INTRODUCCIÓN

Los protocolos forman la base esencial de una red, debido a que estos establecen el lenguaje de comunicación que se va a utilizar entre los distintos equipos de una red para la transmisión de datos entre sí.

PROTOCOLOS

Definen el conjunto de reglas o convenciones establecidas y aceptadas de manera general, que regulan el intercambio de información entre los nodos (conexiones, uniones) de una red. La complejidad de un protocolo radica en dos aspectos: el número de estaciones involucradas en la comunicación a través de un medio de transmisión y el método de acceso al canal.

- Protocolo orientado a carácter:

  En este tipo de protocolos todos los controles están dirigidos a garantizar la calidad de los caracteres en la comunicación, entre este tipo de protocolos se encuentra el de Comunicaciones Síncronas Binarias (BSC).

- Protocolo orientado a bit:

  Con los protocolos orientados a bit, la información se transfiere bit por bit y utilizan el siguiente formato:

Bandera	Campo de Dirección	Campo de Control	Campo de Datos	Campo de Chequeo (BCC)	Bandera
8 Bits	8 Bits	8 bits	n X 8 Bits	16 Bits	8 Bits

- Bandera: Se utilizan al principio y al final del paquete para sincronizar el sistema, se envían aún cuando la línea este en reposo, está formada por 8 bits (01111110).

- Campo de dirección: Es una secuencia de 8 bits que identifica las estaciones en una comunicación.

- Campo de control: Es una secuencia de 8 bits que permite establecer comandos o respuestas codificadas.

- Campo de datos: Contiene toda la información, el número de bits debe ser múltiplo de 8.

- Campo de Chequeo de Errores: Es un polinomio CRC-16 que permite el chequeo por redundancia de errores.

Características de los protocolos:

- Control de errores: Debido a que en todos los sistemas de comunicación cabe la posibilidad de que aparezcan errores por la distorsión de la señal transmitida en el camino que va desde el emisor al receptor, Se hace necesario el uso de un control de errores; a través de un procedimiento de detección y corrección de errores (o retransmisión de los datos).

  Para el control de errores se utilizan unas técnicas necesarias para recuperar pérdidas o deterioros de los datos y de la información de control. Por lo general el control de errores se aplica por medio de dos funciones separadas: La retransmisión y la detección de errores.

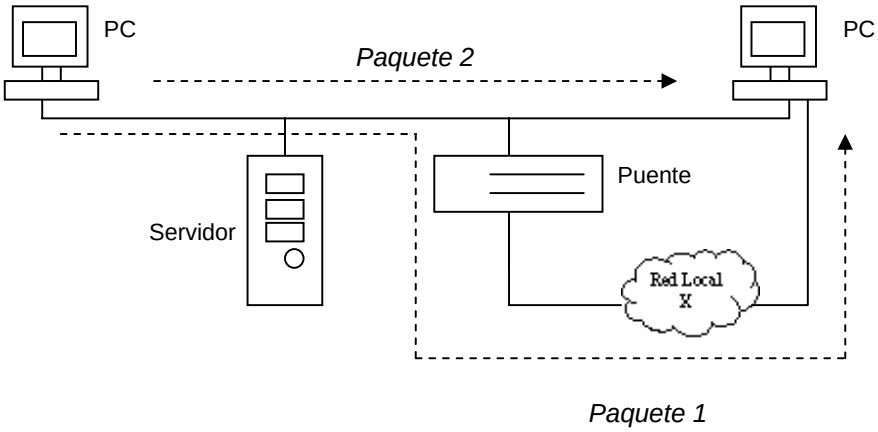
- Control de flujo de datos: Para evitar que el emisor sature al receptor transmitiendo datos más rápido de lo que el receptor o destino pueda asimilar y procesar, se hace necesario el uso de ciertos procedimientos llamados controles de flujo.

  El control de flujo es una operación realizada por el receptor (destino) para limitar la velocidad o cantidad de datos que envía la entidad el emisor (origen o fuente). Una de las maneras de aplicar el control de flujo es mediante el uso de “parada y espera”, en el que se debe confirmar el paquete de información recibido antes de enviar el siguiente.

Otra manera de utilizar un control de flujo es mediante el envío de la información de la cantidad de datos que pueden ser transmitidos sin tener que esperar la confirmación.

- Formato de los datos: Esto tiene que ver con el acuerdo que debe existir entre las dos partes respectos al formato de los datos intercambiados, como por ejemplo el código binario usado para representar los caracteres.

- Orden de los datos: El orden de los datos es esencial en una red donde existen diferentes estaciones (terminales, estaciones de trabajo, servidores, etc.) conectadas, debido a que los paquetes de información pueden ser recibidos de manera diferente, ya sea por que toman caminos distintos a través de la red, por ejemplo, si el paquete 1 toma una ruta larga y el paquete 2 toma una corta, evidentemente el paquete No. 2 llegará primero (suponiendo que los dos paquetes son del mismo tamaño), y los datos recibidos no serán los mismos que están en el emisor (debido a que tendrán un orden diferente en el receptor).



Normas para sistemas abiertos OSI:

El modelo OSI sirve como marco de referencia para reducir la complejidad implícita en el estudio y diseño de las redes (LAN/WAN). El proceso de comunicación se describe como una jerarquía de siete capas o niveles. Cada capa tiene un propósito bien definido: brindar servicios de red a la capa superior, utilizando los servicios que le brinda la capa inferior. La capa “n” de un nodo establece una comunicación virtual con la capa “n” de otro nodo.

Capa	Descripción
Aplicación	Provee el conjunto de aplicaciones de red, como por ejemplo: Transferencia de archivos, emulación de terminal, correo electrónico, discos virtuales, etc. **Aplicaciones:** FTP, Telnet, SMTP, NFS, etc.
Presentación:	Provee las funciones de formato y conversión de códigos, necesarias para que los datos sean más fácilmente interpretados por los programas de aplicación. **Ejemplo:** ASCII, EBCDIC, representación de números enteros y reales, etc.
Sesión	Es responsable del establecimiento y mantenimiento de las sesiones de comunicación entre los programas de comunicación.
Transporte	Define los mecanismos para mantener la confiabilidad de las comunicaciones en la red **Funciones:** Regulación de flujo de mensajes, retransmisión de paquetes, inicio/terminación de sesiones entre nodos, etc. **Protocolos:** TCP, SPX, etc.
Red	Define los mecanismos para determinar las rutas que deben seguir los paquetes dentro de la red y para el control de la congestión. **Unidad de transmisión:** PACKET. **Funciones:** Enrutamiento de paquetes en la red, ofrece un canal libre de errores a la capa de transporte. **Protocolos:** IP, IPX, VTAM, etc.
Enlace	Define el protocolo de comunicación que usan los nodos de la red, para acceder al medio de transmisión. **Unidad de transmisión:** FRAME. **Funciones:** Control de acceso al canal (manejo de colisiones, manejo del testigo, etc.), dividir los paquetes recibidos de la capa superior en grupos de bits. Provee mecanismos para detección y corrección de errores. **Protocolos:** LAN – Ethernet (IEEE 802.3), Token Ring (802.5), FDDI, etc. WAN – SDLC, HDLC, PPP, LAPB.
Física	Define la conexión física entre el nodo y la red, incluyendo los aspectos físicos, mecánicos (cables, conectores, secuencia de pines) y aspectos eléctricos (niveles de voltaje, técnicas usadas para modular la señal), etc. **Unidad de transmisión:** BIT. **Funciones:** Transmisión de bits sobre el canal de comunicación: - Acotados: Par de cables trenzados, cable coaxial, fibra óptica, etc. - No Acotados: Microondas, radio, satélite, etc. **Estándares:** RS-232C, RS-449, V.24, V.35.

En general, los servicios provistos por una capa pueden clasificarse en dos grupos:

Servicio orientado a conexión: La comunicación se lleva a cabo a través del establecimiento de un circuito virtual permanente (sesión) entre dos nodos. Como consecuencia presenta las siguientes características:

- Utiliza técnicas de detección y corrección de errores para garantizar la transmisión. Esto implica mayor utilización de ancho de banda.
- Cada mensaje se recibe en el mismo orden en que se envió.
- Ejemplo: Transferencia de archivos

Servicio no orientado a conexión: No se establece circuito alguno entre nodos de la red. Características:

- Cada mensaje puede ser enrutado independientemente.
- No se garantiza que los mensajes lleguen en el mismo orden en que son enviados.
- Requiere menos ancho de banda, debido a que no utiliza técnicas para detectar o corregir errores. Esto no necesariamente implica que la comunicación es poco confiable. La detección y corrección de errores puede efectuarse en otras capas en referencia al modelo OSI.
- Ejemplo: Correo electrónico, discos virtuales.

TCP/IP:

Constituye una familia de protocolos de comunicación diseñados con una motivación fundamental: Lograr la interoperabilidad entre los diferentes sistemas de comunicación de una red heterogénea/multivendedor en forma transparente para el usuario final. Tal heterogeneidad se manifiesta a diferentes niveles de interconexión los cuales van desde los protocolos de la capa física hasta las aplicaciones.

TCP/IP constituye la familia de protocolos con mayor número de instalaciones a nivel internacional. Sus orígenes se remontan a inicios de los años 70, cuando un conjunto de investigadores del Departamento de Defensa de los Estados Unidos dio inicio a un proyecto cuyo propósito fue diseñar un conjunto de protocolos que pudiera ofrecer

interoperabilidad a la variedad de ambientes de computación conectados a sus redes. Es así como nace ARPANET (Advanced Research Project Agency Net) y posteriormente Internet, la red con mayor cantidad de usuarios y computadores conectados a nivel mundial.

A continuación se presentan los diferentes protocolos pertenecientes a la *suite* TCP/IP tomando como marco de referencia el modelo OSI.

<table>
<tr><td>Aplicación</td><td rowspan="3">Telnet
Tn3270
Tn5250
X-Windows</td><td rowspan="3">FTP
TFTP</td><td rowspan="3">SMTP
(e-Mail)</td><td rowspan="3">DNS</td><td rowspan="3">NFS
RPC</td><td rowspan="3">SNMP
Ping</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td colspan="3">TCP</td><td colspan="3">UDP</td></tr>
<tr><td>Red</td><td colspan="6">IP
(ICMP, ARP, RARP, Proxy ARP)</td></tr>
<tr><td>Enlace</td><td colspan="3">IEEE 802.3,
IEEE 802.5,
ANSI X3T9.5</td><td colspan="3">HDLC, SDLC,
PPP, SLIP, CSLIP</td></tr>
<tr><td>Física</td><td colspan="6">Ethernet, Token Ring, FDDI, X.21, ISDN, RS-232C, V.35, etc.</td></tr>
</table>

Protocolos de la capa de Transporte:

1) TCP (Transmision Control Protocol):
   Es un protocolo orientado a conexión, full-duplex que provee un circuito virtual totalmente confiable para la transmisión de información entre dos aplicaciones. TCP garantiza que la información enviada llegue hasta su destino sin errores y en el mismo orden en que fue enviada.

2) UDP (User Datagram Protocol):
   Es un protocolo no orientado a conexión full duplex y como tal no garantiza que la transferencia de datos sea libre de errores, tampoco garantiza el orden de llegada de los paquetes transmitidos. La principal ventaja del UDP sobre el TCP es el rendimiento; algunas de las aplicaciones que utilizan el UDP son TFTP, NFS, SNMP y SMTP.

Protocolos de la capa de red:

1) IP (Internet Protocol):
   Provee la información necesaria para permitir el enrutamiento de los paquetes en una red. Divide los paquetes recibidos de la capa de transporte en segmentos que son transmitidos en diferentes paquetes. IP es un protocolo no orientado a conexión.

2) ICMP (Internet Control Message Protocol):
   Este protocolo se emplea para el manejo de eventos como fallas en la red, detección de nodos o enrutadores no operativos, congestión en la red, etc., así como también para mensajes de control como "echo request". Un ejemplo típico del uso de este protocolo es la aplicación **PING**.

3) ARP (Address Resolution Protocol):
   Permite localizar la dirección física (Ethernet, Token Ring, etc.) de un nodo de la red, a partir de su dirección lógica (IP) la cual es conocida. A nivel de la capa de red, los nodos se comunican a través del uso de direcciones IP; no obstante, los paquetes IP se entregan a la capa de enlace para su colocación en el canal de comunicación. En ese momento, el protocolo de la capa de enlace no tiene conocimiento de la dirección física del nodo destino. La estrategia que utiliza ARP para investigar la dirección física es enviar un mensaje a todos los nodos de la red (*broadcast*), consultando a quien pertenece la dirección lógica destino. Cuando el nodo destino recibe el mensaje y lo pasa a la capa de red, detecta que es su dirección IP y reconoce que el nodo origen está solicitando su dirección física y responde.

4) RARP (Reverse Address Resolution Protocol):
   Ejecuta la operación inversa al protocolo ARP, permite a un nodo de la red localizar su dirección lógica a partir de su dirección física. Esta aplicación se utiliza en aquellos nodos de la red, que no proveen facilidades para almacenar permanentemente su dirección IP, como por ejemplo: microcomputadores o terminales sin disco duro.

5) Proxy ARP:

Cuando un nodo en la red “A” requiere comunicarse con otro nodo en la red “B”, necesita localizar su dirección física, sin embargo como los nodos se encuentran en redes distintas, es el enrutador quien se encarga de efectuar el cálculo de la dirección. En tal sentido, la dirección física entregada al nodo en la red “A” corresponde al enrutador conectado a esa red.

Aplicaciones y protocolos:

1) Telnet (Tn3270, Tn5250):
   Es el protocolo que define el conjunto de reglas y criterios necesarios para establecer sesiones de terminal virtual sobre la red. Telnet define los mecanismos que permiten conocer las características del computador destino. Así mismo, permite que los dos computadores (cliente y servidor) negocien el entorno y las especificaciones de la sesión de emulación de terminal.

   Telnet ---------- Familia de terminales VT (Unix, VMS)
   Tn3270 ---------- Familia de terminales 3270 (VM, MVS)
   Tn5250 ---------- Familia de terminales 5250 (SAA)

2) X-Windows:
   Fue desarrollado por el MIT con el propósito de proveer un sistema de emulación de ventanas gráficas en computadores con interfaces de despliegue basadas en mapas de bits (bitmaps). El término “Windows” hace referencia a la posibilidad de tener diferentes ventanas en un ambiente multitarea como Unix o Windows en forma simultánea.

3) FTP (File Transfer Protocol):
   Es un protocolo orientado a conexión que define los procedimientos para la transferencia de archivos entre dos nodos de la red (cliente/servidor). Cada nodo puede comportarse como cliente y servidor. FTP maneja todas las conversiones necesarias (código de caracteres [ASCII, EBCDIC], tipos de datos, representación de números enteros y reales, etc.) Para lograr la interoperabilidad entre dos computadores que utilizan sistemas de archivo diferentes y que trabajan bajo sistemas operativos diferentes. FTP está

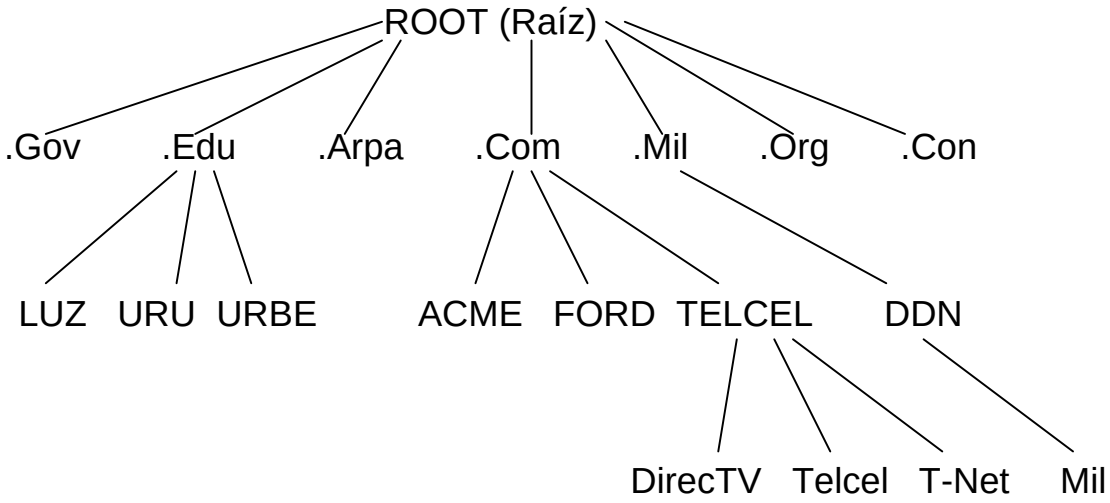
basado en TCP y como tal provee mecanismos de seguridad y autenticidad.

4) TFTP (Trivial File Transfer Protocol):
   Es un protocolo de transferencia de archivos no orientado a conexión. Es mucho menos complejo que FTP, es decir, soporta menos funciones, el código es más pequeño, consume menos memoria y como consecuencia es más rápido. Sin embargo, es menos confiable que FTP y no provee mecanismos de seguridad o autenticidad. Está basado en UDP.

5) SMTP (Simple Mail Transfer Protocol):
   Define los esquemas de envío y recepción de correo electrónico en la red. SMTP está basado en UDP y soporta el concepto de *Spooling*. El correo puede ser almacenado por la aplicación SMTP en memoria o disco y un servidor SMTP de la red, eventualmente chequea si hay correo e intenta enviarlo. Si el usuario o el computador no están disponibles en ese momento, intenta en una segunda oportunidad. Si finalmente el correo no puede ser enviado, el servidor puede borrar el mensaje o enviarlo de regreso al nodo origen.

6) DNS (Domain Name System):
   La estructura de las direcciones IP es un tanto difícil de manejar y recordar. Muchos usuarios han adoptado el uso de acrónimos o nombres para identificar una dirección numérica a través de archivos de configuración (hosts.txt) provistos por cada software de comunicación. Con el crecimiento de las redes, la administración del archivo “HOSTS.TXT” se volvió tediosa, debido a la necesidad de mantener actualizada la información en cada computador conectado a la red. Con esto en mente los administradores de Internet desarrollaron un procedimiento para administrar la asignación de nombres en forma centralizada denominado Domain Name System. DNS utiliza un sistema jerárquico que garantiza una correspondencia única entre cada dirección IP y cada nombre. Esta característica, requiere designar un organismo o comité oficial que garantice la asignación ordenada de dominios y subdominios. A su vez, este esquema permite a cada organización administrar la asignación de sus nombres dentro de un subdominio asignado. El concepto DNS se organiza alrededor de una estructura de árbol. La

raíz del árbol y los dominios de más alto nivel son administrados por el NIC (Network Information Center). Actualmente el DNS contiene siete dominios, debajo de los cuales se asignan subdominios a cada ente organizacional a nivel mundial.



7) NFS (Network File System)
   NFS fue desarrollado por Sun Microsystems, Inc. Para permitir el uso de discos virtuales en una red (RFC 1094). Define mecanismos para exportar e importar segmentos de un disco perteneciente a cualquier computador conectado a la red. NFS es independiente del sistema operativo o del hardware. Actualmente existen versiones NFS para Unix, DOS y Windows, Finder (Macintosh), MVS y VM (Mainframe), entre otros.

8) SNMP (Simple Network Management Protocol):
   Es el protocolo de administración y monitoreo de redes provisto por la *suite* de TCP/IP. SNMP define un esquema basado en el concepto cliente/servidor. En ese sentido, una red consiste de uno o más servidores de administración de red (Network Management Stations) y elementos de red administrables o agentes. El servidor SNMP ejecuta operaciones de monitoreo y control sobre las estaciones que poseen el agente. Un agente SNMP es un componente Hardware/Software que permite a un nodo de la red (micro, servidor, enrutador, etc.) responder a los requerimientos del

servidor SNMP. Toda la información que puede ser accedida a través de SNMP está contenida en una base de datos (MIB: Management Information Base) organizada en módulos y objetos. El servidor SNMP puede ejecutar operaciones de lectura (get) o escritura (set) en la base de datos. Adicionalmente un agente puede emitir mensajes no solicitados por el servidor, conocidos como “traps” para indicar diferentes condiciones como fallas, cambios en la configuración, violaciones de seguridad, etc.

9) PING (Packet Internet Grouper)
   Es un protocolo de verificación de conexiones en la red. Está basado en UDP e ICMP y su función es enviar un paquete a una dirección IP conocida y esperar respuesta (*echo-reply*). Ésta operación básica permite detectar si el nodo destino se encuentra operativo; asimismo, permite comprobar la configuración de hardware y software en el nodo origen y destino, como también en los enrutadores.

Diferencias entre TCP/IP y OSI:

A diferencia del modelo OSI, los servicios provistos por las capas de sesión, presentación y aplicación, fueron desarrollados en una sola capa de TCP/IP conocida como capa de Aplicación.

Una diferencia muy obvia es el número de capas con las que cuenta cada uno, el Modelo OSI tiene 7 capas y el Modelo TCP/IP cuenta solo con 4 capas:

Comparación de Modelos OSI y TCP/IP

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Aplicación</td><td rowspan="2">Aplicación</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td><td rowspan="2">Protocolo (TCP-UDP)</td></tr>
<tr><td>Transporte</td></tr>
<tr><td>Red</td><td rowspan="2">Red</td></tr>
<tr><td rowspan="2">Enlace de Datos</td></tr>
<tr><td>Física</td><td rowspan="2">Física</td></tr>
</table>

Un aspecto muy importante son los conceptos utilizados en el modelo OSI. Este identifica tres conceptos principales que definen su funcionamiento: servicios, los cuales son los procedimientos que realiza cada capa; interfaz, que indica a los procesos de las capas superiores como acceder a ella; y por ultimo, protocolos, los cuales existen para cada capa en pares, es decir, la capa de transporte del emisor y del receptor se comunican por medio del mismo protocolo. Estos protocolos pueden ser cambiados sin afectar a otras capas, siempre y cuando realicen el trabajo que le corresponde a la capa.

El modelo TCP/IP en un principio no distinguía claramente estos tres conceptos, por lo que resultaba complicado ajustar o cambiar protocolos entre capas cuando surgen nuevas tecnologías, pero fue mejorado con el tiempo. Por su parte, el modelo OSI fue creado antes de definir los protocolos, entonces cuando se empiezan a crear redes reales, los diseñadores no tuvieron muy en claro la función específica de cada capa al definir los protocolos, y se generaron muchos problemas para hacer compatibles unas redes con otras, por lo que se tuvieron que crear subcapas para parchear estos errores. Pero el modelo TCP/IP fue definido a partir de los protocolos, así que no se tenía que ajustar el modelo evitando tanto problema.