

Resumen Modulo 15

Capa de aplicación

15.1 Aplicación, presentación y sesión

● Capa de aplicación → Esta capa que proporciona la interfaz entre las aplicaciones utilizada para la comunicación y la red subyacente en la cual se transmiten los mensajes. Los protocolos se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. **Modelo OSI** (Física, enlace de datos, Red, transporte, sesión, presentación, Aplicación). **Modelo TCP/IP** (Acceso a la red, Internet, Transporte, Aplicación). Algunos protocolos de capa de aplicación más conocidos incluyen el protocolo de transferencia de hipertexto (**HTTP**), protocolo de transferencia de archivos (**FTP**), protocolo trivial de transferencia de archivos (**TFTP**), protocolo de acceso a mensajes de Internet (**IMAP**) y protocolo del sistema de nombres de dominios (**DNS**).

● Capa de presentación y sesión → **Presentation Layer** tiene 3 funciones principales: Dar formato a datos del dispositivo origen, en forma compatible para que lo reciba el dispositivo destino. Comprimir los datos. Y cifrar los datos para transmitirlos y descifrarlos. La capa de presentación da formato a datos para aplicación y establece estándares. Los gráficos de imagen conocidos que se utilizan en redes son (**GIF, JPEG, PNG**).

● Capa de sesión → Las funciones de la capa de sesión crean y mantienen diálogos entre aplicaciones de origen y destino. Maneja el intercambio de información para iniciar los diálogos y mantenerlos activos.

● Protocolos de capa de aplicación de TCP/IP → Especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de internet. Protocolos:

Sistemas de nombres → DNS: TCP, UDP cliente 53, traduce nombres de dominio a direcciones IP.

Configuración de host → BOOTP: cliente * UDP 68, servidor 67, Permite una estación de trabajo sin disco obtenga su propia dirección IP. DHCP: cliente UDP 68, servidor 67, permite que direcciones vuelvan a utilizarse cuando ya no son necesarias.

Correo electrónico → SMTP: TCP 25, permite enviar correo a un servidor de correo. POP3: TCP 110, Permite recibir correo electrónico de un servidor de correo, Descarga el correo a la aplicación de correo local. IMAP: TCP 143, Permite que accedan a correos almacenados en un servidor de correo, mantiene el correo en el servidor.

Transferencia de archivos → FTP: TCP 20 a 21, protocolo de entrega de archivos, orientado a conexión y alcuse de recibo. TFTP: cliente UDP 69, menos sobrecarga que FTP, transferencia de archivos simple y sin conexión.

Web → HTTP: TCP 80, reglas para intercambiar texto, imágenes, sonido, video y www. HTTPS: TCP, UDP 443, autentica el sitio web que se conecta el navegador y navegador usa cifrado para comunicaciones HTTP.

15.2 Punto a punto

● **Modelo cliente-servidor** → En este modelo el dispositivo que solicita información se denomina "cliente" y el dispositivo que responde a la solicitud se denomina "servidor". El cliente es una combinación de hardware/software que las personas utilizan para acceder a los recursos en el servidor. Se consideran parte de la capa de aplicación. El cliente comienza el intercambio solicitando datos al servidor, el servidor responde enviando uno o más flujos de datos al cliente. La transferencia de datos de un cliente a un servidor se conoce como "carga". La transferencia de datos de un servidor a un cliente se conoce como "descarga".

● **Redes entre pares** → En el modelo de red entre pares (P2P), se accede a los datos de un dispositivo par sin utilizar un servidor dedicado. Consta de dos partes: Redes P2P y aplicaciones P2P. En red P2P hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos sin tener servidor dedicado. La función cliente y servidor se establecen por solicitud. Se pueden compartir archivos, juegos en red o conexión a internet.

● **Peer-to-Peer Applications** → Permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación. Cada cliente es servidor y cada servidor es un cliente. Requieren que cada terminal proporcione una interfaz de usuario y ejecute su servicio en segundo plano. Algunas utilizan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices que apuntan a las ubicaciones de los recursos están almacenados en un directorio centralizado. Cada punto accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro punto.

● **Aplicaciones P2P comunes** → Cada PC de la red puede funcionar como cliente o servidor para las otras PC en la red que ejecutan la aplicación: Redes P2P comunes: BitTorrent, Conexión directa, eDonkey, Freenet. Algunas se basan en el protocolo Gnutella, donde cada usuario comparte archivos enteros con otros usuarios. Muchas aplicaciones cliente de Gnutella incluyen uTorrent, BitComet, DCTT, Deluge y eMule.

Gnutella permite que las aplicaciones P2P busquen recursos compartidos entre puentes. Los clientes utilizan

15.3 Protocolos web y de correo electrónico

Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto
Hay protocolos específicos como navegación web y correo electrónico. Cuando se escribe una dirección web o localizador uniforme de recursos (URL) en un navegador web. El servicio web se ejecuta en el servidor que está utilizando el protocolo HTTP. Los nombres que la mayoría de personas asocia con direcciones web son (URL) e (URI).

Paso 1 → El explorador interpreta las 3 partes del URL: HTTP, nombre del servidor, index.html (nombre de archivo específico solicitado).

Paso 2 → El navegador luego verifica con un servidor de nombres de dominio (DNS) para convertir a URL en dirección numérica que utiliza para conectarse con el servidor.

Paso 3 → En respuesta a la solicitud, el servidor envía el código HTML de esta página web al navegador.

Paso 4 → El navegador decifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del navegador.

HTTP y HTTPS → HTTP es un protocolo de solicitud / respuesta, se envía una solicitud a un servidor web. Especifica los tipos de mensaje para esa comunicación. Tipos:

GET → Solicitud de datos por parte del cliente. Envía mensaje GET para solicitar páginas HTML.

POST → Carga archivos de datos, como datos, como datos de formulario, al servidor web.

PUT → Carga recursos o contenido, como imagen en el servidor web.

HTTP es sumamente flexible, no es un protocolo seguro. Las respuestas del servidor, generalmente páginas HTML, son sin cifrar. HTTPS utiliza autenticación y cifrado para proteger datos mientras viajan entre cliente y servidor. El flujo de datos se cifra con capa de sockets seguros SSL antes de transportarse a través de la red.

Protocolos de correo electrónico → ISP ofrece hosting de correo electrónico. Para ejecutar el correo electrónico en una PC en otro terminal, se requieren varios servicios y aplicaciones. Método de guardado y desvío que se utiliza para enviar, guardar y recuperar mensajes electrónicos a través de una red. Los servidores de correo para transportar mensajes desde un dominio a otro. Ambos clientes dependen del servidor de correo para transportar los mensajes. Admite SMTP, POP y IMAP.

● Protocolos de correo electrónico → **SMTP** necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo puede contener la cantidad de texto que se desee, el encabezado debe contar con dirección de correo electrónico de destinatario formateada y dirección de emisor. Se conecta a un proceso SMTP del servidor en el puerto bien conocido 25. Cuando el servidor recibe el mensaje, lo ubica en cuenta local o reenvía a otro servidor de correo para entrega.

POP → Recupera correo electrónico de un servidor de correo. El correo se descarga desde el servidor al cliente y se elimina en el servidor. Es una conexión de manera pasiva en el puerto TCP 110. El cliente y servidor POP intercambian comandos y respuestas hasta que la conexión se cierra o cancela.

IMAP → Describe un método para recuperar mensajes de correo electrónico. IMAP se descargan copias de mensajes a la aplicación cliente. Los mensajes originales se mantienen en el servidor hasta que se eliminan manualmente. Los usuarios ven copias de los mensajes en su software de cliente de correo electrónico.

15.4 Servicios de direccionamiento IP

● Servicio de nombres de dominios → En redes, los dispositivos se etiquetan con IP para enviar y recibir datos en la red. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible. Los nombres de dominio como cisco.com son más fáciles de recordar una IP. **DNS** define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye formato de consultas, respuestas y datos. Utilizan el formato **mensaje**.

Paso 1 → El usuario escribe un FQDN en un campo de dirección de aplicación del explorador.

Paso 2 → Se envía una consulta DNS al servidor DNS para el equipo cliente.

Paso 3 → El servidor DNS coincide con el FQDN con su dirección IP.

Paso 4 → La respuesta de consulta DNS se envía de nuevo al cliente con la IP del FQDN.

Paso 5 → El equipo cliente utiliza la IP para solicitud del servidor.

● Formato de mensaje DNS → Almacenan diferentes tipos de registros de recursos utilizados para resolver nombres. **A** - Una dirección IPv4 de terminal. **NS** - Un servidor de nombre autoritativo. **AAAA** - Dirección IPv6 de terminal. **MX** - Un registro de intercambio de correo. DNS primero observa sus propios registros para resolver el nombre. Si no puede resolverlo, contacta a otros servidores para hacerlo.

● Jerarquía DNS → DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres. Cada servidor mantiene un archivo de base de datos específico y responsable de administrar asignaciones de nombre a IP para esa porción de toda la estructura DNS. DNS es escalable, porque la resolución de nombres de hosts se distribuye entre varios servidores. Ejemplos de dominios de nivel superior son los sig:

• .com - Una empresa o industria. • .org - organización sin fines de lucro. • .au - Australia.

• .co - Colombia. • .net

● El comando nslookup → Al configurar un dispositivo de red, se proporciona una o más direcciones de Servidor DNS puede utilizar para resolución de nombres. ISP suministra las direcciones para utilizar los servidores DNS. NSLOOKUP permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. También puede utilizarse para solucionar problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

● Protocolo de configuración dinámica de host → Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. DHCP elige una dirección de un rango de direcciones configurado llamado grupo y la asigna al host. DHCP puede asignar direcciones IP durante un período de tiempo configurable, denominado período de concesión. Este período es importante para un DHCP. Cuando caduca el servidor DHCP recibe un mensaje DHCP RELEASE, la dirección se devuelve al grupo DHCP para su reutilización. Muchas redes utilizan tanto el direccionamiento estático como DHCP. DHCP se utiliza para hosts de propósito general, dispositivos finales. El direccionamiento estático se utiliza para dispositivos de red, gateways, switches, servidores e impresoras. DHCP no brinda un gateway predeterminado. Solo se obtiene del anuncio del router.

● Funcionamiento de DHCP → Cuando hay una conexión de inicio para DHCP el cliente manda un mensaje de detección DHCP (DHCP discover) para identificar cualquier servidor de DHCP disponible en la red. DHCP responde con un mensaje de oferta (DHCP OFFER) que ofrece concesión al cliente. Este mensaje contiene la IPV4 y la máscara de subred. Como existen varios DHCPOFFERS, el cliente elige entre ellos y envía un mensaje de solicitud de (DHCP REQUEST) que identifica que el servidor explícito y oferta de concesión que acepta. Por último (DHCP ACK) le informa al cliente que finalizó la concesión. Si la oferta ya no es válida el servidor responde con reconocimiento negativo (DHCP NAK).

15.5 Servicios de intercambio de archivos

Protocolo de transferencia de archivos → El protocolo **FTP** se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.

1 Conexión de control: El cliente abre la primera conexión al servidor para el tráfico de control.

2 Conexión de datos: El cliente abre la segunda conexión para el tráfico de datos.

3 Data transfer: El servidor transfiere datos al cliente. En el comando a través de la conexión de control, los datos pueden descargarse desde el servidor o subirse desde el cliente.

Para el control del tráfico se usa el puerto TCP 21. Para transferencia de datos se usa el puerto 20 de TCP. Esta conexión se crea cada vez que hay datos para transferir.

Bloque de mensajes del servidor → **SMB** es un protocolo de intercambio de archivos cliente/servidor que describe la estructura de recursos de red compartidos, archivos, directorios, impresoras y puertos serie. Usa un encabezado de tamaño fijo, después un parámetro de tamaño variable y un componente de datos - Funciones:

- Iniciar, autenticar y terminar sesiones,
- Controlar el acceso a archivos e impresoras,
- Autorizar una app para enviar y recibir mensajes.

A comparación con FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de la conexión, el usuario cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

Linux y UNIX proporcionan un método de intercambio de recursos con redes de Microsoft mediante una versión de SMB llamado **SAMBA**.