las redes que acceden a Internet, hay bloques de direcciones que son usadas en redes que deseen limitar o denegar el acceso a Internet. Estas direcciones son llamadas direcciones privadas.

Direcciones privadas

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

El bloque de direcciones privadas, es mostrado en la parte superior, y son usadas en redes privadas, es decir sin salida directa hacia Internet.

Los hosts que no requieren ganar acceso a Internet quizás puedan hacer uso irrestricto de direcciones privadas. Sin embargo, los administradores de redes internas deben diseñar esquemas de direccionamiento de red para asegurar que los hosts de las redes privadas usen direcciones IP que son únicas dentro de su ambiente de red.

Muchos hosts en redes diferentes quizás usen las mismas direcciones privadas. Esto no es ningún problema pues el router o el firewall es el que delimita el perímetro de estas redes privadas y deben bloquear o deben traducir estas direcciones. Aun si estos paquetes de alguna manera estuvieran siendo diseccionados hacia Internet, los routers no tendrían rutas para reenviarlas a las redes privadas apropiadas.

La técnica del NAT permite a los hosts que están dentro de una red prestarles una dirección pública para comunicarse con las redes exteriores. Si bien hay algunas limitaciones y problemas de rendimiento cuando se usa el NAT, los hosts que hacen uso de esta técnica pueden acceder a los servicios sobre Internet sin problemas notables.

Direcciones públicas

La inmensa mayoría de direcciones IPv4 unicast son direcciones públicas. Estas direcciones son diseñadas para ser usadas en los hosts que son accesibles públicamente desde Internet. Aun dentro de estos bloques de dirección, hay muchas direcciones que son designadas para otros propósitos especiales.

8.2.6 Direcciones IPv4 especiales

Hay ciertas direcciones que no pueden ser asignadas a los hosts por varias razones. Hay también direcciones especiales que pueden ser asignadas a los hosts pero con restricciones.

Direcciones de red y Broadcast

Como explicamos anteriormente, dentro de cada red la primera y la última dirección no pueden ser asignadas a los hosts. Éstas son la dirección de la red y la dirección de broadcast respectivamente.

Ruta por defecto

También anteriormente vimos la ruta por defecto de IPv4 como 0.0.0.0. La ruta por defecto es utilizada como una ruta "captura todo".

Retroalimentación Loopback

Una de las direcciones reservadas es la dirección loopback IPv4 de la dirección 127.0.0.1. El loopback es una dirección especial que los hosts usan cuando desean no dirigir tráfico hacia ellos mismos. También puede usar el ping la dirección de loopback para testear la configuración del TCP/IP.

Aunque sólo la sola dirección 127.0.0.1 es usada, las direcciones 127.0.0.0 al 127.255.255.255 están reservadas, cualquier dirección dentro de este bloque se retroalimentará dentro del host local. Ninguna dirección dentro de este bloque debería aparecer en una red.

Direcciones de enlace local

Las direcciones IPv4 en el bloque 169.254.0.0 a 169.254.255.255 (169.254.0.0 /16) son definidas como direcciones de enlace local. Estas direcciones pueden ser asignadas automáticamente al host local por el sistema operativo en un ambiente donde la configuración IP no está disponible. Esto quizás sea usado en redes peer-to-peer pequeñas o por un host que no pueda obtener una dirección automáticamente desde un servidor (Dynamic Host Configuration Protocol DHCP).

Las direcciones de enlace local no brindan servicios fuera del red local. Sin embargo, muchas aplicaciones cliente/servidor y peer-to-peer operarán correctamente con direcciones de enlace local IPv4.

8.2.7 Direcciones IPv4 tradicionales

Clases de red históricas

Históricamente, RFC1700 agrupó los rangos de las direcciones unicast dentro de un rango específico llamado las direcciones de clase A, B, C. También definió la clase D (multicast) y direcciones de clase E (experimental), como vimos anteriormente

Las clases de direcciones unicast A, B, y C también definen el tamaño de las redes así como también bloques específicos de direcciones para estas redes. Este uso de las direcciones es referido como el direccionamiento basado en clases.

Clase A

Una dirección de clase A fue diseñado para soportar redes extremadamente grandes con más de 16 millones de direcciones para los hosts. Las direcciones de clase A usan un prefijo fijo de /8 con el primer octeto para indicar la dirección de red. Los 3 octetos restantes son usados para identificar las direcciones de los hosts.

Todas las direcciones de clase A requieren que el bit más significativo del octeto sea un cero. Esto quiere decir que sólo 128 redes serán posibles de configurar en clase A, 0.0.0.0 /8 a 127.0.0.0 /8, antes de sacar los bloques reservados de la direcciones. Si bien las direcciones de clase A se reservan la mitad del espacio de direcciones, están limitadas a 128 redes, e incluso sólo podrían ser asignadas a aproximadamente 120 compañías u organizaciones.

Clase B

Las direcciones de clase B fueron diseñadas para soportar un moderado tamaño de redes con más de 65,000 hosts. Una dirección de clase B usa los 2 primeros octetos para la dirección de red. Los otros 2 octetos especifican las dirección del host.

Para las direcciones de clase B, los 2 bits más significativo del primer octeto serán 10. Esto restringe el bloque de direcciones para la clase B de 128.0.0.0 /16 a 191.255.0.0 /16.

Clase C

Las direcciones de clase C son las más comúnmente usadas de las otras direcciones. Esta dirección proporciona las direcciones para las redes con el menor número de hosts, esto es un máximo de 254 hosts.

La dirección de clase C es usada con un prefijo de /24. Esto significa que las redes de clase C solo usan el último octeto como dirección de host con los 3 primeros octetos para identificar la dirección de red.

La dirección de clase C tiene los 3 bits más altos con el valor de 110. Esto restringe las direcciones de clases C desde 192.0.0.0 /16 a 223.255.255.0 /16.

Autoevaluación

1. Mediante un diagrama identificar las clases de direcciones IPv4.
2. Diferenciar el funcionamiento de las direcciones broadcast y las direcciones multicast.
3. ¿Cuál es el número máximo de direcciones de host que pueden ser identificadas usando direcciones clase C?
4. ¿En qué casos recomendaría utilizar direcciones del tipo localhost?

Para recordar

La comunicación Unicast es usada por la comunicación normal host-a-host en ambas redes basadas en arquitectura cliente/servidor y peer-to-peer. Los paquetes Unicast usan la dirección host del dispositivo destino como la dirección destino y pueden ser ruteadas en una internetwork.

La comunicación Unicast es usada por la comunicación normal host-a-host en ambas redes basadas en arquitectura cliente/servidor y peer-to-peer. Los paquetes Unicast usan la dirección host del dispositivo destino como la dirección destino y pueden ser ruteadas en una internetwork. La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación de todos los hosts en esa red. Para enviar data a todos los hosts en una red, un host puede enviar un solo paquete que es direccionado a la dirección de broadcast de la red.

El broadcast limitado es usado para la comunicación a los hosts en la red local. Estos paquetes usan la dirección IPv4 destino 255.255.255.255. Los Routers no reenvían este broadcast.



Capa de Enlace de datos

TEMA

- Aplicaciones TCP/IP
- Servicios Peer-to-Peer

OBJETIVOS ESPECÍFICOS

- Explicar la utilidad de la capa de transporte.
- Identificar el rol de la capa de transporte y como ésta brinda la transferencia de data en el punto final de las aplicaciones.
- Describe el rol de los dos protocolos TCP/IP que usa la capa de transporte: TCP y UDP.
- Explicar las funciones principales de la capa transporte, seguridad, direccionamiento del puerto, y segmentación.
- Explicar cómo el TCP y UDP usan las principales funciones.

CONTENIDOS

- Servicios de correo y Protocolos SMTP/POP
- FTP
- DHCP
- Servicios para compartir archivos y protocolo SMB
- Servicios Peer-to-Peer y el Protocolo Gnutella
- Servicios Telnet

9. Capa de enlace de datos

Apoyando y conectando los servicios de las capas superiores

La capa de enlace de datos es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. El nivel de enlace (del inglés data link level) es el segundo nivel del modelo OSI. Recibe peticiones del nivel de red y utiliza los servicios del nivel físico.

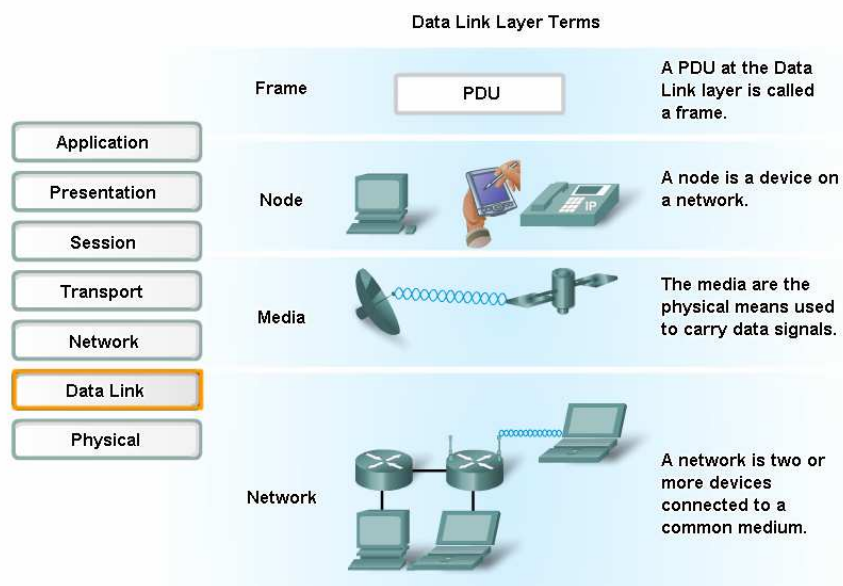
El objetivo del nivel de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a conexión). Para lograr este objetivo tiene que montar bloques de información (llamados tramas en este nivel), dotarles de una dirección de nivel de enlace, gestionar la detección o corrección de errores, y ocuparse del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento).

Cuando el medio de comunicación está compartido entre más de dos equipos es necesario arbitrar el uso del mismo. Esta tarea se realiza en el subnivel de acceso al medio. Dentro del grupo de normas IEEE 802, el subnivel de enlace lógico se recoge en la norma IEEE 802.2 y es común para todos los demás tipos de redes (Ethernet o IEEE 802.3, IEEE 802.11 o Wi-Fi, IEEE 802.16 o WiMAX, etc.); todas ellas especifican un subnivel de acceso al medio así como un nivel físico distintos.

Otro tipo de protocolos de nivel de enlace serían PPP (Point to point protocol o protocolo punto a punto), HDLC (High level data link control o protocolo de enlace de alto nivel), por citar dos.

En la práctica el subnivel de acceso al medio suele formar parte de la propia tarjeta de comunicaciones, mientras que el subnivel de enlace lógico estaría en el programa adaptador de la tarjeta (driver en inglés).

Tramas



En la capa de enlace, los datos se organizan en unidades llamadas tramas. Cada trama tiene una cabecera que incluye una dirección e información de control y una cola que se usa para la detección de errores.

La cabecera de una trama de red de área local (LAN) contiene las direcciones físicas del origen y el destino de la LAN. La cabecera de una trama que se transmite por una red de área extensa (WAN) contiene un identificador de circuito en su campo de dirección.

Recuerde que un enlace es una red de área local, una línea punto a punto o alguna otra facilidad de área extensa por la que se pueden comunicar los sistemas mediante un protocolo de la capa de enlace de datos.

9.2 Funciones de la Capa de Enlace

La Capa de enlace de datos es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. La transmisión de datos la realiza mediante tramas que son las unidades de información con sentido lógico para el intercambio de datos en la capa de enlace. También hay que tener en cuenta que en el modelo TCP/IP se corresponde a la segunda capa

Sus principales funciones son:

- Iniciación, terminación e identificación.
- Segmentación y bloqueo.
- Sincronización de octeto y carácter.
- Delimitación de trama y transparencia.
- Control de errores.
- Control de flujo.
- Recuperación de fallos.
- Gestión y coordinación de la comunicación.

Iniciación, terminación e identificación

La función de iniciación comprende los procesos necesarios para activar el enlace e implica el intercambio de tramas de control con el fin de establecer la disponibilidad de las estaciones para transmitir y recibir información. Las funciones de terminación sirven para liberar los recursos ocupados hasta la recepción/envío de la última trama. La identificación es para saber a que terminal se debe enviar una trama o para conocer quien envía la trama. Se lleva a cabo mediante la dirección del nivel de enlace.

Segmentación y bloqueo

La segmentación surge por la longitud de las tramas ya que si es muy extensa, se debe de realizar tramas más pequeñas con la información de esa trama excesivamente larga.

Si estas tramas son excesivamente cortas, se ha de implementar unas técnicas de bloque que mejoran la eficiencia y que consiste en concatenar varios mensajes cortos de nivel superior en una única trama de nivel de enlace más larga.

Sincronización de octeto y carácter

En las transferencias de información en el nivel de enlace es necesario identificar los bits y saber que posición les corresponde en cada carácter u octeto dentro de una serie de bits recibidos.

Esta función de sincronización comprende los procesos necesarios para adquirir, mantener y recuperar la sincronización de carácter u octeto. Es decir, poner en fase los mecanismos de codificación del emisor con los mecanismos de decodificación del receptor.

Delimitación de trama

La capa de enlace debe de ocuparse de la delimitación y sincronización de la trama. Para la sincronización puede usar 3 métodos, el primero de ellos es Principio y fin (caracteres específicos para identificar el principio o el fin de cada trama). También se puede usar Principio y cuenta (Utiliza un carácter para indicar comienzo y seguido por

un contador que indica su longitud). Por último se puede usar el Guión (Se emplea una agrupación específica de bits para identificar el principio y fin mediante banderas/flags).

Control de errores

Proporciona detección y corrección de errores en el envío de tramas entre las computadoras, y provee el control de la capa física. Sus funciones, en general, son:

- Identificar Trama de datos
- Códigos detectores y correctores de error
- Control de flujo
- Gestión y coordinación de la comunicación.

Para la Identificación de tramas puede usar distintas técnicas como:

9.3. Contador de caracteres

Caracteres de inicio y final con caracteres de relleno

Secuencia de bits indicadora de inicio y final, con bits de relleno

El control de flujo es necesario para no 'agobiar' al receptor. Se realiza normalmente a nivel de transporte, también a veces a nivel de enlace. Utiliza mecanismos de retroalimentación. Suele ir unido a la corrección de errores y no debe limitar la eficiencia del canal.

Los métodos de control de errores son básicamente 2:

- FEC o corrección de errores por anticipado y no tiene control de flujo
- ARQ: Posee control de flujo mediante parada y espera, o/y ventana deslizante.

Las posibles implementaciones son:

Parada y espera simple:

El emisor envía trama y espera una señal del receptor para enviar la siguiente señal o la que acaba de enviar en caso de error.

Envío continuo y rechazo simple:

El emisor envía continuamente las tramas y el receptor las va validando. Si encuentra una trama errónea, elimina todas las posteriores y pide al emisor que envíe a partir de la trama errónea.

Envío continuo y rechazo selectivo:

Transmisión continua salvo que solo retransmite la trama defectuosa.

La detección de errores la realiza mediante diversos tipos de códigos del que hay que resaltar:

CRC (códigos de redundancia cíclica)

Paridad simple

Paridad cruzada (Paridad horizontal y vertical)

Suma de verificación

La corrección de errores está basado en el Código Hamming, por repetición, verificación de paridad cruzada, Reed-Solomon y de Goyle.

También cabe destacar los protocolos HDLC que es un control de enlace de datos a alto nivel, orientado a bit y obedece a una ARQ de ventana deslizante o continuo. También existen protocolos orientados a carácter.

Control de flujo

El control de flujo es necesario para no 'agobiar' al receptor. Se realiza normalmente a nivel de la capa de transporte, también a veces a nivel de la capa de enlace. Utiliza mecanismos de retroalimentación. Suele ir unido a la corrección de errores y no debe limitar la eficiencia del canal.

El control de flujo conlleva dos acciones importantísimas que son la detección de errores y la corrección de errores.

La detección de errores se utiliza para detectar errores a la hora de enviar tramas al receptor e intentar solucionarlos. Se realiza mediante diversos tipos de códigos del que hay que resaltar el CRC (códigos de redundancia cíclica), simple paridad (puede ser par, números de 1's par, o impar) paridad cruzada (Paridad horizontal y vertical).

Suma de verificación

La corrección de errores surge a partir de la detección para corregir errores detectados y necesitan añadir a la información útil un número de bits redundantes bastante superior al necesario para detectar y corregir. Sus técnicas son variadas. El Código Hamming, Repetición, que cada bit se repite 3 veces y en caso de fallo se toma el bit que más se repite; También puede hacerse mediante verificación de paridad cruzada, Reed-Solomon y de Goyle.

También cabe destacar los protocolos HDLC que es un protocolo de control de enlace de datos a alto nivel, orientado al bit y obedece a una ARQ de ventana deslizante. También existen protocolos orientados a carácter.

Recuperación de fallos

Se refiere a los procedimientos para detectar situaciones y recuperarse de situaciones anómalas como la ausencia de respuesta, recepción de tramas inválidas. Las situaciones mas típicas son la pérdida de tramas, aparición de tramas duplicadas y llegada de tramas fuera de secuencia.

Si no se tratasen correctamente estos eventos se perderán información y se aceptarán datos erróneos como si fuesen correctos.

Generalmente se suelen utilizar contadores para limitar el número de errores o reintentos de los procesos y procedimientos. También se pueden usar temporizadores para establecer plazos de espera (timeout) de los sucesos.

Autoevaluación

1. ¿Qué protocolos están definidos para trabajar en la capa de enlace de datos?
2. Identificar las funciones de la capa de enlace de datos
3. Brevemente definir Control de Flujo
4. Identificar Suma de verificación de error

Para recordar

La capa de enlace de datos es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. El nivel de enlace (del inglés data link level) es el segundo nivel del modelo OSI. La cabecera de una trama de red de área local (LAN) contiene las direcciones físicas del origen y el destino de la LAN. La cabecera de una trama que se transmite por una red de área extensa (WAN) contiene un identificador de circuito en su campo de dirección.

La Capa de enlace de datos es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. La capa de enlace debe ocuparse de la delimitación y sincronización de la trama. Para la sincronización puede usar 3 métodos, el primero de ellos es Principio y fin (caracteres específicos para identificar el principio o el fin de cada trama).

La capa de enlace debe ocuparse de la delimitación y sincronización de la trama. Para la sincronización puede usar 3 métodos, el primero de ellos es Principio y fin (caracteres específicos para identificar el principio o el fin de cada trama).

La Capa de enlace de datos es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos.



Capa Física del Modelo OSI

TEMA

- Capa Física del modelo OSI

OBJETIVOS ESPECÍFICOS

- Describir la estructura de la capa física del modelo OSI
- Identificar los tipos de señalización
- Identificar los tipos de códigos

CONTENIDOS

- Capa Física del Modelo OSI
- Tecnologías de la capa física y hardware
- Señalizando bits para el medio
- Codificando - Agrupando bits

10. Capa Física del Modelo OSI

10.1.1 La capa física – Propósito

La capa física del modelo OSI proporciona la manera para transportar a través del medio de red los bits que son construidos en la capa de enlace de datos como una trama o frame.

Esta capa acepta un frame completo desde la capa de enlace de datos y lo codifica como una serie de señales que son transmitidas dentro del medio local. La codificación de los bits que comprende un frame es recibido por cualquier dispositivo final o dispositivo intermediario.

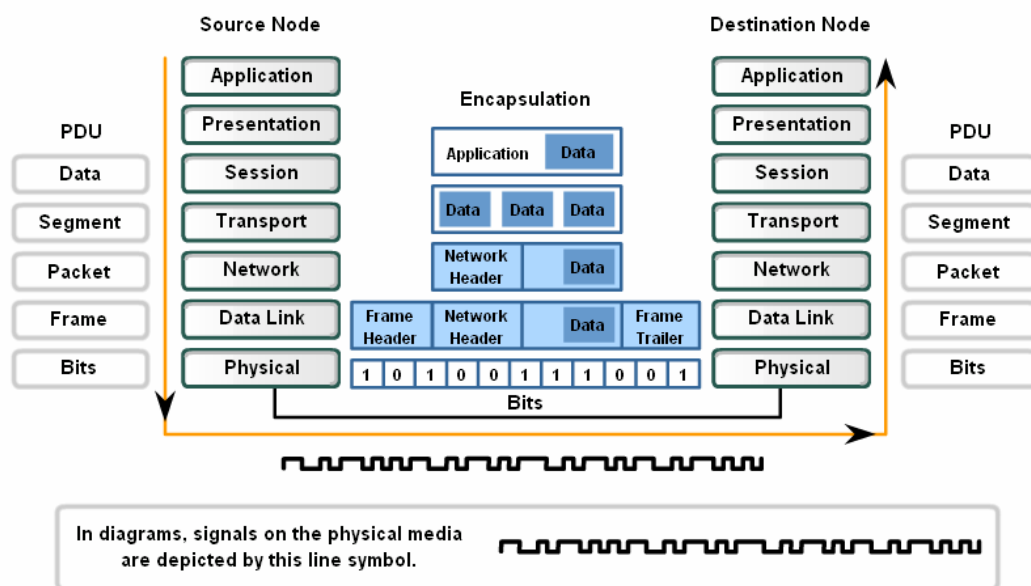
La entrega de frames a través del medio local requiere los siguientes elementos en la capa física:

- El medio físico y los conectores asociados
- Una representación de bits en el medio
- Codificar la data y la información de control
- Los circuitos de transmisión y recepción en los dispositivos de red

A estas alturas del proceso de comunicación, los datos del usuario han sido segmentados por la capa de transporte, ubicada dentro de los paquetes en la capa de red, y adicionalmente han sido encapsulados como frames por la capa de Enlace de datos. El propósito de la capa física es convertir los bits en señales eléctricas, ópticas, o en microondas que representa a los bits en cada frame. Estas señales son entonces las que se enviarán a través del medio.

Es también trabajo de la capa física rescatar estas señales individuales desde el medio, restaurarlas a partir de sus representaciones de bits, y pasar los bits hacia arriba a la capa de Enlace de datos como un frame completo.

Transforming Human Network Communications to Bits



10.1.2 La capa física - Operación

Los medios no lleva el frame como una sola entidad, el medio lleva las señales, una a la vez, para representar los bits que forman el frame.

Hay tres formas básicas de medios de red en el cual la data es representada:

- El cable de cobre
- La fibra óptica
- Medio Inalámbrico

La representación de los bits - esto es, el tipo de señal - depende del tipo de medio. Para el medio con cables de cobre, las señales son patrones de pulsos eléctricos. Para la fibra óptica, las señales son patrones de luz. Para el medio inalámbrico, las señales son patrones de radio transmisiones.

Identificar una trama

Cuando la capa física codifica los bits para un medio particular, también debe distinguir acerca de donde termina un frame termina y empieza el siguiente frame. De otra manera, los dispositivos en los medios no reconocerían un frame cuando esté siendo recibido. De otra manera, el dispositivo de destino sólo recibiría una cadena de señales y no podría reconstruir correctamente el frame. Indicar el comienzo de una trama es a menudo una función de la capa enlace de datos. Sin embargo, en muchas tecnologías, la capa física puede agregar sus propias señales para indicar donde comienza y donde termina un frame.

Para permitir que un dispositivo receptor pueda reconocer claramente el límite del frame, el dispositivo transmisor añade señales para designar el principio y el fin de un frame. Estas señales representan bits en particular que son usados para identificar el principio o fin de un marco.

El proceso de codificación de un marco de datos desde los bits lógicos dentro de las señales físicas en el medio, y las características de medios físicos en particular, están cubiertas en detalle en las siguientes secciones de este capítulo.

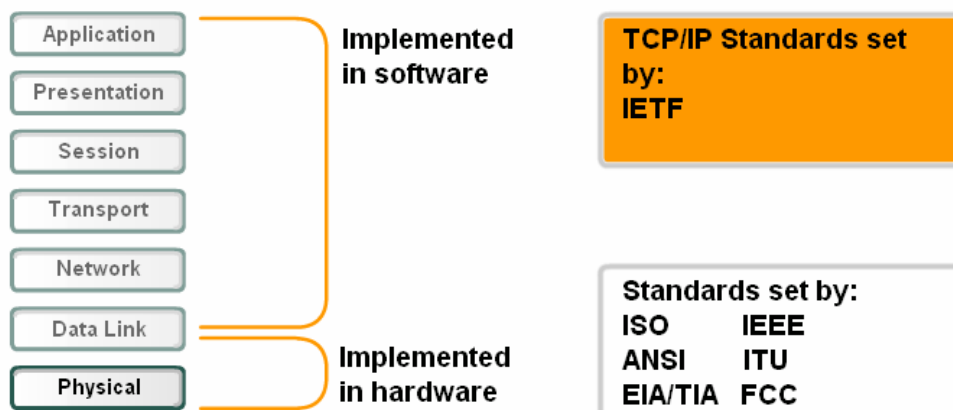
Estándares

El medio físico consta del hardware, desarrollado por los diseñadores, bajo la forma de circuitos electrónicos, el medio, y los conectores. Por consiguiente, es apropiado que las normas que gobiernan este hardware estén definidas por las organizaciones del tipo IEEE. En contraste, los protocolos y las operaciones de las capas superiores de OSI que están hechas por software son diseñados por ingenieros informáticos y científicos de computadoras. Como se vio en anteriores capítulos, los servicios y los protocolos en la suite del TCP/IP están definidos por la Fuerza de trabajo de la Internet (IETF) en los documentos técnicos denominados RFCs.

Parecidas a las tecnologías asociadas con la capa de enlace de datos, las tecnologías de la capa física están definidas por organizaciones tales como:

- La organización internacional para la estandarización (ISO)
- Instituto de ingenieros electricistas y eléctricos (IEEE)
- El instituto americano de estándares (ANSI)
- La unión internacional de telecomunicaciones (ITU)
- La alianza industrial eléctrica /la asociación internacional de telecomunicaciones (EIA/TIA)

Comparison of Physical Layer Standards and Upper Layer Standards



Tecnologías de la capa física y hardware

Las tecnologías definidas por estas organizaciones incluyen cuatro áreas de la capa física:

- Propiedades del medio físico y eléctrico.
- Las propiedades mecánicas (materiales, dimensiones, pines de salida) de los conectores.
- La representación de los bits por medio de señales (la codificación).
- La definición de las señales de control de información.
- Los componentes del hardware tales como adaptadores de red (NICs), interfaces, conectores, cables, y los diseños del cable son todos especificados en las normas de la capa física.

Principios fundamentales de la capa física

Las tres funciones fundamentales de la capa física son:

- Los componentes físicos
- Los datos codificados
- Señalización

Los elementos físicos son los dispositivos físicos electrónicos, el medio, conectores y las señales representadas bajo la forma de bits.

La codificación

La codificación es un método para convertir un flujo de bits de data dentro de un código predefinido. Los códigos son agrupamientos de bits usados para proveer un patrón previsible que puedan ser reconocidos por el receptor y el remitente. Usar patrones previsible ayuda a distinguir los bits de data de los bits de control y proporciona mejor detección de error en el medio.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proveer códigos para los propósitos de control como identificar el comienzo y el fin de un frame. El host transmisor transmitirá el patrón específico de bits o un código para identificar el comienzo y el fin del frame.

Señalización

La capa física debe generar señales eléctricas, ópticas, o inalámbricas que representan 1 y "0" en los medios. El método para representar los bits es llamado el

método de señalización. Las normas de la capa física deben definir lo que representa el tipo de señal un “1” y un “0”. Esto puede ser tan simple como un cambio en el nivel de una señal eléctrica o el pulso óptico o un más complicado método de señalización.

Señalización y codificación: Representando los bits

Eventualmente, toda comunicación desde la red humana se convierte en dígitos binarios, que son transportados individualmente a través del medio físico

Aunque todos los bits que forman un frame son representados por la capa física como una unidad, la transmisión del frame a través del medio ocurre como una corriente de bits enviados uno cada vez. La capa física representa cada uno de los bits en el frame como una señal. Cada señal es ubicada encima del medio que especifica una cantidad de tiempo para ocupar el medio, esto es denominado como en bit de tiempo. Las señales son procesadas por el dispositivo receptor y convertidas a una representación de bits.

El nodo receptor de la capa física, convierte las señales nuevamente en bits. Los bits son entonces examinados por la trama de inicio y final para determinar que un marco completo ha sido recibido, la capa física luego envía todos los bits del frame a la capa de Enlace de datos.

La entrega exitosa de los bits requiere algún método de sincronización entre el equipo transmisor y receptor. La representación de las señales de bits deben ser examinados en un tiempo específico durante el tiempo de bit para determinar si han sido leídos correctamente, es decir si la señal representada es un “1” o un “0”. La sincronización se realiza mediante el uso de un reloj. En las redes LAN, cada fin de la transmisión mantiene su propio reloj. Muchos métodos de señalización usan transiciones previsibles en la señal para proporcionar la sincronización entre los relojes de los transmisores y los dispositivos receptores.

Métodos de señalización

Los bits son representados en el medio cambiando uno o más de las siguientes características de una señal:

- Amplitud
- Frecuencia
- Fase

La naturaleza de las señales actuales representan los bits en el medio dependerá del método de señalización usado. Algunos métodos pueden usar un atributo de señal para representar un solo 0 y usar otro atributo de señal para representar un solo 1.

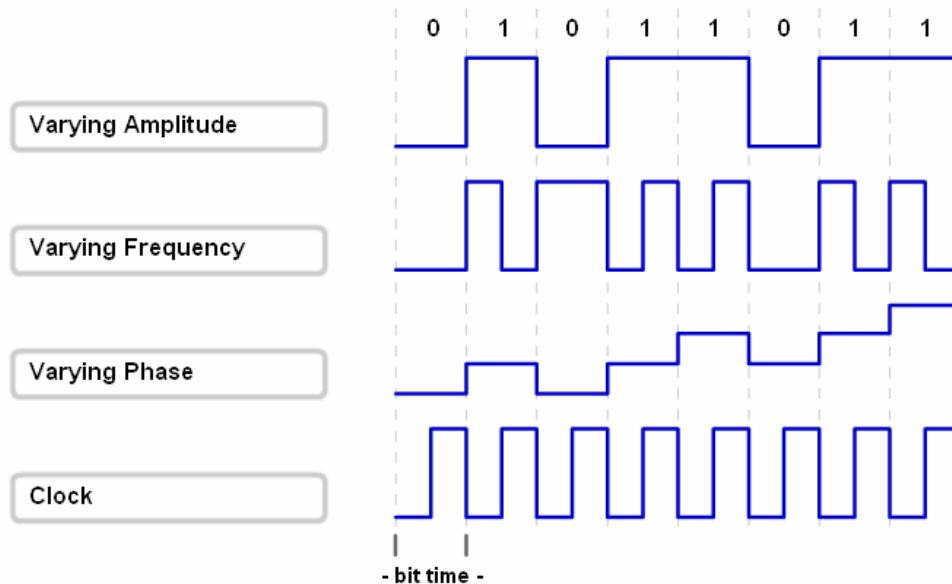
Por poner un ejemplo, con un no-retorno a Zero (NRZ), un 0 quizás puede ser representado por un nivel de voltaje en el medio durante el bit de tiempo y un 1 podría ser representado por un voltaje diferente en el medio durante el bit de tiempo.

Hay también métodos de señalización que usan transiciones, o la ausencia de transiciones, indicar un nivel lógico. Por ejemplo, la codificación Manchester indica un 0 por la transmisión de un voltaje alto a uno bajo en la mitad del bit de tiempo. Para un 1 la transmisión es un voltaje bajo aún alto en la mitad del bit de tiempo.

El método de señalización usado debe ser compatible con un estándar a fin de que el receptor pueda detectar las señales y los puede descifrar. El estándar contiene un contrato entre el transmisor y el receptor de cómo representar 1s y 0s. Si sino ahí contrato en la señalización - esto ocasionaría normas diferentes usadas en cada dispositivo final y la comunicación a través del medio físico fallará.

Los métodos de señalización para representar los bits en el medio pueden ser complejos. Miremos dos técnicas muy simples para ilustrar el concepto.

Ways to Represent a Signal on the Medium



10.2.1 Señalizando bits para el medio

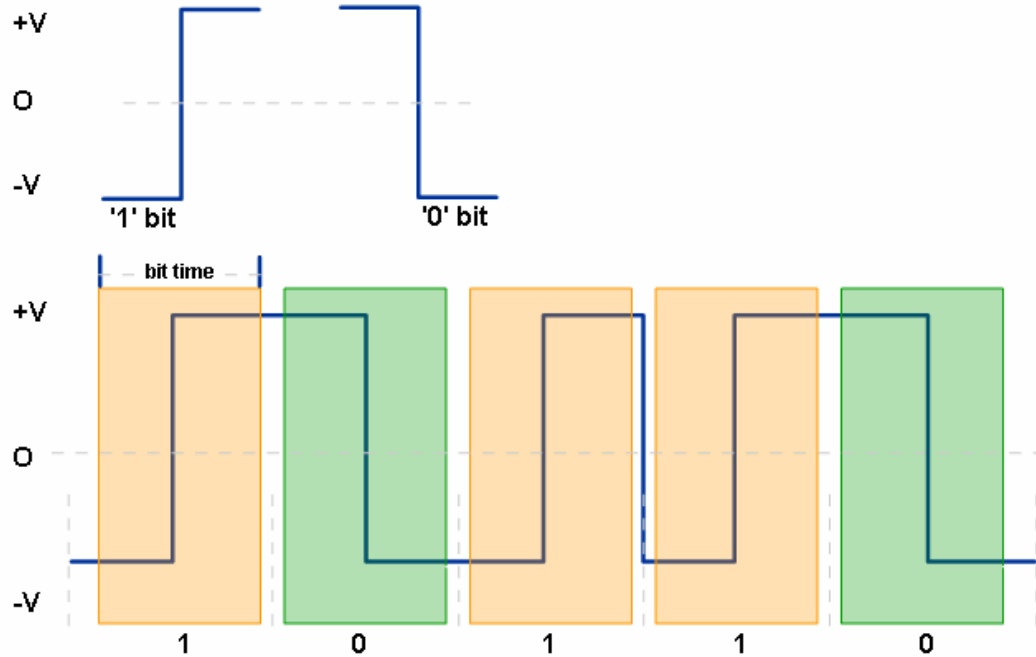
Señalización NRZ

Este código, se denomina **NRZ** porque el voltaje no vuelve a cero entre los bits consecutivos de valor uno. Mediante la asignación de un nivel de tensión a cada símbolo se simplifica la tarea de codificar un mensaje. Esta es la teoría que desarrolla el código NRZ (non return to zero). La codificación en banda base se considera como una disposición diferente de los bits de la señal on/off, de este modo se adapta la señal al sistema de transmisión utilizado. Para ello se emplean los códigos tipo NRZ. Una clasificación atendiendo a las modulaciones situaría el código NRZ dentro de las portadoras digitales y los moduladoras digitales como los códigos Manchester, Bifase, RDSI, etc... Atendiendo a la forma de onda binaria se pueden clasificar estos códigos como unipolares (el voltaje que representa los bits varía entre 0 voltios y +5 voltios).

Codificación Manchester

La codificación Manchester, también denominada codificación bifase-L, es un método de codificación eléctrica de una señal binaria en el que en cada tiempo de bit hay una transición entre dos niveles de señal. Es una codificación autosincronizada, ya que en cada bit se puede obtener la señal de reloj, lo que hace posible una sincronización precisa del flujo de datos. Una desventaja es que consume el doble de ancho de banda que una transmisión asíncrona. Hoy en día hay numerosas codificaciones (8B/10B) que logran el mismo resultado pero consumiendo menor ancho de banda que la codificación Manchester. La codificación Manchester se usa en muchos estándares de telecomunicaciones, como por ejemplo Ethernet.

Signaling Bits for Transmission Manchester Encoding



10.2.2 Codificando - Agrupando bits

En el capítulo anterior, describimos el proceso de señalización como la manera en que los bits están representados en el medio físico. En esta sección, usamos la codificación de palabra para representar el agrupamiento simbólico de bits que van a presentados en el medio al usar un paso de codificación las señales son colocadas en el medio, mejoramos la eficiencia en la transmisión de data de alta velocidad.

Como usamos velocidades superiores en el medio, tenemos la posibilidad que los datos puedan estar corruptos al usar grupos de codificación, podemos detectar errores más eficazmente. Adicionalmente, como la demanda para la velocidad de datos se incrementa, buscamos formas para representar más datos a través del medio, transmitiendo menos bits los grupos de codificación brindan un método para crear la representación de data.

La capa física de un dispositivo de red necesita poder detectar señales de data legítimas e ignorar señales aleatorias que quizás también estén en el medio físico. La corriente de señales es transmitida de una manera que el receptor reconozca el comienzo y el fin de la trama.

La señal Patrón

Una forma de proporcionar la detección de la trama es empezar cada trama con un patrón de señales que denoten el principio de un frame. Otro patrón de bits similar enviará señales de fin de trama. Las señales de aquellos bits que no están en la trama son ignoradas por la capa física de este siendo usada.

Los grupos de código

Las técnicas de codificación usan patrones de bit llamados símbolos. La capa física usa un juego de símbolos de codificación- llamado grupos de códigos - para representar datos codificados o controlar la información. Un grupo de código es una secuencia consecutiva de código de bits que son interpretados y enviados como los patrones de bits de datos. Por ejemplo, el código de bits 10101 podrían representar los bits de datos 0011.

Los grupos de código son a menudo utilizados como una técnica intermediaria de codificación para las tecnologías LAN de alta velocidad. Este paso ocurre en la capa física antes de generar las señales de voltajes, los pulsos de luz, o las radiofrecuencias. Al transmitir los símbolos, las capacidades de detección de error y sincronización entre dispositivos transmisores y receptores son mejoradas. Éstas son consideraciones importantes en la transmisión de alta de velocidad sobre el medio.

Aunque usar grupos de código introduce una sobrecarga por los bits adicionales que se transmitirán, mejoran la robustez de los enlaces de comunicación. Esto es particularmente cierto para la transmisión de datos en altas velocidades.

Las ventajas usar grupos de código incluyen:

- Reducido error en el nivel de los bits.
- Limitar la energía efectiva transmitida dentro del medio.
- Ayudar a distinguir los bits de datos de los bits de control.
- Mejorar la detección de errores en el medio.

Para detectar adecuadamente los bits individual como un 0 o como un 1, el receptor debe saber cómo y cuando testear la señal en el medio. Esto requiere que el tiempo entre el receptor y el transmisor esté sincronizado. En muchas tecnologías de la capa física, las transiciones en los medios son usados para efectuar esta sincronización. Si por alguna razón los patrones de bits que están siendo transmitidos en el medio no crean transiciones frecuentes, esta sincronización quizás se pierda y pueden ocurrir errores de bit.

Limitar la energía transmitida

En muchos grupos de código, los símbolos aseguran que el número de 1s y 0s en una cadena de símbolos sean simétricos. El proceso de balancear el número de 1s y 0s transmitidos es llamado balanceo DC. Esto impide que cantidades excesivas de energía sean inyectados desde los medios durante la transmisión de los datos, por consiguiente esto reduce la interferencia radiada desde los medios. En muchos métodos de señalización del medio, a un nivel lógico, como por ejemplo un 1, se le representa por la presencia de energía siendo así enviado en el medio, mientras el nivel lógico opuesto, un 0, está representado como la ausencia de energía. Esto es muy importante pues transmitir una serie larga de 1s podría recalentar el láser transmisor y los fotodiodos en el receptor, y esto potencialmente causaría tasas de error superiores.

Distinguir la data de control

Los grupos de código tienen tres tipos de símbolos:

Símbolos de data:

Símbolos están presentes en el frame de datos y son enviados abajo a la capa física.

Símbolos de control:

Códigos especiales inyectados por la capa física usados para controlar la transmisión. Esto incluye el final del frame y los símbolos idle.

Símbolos inválidos:

Los símbolos que no tienen patrones permitido en el medio. La recepción de un símbolo inválido indica un error del frame.

Los símbolos codificados encima de un medio único

Los símbolos representan la data que está siendo enviado a través de la red y tiene diferentes patrones de bits usados para el control. Estas diferencias permiten a la capa física en el nodo receptor distinguir inmediatamente la data de la información de control.

Capacidad de transmisión de datos

Diferentes medios físicos soportan la transferencia de bits a diferentes velocidades. La velocidad de transferencia se puede medir de tres maneras:

- Ancho de banda
- El rendimiento específico
- Goodput

Ancho de banda

La capacidad de un medio para transmitir datos está descrita como el ancho de banda total de datos en el medio. El ancho de banda digital mide la cantidad de información que puede fluir de un lugar a otro en un tiempo dado. El ancho de banda está típicamente medido en kilobits por segundo (kilobits por segundo) o megabits por segundo (megabits por segundo).

El ancho de banda típico de una red es determinado por una combinación de factores: Las características del medio físico y las tecnologías escogido para la señalización y detección de señales de red. Las propiedades físicas del medio, las actuales tecnologías, y todas las leyes físicas juegan un rol para determinar la disponibilidad del ancho de banda.

El rendimiento específico

El rendimiento específico es medido por la transferencia de bits a través del medio sobre un período de tiempo dado. Debido a varios factores, el rendimiento específico usualmente no hace juego con el ancho de banda especificado en las implementaciones de la capa física como Ethernet.

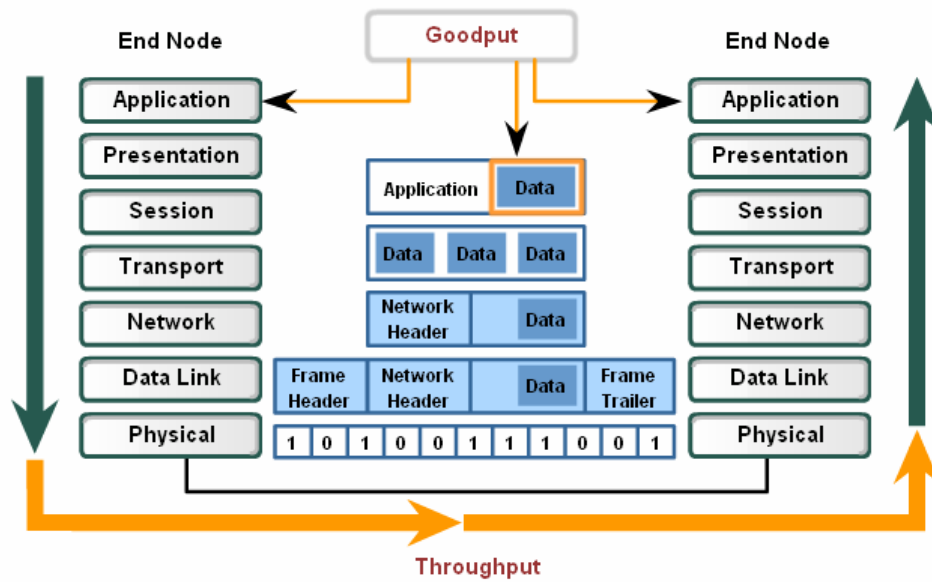
Muchos factores influyen el rendimiento específico. Entre estos factores esta la cantidad de tráfico, el tipo de tráfico, y el número de red que los dispositivos encontraran en la red. En una topología de acceso múltiple como Ethernet, los nodos compiten por el acceso al medio y su uso. Por consiguiente, el rendimiento específico de cada nodo es degradado por la cantidad de incrementos en el medio.

Goodput

Una tercera medida ha sido creada para medir la transferencia de data utilizable. Esa medida es conocida como el Goodput, el cual es la medida de datos utilizables sobre un período de tiempo dado, y es por consiguiente la medida de mayor interés en la red por parte de los usuarios.

Por poner un ejemplo, considere a dos hosts en una LAN transfiriendo un archivo. El ancho de banda de la LAN es de 100 mbps. Debido al uso compartido y la sobrecarga del medio, entre las computadoras se tiene solamente un ancho de banda de 60 mbps, si a esto le agregamos la sobrecarga del proceso de encapsulamiento del stack TCP/IP, la tasa real de datos recibidos por la computadora destino es de sólo 40Mbps de Goodput.

Data Throughput and Goodput



Data **throughput** is actual network performance. **Goodput** is a measure of the transfer of usable data after protocol overhead traffic has been removed.

Autoevaluación

1. ¿Por qué es importante la data de control que se incorpora en las tramas Ethernet?
2. Brevemente definir:
 - a. Ancho de banda
 - b. Goodput
 - c. Troughput
3. ¿Por qué es importante incorporar códigos de línea para el proceso de transmisión de datos?
4. Identificar y graficar los códigos NRZI, NRZ, Bipolar AMI y 4B/5B

Para recordar

Cuando la capa física codifica los bits para un medio particular, también debe distinguir acerca de donde termina un frame termina y empieza el siguiente frame. De otra manera, los dispositivos en los medios no reconocerían un frame cuando esté siendo recibido. De otra manera, el dispositivo de destino sólo recibiría una cadena de señales y no podría reconstruir correctamente el frame.

El medio físico consta del hardware, desarrollado por los diseñadores, bajo la forma de circuitos electrónicos, el medio, y los conectores. Por consiguiente, es apropiado que las normas que gobiernan este hardware estén definidas por las organizaciones del tipo IEEE.

La codificación es un método para convertir un flujo de bits de data dentro de un código predefinido. Los códigos son agrupamientos de bits usados para proveer un patrón previsible que puedan ser reconocidos por el receptor y el remitente. Usar patrones previsibles ayuda a distinguir los bits de data de los bits de control y proporciona mejor detección de error en el medio.

La capa física debe generar señales eléctricas, ópticas, o inalámbricas que representan 1 y "0" en los medios.



Principios básicos de Ethernet

Parte I

TEMA

- Principios básicos de Ethernet - Parte I

OBJETIVOS ESPECÍFICOS

- Describir os principios básicos de la tecnología Ethernet
- Identificar la relación entre Ethernet y el modelo OSI
- Describir la estructura de la trama Ethernet

CONTENIDOS

- Introducción a Ethernet
- Ethernet y el Modelo OSI
- Estructura de la trama de Ethernet

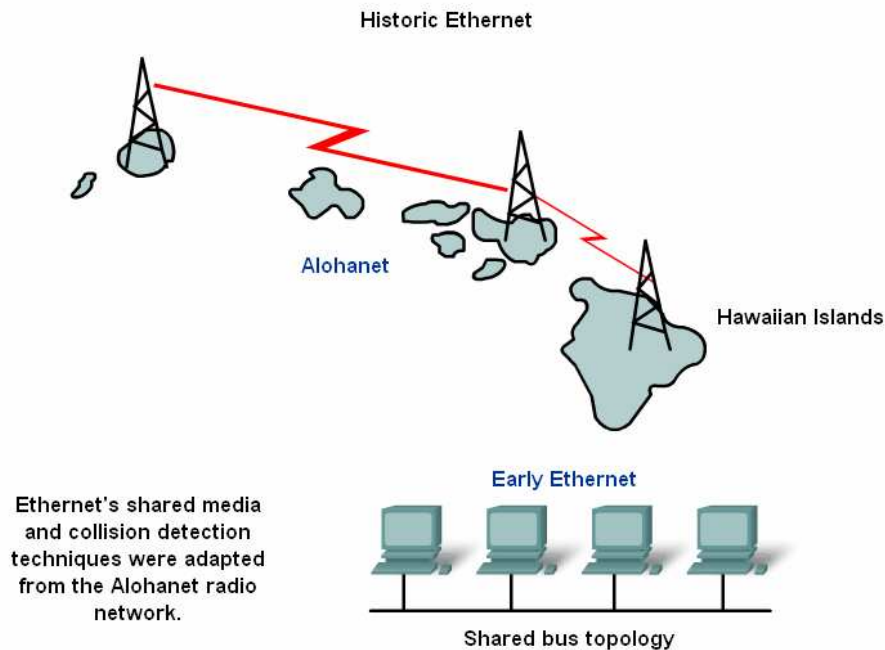
11.1 Introducción a Ethernet

El protocolo Ethernet ha evolucionado para satisfacer la creciente demanda de las redes LAN de alta velocidad, tanto así que la mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet.

El éxito de Ethernet se debe a los siguientes factores:

- Sencillez y facilidad de mantenimiento
- Capacidad para incorporar nuevas tecnologías
- Confiabilidad
- Bajo costo de instalación y de actualización

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales transmitidas interfirieran entre sí. La primera LAN del mundo fue la versión original de Ethernet. Sin embargo, el mérito mayor se le debe a Robert Metcalfe quien con sus compañeros de Xerox la diseñaron hace ya más de treinta años. Sin embargo la idea original fue desarrollado en la Universidad de Hawaii, donde se desarrollo la Alohanet. Alohanet fue una red de radio diseñada para transmitir información sobre ondas de radiofrecuencia entre las islas de Hawaii.



En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802.

El estándar con el que se identifica a Ethernet es el 802.3, que fue el nombre que la IEEE para asegurar que sus estándares fueran compatibles con el modelo OSI de la

Organización Internacional de Estándares (ISO). Para este fin, se realizaron pequeñas modificaciones al estándar original de Ethernet, dando cuerpo al 802.3. Sin embargo, cualquier tarjeta de red Ethernet (NIC) puede transmitir y recibir tanto tramas de Ethernet como de 802.3. Básicamente, Ethernet y IEEE 802.3 son un mismo estándar.

En 1995, el IEEE anunció un estándar para la Ethernet de 100 Mbps, el FastEthernet. Más tarde, en 1998 y 1999 siguieron los estándares para Ethernet de un gigabit por segundo.

Una trama de Ethernet puede partir desde una antigua NIC de 10 Mbps de cable coaxial de un PC, subir a un enlace de fibra de Ethernet de 10 Gbps y terminar en una NIC de 100 Mbps. Siempre que permanezca en redes de Ethernet, el paquete no cambia.

11.2 Reglas del IEEE para la denominación de Ethernet

Es importante recalcar que Ethernet no es una tecnología para networking, sino una familia de tecnologías para networking que incluye Legacy Ethernet , Fast Ethernet y Gigabit Ethernet.

El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet.

Siempre que es necesario expandir Ethernet para agregar un nuevo medio o capacidad, el IEEE publica un nuevo suplemento del estándar 802.3

La descripción abreviada consta de:

- Un número que indica el número de Mbps que se transmiten.
- La palabra "base", que indica que se utiliza la señalización banda base.
- Una o más letras del alfabeto que indican el tipo de medio utilizado (F = cable de fibra óptica, T = par trenzado de cobre no blindado).

10 BASE 10

100 BASE TX

Ethernet emplea señalización banda base, lo que significa que utiliza todo el ancho de banda del medio de transmisión. La data es transmitida directamente sobre el medio de transmisión sin efectuar ningún tipo de modulación.

11.3 Ethernet y el Modelo OSI

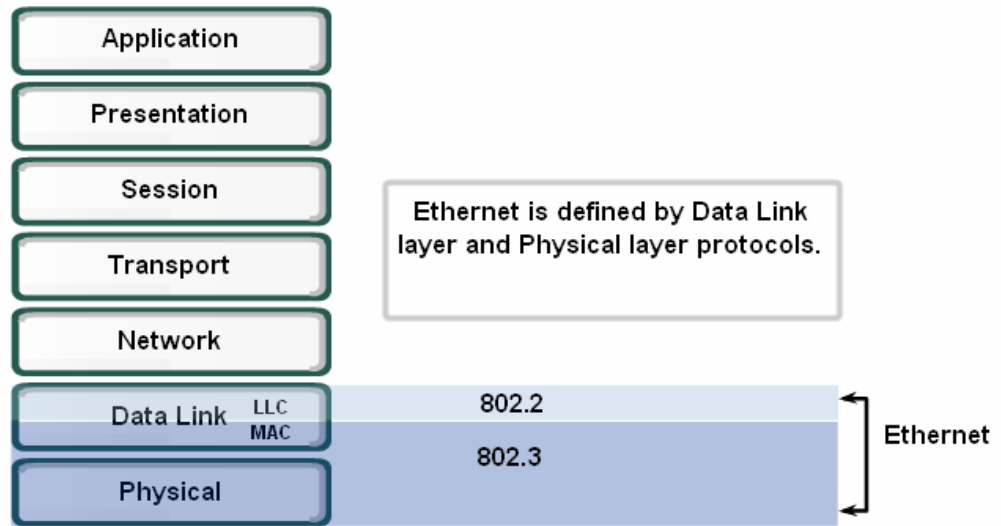
Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física.

Para mover datos de una estación Ethernet a otra, a menudo, estos pasan a través de un repetidor. En este caso todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor.

Un dominio de colisión es un recurso compartido. Los problemas que se originan en una parte del dominio de colisión, generalmente, tienen impacto en todo el dominio.

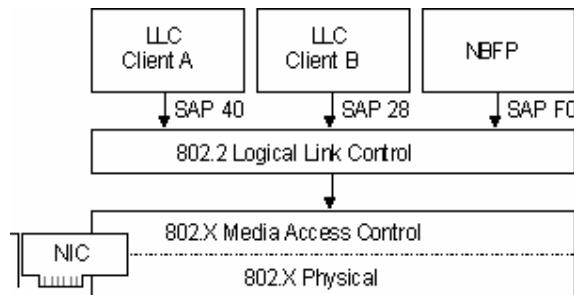
Las estaciones separadas por repetidores se encuentran dentro del mismo dominio de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes.

Ethernet



La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones. La Capa 2 se ocupa de estas limitaciones.

La subcapa MAC trata los componentes físicos que se utilizarán para comunicar la información. La subcapa de Control de Enlace Lógico (LLC) sigue siendo relativamente independiente del equipo físico que se utiliza en el proceso de comunicación.



Capa 1 vs Capa2

Capa 1 Características	Capa 2 Características
No se comunica con las capas de niveles superiores	Se comunica con las capas superiores Con LLC (Control de Enlace Lógico)
No identifica computadoras	Maneja un proceso de direccionamiento
Solo describe corriente de bits	Organiza la data bajo la forma de tramas
No identifica la computadora que transmitirá los datos binarios.	Utiliza la técnica de Control de Acceso al Canal (MAC).

Logical Link Control (LLC)

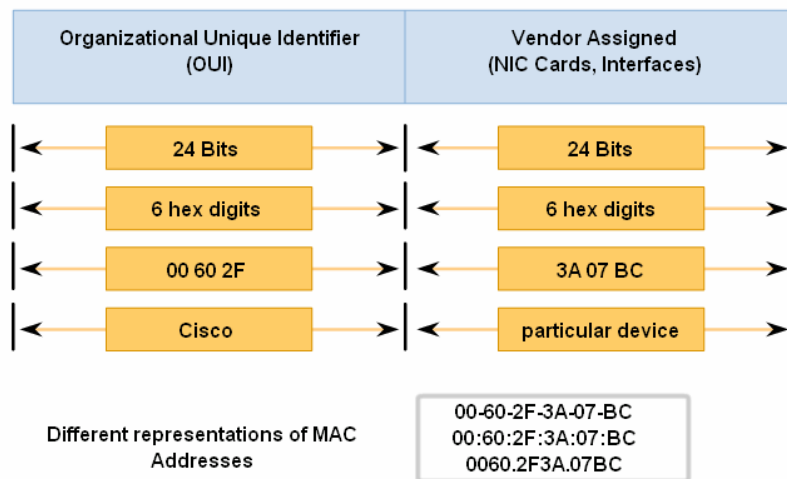
- Makes the connection with the upper layers
- Frames the Network layer packet
- Identifies the Network layer protocol
- Remains relatively independent of the physical equipment

Logical Link Control Sublayer								
802.3 Media Access Control								
Physical Signaling Sublayer	10BASE5 (500m) 50 Ohm Coax N-Style	10BASE2 (185m) 50 Ohm Coax BNC	10BASE-T (100m) 100 Ohm UTP RJ-45	100BASE-TX (100m) 100 Ohm UTP RJ-45	1000BASE-CX (25m) 150 Ohm STP mini-DB-9	1000BASE-T (100m) 100 Ohm UTP RJ-45	1000BASE-SX (220-550m) MM Fiber SC	1000BASE-LX (550-5000m) MM or SM Fiber SC
Physical Medium								

11.4 Denominación

Para efectuar el envío local de las tramas en una red Ethernet, se debe contar con un sistema de direccionamiento, una manera de identificar a las computadoras y las interfaces de manera exclusiva. Para esto, Ethernet utiliza direcciones MAC que tienen 48 bits de largo, y se expresan como doce dígitos hexadecimales. Los primeros seis dígitos hexadecimales, son administrados por la IEEE, y permiten identificar al fabricante o al vendedor. Esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI).

The Ethernet MAC Address Structure



Direcciones MAC

Las direcciones MAC también se denominan direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la tarjeta de red.

11.4.1 Forma de la trama Ethernet

Los datos que serán enviados son organizados de una manera particular en la capa de enlace de datos, que es conocida como la trama Ethernet. El entramado ayuda a obtener información esencial que, de otro modo, no se podría obtener solamente con las corrientes de bits codificadas.

Esta información sirve para lo siguiente:

- Cuáles son los computadores que se comunican entre sí
- Cuándo comienza y cuándo termina la comunicación entre las computadoras
- Proporciona un método para detectar los errores que se produjeron durante la comunicación.

La trama esta conformada por una serie de campos que a continuación describiremos:

Preámbulo	SOF	Destino	Origen	Tipo	Datos	FCS
7 bytes	1 byte	6 bytes	6bytes	2 bytes	1500 bytes	4 bytes

Preámbulo

El preámbulo es una secuencia de bits que se utiliza para sincronizar y estabilizar al medio físico antes de comenzar la transmisión de datos. El patrón del preámbulo es:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

Estos bits se transmiten en orden de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

SOF Delimitador del inicio de la trama (Start-of-frame delimiter)

Consiste de un byte y es un patrón de unos y ceros alternados que finaliza en dos unos consecutivos (10101011), estos indica que el siguiente bit será el más significativo del campo de dirección de destino.

Aun cuando se detecte una colisión durante la emisión del preámbulo o del SOF se deben continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino

El campo de dirección destino es un campo de 48 bits (6 Bytes) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama, pudiendo ser esta la dirección de una estación, de un grupo *multicast* o la dirección de *broadcast*. Cada estación examina este campo para determinar si debe aceptar el paquete.

Tipo

El campo de tipo es un campo de 16 bits (2 bytes) que identifica el protocolo de red de alto nivel asociado con el paquete o en su defecto la longitud del campo de datos. Es interpretado en la capa de enlace de datos.

Datos

El campo de datos varia en tamaño entre 46 a 1500 Bytes. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida al nivel de red.

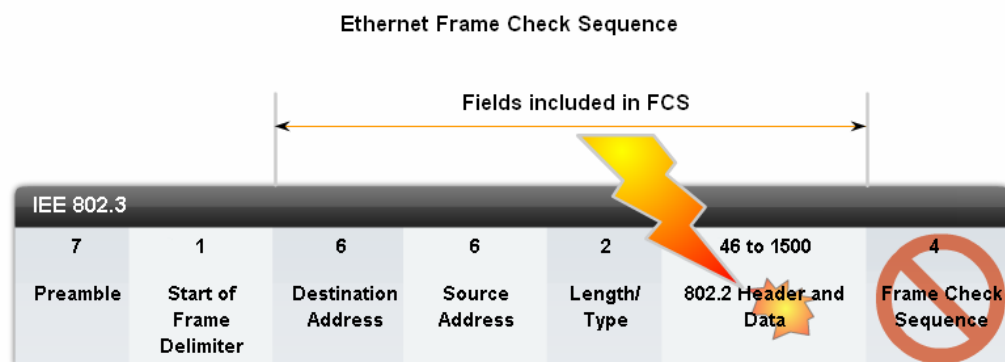
FCS

El campo Secuencia de verificación de la trama (Frame Check Sequence) contiene un valor de verificación CRC (código de redundancia cíclica) de 32 bits o 4 bytes, calculado por el dispositivo emisor en base al contenido de la trama y recalculado por el dispositivo receptor para verificar la integridad de la trama.

Existen tres formas principales para calcular el número de Secuencia de verificación de trama:

- Verificación por redundancia cíclica (CRC): Realiza cálculos en los datos.
- Paridad bidimensional: Coloca a cada uno de los bytes en un arreglo bidimensional y realiza chequeos verticales y horizontales de redundancia sobre el mismo, creando así un byte extra, que resulta en un número par o impar de unos binarios.
- Checksum (suma de verificación) de Internet: Agrega los valores de todos los bits de datos para obtener una suma.

Todos los dispositivos conectados a la red LAN Ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, routers y switches.



If the FCS calculated by the receiver (based on the contents of the received frame), does not equal the FCS calculated by the source (which is included in the frame), the frame is considered invalid and is dropped.

11.4.2 Estructura de la trama de Ethernet

La estructura de la trama es casi idéntica para todas las velocidades de Ethernet desde 10 Mbps hasta 10000 Mbps. Sin embargo, en la capa física, casi todas las versiones de Ethernet son sustancialmente diferentes las unas de las otras, teniendo cada velocidad un juego distinto de reglas de codificación.

En la versión de Ethernet desarrollada por DIX antes de la adopción de la versión IEEE 802.3 de Ethernet, el Preámbulo y el Delimitador de Inicio de Trama (SFD) se combinaban en un solo campo, aunque el patrón binario era idéntico.

El campo que se denomina Longitud/Tipo aparecía como sólo Longitud en las primeras versiones de IEEE y sólo como Tipo en la versión de DIX.

El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3.

El nodo receptor debe determinar cuál de los protocolos de capa superior está presente en una trama entrante examinando el campo Longitud/Tipo.

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence

Ethernet II es el formato de trama Ethernet utilizado en redes TCP/IP.

Autoevaluación

1 ¿Cuál del siguiente es características de una red del Token Ring? (elija dos opciones)

- a. Entorno sin colisiones
- b. No determinístico
- c. Determinístico
- d. Utiliza CSMA/CD
- e. Propensa a las colisiones

2 ¿Cuáles de las siguientes características describen lo que es el acceso múltiple con detección de portadora y detección de colisiones? (Elija dos opciones).

- a. Entorno sin colisiones
- b. No determinístico
- c. Determinístico
- d. Utiliza un método de "el primero que llega, el primero que se sirve"
- e. Utiliza un token para transmitir datos

3 ¿Cuáles de las siguientes opciones son verdaderas con respecto a la operación de Ethernet full duplex? (Elija dos opciones).

- a. Soporta full duplex en medios compartidos
- b. En full duplex, sólo una estación puede transmitir a la vez
- c. Se prefiere full duplex sobre half duplex a la hora de la negociación para establecer el enlace
- d. Todas las implementaciones de Ethernet soportan tanto half duplex como full duplex
- e. Las dos formas de lograr full duplex son la auto negociación y la configuración administrativa

4 ¿Cuáles son los puertos que utiliza un hub para enviar el tráfico que recibe en uno de sus puertos?

- a. Al puerto donde se encuentra el host destino solamente
- b. A los puertos en todos los demás dominios de colisión
- c. Todos los puertos menos el puerto de origen
- d. Todos los puertos

5 ¿Qué ocurre en una red Ethernet después de haberse producido una colisión? (Elija tres opciones).

- a. Se invoca un algoritmo de postergación y la transmisión se detiene.
- b. Los dispositivos involucrados en la colisión tienen un período de tiempo aleatorio para la retransmisión de prioridad del paquete dañado.
- c. Los dispositivos involucrados en la colisión lanzan un token que indica la hora en que cada estación puede comenzar a retransmitir.
- d. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

- e. Los dispositivos que tienen datos para transmitir retornan al modo "escuchar antes de transmitir".
- f. El trabajo de transmisión se reinicia una vez que se vuelven a emitir todos los datos.

6 ¿En cuáles de las siguientes capas del modelo OSI funciona Ethernet? (Elija dos opciones).

- a. Aplicación
- b. Sesión
- c. Transporte
- d. Red
- e. Enlace de datos
- f. Física

7 ¿Cuáles de las siguientes opciones corresponden a nombres de campos de una trama genérica? (Elija tres opciones).

- a. Encabezado IP
- b. Referencia de voltaje
- c. Datos
- d. Descripción
- e. Longitud
- f. Secuencia de verificación de trama

8 ¿Dónde se origina la dirección MAC?

- a. Base de datos del servidor DHCP
- b. Configurada por un administrador
- c. Grabada en ROM en la tarjeta NIC
- d. Configuración de red en el computador
- e. Incluida en la creación del procesador

9 ¿Cómo responden las estaciones Ethernet a las colisiones en la red? (Elija tres opciones).

- a. Una vez que todas las estaciones detectan la colisión, se aplica un algoritmo de postergación.
- b. Las estaciones siguen transmitiendo por un breve periodo de tiempo después de haberse detectado la colisión.
- c. Todas las estaciones que se vieron involucrados en la colisión negocian su estado de prioridad de transmisión que se aplicará después del período de espera.
- d. Al vencerse el período de espera de una estación de trabajo, éste intentará acceder a los medios de red.
- e. El período de espera es igual para todas las estaciones.

10 ¿Cuáles de las siguientes afirmaciones acerca de Ethernet son verdaderas? (Elija tres opciones).

- a. Se ocupa de las necesidades de la Capa 2 y la Capa 3 del modelo OSI
- b. Se lanzó al principio como estándar propietario de Xerox
- c. Básicamente igual a los estándares 802.3
- d. El ancho de banda se puede aumentar sin cambiar la tecnología subyacente
- e. Esencialmente igual a los estándares 802.2
- f. Idea original desarrollada por la Universidad de Hawaii

11 ¿Qué características de Ethernet contribuyen a su uso extendido? (Elija tres opciones).

- a. Facilidad de mantenimiento
- b. Tecnología libre de colisiones
- c. Escalabilidad
- d. Bajo costo de instalación
- e. Compatibilidad con el estándar 802.5
- f. Capacidades que permiten evitar colisiones

12 ¿Cuál de las siguientes opciones se incluye en un campo de direcciones de trama? (Elija dos opciones.)

- a. Dirección IP origen
- b. Dirección IP destino
- c. Máscara de subred destino
- d. Dirección MAC origen
- e. Dirección MAC destino

Para recordar

Ethernet a 10 Mbps usa transmisiones asíncronas. El equipo receptor utiliza los 8 bytes de la información de temporización para sincronizar su circuito de recepción.

Ethernet a 100 Mbps usa transmisiones síncronas. Esto significa que la información de sincronización no es necesaria.

El espacio intertrama es el espacio mínimo que debe existir entre 2 paquetes que no chocan.

En el Ethernet a 10 mbps el espacio intertrama es igual a 96 tiempos de bits, 9.6 microseg.

En el Ethernet a 100 mbps el espacio intertrama es igual a 96 tiempos de bits, 0.96 microseg.

El "jam signal", es la señal de 32 bits enviada a la red para anunciar una colisión.



Principios básicos de Ethernet

Parte II

TEMA

- Principios básicos de Ethernet

OBJETIVOS ESPECÍFICOS

- Identificar la mecánica de funcionamiento de CSMA/CD
- Describir los aspectos claves de la temporización Ethernet
- Definir los errores y las colisiones de Ethernet

CONTENIDOS

- Control de Acceso al Medio (MAC)
- Tipos de colisiones
- Errores de Ethernet

12.1 Control de Acceso al Medio (MAC)

El termino MAC se refiere a los protocolos que determinan cuál de las computadoras de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la Capa 2 del modelo OSI.

Existen dos categorías bastante utilizadas para efectuar el Control de acceso al medio:

- Determinísticos (por turnos)
- No determinísticos (el que primero llega, primero se sirve)

Los protocolos determinísticos son: el Token Ring y el FDDI.

En el caso de Token Ring, los host individuales se disponen en forma de anillo y un token de datos especial (señal eléctrica) se transmite por el anillo a cada host en secuencia. Cada vez que un host desea transmitir, retiene el token, transmite los datos por un tiempo limitado y luego envía el token al siguiente host del anillo. El Token Ring es un entorno sin colisiones ya que sólo un host es capaz de transmitir a la vez.

Los protocolos MAC no determinísticos utilizan el enfoque de "el primero que llega, el primero que se sirve", esta técnica es el CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Las tres tecnologías comunes de Capa 2 son Token Ring, FDDI y Ethernet.

Las tecnologías específicas para cada una son las siguientes:

- Ethernet: topología de bus lógica (el flujo de información tiene lugar en un bus lineal) y en estrella o en estrella extendida física (cableada en forma de estrella)
- Token Ring: topología lógica de anillo (en otras palabras, el flujo de información se controla en forma de anillo) y una topología física en estrella (en otras palabras, está cableada en forma de estrella)
- FDDI: topología lógica de anillo (el flujo de información se controla en un anillo) y topología física de anillo doble (cableada en forma de anillo doble)

12.2 Funcionamiento de MAC

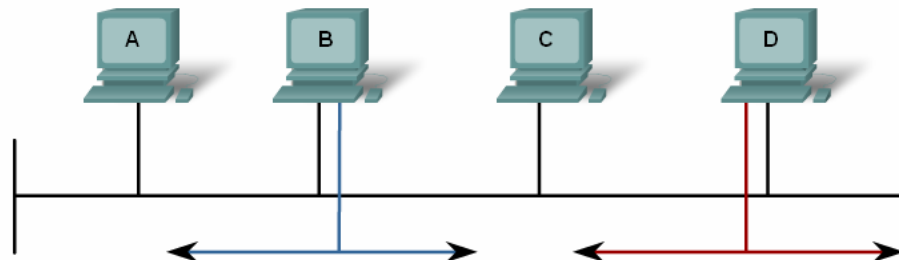
El método de acceso CSMA/CD que se usa en Ethernet realiza tres funciones:

- Transmitir y recibir tramas de datos
- Decodificar tramas de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI
- Detectar errores dentro de los tramas de datos o en la red

Los dispositivos de networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo aleatorio antes de efectuar un sensado. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar.

Media Access Control in Ethernet

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



CSMA/CD controls access to the shared media. If there is a collision, it is detected and frames are retransmitted.

Técnica CSMA/CD

Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

Cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurarse que todos los dispositivos detecten la colisión.

Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado aleatorio, que es diferente para cada dispositivo. Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de networking. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

12.3 Espacio entre las tramas

El espacio mínimo entre dos tramas que no han sufrido una colisión recibe el nombre de espacio entre tramas. Una vez enviada la trama, todas las estaciones de Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir.

El propósito del intervalo es permitir que las estaciones lentas tengan tiempo para procesar la trama anterior y prepararse para la siguiente trama. Una vez producida la colisión y que todas las estaciones permitan que el cable quede inactivo (cada una espera que se cumpla el intervalo completo entre las tramas), entonces, las estaciones que sufrieron la colisión deben esperar un período adicional y cada vez potencialmente mayor antes de intentar la retransmisión de la trama que sufrió la colisión.

El período de espera se mide en incrementos de la ranura temporal del parámetro.

Si la capa MAC no puede enviar la trama después de dieciséis intentos, abandona el intento y genera un error en la capa de red. Una vez enviada la trama, todas las estaciones de Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir. El propósito del intervalo es permitir que las estaciones lentas tengan tiempo para procesar la trama anterior y prepararse para la siguiente trama. Una vez que se ha producido la colisión y que todas las estaciones permitan que el cable quede inactivo, entonces, las estaciones que sufrieron la colisión deben esperar un período adicional y cada vez

potencialmente mayor antes de intentar la retransmisión de la trama que sufrió la colisión.

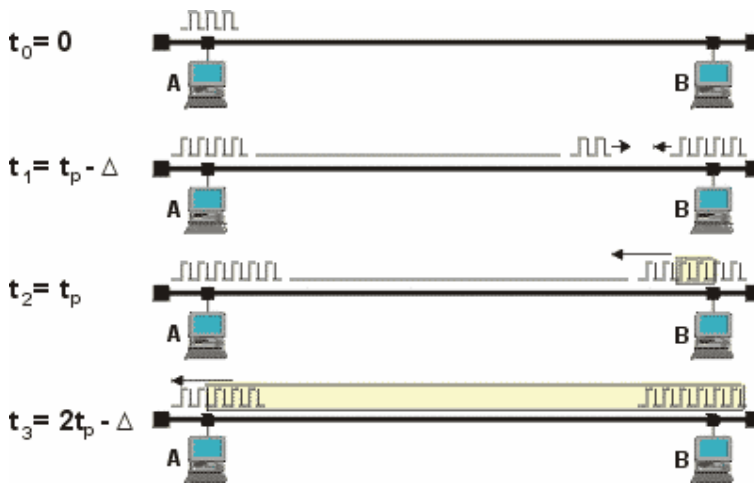
12.4 Manejo de errores

El estado de error más común en las redes Ethernet son las colisiones. Unas pocas colisiones proporcionan una forma simple y sin problemas de transmitir datos, que usa pocos recursos, para que los nodos de la red arbitren la contención para el recurso de red. Sin embargo, las colisiones producen una pérdida del ancho de banda de la red equivalente a la transmisión inicial y a la señal de congestión de la colisión. La mayoría de las colisiones se producen cerca del comienzo de la trama, a menudo, antes de la SFD.

Tan pronto como se detecta una colisión, las estaciones transmisoras envían una señal de congestión de 32 bits. Esta señal de congestión puede estar compuesta por cualquier dato binario siempre que no forme un checksum apropiado para la porción de la trama ya transmitida.

Los mensajes corrompidos, transmitidos de forma parcial, generalmente se conocen como fragmentos de colisión o “runts”.

Las colisiones normales tienen menos de 64 octetos de largo y, por lo tanto, reprueban tanto la prueba de longitud mínima como la prueba de la checksum de FCS.



Estado de colisión

12.5 Tipos de colisiones

Las colisiones se producen cuando dos o más estaciones de Ethernet transmiten al mismo tiempo dentro de un dominio de colisión.

Una colisión simple es una colisión que se detecta al tratar de transmitir una trama, pero con la condición que en el siguiente intento es posible transmitir la trama con éxito.

Las colisiones múltiples indican que la misma trama colisionó una y otra vez antes de ser transmitida con éxito.

Los tres tipos de colisiones son:

- Locales
- Remotas
- Tardías

Colisión local:

La señal viaja por el cable hasta que encuentra una señal de otra tensión.

Las ondas se solapan, cancelándose o doblando su valor. El umbral de sobre tensión 1.5 voltios

En el UTP, la colisión se detecta en el segmento local cuando una estación detecta una señal en el par receptor, al mismo tiempo que se envía por el par transmisor.

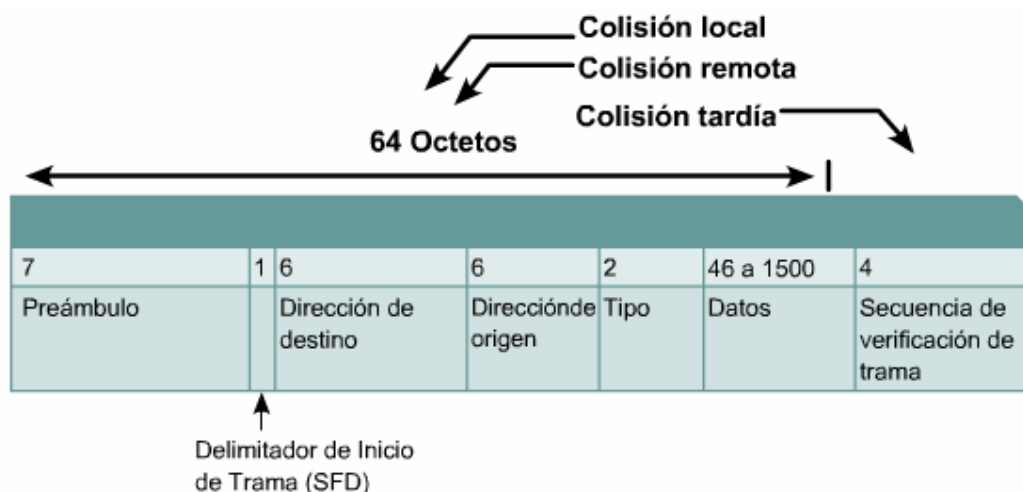
Colisión remota:

La trama tiene menos de la longitud mínima, y tiene una suma de comprobación no válida.

No exhibe síntomas de colisión local, sobre tensión o una actividad e recepción/transmisión simultánea.

Colisión tardía:

Son aquellas colisiones que ocurren después de los primeros 64 bytes. Se detectan en el segmento local como un error FCS.

**12.6 Errores de Ethernet**

Se define al jabber como una transmisión de al menos 20.000 a 50.000 tiempos de bit de duración. Sin embargo, la mayoría de las herramientas de diagnóstico informan de la presencia de jabber siempre que se detecta una transmisión que excede el tamaño máximo legal de la trama

Una trama larga es aquella cuya longitud excede el tamaño máximo legal y que tiene en cuenta si la trama está rotulada o no.

Una trama corta es aquella cuya longitud es menor al tamaño mínimo legal de 64 bytes, con una secuencia de verificación de trama correcta.

Algunos analizadores de protocolos y monitores de red llaman a estas tramas "runts".

12.7 Errores FCS

En una trama con error de FCS, es probable que la información del encabezado sea correcta, pero la checksum que calcula la estación receptora no concuerda con la checksum que adjunta la estación transmisora al extremo de la trama. Por lo tanto, se descarta la trama.

Un mensaje que no termina en un límite de octeto se conoce como error de alineamiento.

Una trama así se trunca en el límite del octeto más cercano, y si la checksum de FCS falla, entonces, se informa un error de alineamiento

12.8 Auto negociación de Ethernet

Al crecer Ethernet de 10 a 100 y 1000 Mbps, fue necesario hacer que cada tecnología pudiera operar con las demás de manera armónica. Para tal fin se desarrolló un proceso que recibe el nombre de Auto-negociación de las velocidades en half duplex o en full duplex.

El estándar 10BASE-T requirió que cada estación transmitiera un pulso de enlace aproximadamente cada 16 milisegundos, siempre que la estación no estuviera transmitiendo un mensaje.

La Auto-Negociación adoptó esta señal y la nombro Pulso de enlace normal (NLP). Cuando se envía una serie de NLPs a un grupo con el propósito de Auto-Negociación, el grupo recibe el nombre de ráfaga de Pulso de enlace rápido (FLP). Cada ráfaga de FLP se envía a los mismos intervalos que un NLP y tiene como objetivo permitir que los antiguos dispositivos de 10BASE-T operen normalmente en caso de que reciban una ráfaga de FLP.

Autoevaluación

1. ¿Cuáles de las siguientes opciones describen las direcciones MAC? (Elija tres opciones).

1. OUI de 24 bits y número serial de 24 bits
2. Red de 32 bits y dirección de host de 48 bits
3. 6 pares de dígitos hexadecimales
4. 48 dígitos hexadecimales
5. Dirección lógica de host
6. Dirección física

2. ¿Cómo se detectan las colisiones en una red Ethernet?

1. Las estaciones identifican el campo FCS alterado en los paquetes que han tenido una colisión.
2. La amplitud de la señal en los medios de red es mayor que la normal.
3. El tráfico de la red no se puede detectar debido a que está bloqueada
4. La amplitud de la señal en los medios de redes menor que la normal.

3. Después de una colisión en Ethernet, ¿qué dispositivo recibe la prioridad para el envío de datos al aplicar el algoritmo de postergación?

1. El dispositivo involucrado en la colisión con la menor dirección MAC
2. El dispositivo involucrado en la colisión con la menor dirección IP
3. El dispositivo del dominio de colisión cuyo temporizador de postergación se vence primero
4. Los que comiencen a transmitir al mismo tiempo

4. ¿Cuáles de las siguientes son funciones de CSMA/CD? (Elija tres opciones).

1. Transmitir y recibir paquetes de datos
2. Liberar un token cuando la red está libre
3. Detectar errores en los paquetes de datos o en la red
4. Enviar un token a cada estación de la red
5. Decodificar los paquetes de datos y controlar si tienen direcciones válidas antes de enviarlos a las capas superiores del modelo OSI

5 ¿Qué indica la palabra "Base" en 10Base2?

1. La cantidad de estándares utilizados.
2. Se utiliza la señalización de banda base.
3. Sólo se utiliza una porción del medio de transmisión.
4. Se utiliza la señalización de banda ancha.

6 ¿Cuál es el propósito del preámbulo de una trama Ethernet?

1. Se usa como relleno para los datos
2. Identifica la dirección origen
3. Identifica la dirección destino

4. Marca el final de la información de temporización
5. Se utiliza para sincronizar la temporización mediante un patrón alterno de unos y ceros

7 ¿Cuáles de las siguientes opciones se especifican en las normas IEEE como subcapas de la capa de enlace de datos del modelo OSI? (Elija dos opciones).

1. Control de enlace lógico
2. Control de capa lógica
3. Control de acceso al medio
4. Comunicación de enlace lógico
5. Comunicación de acceso al medio
6. Comunicación de acceso físico

Para recordar

Colisión o runt: Transmisión simultánea que se produce antes de haber transcurrido la ranura temporal

Fantasma o jabber: Preámbulo inusualmente largo o evento de congestión

La 10BASE-T requirió que cada estación transmitiera un pulso de enlace aproximadamente cada 16 milisegundos, siempre que la estación no estuviera transmitiendo un mensaje

La Auto-Negociación es optativa para la mayoría de las implementaciones de Ethernet.

La Auto-Negociación evita la mayoría de las situaciones donde una estación de un enlace punto a punto transmite de acuerdo a las reglas de half-duplex y la otra de acuerdo a las reglas de full-duplex



Planeando la red - Parte I

TEMA

- Planeando la red – Parte I

OBJETIVOS ESPECÍFICOS

- Identificar las características de una red WAN
- Identificar las funciones del Cisco IOS
- Identificar los modos de trabajo del router

CONTENIDOS

- Introducción a las redes WAN
- Operación del software Cisco IOS

13 Redes WAN

13.1 Introducción a las redes WAN

Una WAN es una red de transmisión de datos que se caracteriza por abarcar un área geográfica extensa, como por ejemplo una provincia o un país.

Entre sus principales características tenemos:

- Comunican dispositivos que están separados por áreas geográficas extensas.
- Hacen uso de los servicios de terceros (proveedores de telecomunicaciones)
- Utilizan varios tipos de conexiones seriales.

Las empresas usan las redes WAN para conectar sus distintas sucursales de tal modo que se pueda intercambiar información entre ellas. Una WAN trabaja a nivel de la capa física y la capa de enlace de datos según el modelo OSI.

Desde el punto de vista de la internetworking una red WAN permiten el intercambio de paquetes y tramas de datos entre los routers y switches, así como las LAN que mantienen comunicadas.

Una WAN hace uso de los siguientes dispositivos:

Los routers:

Ofrecen varios servicios, entre ellos el internetworking, así como los puertos de interfaz serial WAN.

Los módems:

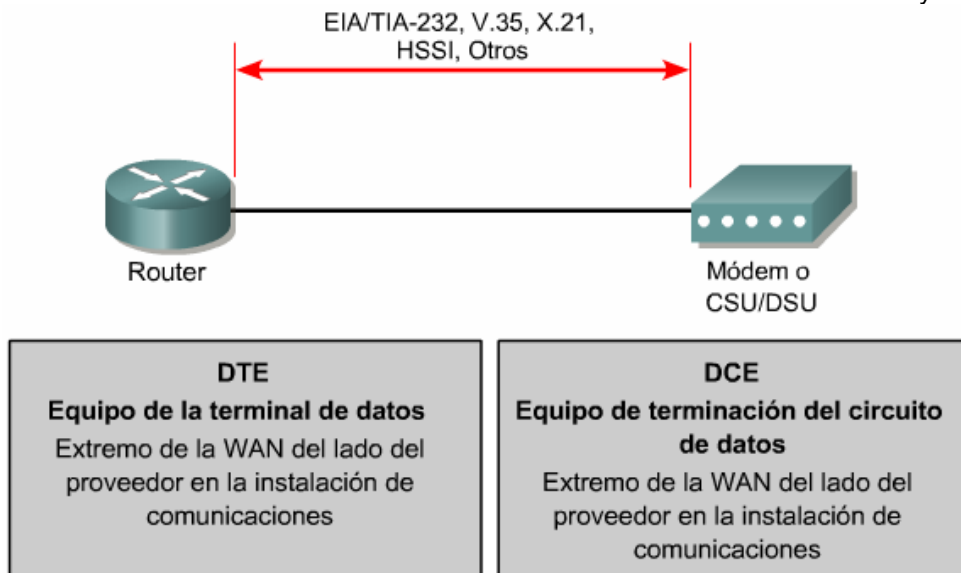
Incluyen servicios de interfaz de grado de voz; unidades de servicio de canal/unidades de servicio de datos (CSU/DSU) que realizan la interfaz con los servicios T1/E1; y los

Adaptadores de Terminal/Terminación de red 1 (TA/NT1):

Realizan la interfaz con los servicios de Red digital de servicios integrados (RDSI).

Los servidores de comunicación:

Concentran las comunicaciones de usuarios de acceso telefónico entrante y saliente.



Los protocolos de enlace de datos WAN:

Describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos

13.1.1 Introducción a los routers de una WAN

Un router es un computador de propósito específico, pues presenta una CPU, memoria, bus de sistema e interfaces de entrada/salida.

Los routers conectan y permiten la comunicación entre dos o más redes y calculan la mejor ruta para realizar la transmisión de datos a través de las redes conectadas.

Como toda computadora, los routers necesitan de un sistema operativo para poder controlar el hardware y ejecutar los archivos de configuración del sistema.

El CISCO IOS, es un sistema operativo completo que hace uso de una serie de modos de funcionamiento y comandos que permitirán la configuración del router y también nos permitirán interactuar con el mismo.

Los archivos de configuración contienen toda la información necesaria para una correcta configuración del router (nombre, direcciones IP, interfaces habilitadas, etc) y los usos de los protocolos enrutados y de enrutamiento seleccionados, o habilitados, en el router.



Router de la Serie 2500

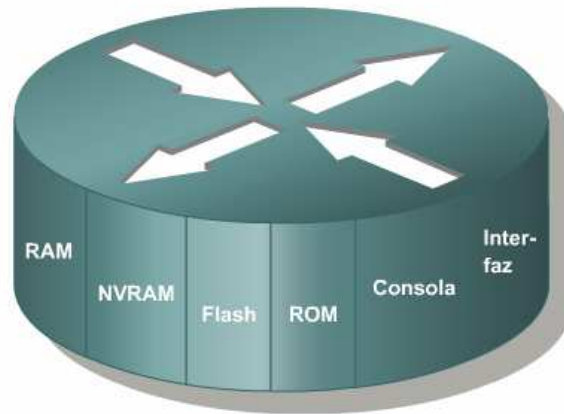


Router 1760

Los principales componentes internos del router son la memoria de acceso aleatorio (RAM), la memoria de acceso aleatorio no volátil (NVRAM), la memoria flash, la memoria de sólo lectura (ROM) y las interfaces.

La memoria RAM, también llamada RAM dinámica (DRAM), tiene las siguientes características y funciones:

- Guarda momentáneamente las tablas de enrutamiento.
- Almacena el caché ARP.
- Guarda el caché de conmutación rápida.
- Crea el buffer de los paquetes (RAM compartida).
- Mantiene las colas de espera de los paquetes.
- Proporciona una memoria temporal para el archivo de configuración del router mientras está encendido.
- Como toda RAM pierde el contenido cuando se apaga o reinicia el router.



13.2 Operación del software Cisco IOS

13.2.1 Funciones del software Cisco IOS

Un router o switch al ser dispositivos complejos requieren muchas pautas de configuración por lo tanto no puede funcionar sin un sistema operativo. El nombre oficial del Sistema operativo de internetworking de Cisco, es el de Cisco IOS.

El Cisco IOS se encuentra incorporada en todos los routers Cisco y también es el sistema operativo usado por los switches Catalyst. Lógicamente dependiendo del tipo de dispositivo se tendrán comandos adicionales.

El Cisco IOS brinda los siguientes servicios de red:

- Funciones básicas de enrutamiento y conmutación
- Acceso confiable y seguro a los recursos de la red
- Escalabilidad de la red
- Configuración del router

13.2.2 Interfaz de usuario del router

El software Cisco IOS principalmente usa una interfaz de línea de comando (CLI) como entorno de consola tradicional, a través de esta consola se ingresan los comandos de configuración del sistema.

Una de las formas de acceder al CLI es a través de una sesión de consola. Esta sesión de consola se puede habilitar a través de una conexión serial directa, de baja velocidad, desde una computadora o terminal a la conexión de consola del router.

También existe la posibilidad de realizar una conexión de acceso telefónico, con un módem usando la conexión al puerto AUX del router.

Lo bueno de estos métodos es que ninguno de ellos requiere que el router tenga activo o configurado algún servicio de red.

Para establecer una sesión Telnet al router, se debe configurar por lo menos una interfaz con una dirección IP, y asegurar las conexiones mediante la asignación de contraseñas a las sesiones de terminal virtual.

```
Image text-base: 0x80008080, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fcl)
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K by
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

cibertec#
```

Línea de comando del CISCO IOS

13.2.3 Modos de interfaz de usuario

La interfaz de línea de comando (CLI) de Cisco trabaja sobre la base de una estructura jerárquica. Esto significa que existen varios modos de acceso al router para realizar tareas particulares.

El IOS proporciona un servicio de intérprete de comandos, denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y ejecuta.

Como medida de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso:

- El modo EXEC usuario
- El modo EXEC privilegiado (modo enable)

Modo EXEC Usuario:

Permite sólo una cantidad limitada de comandos de monitoreo básicos.

No permite ningún comando que pueda cambiar la configuración del router.

Este modo se puede reconocer por la petición de entrada: ">".

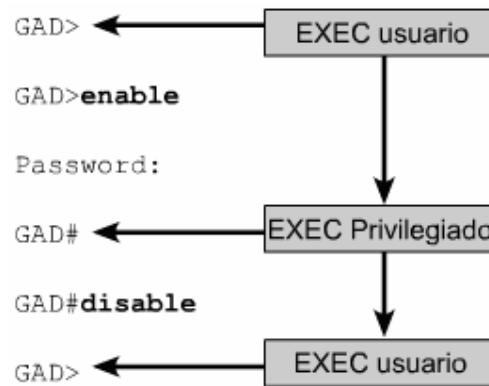
Modo EXEC privilegiado:

Otorga acceso a todos los comandos de configuración del router.

Se recomienda asignarle una contraseña de acceso por seguridad.

En este modo se acceden a los comandos de configuración y administración requeridos por el administrador de la red.

Este modo también sirve de plataforma de acceso al modo de configuración global y a todos los demás modos específicos. El modo EXEC privilegiado se puede reconocer por la petición de entrada "#".



Modos de funcionamiento del Cisco IOS

13.2.4 Características resaltantes del software Cisco IOS

Cisco suministra múltiples imágenes de su IOS dependiendo del tipo de dispositivo donde vaya a ser instalado. Para adecuar óptimamente el software Cisco IOS que requieren dichas plataformas, Cisco desarrolla muchas y variadas imágenes del software Cisco IOS.

Cada imagen proporciona una funcionalidad distinta, adecuada a las diversas plataformas de los dispositivos, los recursos de memoria disponibles y las necesidades de los clientes. Eso sí la estructura básica de los comandos de configuración es la misma. Esto es muy útil pues permite que se maneje un entorno común que facilita al administrador adecuarse rápidamente a las distintas versiones del CISCO IOS.

El esquema de denominación de las distintas versiones del software Cisco IOS consta de tres partes:

- La plataforma en la que se ejecuta la imagen.
- Las características especiales que permite la imagen.
- El lugar donde se ejecuta la imagen y si la imagen ha sido comprimida en formato zip.

Una de las consideraciones principales al momento de seleccionar una nueva imagen del IOS, es la compatibilidad con las memorias flash y RAM del router

Autoevaluación

1. Identificar los modos de trabajo que presenta un router Cisco. Definir cada una de ellas.
2. Identificar las distintas interfaces que maneja un router Cisco.
3. ¿Identifique las características del Cisco IOS?
4. ¿Es posible realizar un upgrade del sistema operativo de los routers?

Para recordar

Las empresas usan las redes WAN para conectar sus distintas sucursales de tal modo que se pueda intercambiar información entre ellas. Una WAN trabaja a nivel de la capa física y la capa de enlace de datos según el modelo OSI.

Un router es un computador de propósito específico, pues presenta una CPU, memoria, bus de sistema e interfaces de entrada/salida.

Los routers conectan y permiten la comunicación entre dos o más redes y calculan la mejor ruta para realizar la transmisión de datos a través de las redes conectadas.

El software Cisco IOS principalmente usa una interfaz de línea de comando (CLI) como entorno de consola tradicional, a través de esta consola se ingresan los comandos de configuración del sistema.

Cisco suministra múltiples imágenes de su IOS dependiendo del tipo de dispositivo donde vaya a ser instalado. Para adecuar óptimamente el software Cisco IOS que requieren dichas plataformas, Cisco desarrolla muchas y variadas imágenes del software Cisco IOS.



Planeando la red - Parte II

TEMA

- Planeando la red – Parte II

OBJETIVOS ESPECÍFICOS

- Identificar la función del router en una red WAN
- Identificar las interfaces del router
- Identificar la secuencia de conexión a las interfaces administrativas del router.

CONTENIDOS

- Los routers en las LAN y WAN
- La función del router en una WAN
- Conexiones externas del router
- Conexiones del puerto de administración
- Conexión de las interfaces de consola

14 Los routers en las LAN y WAN

Los routers tienen interfaces LAN y WAN. Es más, los routers se comunican entre sí haciendo uso de conexiones seriales de tipo WAN. Trabajan a nivel de la capa 3 del modelo OSI, y toman decisiones basándose en las direcciones de red.

Las dos funciones principales de un router son: determinar la mejor ruta y conmutar los paquetes a la interfaz correcta.

Los routers logran esto haciendo uso de las tablas de ruteo y el intercambio de la información de estas tablas con otros routers vecinos.

Un administrador puede mantener las tablas de enrutamiento a través de la configuración de las llamadas rutas estáticas, pero, por lo general, las tablas de enrutamiento se mantienen de manera dinámica a través del uso de algún protocolo de enrutamiento que intercambia información acerca de la topología (forma de la red) de red con otros routers.

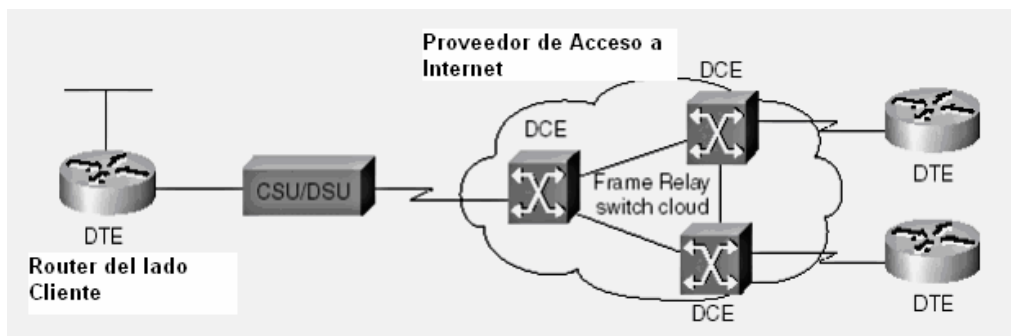
Una inter-red configurada correctamente brinda lo siguiente:

- Direccionamiento coherente de extremo a extremo
- Direcciones que representan topologías de red
- Selección de la mejor ruta
- Ruteo estático o dinámico.
- Conmutación.

14.1 La función del router en una WAN

El elemento diferencial entre una red WAN y una LAN, en general, se dan en la capa física y en la capa de enlace de datos.

Es importante aclarar que una WAN opera en la capa física y en la capa de enlace de datos. La capa física de una WAN se encarga de describir la interfaz entre el equipo terminal de datos (DTE) y el equipo de transmisión de datos (DCE). Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado que se encuentra en el lado del cliente.



Los routers del lado del Proveedor son de tipo DCE y los del lado cliente son DTE.

Un router puede ser exclusivamente un dispositivo LAN, o puede ser exclusivamente un dispositivo WAN. Esto último depende de la función de interconexión que se encuentre realizando. El ruteo no es una función que únicamente se pueda dar a nivel de una WAN, sino que también puede darse a nivel LAN.

A nivel WAN las funciones principales de un router no son principalmente la conmutación de paquetes sino el proporcionar conectividad con los diversos protocolos de la capa de enlace de datos y capa física WAN.

A continuación se muestran los principales protocolos WAN, correspondientes a la capa Física y de Enlace de Datos.

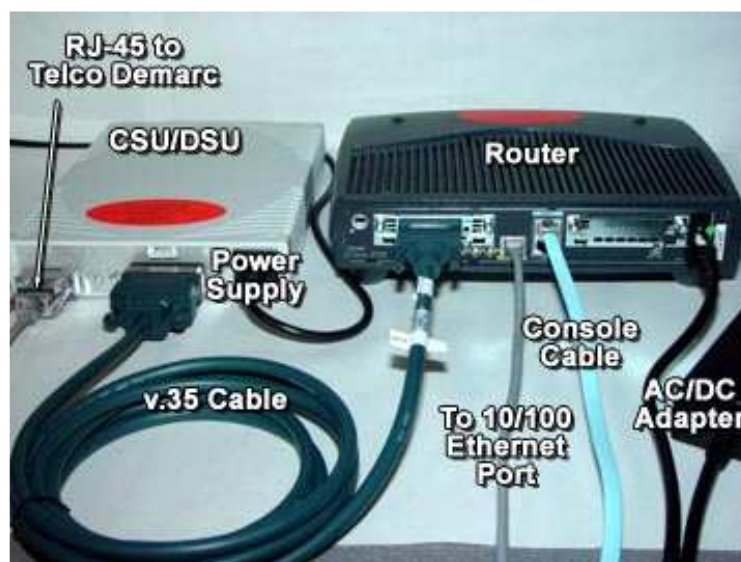
Protocolos de la Capa Física	Protocolos de la Capa de Enlace de Datos
EIA/TIA 232	HDLC
EIA/TIA 449	Frame Relay
V.24	Point-to-Point Protocol (PPP)
V.35	SDLC/ADLC
X.21	SLIP
ISDN	X.25
TI/T3	ATM
E1/E3	
SONET	
xDSL	

14.2 Conexiones externas del router

Las tres conexiones básicas de un router son: las interfaces LAN, las interfaces WAN y los puertos de administración. Las interfaces LAN permiten que el router se conecte a la red LAN propiamente dicha, generalmente usando el protocolo Ethernet o una de sus variantes.

Las conexiones WAN, son generalmente conexiones seriales y sirven para proporcionar las conexiones del router a otro.

En algunos tipos de interfaces WAN, se requiere de un dispositivo externo, como por ejemplo una CSU, para conectar el router a la conexión local del proveedor del servicio. En otros casos, el router puede estar conectado directamente al proveedor del servicio.



Router: Vista posterior

El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router

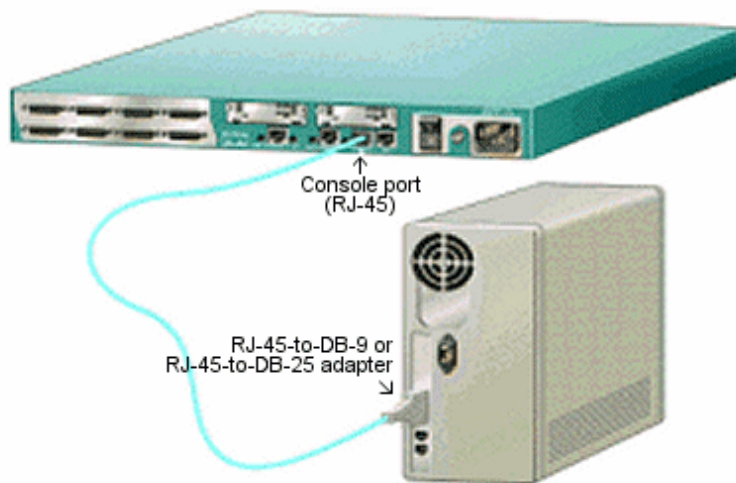
Los puertos auxiliares y de consola constituyen las interfaces usadas para la administración del router. Estos son puertos seriales asíncronos de tipo EIA-232. A través de este puerto se efectúa la conexión a un puerto de comunicaciones de un computador, generalmente el puerto COM1. El computador debe ejecutar un programa de emulación de Terminal (HyperTerminal) para iniciar la sesión basada en texto plano de tipo ASCII con el router. Usando esta sesión, el administrador de la red puede inicialmente administrar el dispositivo.

14.2.1 Conexiones del puerto de administración

El puerto de consola y el puerto auxiliar (AUX) son puertos de administración. A diferencia de los routers domésticos, cuando un router Cisco entra en servicio por primera vez, los parámetros de networking no están configurados. Es decir, no tiene una dirección IP prefijada, ni nombre, ni usuarios. Todo debe hacerse de cero. Para configurar el router por primera vez, se usa un conector RS-232 al puerto de consola del sistema, y de esta manera se podrán ingresar los comandos de configuración para poner en marcha el router. Una vez que la configuración inicial se ha efectuado, se puede conectar el router a la red para realizar un diagnóstico de fallas o monitoreo. Se pueden realizar estas tareas haciendo telnet a una línea de terminal virtual (vty0) o marcando el número de un módem conectado al puerto de consola o auxiliar del router. Se prefiere el puerto de consola al puerto auxiliar para el diagnóstico de fallas. Esto es porque muestra por defecto la puesta en marcha del router, la depuración y los mensajes de error. El puerto de consola también puede usarse cuando han fallado los servicios de networking. Por lo tanto, el puerto de consola se puede usar para los procedimientos de recuperación de contraseñas y de desastre.

14.2.2 Conexión de las interfaces de consola

Para realizar la conexión al puerto de consola, se usa un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al PC. Se usa para la configuración inicial de router, el monitoreo y los procedimientos de recuperación de desastres.



**Conexión serial al puerto
De consola**

En esta operación es necesario un software de emulación de terminal, como el HyperTerminal, que viene incluido con el mismo Windows o el Minicom, si se esta trabajando con Linux.

Para conectar un PC a un router:

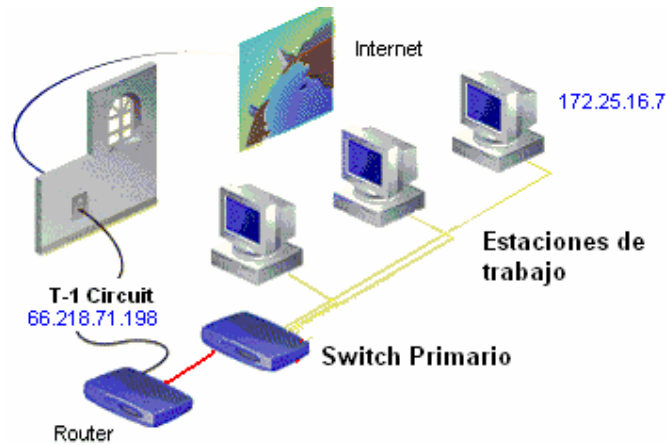
1. Configure el software de emulación de terminal en el PC para:
 - El puerto serial adecuado (COM1,COM2,etc)
 - 9600 baudios
 - 8 bits de datos
 - Sin paridad
 - 1 bit de parada
 - Sin control de flujo
2. Conecte el conector RJ-45 del cable transpuesto (rollover) al puerto de consola del router.



Configuración del Hyperterminal

14.2.3 Conexión de las interfaces LAN

El router se conecta a la red LAN a través de una interfaz de Ethernet o Fast Ethernet. Eso si haciendo uso de un hub o de un switch. Para conectar el router al hub o switch se requiere un cable de conexión directa.



Conexión del router a un switch

14.2.4 Conexión de interfaces WAN

Una WAN utiliza distintos tipos de tecnologías para realiza conexiones de datos a través de una amplia área geográfica.

Entre los tipos de conexión WAN tenemos los de línea arrendada, de conmutación de circuitos y de conmutación de paquetes.

Un router, es identificado como el equipo terminal de datos (DTE) y se conecta al proveedor del servicio por medio de un dispositivo del equipo de transmisión de datos (DCE), en general, un módem o una unidad de servicio de canal/unidad de servicio de datos (CSU/DSU). Este dispositivo se usa para convertir los datos del DTE a una forma reconocible para el proveedor del servicio WAN.

Autoevaluación

1. ¿Cuáles son las funciones primarias de la memoria FLASH?
2. ¿Cuáles son funciones de la memoria NVRAM
3. Identificar los pasos a seguir para configurar el programa HyperTerminal
4. ¿Dónde se encuentran las instrucciones que utiliza un router para controlar el flujo de tráfico a través de sus interfaces?
5. ¿En los routers Cisco, cuáles puertos se pueden usar para la configuración inicial?
6. ¿Qué componentes básicos tienen en común un router y un PC de escritorio estándar?
7. Identificar las características que deben estar presentes en una internetworking (Elija tres)
 - a. Conmutación
 - b. Direccionamiento estático
 - c. Estandarización IETF
 - d. Enrutamiento dinámico o estático
 - e. Direccionamiento de punto a punto constante
8. Identificar las opciones verdaderas con respecto a las interfaces de un router (Elija tres opciones).
 - a. Proporcionan memoria temporal para los archivos de configuración del router
 - b. Conecta el router a la red para la entrada y salida de tramas
 - c. Pueden estar en el chasis del router o en un módulo distinto
 - d. Contienen la imagen IOS
 - e. Conecta el router a las LAN y WAN
9. Seleccione las opciones que describen correctamente la memoria flash de un router Cisco de la serie 2600. (Elija dos.)
 - a. Por defecto contiene la configuración inicial
 - b. Se puede actualizar con módulos de memoria en línea
 - c. Almacena las imágenes del software Cisco IOS
 - d. Por defecto almacena la información de las tablas de enrutamiento
 - e. Mantiene la única copia de una imagen del IOS después de que se arranca el router

Para recordar

1. El programa que permite conectar la computadora al puerto de consola de configuración del router es el Hyperterminal.
2. Los parámetros de configuración del Hyperterminal son los siguientes:
 - a. El puerto serial adecuado (COM1,COM2)
 - b. 9600 baudios
 - c. 8 bits de datos
 - d. Sin paridad
 - e. 1 bit de parada
 - f. Sin control de flujo
3. El CISCO IOS, es un sistema operativo completo que hace uso de una serie de modos de funcionamiento y comandos que permitirán la configuración del router y también nos permitirán interactuar con el mismo.
4. El CISCO IOS presenta modos de funcionamiento que permiten efectuar desde configuraciones básicas a complejas.
5. La memoria NVRAM es una memoria no volátil que permite almacenar los archivos de configuración del router.
6. La memoria RAM se puede incrementar mediante la adición de módulos DIMM.
7. La memoria FLASH contiene la imagen comprimida del sistema operativo
8. La memoria ROM contiene el código para arrancar el router antes que se efectúe la carga del sistema operativo completo.



Configurando y examinando la red - Parte I

TEMA

- 15Configurando y examinando la red – Parte I

OBJETIVOS ESPECÍFICOS

- Configurar una interfaz serial
- Comprender los modos de comando del CLI
- Usar comandos de configuración básicos

CONTENIDOS

- Modos de comando CLI
- Configuración de contraseñas de router
- Configuración de una interfaz serial

ACTIVIDADES

- Modos de comando e identificación del router
- Configuración de contraseñas

15.1 Configuración del router

En un primer momento es posible que el trabajo de configurar un router nos pueda parecer una tarea compleja. Sin embargo, los procedimientos iniciales para configurar el router no son difíciles en absoluto y solo requieren de una mayor práctica inicial.

Este módulo nos permite familiarizarnos con los modos básicos de configuración del router y efectuar tareas de configuraciones simples.

Es muy importante que aquella persona que administra un router agregue comentarios al archivo de configuración como efecto de documentación. Esto es muy importante en caso que otra persona asuma la administración de la red, y requiera informarse acerca de los detalles del router.

151.1 Modos de comando CLI

El sistema operativo CISCO IOS tiene modos de trabajo. Cada uno de ellos presenta características propias. A continuación tenemos un resumen de los principales modos:

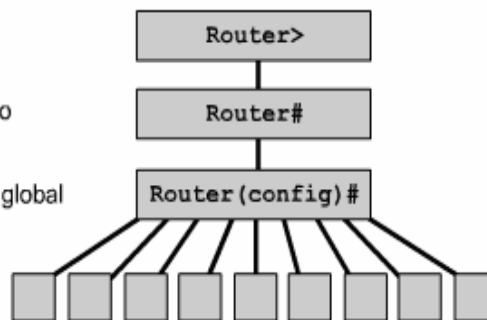
Modo de trabajo	Características
Modo EXEC de usuario	El usuario puede visualizar alguna información, pero no puede hacer cambios
Modo EXEC privilegiado	Comandos de depuración y prueba, análisis detallado del router, manipulación de archivos y acceso a modos de configuración
Modo de configuración global	Permite la configuración del router
Modo SETUP	Se utiliza para crear una configuración inicial básica
Modo RXBOOT	Modo de mantenimiento, permite entre otras cosas recuperar contraseñas perdidas

• Modo EXEC usuario

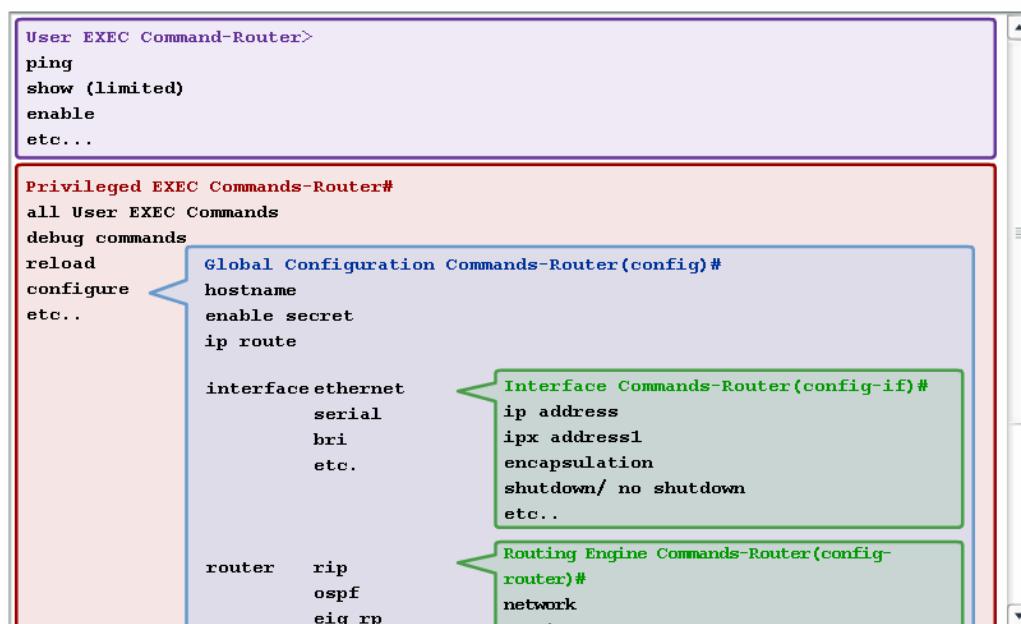
• Modo EXEC privilegiado

• Modo de configuración global

• Modos de configuración específicos



IOS Mode Hierarchical Structure



Como se puede apreciar en el gráfico el modo de configuración global, a menudo abreviado como 'global config', es el modo de configuración principal. Sin embargo, para ingresar a este modo previamente se debe ingresar al modo Privilegiado. Los comandos del modo de configuración global se caracterizan por realizar cambios globales en el router como un todo.

El siguiente comando lleva al router al modo de configuración global:

```
Router# configure terminal
Router (config)#
```

Existen muchos otros modos de operación más particulares que serán invocados según la necesidad requerida, pero todos esos modos específicos son subconjuntos del modo de configuración global.

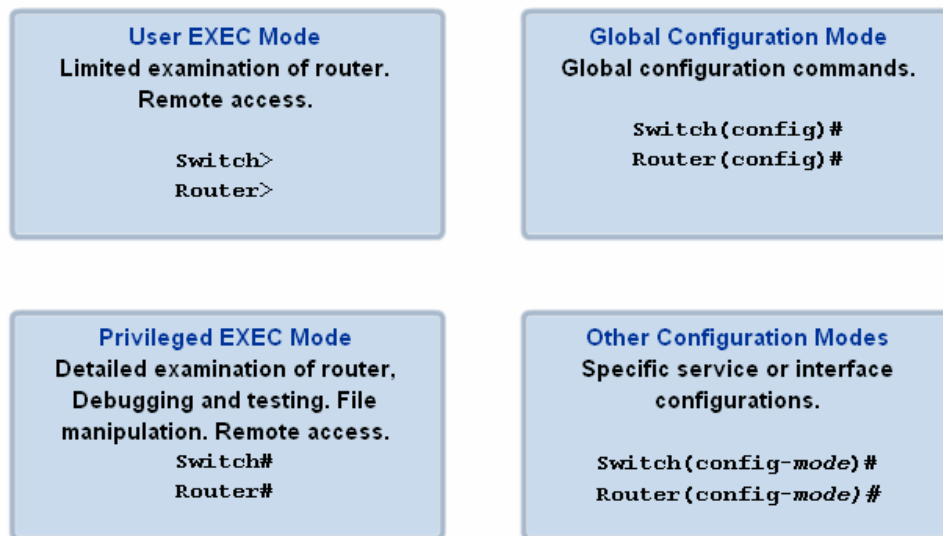
Modo de configuración	Símbolo del "prompt" del CLI
Interfaz	Router(config-if)#
Subinterfaz	Router(config-subif)#
Controlador	Router(config-controller)#
Lista de mapa	Router(config-map-list)#
Clase de mapa	Router(config-map-class)#
Línea	Router(config-line)#
Router	Router(config-router)#
Router IPX	Router(config-ipx-router)#
Mapa de ruta	Router(config-route-map)#

Como podemos apreciar cada uno de estos modos específicos presenta un modo particular de prompt, que permite identificar el modo en el que se está trabajando. Todos los cambios de configuración que se den, únicamente tendrán efecto en las interfaces o los procesos relativos a ese modo particular.

Al ingresar el comando exit desde alguno de estos modos de configuración específicos, el router regresa al modo de configuración global. Al presionar Control-Z, se sale por completo del modo de configuración y el router vuelve al modo EXEC privilegiado.

```
Router (config)#interface fastEthernet 0/0
Router (config-if)#exit
Router(config)#
```

IOS Primary Modes



15.1.2 Configuración del nombre de router

Es importante asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Router (config)#hostname Cibertec
Cibertec(config)#
```

15.1.3 Configuración de contraseñas de router

Las contraseñas controlan el acceso a los routers. Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas también se usan para controlar el acceso al modo EXEC privilegiado, a fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.

Contraseña de la consola:

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

```
Router (config) #line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

Contraseña del Terminal Virtual:

Se debe fijar contraseñas en una o más de las líneas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante sesiones Telnet. Por defecto, los routers Cisco permiten cinco líneas de tipo "vty" identificadas del 0 al 4,

```
Router (config) #line vty 0 4
Router (config-line) #password cisco
Router (config-line)#login
```

Contraseña del Modo EXEC Privilegiado:

Los comandos enable password y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado.

No es necesario utilizar ambos a la vez. El comando enable password se utiliza sólo si no se ha configurado previamente enable secret. Sin embargo se recomienda utilizar siempre enable secret, ya que a diferencia de enable password, la contraseña estará siempre cifrada.

```
Router(config)#enable password cisco
o
Router(config)#enable secret cisco
```

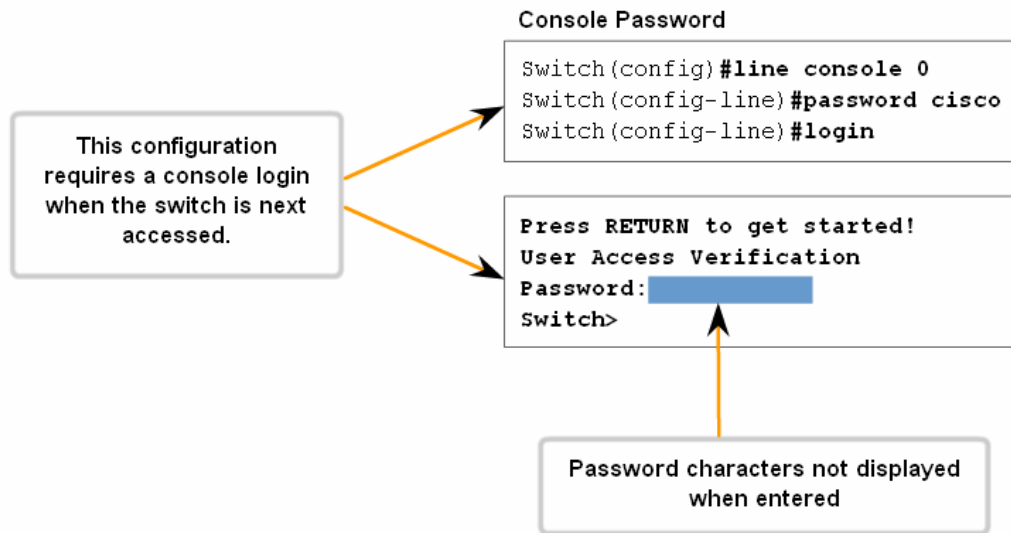
Siempre es conveniente evitar que las contraseñas se muestren en texto plano, pues al ejecutar los comandos show running-config o show startup-config estas podrían ser vistas sin problemas.

El siguiente comando permitirá cifrar las contraseñas al mostrar los datos de configuración:

```
Router(config)#service password-encryption
```

El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar que hayan sido ingresadas. Mientras que el comando: enable secret <password> usa un fuerte algoritmo MD5 para cifrar, sin embargo no hay que olvidar que este último comando solo asegura la contraseña del modo enable.

Limiting Device Access - Configuring Console Passwords



Para esto usamos el comando: `copy tftp running-config`

Autoevaluación

- Identificar el comando que permite habilitar una interfase que previamente fue administrativamente deshabilitada
 - No shutdown
 - Shutdown
 - Enable
 - No disable
 - Up
- Imagine que Ud. Uso el comando ping exitosamente. ¿Qué mensajes fueron enviados por el comando ping?
 - Icmp ping
 - Icmp echo request
 - Icmp echo management
 - Icmp Query
- ¿Con qué comandos obtenemos información sobre el IOS o los archivos de configuración almacenados en la memoria del router? (Elija tres opciones).
 - Router# **show ram**
 - Router# **show flash**
 - Router# **show hosts**

- d. Router# **show history**
 - e. Router# **show version**
 - f. Router# **show startup-config**
4. ¿Cuál es la respuesta del router después de introducir el comando, "router(config)# **hostname cibertec**"?
- a. cibertec#
 - b. cibertec (config)#
 - c. invalid input detected
 - d. router(config-host)#
 - e. hostname = cibertec
 - f. cibertec # ? command not recognized
 - g. router(config)#
5. Seleccione los comandos que guardan el archivo de configuración activa a un servidor TFTP de red? (Elija dos opciones).
- a. Router# **copy run tftp**
 - b. Router# **copy tftp run**
 - c. Router# **copy running-config tftp**
 - d. Router# **copy tftp running-config**
 - e. Router(config)# **copy running-config tftp**
 - f. Router(config)# **copy tftp running-config**
6. Es posible asociar los nombres de router con las direcciones IP. ¿Cuál es el nombre de la tabla creada por esta asociación?
- a. tabla IP
 - b. tabla SAP
 - c. tabla ARP
 - d. tabla MAC
 - e. tabla HOST
 - f. tabla RARP
7. Seleccione los comandos necesarios para eliminar cualquier configuración existente en un router. (Elija dos opciones).
- a. **delete flash**
 - b. **erase startup-config**
 - c. **erase running-config**
 - d. **restart**
 - e. **reloaddelete NVRAM**

Para recordar

- Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola.
- El comando `service password-encryption` aplica un cifrado débil a todas las contraseñas sin cifrar que hayan sido ingresadas.
- Los comandos `show` se pueden utilizar para examinar el contenido de los archivos de configuración en el router y para diagnosticar fallas leves.
- Por defecto, los routers Cisco son dispositivos DTE, pero se pueden configurar como dispositivos DCE.
- Es posible agregar un mensaje de inicio de sesión para que sea visualizado por el usuario al momento de hacer login en el router, y es utilizado para comunicar información de interés a todos los usuarios de la red.
- El sistema operativo CISCO IOS tiene modos de trabajo. Cada uno de ellos presenta características propias.
- Cada uno de estos modos específicos presenta un modo particular de prompt, que permite identificar el modo en el que se está trabajando



Configurando y examinando la red - Parte II

TEMA

- Configurando y examinando la red

OBJETIVOS ESPECÍFICOS

- Configurar una interfaz serial
- Comprender los modos de comando del CLI
- Usar comandos de configuración básicos

CONTENIDOS

- Modos de comando CLI
- Configuración de contraseñas de router
- Configuración de una interfaz serial

ACTIVIDADES

- Modos de comando e identificación del router
- Configuración de contraseñas

16 Comandos de configuración del router

16.1 Uso de los comandos show

Los comandos show se pueden utilizar para examinar el contenido de los archivos de configuración en el router y para diagnosticar fallas leves.

La lista en el modo EXEC privilegiado es considerablemente más larga que en el modo EXEC de usuario.

- **show history:** Muestra un historial de los comandos ingresados

0

- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí

```
Router#show flash
```

```
System flash directory:
```

```
File Length Name/status
```

```
1 4902344 c2500-i-1.113-4
```

```
[4902408 bytes used, 3486200 available, 8388608 total]
```

```
8192K bytes of processor board System flash (Read ONLY)
```

```
Router#_
```

Comando show version:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 11.3(4), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 16-Jun-98 02:54 by phanguye
Image text-base: 0x03028EE0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-B00T-R), Version 11.0(10c), RELEASE SOFTWARE (fc1)

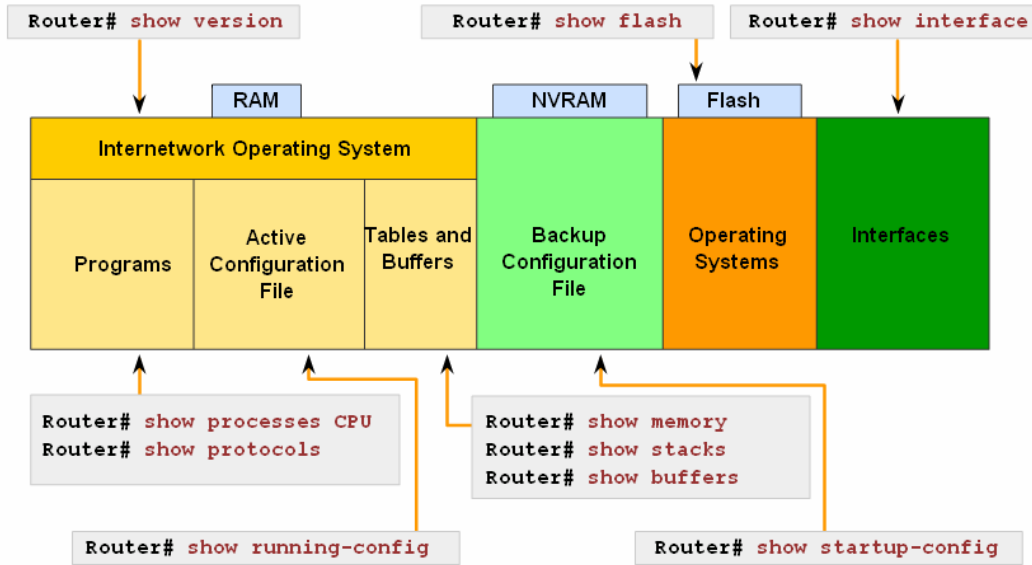
Router uptime is 1 hour, 15 minutes
System restarted by reload
System image file is "flash:c2500-i-1.113-4", booted via flash

cisco 2500 (68030) processor (revision N) with 2048K/2048K bytes of memory.
Processor board ID 11832659, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102
```

Comandos	Función
show interfaces	Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido de la interfaz específica y el número de puerto. Por ejemplo: Router#show interfaces serial 0/1
show controllers serial	Muestra información específica de la interfase de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz. Por ejemplo: Router#show controllers serial 0/1
show clock:	Muestra la hora fijada en el router
show hosts	Muestra la lista en caché de los nombres de host y sus direcciones
show users	Muestra todos los usuarios conectados al router
show history	Muestra un historial de los comandos ingresados
show flash	Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí
show version	Despliega la información acerca del router y de la imagen de IOS que esté corriendo en la RAM. Este comando también muestra el valor del registro de configuración del router
show ARP:	Muestra la tabla ARP del router
show protocols	Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado
show startup-configuration	Muestra el archivo de configuración almacenado en la NVRAM
show running-configuration	Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class

IOS show commands can provide information about the configuration, operation and status of parts of a Cisco router.



16.2. Configuración de una interfaz serial

Las tarea de configurar una interfaz serial es muy simple y se realiza desde la consola o usando una sesión telnet.

Siga estos pasos para configurar una interfaz serial:

1. Ingrese al modo de configuración global
2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. Si el cable de conexión es DCE, fije la velocidad de sincronización. Esto no es necesario si el cable es DTE.
5. Active la interfaz.

Cada interfaz serial activa debe tener una dirección IP y la correspondiente máscara de subred, si se necesita que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

```
Router (config)#interface serial 0/0
Router(config-if)#ip address <ip address> <netmask>
```

Una necesidad para las interfaces seriales es que requieren una señal de sincronización que controle la comunicación. Generalmente, un dispositivo DCE, por ejemplo un CSU, proporciona dicha señal. Por defecto, los routers Cisco son dispositivos DTE, pero se pueden configurar como dispositivos DCE.

Otro dato importante es que el estado predeterminado de las interfaces es APAGADO (DOWN), es decir están apagadas o inactivas. Para encender o activar una interfaz, ingresamos el comando: `#no shutdown`. En caso sea necesario inhabilitar administrativamente una interfaz para realizar algún tipo de mantenimiento o de diagnóstico de fallas, se hace uso del comando `shutdown` para desactivarla.

Generalmente en el entorno del laboratorio, se utilizará una velocidad de sincronización de 56000. Los comandos para fijar la velocidad de sincronización y activar una interfaz serial son los siguientes:

```
Router (config)#interface serial 0/0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

16.3 Cambios en la Configuración

Si es necesario modificar una configuración, se debe ir al modo de operación apropiado e ingresar el comando correspondiente. Así tenemos que para activar una interfaz, ingrese al modo de configuración global, luego al modo de configuración de interfaces, y ejecute el comando **no shutdown**

Para comprobar los cambios, use el comando **show running-config**. Este comando mostrará la configuración actual. Si las variables que se muestran no son las esperadas, es posible corregir el entorno efectuando uno o más de los siguientes pasos:

- Ejecute la forma negada (usar no previamente al comando) de un comando de configuración.
- Vuelva a cargar el sistema para regresar a la configuración original de configuración almacenada en la NVRAM.
- Copie un archivo de configuración desde un servidor TFTP.
- Elimine el archivo de configuración de inicio con `erase startup-config`, luego reinicie el router e ingrese al modo de configuración inicial (setup).

Para guardar las modificaciones hechas en el archivo de configuración de inicio en NVRAM, ejecute el siguiente comando al estar en EXEC privilegiado:

```
Router#copy running-config startup-config
```

16.4 Configuración de una interfaz Ethernet

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual (sesión telnet).

Cada interfaz Ethernet que requiera rutear paquetes IP debe estar activa y se le debe asignar una dirección IP y la correspondiente máscara de subred.

Para configurar una interfaz Ethernet, siga estos pasos:

- Ingrese al modo de configuración global
- Ingrese al modo de configuración de interfaz
- Especifique la dirección de la interfaz y la máscara de subred
- Active la interfaz

```
Router (config) #interface e0
Router (config-if) #ip address 183.8.126.2 255.255.255.128
Router (config-if) #no shutdown
```

16.5 Pasos finales de la configuración

16.5.1 Descripción de interfaces

El comando descripción es sólo un comentario escrito que se agrega acerca de la interfaz. Esta descripción se agrega en los archivos de configuración en la memoria del router, sin embargo no tiene efectos sobre la operación de la interfaz.

```
Cibertec(config-if)#description Academico
Cibertec(config-if)#
```

Luego de haber ingresado este comando si regresamos al modo “enable”, e ingresamos el comando: #show running-config, veremos la siguiente información en relación a la interfase Ethernet:

```
interface FastEthernet0/0
description Academico
no ip address
duplex auto
speed auto
shutdown
```

16.5.2 Mensajes de inicio de sesión

Existe la posibilidad de agregar un mensaje de inicio de sesión para que sea visualizado por el usuario al momento de hacer login en el router, y es utilizado para comunicar información de interés a todos los usuarios de la red.

Para esto ingrese al modo de configuración global para configurar un texto como mensaje del día (MOTD). Use el comando banner motd, seguido de un espacio y un delimitador, como por ejemplo el signo numeral (#). Escriba el mensaje del día (MOTD) seguido de un espacio y de nuevo el delimitador.

```
Cibertec(config)#banner motd #Bienvenidos a la red #
Cibertec(config)#
```

16.5.3 Resolución de nombres de host

Mecanismo que utiliza un computador para relacionar un nombre de host con una dirección de IP. Una tabla de host puede incluir todos los dispositivos de una red. Cada dirección de IP individual puede estar vinculada a un nombre de host. Ejecute el comando ip host seguido del nombre de destino y todas las direcciones de IP con las que se puede llegar al dispositivo.

```
Cibertec(config)#ip host Cibertec 172.16.0.1
```

El comando show hosts, nos muestra los nombres asociadas a las interfaces.

```
Cibertec#show hosts
```

16.5.4 Hacer copias de respaldo y documentar la configuración

La administración de las configuraciones de los dispositivos incluyen las siguientes tareas:

- Confeccionar una lista y comparar los archivos de configuración de los dispositivos activos
- Almacenar los archivos de configuración en servidores de red
- Instalar y actualizar software

16.5.5 Copiar, modificar y pegar configuraciones

Es muy útil almacenar una copia de la configuración en uso, en un servidor TFTP.

Para esto se puede usar el comando: copy running-config tftp

También es posible restaurar la información desde un servidor TFTP al router:

Autoevaluación

1. ¿Cuál es el estado por defecto de las interfaces de un router?
 - a. activadas, protocolo de línea desactivado
 - b. desactivadas, protocolo de línea desactivado
 - c. administrativamente desactivadas, protocolo de línea desactivado
 - d. activadas, protocolo de línea activado

2. Un administrador de red desea asegurarse de que cualquier contraseña que permita el acceso al modo EXEC privilegiado aparezca encriptada en los archivos de configuración. Escoja los comandos que puedan realizar esto (Elija dos opciones).
 - a. Router(config)#**enable cisco secret**
 - b. Router(config)#**enable cisco**
 - c. Router(config)#**service password-encryption**
 - d. Router(config)#**enable secret cisco**
 - e. Router(config)#**encrypt-all cisco**
 - f. Router(config)#**service encryption-password**

3. ¿Que valores se asignan por defecto a una interfaz serial?
(Elija tres opciones).
 - a. DTE
 - b. DCE
 - c. apagado
 - d. sin dirección IP
 - e. velocidad de reloj 56000
 - f. encapsulamiento ARPA

Para recordar

Si es necesario modificar una configuración, se debe ir al modo de operación apropiado e ingresar el comando correspondiente. Así tenemos que para activar una interfaz, ingrese al modo de configuración global, luego al modo de configuración de interfaces, y ejecute el comando **no shutdown**

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual (sesión telnet).

Cada interfaz Ethernet que requiera rutear paquetes IP debe estar activa y se le debe asignar una dirección IP y la correspondiente máscara de subred.