UNIVERSIDAD NACIONAL DE COLOMBIA
TELEMEDICINA

Alexei Ochoa Duarte
285295

Septiembre 9 de 2009

TECNOLOGÍAS Y PROTOCOLOS DE RED

Introducción:

Desde hace mucho tiempo, la comunicación ha jugado un papel fundamental en el desarrollo humano, permitiendo que las personas se relacionen estableciendo vínculos sociales mediante los cuales comparten ideas, conocimientos e información que enriquece muchos aspectos de su vida. Con el desarrollo tecnológico, se hizo notable la necesidad de extender el concepto de comunicación de tal forma que mediante él se pudieran integrar elementos tecnológicos que facilitaran el intercambio de ideas y conocimientos con personas en diferentes lugares del mundo.

La comunicación puede darse mediante diferentes métodos, los cuales tienen tres elementos en común. El primero de estos elementos es el origen del mensaje o emisor. Los emisores 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, está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.

Para que la comunicación sea efectiva, existen unas reglas básicas como hablar el mismo idioma, escuchar y esperar el turno para hablar, estar atento al mensaje, etc; dichas reglas se denominan protocolos y éste concepto se extiende a las redes informáticas.

¿Qué es una red informática?

El término red se refiriere un conjunto de dispositivos interconectados capaces de compartir recursos, proveer servicios y transportar gran cantidad de información como datos informáticos, voz interactiva, video y productos de entretenimiento. El objetivo de una red informática es que los dispositivos se comuniquen y compartan archivos.

Los mensajes pueden enviarse convirtiéndolos en dígitos binarios o bits. Luego, estos bits se codifican en una señal que se puede transmitir por el medio apropiado. En las redes de computadoras, el medio generalmente es un tipo de cable o una transmisión inalámbrica.

Los avances de la tecnología nos permiten consolidar el flujo de voz, vídeo y datos en una misma red, eliminando la necesidad de crear y mantener redes separadas. Esto se conoce como red convergente, y en ellas hay muchos puntos de contacto y muchos dispositivos especializados, como lo son las computadoras personales, teléfonos, televisores, asistentes personales; pero una sola infraestructura de red común.

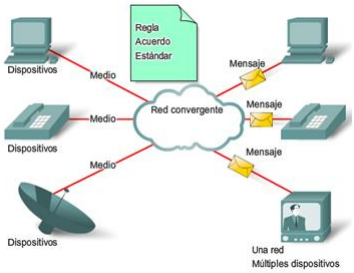

FIGURA 1. Red Convergente

Componentes de una red

Para lograr una buena comunicación, la red debe integrar correctamente ciertos dispositivos, medios, servicios y procesos.

Los dispositivos y los medios son los elementos físicos o hardware de la red, mientras que los servicios y procesos son los programas de comunicación, denominados software, que se ejecutan en los dispositivos conectados a la red.

Dispositivos

Las personas reconocen más fácilmente los dispositivos finales ya que constituyen la interfaz entre la red humana y la red de comunicación.

Algunos ejemplos de dispositivos finales son: Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web), impresoras de red, teléfonos VoIP, cámaras de seguridad, dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

En el contexto de una red informática, los dispositivos finales se denominan host y pueden ser el origen o el destino de un mensaje transmitido a través de la red. Además para facilitar su identificación, se les asigna una dirección.

También existen los dispositivos intermediarios para proporcionar conectividad y garantizar que los datos fluyan a través de la red. También es una función de los dispositivos intermediarios la administración de datos mientras fluyen a través de la red. Algunos dispositivos de red intermediarios son hubs, switches, puntos de acceso inalámbricos, routers, servidores de comunicación, módems, y firewalls.

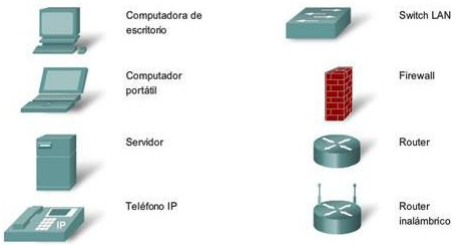

FIGURA 2. Dispositivos de una Red

Medios

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

La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los criterios para elegir un medio de red son: la distancia en la cual el medio puede transportar exitosamente una señal, el ambiente en el cual se instalará el medio, la cantidad de datos y la velocidad a la que se deben transmitir, y el costo del medio y de la instalación.

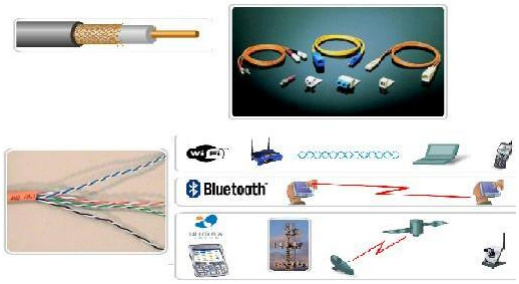

FIGURA 3. Medios que puede usar una Red

Servicios y procesos

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son: acceso, archivos, impresión, correo, información.

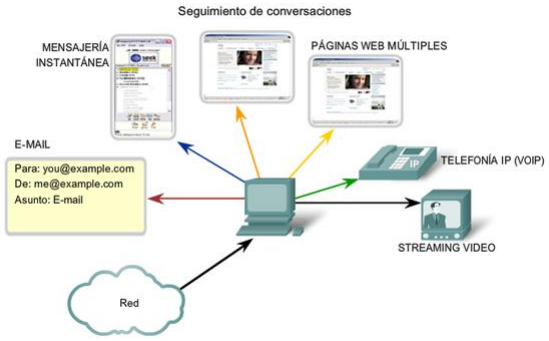

FIGURA 4. Servicios que ofrece una Red

Entre los procesos se pueden encontrar: encapsulación (se envuelven datos en un encabezado de protocolo particular), segmentación (se divide la información para facilitar su transporte) y formateo (se definen la forma como se almacena y transporta la información).

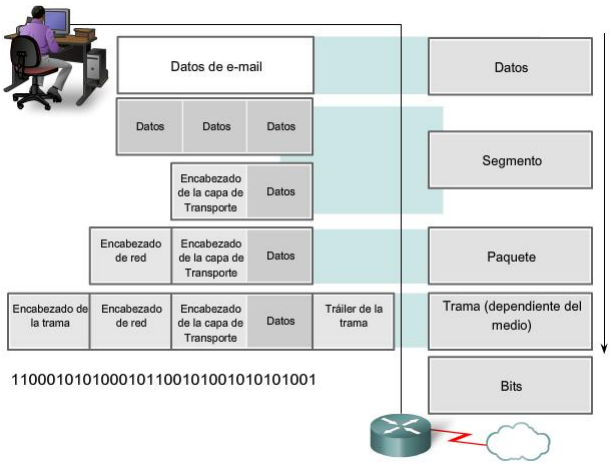

FIGURA 5. Proceso de Encapsulación

Arquitectura de Red

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo.

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales.

Los mecanismos de calidad del servicio (QoS) permiten el establecimiento de estrategias de administración de filas que implementan prioridades para las diferentes clasificaciones de los datos de aplicación.

Existen muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red y cumplir las expectativas de privacidad de los usuarios.

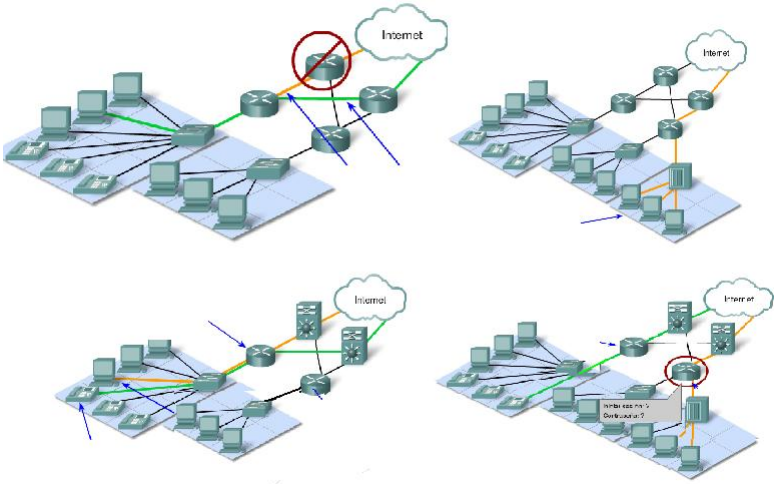

FIGURA 6. Arquitectura de Red

Infraestructura de redes

Las infraestructuras de red pueden variar en gran medida en términos de: el tamaño del área cubierta, la cantidad de usuarios conectados, y la cantidad y tipos de servicios disponibles. Una red cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN), la cual es administrada por una organización única. Las redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN)

Las LAN y WAN son de mucha utilidad para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de información, imágenes, video, e-mails, capacitación corporativa y acceso a recursos.

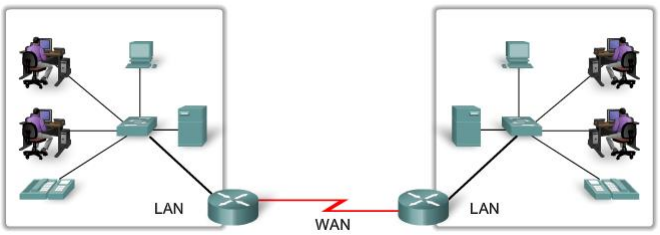

FIGURA 7. Redes LAN y WAN

Protocolos

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas denominadas protocolos. En las redes informáticas, los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores competen a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz del usuario. Los

protocolos describen procesos como los siguientes: el formato o estructura del mensaje, el método por el cual los dispositivos de red comparten información sobre rutas con otras redes, cómo y cuando se pasan los mensajes de error y del sistema entre dispositivos, o el inicio y terminación de las sesiones de transferencia de datos.

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas el cual muestra el funcionamiento de los protocolos que se produce dentro de cada capa, al igual que la interacción de las capas sobre y debajo de él. Algunos de los beneficios de los modelos en capas son: Asiste en el diseño del protocolo, fomenta la competencia, evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores y proporciona un lenguaje común.

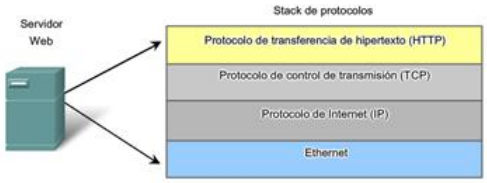

FIGURA 8. Protocolos en capas

Existen dos tipos básicos de modelos de red: modelos de protocolo y modelos de referencia. Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. Mientras que un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red.

Cuando se realiza un proceso de comunicación ocurre lo siguiente:
En el dispositivo de origen, a nivel de la capa de aplicación, se crean los datos del mensaje que se van a transmitir. Éstos pasan por capas de protocolos donde se segmentan y encapsulan. Luego, en la capa de acceso a red se generan esos datos sobre el medio dependiendo la codificación requerida. A continuación esos datos viajan a través del medio físico hasta el dispositivo de destino, el cual recibe los datos y los desencapsula para rearmarlos y pasarlos a la capa de aplicación del receptor.

Los métodos para realizar lo anterior se definen de forma diferente según el modelo utilizado.

Modelo OSI

El modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO). Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.

El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red

Las capas que componen el modelo OSI son:

1. *Física:* describe los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar las conexiones del dispositivo.
2. *Enlace de datos:* describe los métodos para intercambiar tramas de datos entre dispositivos en común.
3. *Red:* brinda servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.

4. *Transporte:* define los servicios para segmentar, transferir y re ensamblar los datos. También realiza funciones como acuse de recibo, recuperación de errores y secuenciamiento.
5. *Sesión:* ofrece servicios a la capa de presentación para organizar su dialogo y administrar el intercambio de datos.
6. *Presentación:* ofrece una representación común de los datos transferidos entre los servicios de la capa de aplicación.
7. *Aplicación:* es el enlace entre las demás capas y las personas para que puedan realizar sus actividades.

Modelo TCP/IP

En este modelo, las capas se encuentran dividas de la siguiente manera:

1. *Acceso a la red:* controla los dispositivos de hardware y los medios que conforman la red.
2. *Internet:* determina la mejor ruta a través de la red.
3. *Transporte:* admite la comunicación entre diversos dispositivos de diferentes redes.
4. *Aplicación:* representa datos para el usuario además tiene control de codificación y de dialogo.

Cuando se envía un mensaje, los datos se dividen en paquetes, y se ordenan en una secuencia, agrega cierta información para control de errores y después los lanza hacia la red, y los distribuye. Luego, se reciben los paquetes en el destino, se verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el host de destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

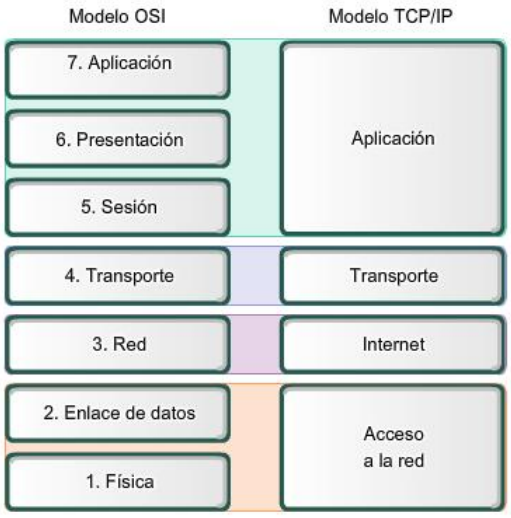

FIGURA 9. Modelos de Red

Capa de Red

En esta capa se realizan cuatro procesos básicos para enviar datos de un host a otro, dichos procesos son: direccionamiento, encapsulamiento, enrutamiento y desencapsulamiento.

Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única, por ello esta capa tiene un mecanismo de direccionamiento que utiliza el protocolo IP.

El enrutamiento tiene que ver con cómo se determina la ruta entre el host de origen y el de destino. En este proceso interviene el router seleccionando las rutas y dirigiendo los paquetes hacia su destino.

Protocolo IP

IP es la abreviatura de protocolo de Internet. Este protocolo se encuentra en la capa de red y brinda un servicio no orientado a la conexión suministrando características de direccionamientos, especificación de servicios, segmentación, reensamblaje y seguridad. Cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como las señales de radio.

Cuando se va a enviar un mensaje, éste se divide en varios paquetes a los cuales se les coloca un encabezado con características importantes para que el host destino pueda ensamblarlos de nuevo e interpretar correctamente la información.

El protocolo IP no sobrecarga el servicio IP suministrando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño por lo cual transportar los paquetes genera una menor sobrecarga, es decir, menos demora en la entrega.

La capa de Red tampoco está cargada con las características de los medios mediante los cuales se transportarán los paquetes, lo cual significa que el protocolo es independiente de la tecnología que se use para la comunicación.

El encabezado de un paquete IP no incluye los campos requeridos para la entrega confiable de datos. No hay acuses de recibo de entrega de paquetes. No hay control de error para datos. Tampoco hay forma de rastrear paquetes; por lo tanto, no existe la posibilidad de retransmitir paquetes.

Este encabezado contiene campos importantes con valores binarios que determinan la siguiente información:

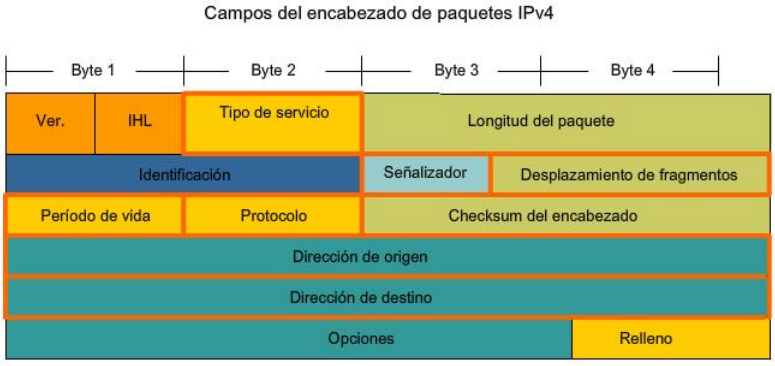

FIGURA 10. Encabezado IP

Dirección IP destino: valor de 32 bits que representa la dirección de host de capa de red de destino del paquete.

Dirección IP origen: valor de 32 bits que representa la dirección de host de capa de red de origen del paquete.

Tiempo de vida (TTL): valor de 8 bits que indica el tiempo remanente de "vida"del paquete y que va disminuyendo cada vez que se encuentra con un router. Este mecanismo evita que los paquetes que no pueden llegar a destino sean enviados indefinidamente entre los routers.

Protocolo: valor de 8 bits que indica el tipo de relleno de carga que el paquete traslada. El campo de protocolo permite a la Capa de red pasar los datos al protocolo apropiado de la capa superior.

Tipo de servicio: valor de 8 bits que se usa para determinar la prioridad de cada paquete.

Desplazamiento de fragmentos: identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

Señalizador de Más fragmentos: es un único bit que indica si hay o no más fragmentos.

Señalizador de No Fragmentar: es un solo bit en el campo del señalizador que indica que no se permite la fragmentación del paquete. Si se establece el bit del señalizador No Fragmentar, entonces la fragmentación de este paquete NO está permitida. Si un router necesita fragmentar un paquete para permitir el paso hacia abajo hasta la capa de Enlace de datos pero el bit DF se establece en 1, entonces el router descartará este paquete.

Versión: Contiene el número IP de la versión.

Longitud del encabezado (IHL). Especifica el tamaño del encabezado del paquete.

Longitud del Paquete: Este campo muestra el tamaño completo del paquete, incluyendo el encabezado y los datos, en bytes.

Identificación: Este campo es principalmente utilizado para identificar únicamente fragmentos de un paquete IP original.

Checksum del encabezado: El campo de checksum se utiliza para controlar errores del encabezado del paquete.

Opciones: Existen medidas para campos adicionales en el encabezdo IPv4 para proveer otros servicios pero éstos son rara vez utilizados.

Direccionamiento IP

La dirección IP es un identificador numérico asignado a cada máquina en una red. Designa la ubicación del dispositivo en la red. Es una dirección lógica y no física, que se encuentra codificada en la tarjeta de interfaz de red (NIC) y fue diseñada para que un host se comunique con otro.

En este tipo de direccionamiento se tienen tres tipos de direcciones: una de red (se usa para enviar paquetes a una red remota), una de host (usada para enviar información a un solo dispositivo de la red), y una de broadcast (usada para enviar información a todos los nodos de una red). Las direcciones IP tienen 32 bits, divididos en 4 secciones llamadas octetos, cada uno con un byte.

Estas direcciones se pueden escribir en forma binaria, decimal punteada o hexadecimal. La más usada es la de decimal punteado.

Después de la dirección se escribe un número al cual generalmente se llama máscara de red y que es la cantidad de bits en la dirección que conforma la porción de red. Estas máscaras se utilizan en el direccionamiento sin clase, y para crear subredes que permiten reducir el tráfico en la red, simplificar la administración de la misma facilitar la comunicación a larga distancia y optimizar el funcionamiento de la red.

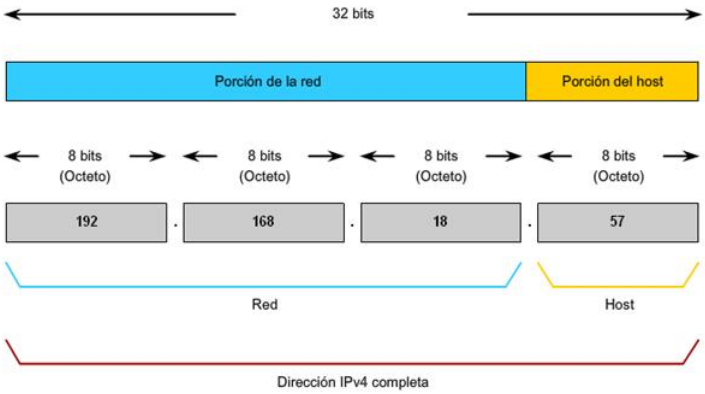

FIGURA 11. Dirección IP V4

Capa de Transporte

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

Para identificar todos los segmentos de datos, en esta capa se agrega un encabezado a la sección que contiene datos binarios, el cual contiene campos de bits que permiten que los protocolos de la capa de Transporte lleven a cabo las diversas funciones.

Además de utilizar la información contenida en los encabezados para las funciones básicas de segmentación y reensamblaje de datos, algunos protocolos de la capa de Transporte proveen: conversaciones orientadas a la conexión, entrega confiable, reconstrucción ordenada de datos, y control del flujo.

Protocolo TCP y UDP

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

UDP es un protocolo simple, sin conexión y provee la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de Transporte envía estos datagramas como "mejor intento".

Entre las aplicaciones que utilizan UDP se incluyen: sistema de nombres de dominios (DNS), streaming de vídeo, y Voz sobre IP (VoIP).

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

Las aplicaciones que utilizan TCP son: exploradores Web, e-mail, y transferencia de archivos. La diferencia clave entre TCP y UDP es la confiabilidad, pero además, TCP y UDP gestionan la segmentación de forma distinta.

Los servicios basados en TCP y UDP mantienen un seguimiento de las varias aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones. Estos identificadores únicos son los números de los puertos.

En el encabezado de cada segmento o datagrama hay un puerto de origen y destino. El número de puerto de origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino en el host remoto.

Protocolo TCP

Con TCP, cada encabezado de segmento contiene un número de secuencia que permite que las funciones de la capa de Transporte del host de destino reensamblen los segmentos en el mismo orden en el que fueron transmitidos. Esto asegura que la aplicación de destino cuente con los datos en la forma exacta en la que se enviaron.

La confiabilidad de la comunicación TCP se lleva a cabo utilizando sesiones orientadas a la conexión. Antes de que un host que utiliza TCP envíe datos a otro host, la capa de Transporte inicia un proceso para crear una conexión con el destino. Esta conexión permite el rastreo de una sesión o stream de comunicación entre los hosts. Este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare. Una conversación TCP completa requiere el establecimiento de una sesión entre los hosts en ambas direcciones.

Luego de establecida la sesión, el destino envía acuses de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino.

Parte de la carga adicional que genera el uso de TCP es el tráfico de red generado por los acuses de recibo y las retransmisiones. El establecimiento de las sesiones genera cargas en forma de segmentos adicionales intercambiados. También existen cargas adicionales en los hosts individuales, generadas por la necesidad de mantener un seguimiento de los segmentos que esperan acuse de recibo y por el proceso de retransmisión.

Esta confiabilidad se logra contando con campos en el segmento TCP, cada uno con una función específica.

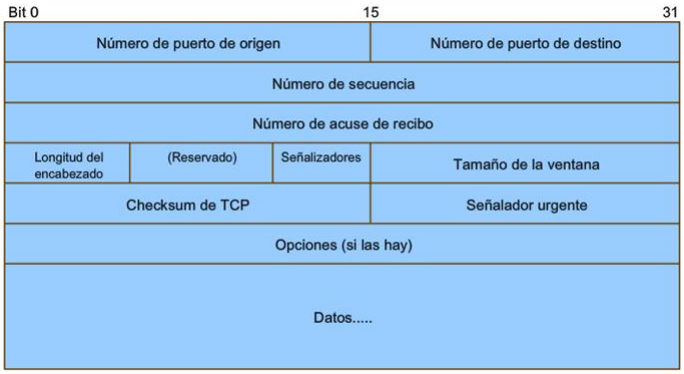

FIGURA 12. Datagrama TCP

Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de Aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga.

Protocolo UDP

A pesar de que los servicios que utilizan UDP también rastrean las conversaciones entre aplicaciones, no tienen en cuenta el orden en el que se transmitió la información ni el mantenimiento de la conexión. UDP es un diseño simple; que no tiene número de secuencia en el encabezado y genera menos carga que TCP, lo que produce una transferencia de datos más rápida.

Este protocolo tampoco es orientado a la conexión y no cuenta con los sofisticados mecanismos de retransmisión, secuenciación y control del flujo. Esto no significa que las aplicaciones que utilizan UDP no sean confiables. Sólo quiere decir que estas funciones no son contempladas por el protocolo de la capa de Transporte y deben implementarse aparte, si fuera necesario.

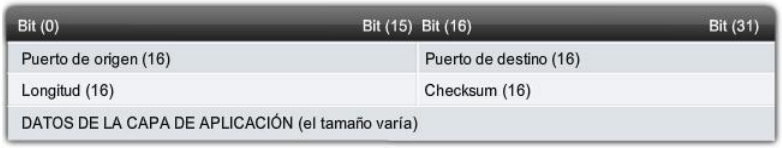

FIGURA 13. Datagrama UDP

Ya que UDP opera sin conexión, las sesiones no se establecen antes de que se lleve a cabo la comunicación, como sucede con TCP. Se dice que UDP es basado en transacciones. En otras palabras, cuando una aplicación posee datos para enviar, simplemente los envía.

Cuando se envían múltiples datagramas a un destino, los mismos pueden tomar rutas distintas y llegar en el orden incorrecto. UDP no mantiene un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no puede reordenar los datagramas en el orden de la transmisión.

Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de los datos es importante para la aplicación, la misma deberá identificar la secuencia adecuada de datos y determinar cómo procesarlos.

Referencias

- Torres Nieto, Alvaro. Telecomunicaciones y telemática. Escuela Colombiana de Ingeniería. 2007
- Comer, Douglas E. Internetworking with TCP/IP. Ed. Prentice Hall. 2006
- Stallings, William. Comunicaciones y redes de computadores. Ed. Prentice Hall. 2005
- Tanenbaum, Andrew S. Redes de computadoras. Pearson Educación. 2003
- Cisco CCNA Exploration 4.0. Aspectos Básicos de Networking.