CAPÍTULO 2. COMUNICACIÓN A TRAVÉS DE LA RED

1. Qué es la segmentación

Dividir los datos en partes más pequeñas y manejables para enviarlas por la red. La segmentación aumenta la confiabilidad de las comunicaciones de red. Si parte del mensaje no llega al destino, sólo se deben retransmitir las partes fallantes.

2. Qué es la multiplexación

Se pueden intercalar diversas conversaciones en la red al enviar partes individuales más pequeñas de origen al destino. Es el proceso que se utiliza para intercalar piezas de conversaciones separadas en la red.

3. Definición de Red, LAN, WAN, Internetwork e Internet

LAN: red local o grupo de redes locales interconectadas que están bajo el mismo control administrativo. Las LAN incluyen redes locales interconectadas que constan de muchos cientos de hosts, instalados en varios edificios y ubicaciones.

WAN: redes que conectan las LAN en ubicaciones separadas geográficamente. Son redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones las controla el TSP.

Internetwork: una malla de redes interconectadas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas y están reservadas para su uso exclusivo. La internetwork de acceso público más conocida es Internet.

Internet: es la internetwork más conocida. Se crea por la interconexión de redes que pertenecen a los Proveedores de Servicios de Internet (ISP).

4. Qué es un protocolo de red

Descripción de procesos según las suites de protocolos de networking:

- Estructura del mensaje.
- Proceso en el que comparten información los dispositivos de networking sobre las rutas con otras redes.
- Mensajes de error y del sistema entre los dispositivos.
- Terminación de sesiones de transferencia de datos.

Los protocolos individuales en una suite de protocolos puede ser específica y exclusiva.

5. Función de los protocolos de: Aplicación, Transporte, Internet y Acceso a la red

Protocolos de Aplicación: el protocolo de transferencia de hipertexto (HTTP) rige la forma en que interactúan un servidor web y un cliente web. Define el contenido y formato de las solicitudes y respuestas. Se basa en otros protocolos.

Protocolos de Transporte: el protocolo de control de transmisión (TCP) administra las conversaciones individuales entre servidores web y clientes web. Divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al cliente de destino.

Protocolos de Internet: el protocolo de internet (IP) es responsable de tomar los segmentos del TCP, encapsularlos en paquetes, asignar direcciones y seleccionar la mejor ruta al host de destino.

Protocolos de Acceso a la red: administración de enlace de datos y transmisión física de datos en los medios. Los protocolos de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los protocolos de medios físicos rigen de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben.

6. Dibuja el Modelo OSI. Capas

El modelo de interconexión de sistema abierta (OSI) de 7 capas es el modelo de referencia de internetwork más conocido. Se usa para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas. Se utiliza para describir los procedimientos necesarios que hay que realizar en cada capa. Sus capas son: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

7. Dibuja muy detalladamente el Modelo TCP/IP

El modelo de protocolo TCP/IP tiene 4 capas y describe las funciones que se producen en cada capa de los protocolos dentro del suite TCP/IP. Sus capas son: acceso a la red, internet, transporte y aplicación.

8. **Qué es la encapsulación**

A medida que los datos de aplicación pasan por el stack del protocolo en su recorrido para ser transmitidos por los medios de red, distintos protocolos les agregan información en cada nivel.

9. **Qué es una PDU (Unidad de Datos del Protocolo)**

Es la forma que toman los datos en cualquier capa. Las PDU que están dentro de los protocolos del suite TCP/IP son:

- Datos: PDU de la capa de aplicación.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de red.
- Trama: PDU de la capa de acceso a la red.

10. **Direccionamiento en la red (por cada capa)**

Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino que se ejecuta en otro.

- Física: bits de sincronización y temporización.
- Enlace de datos: direcciones físicas de origen y destino.
- Red: direcciones de red lógicas de origen y destino.
- Transporte: número de proceso de origen y destino (puertos).
- Capas superiores: datos de aplicaciones codificados.

CAPÍTULO 3. FUNCIONALIDAD Y PROTOCOLOS DE LA CAPA DE APLICACIÓN

1. **Enumera al menos 4 protocolos de la capa de aplicación**

- DNS (Servicios de nombres de dominios)
- FTP (Servicio de transferencia de archivos)
- HTTP (Protocolo de transporte de hipertexto)
- Telnet (Servicio de red de teletipo)

2. **Modelo cliente-servidor**

El extremo de origen de la comunicación de datos es el servidor y el extremo receptor es el cliente. Los procesos de cliente-servidor son servicios de la capa de aplicación que proporcionan las bases para la conectividad de red de datos.
La función del servidor puede ser administrar las comunicaciones a medida que se producen. Esto se denomina comunicación en tiempo real. Se dice que los procesos de servidor escuchan la solicitud de un cliente. Cuando un servidor recibe una solicitud de un cliente, intercambia los mensajes apropiados con el cliente de acuerdo con lo requerido por el protocolo en uso y luego envía los datos solicitados. Este intercambio puede incluir la autentificación del usuario y la identificación del archivo de datos que se transferirá.
A la transferencia de datos del cliente al servidor se le denomina carga y a la transferencia de datos de un servidor se le denomina descarga.

3. Modelo de redes entre pares

En una red punto a punto, dos o más computadoras están conectadas por medio de una red y pueden compartir recursos (impresoras y archivos) sin tener un servidor dedicado. Cada dispositivo final conectado (conocido como punto) puede funcionar como un servidor o un cliente. En las aplicaciones punto a punto (P2P) cada cliente es un servidor y cada servidor es un cliente. Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación.

4. Qué es MUA y MTA

MUA: Agente de Usuario de Correo o cliente de correo electrónico. Permite enviar los mensajes y colocar los recibidos en el buzón del cliente. Los clientes envían correo electrónico a un servidor mediante SMTP y reciben el correo electrónico mediante POP3.

MTA: el agente de transferencia de correo se utiliza para enviar correo electrónico. Rige el manejo de correo electrónico entre servidores. El MTA recibe mensajes desde el MUA u otro MTA en otro servidor de correo electrónico.

5. Qué es el protocolo SMB

SMB: el bloque de mensajes del servidor describe la estructura para compartir recursos de red como directorios, archivos, impresoras y puertos seriales entre computadoras.

6. Qué es el protocolo GNutella

GNutella: con las aplicaciones P2P basadas en este protocolo, las personas pueden colocar sus archivos en sus discos rígidos para que otros los descarguen. Permite que las aplicaciones P2P busquen recursos compartidos entre puntos. Define 5 tipos de paquetes:

- Ping: descubrimiento del dispositivo.
- Pong: respuesta a un ping.
- Query: encontrar un archivo.
- Query hit: respuesta a una consulta.
- Push: solicitud de descarga.

CAPÍTULO 4. CAPA DE TRANSPORTE DEL MODELO OSI

1. Función de los puertos en la capa de transporte

Tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva aplicaciones. Estos identificadores son números de puerto. En el encabezado de cada segmento o datagrama hay un puerto de origen y uno de destino. Los números de puerto se asignan de distinta manera, dependiendo de si el mensaje es una solicitud o una respuesta. Mientras que los procesos del servidor tienen números de puerto estáticos asignados, los clientes eligen de forma dinámica un número de puerto para cada conversación.

2. Qué es la entrega confiable y el control de flujo en la capa de transporte

Entrega confiable: la capa de transporte puede asegurar que todas las partes alcancen su destino haciendo que el dispositivo origen retransmita todos los datos perdidos.

Control de flujo: los hosts de la red cuentan con recursos limitados. Cuando la capa de transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación que envía reduzca la velocidad del flujo de datos. El control de flujo puede evitar la pérdida de segmentos en la red y evitar la necesidad de la retransmisión.

3. **Diferencia entre TCP y UDP**

TCP: es un protocolo orientado a conexión. Utiliza recursos adicionales para ganar 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 TCP posee 20 bytes de carga en el encabezado que encapsulan los datos de la capa de aplicación. Las aplicaciones que utilizan TCP son: exploradores web, correo electrónico y transferencias de archivo.

UDP: es un protocolo simple, sin conexión. Entrega de datos sin utilizar muchos recursos. Envía datagramas (porciones de comunicación en UDP) como mejor intento. Cada segmento UDP sólo posee 8 bytes de carga. Las aplicaciones que utilizan UDP son: sistemas de nombres de dominios (DNS), streaming video y voz sobre IP (VOIP).

4. **Qué es IANA**

Es la Autoridad de Números Asignados de Internet que asigna números de puerto. Es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.

5. **Tipos de número de puerto**

Puertos bien conocidos (del 0 al 1023): están reservados para servicios y aplicaciones como HTTP, POP3/SMTP y Telnet.

Puertos registrados (del 1024 al 49151): están asignados a los procesos de usuarios o aplicaciones individuales escogidas por un servidor para instalar aplicaciones universales.

Puertos dinámicos o privados (del 49152 al 65535): también conocidos como puertos efímeros que se asignan en forma dinámica a las aplicaciones de clientes al iniciarse una conexión, como los programas que comparten archivos punto a punto.

6. **Comandos Route, Nslookup y Netstat**

Route: se utiliza para visualizar y modificar la tabla de rutas. Para que dos host intercambien datagramas IP, ambos deberán tener una ruta al otro o utilizar un Gateway que conozca una ruta.

Nslookup: es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o el host y así diagnosticar problemas de configuración en el DNS.

Netstat: es una utilidad de red que puede usarse para verificar conexiones TCP activas que están abiertas y en ejecución en el host de red. Indica el protocolo en uso, la dirección y número de puerto local, la dirección y número de puerto ajeno y el estado de la conexión.

7. **Intercambio de señales mediante tres vías**

Para establecer la conexión los hosts realizan un protocolo de enlace de tres vías. En las conexiones TCP, el host que sirve como cliente inicia la sesión para el servidor. Los tres pasos para el establecimiento de una conexión TCP son:

- El cliente de origen envía un segmento que contiene un valor de secuencia inicial, el cual sirve como solicitud para que el servidor comience una sesión de comunicación.
- El servidor responde con un segmento que contiene un valor de reconocimiento igual al valor de secuencia recibido más 1, más su propio valor de secuencia de sincronización. Esto permite al cliente unir la respuesta al segmento original que fue enviado al servidor.
- El cliente que inicia la conexión responde con un valor de reconocimiento igual al valor de secuencia que recibió más 1. Esto completa el proceso de establecimiento de la conexión.

8. **Qué es el tamaño de ventana**

Es la cantidad de datos que puede transmitirse en forma previa a la recepción de un acuse de recibo de TCP.

9. **Qué son los datagramas**

Es la PDU de UDP.

CAPÍTULO 5. CAPA DE RED OSI

1. **Enumera al menos 4 protocolos de la capa de red.**

- Versión 4 del Protocolo de Internet (IPv4).
- Versión 6 del Protocolo de Internet (IPv6).
- Intercambio Novell de paquetes de Internetwork (IPX).
- Apple talk.
- Servicio de Red sin conexión (CLNS/DECNet)

2. **Qué son los protocolos de enrutamiento. Enumera al menos dos.**

El enrutamiento requiere que cada salto o router hacia el destino del paquete tenga una ruta para reenviar el paquete. La tabla de enrutamiento contiene información que un router usa en sus decisiones al reenviar paquetes. La información de enrutamiento desactualizada significa que los paquetes no pueden reenviarse al siguiente salto, causando pérdidas de paquetes. Esta información se puede configurar en el router. Hay dos tipos:

- Enrutamiento estático: las rutas a redes remotas con saltos asociados se pueden configurar manualmente en el router. Una ruta default también puede ser configurada estáticamente.
- Enrutamiento dinámico: se utilizan los protocolos de enrutamiento como el protocolo de información de enrutamiento (RIP), protocolo de enrutamiento de 180ersión interior mejorada (EIGRP) y Open Shortest Path First (OSPF).

CAPÍTULO 6. DIRECCIONAMIENTO DE LA RED: IPV4

1. Dirección de red, de host y de broadcast

- Dirección de red: la dirección con la cual hacemos referencia a la red.
- Dirección de host: las direcciones asignadas a los dispositivos finales de la red.
- Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.

2. Para qué se utiliza la máscara de red

La utilizan los dispositivos de red para determinar la dirección de red o subred de una dirección IP que el dispositivo está procesando.

3. Qué es unicast, multicast y broadcast

- Unicast: el proceso de enviar un paquete de un host a otro host individual.
- Multicast: el proceso de enviar un paquete desde un host a un grupo de hosts seleccionado.
- Broadcast: el proceso de enviar un paquete de un host a todos los hosts de la red.

4. Rangos de direcciones IPv4

Direcciones Multicast: de 224.0.0.0 a 239.255.255.255 se encuentra reservado para fines específicos.
Direcciones Privadas:

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

Ruta default: es 0.0.0.0. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 a 0.255.255.255 (/8).

Loopback: es 127.0.0.1. Las direcciones 127.0.0.0 a 127.255.255.255 donde los hosts dirigen el tráfico hacia ellos mismos.

Direcciones de enlace link-local: desde 169.254.0.0 hasta 169.254.255.255 (/16). El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP.

Direcciones TEST-NET: de 192.0.2.0 a 192.0.2.255 (/24) para fines de enseñanza y aprendizaje.

5. Bloques de clase A, B, C, D y E.

Bloques de Clase A: para redes extremadamente grandes con más de 16 millones de direcciones host. Usaban un prefijo /8, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host. Esto significaba que sólo había 128 redes de clase A posibles, de 0.0.0.0 a 127.0.0.0 (/8) antes de excluir los bloques de direcciones reservadas. Debido a que reservaban la mitad, sólo podían ser asignadas 120.

Bloques de Clase B: de tamaño moderado a grande con más de 65.000 hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para la dirección de red. Los dos octetos

restantes especificaban las direcciones de host. De esta forma, se restringía el bloque de direcciones a 128.0.0.0 hasta 191.255.0.0 (/16). Dividía el 25% del total del espacio de direcciones entre 16.000 redes.

Bloques de Clase C: para redes pequeñas con un máximo de 254 hosts. Utilizaban el prefijo /24. Sólo usaba el último octeto como direcciones host con los tres octetos de orden superior para indicar la dirección de red. Reservaban el espacio de direcciones para la clase D (multicast) y la clase E (experimental). Esto restringió el bloque de direcciones a 192.0.0.0 a 223.255.255.0 (/16). Podía suministrar direcciones a 2 millones de redes.

Bloques de Clase D: de 224 a 239.

Bloques de Clase E: de 240 a 255.

6. **Registros de Internet regionales**

AfriNIC: región de África.
APNIC: Asia/Región del Pacífico.
LACNIC: Región de América Latina y el Caribe.
ARIN: Región de América del Norte.
RIPE NCC: Europa, Medio Oriente, Región de Asia Central.

CAPITULO 7. CAPA DE ENLACE DE DATOS

1. **Servicios básicos de la capa de enlace de datos.**

- Permite a las capas superiores acceder a los medios usando técnicas, como tramas.
- Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

2. **Términos específicos de la capa de enlace de datos.**

Trama: el PDU de la capa de enlace de datos.
Nodo: la notación de la Capa 2 para dispositivos de red conectados a un medio común.
Medios/medio (físico): los medios físicos para la transferencia de información entre dos nodos.
Red (física): dos o más nodos conectados a un medio común.

3. **Diferencias entre una red física y una red lógica.**

Una red física es diferente de una red lógica. Las redes lógicas se definen en la capa de red mediante la configuración del esquema de direccionamiento jerárquico. Las redes físicas representan la interconexión de dispositivos de medios comunes. Algunas veces, una red física también es llamada segmento de red.

4. **Qué incluye la PDU de la capa de enlace de datos.**

Incluye datos, encabezado y tráiler.

5. **Subcapas de la capa de enlace de datos y funciones.**

La subcapa superior define los procesos de software que proveen servicios a los Protocolos de capa de red.

La subcapa inferior define los procesos de acceso a los medios realizados por el hardware.
Control de enlace lógico (superior): entrama el paquete de la capa de red e identifica el protocolo de la capa de red.
Control de acceso al medio (inferior): direcciona la trama y marca el comienzo y el fin de la trama.

6. Métodos de control de acceso al medio.

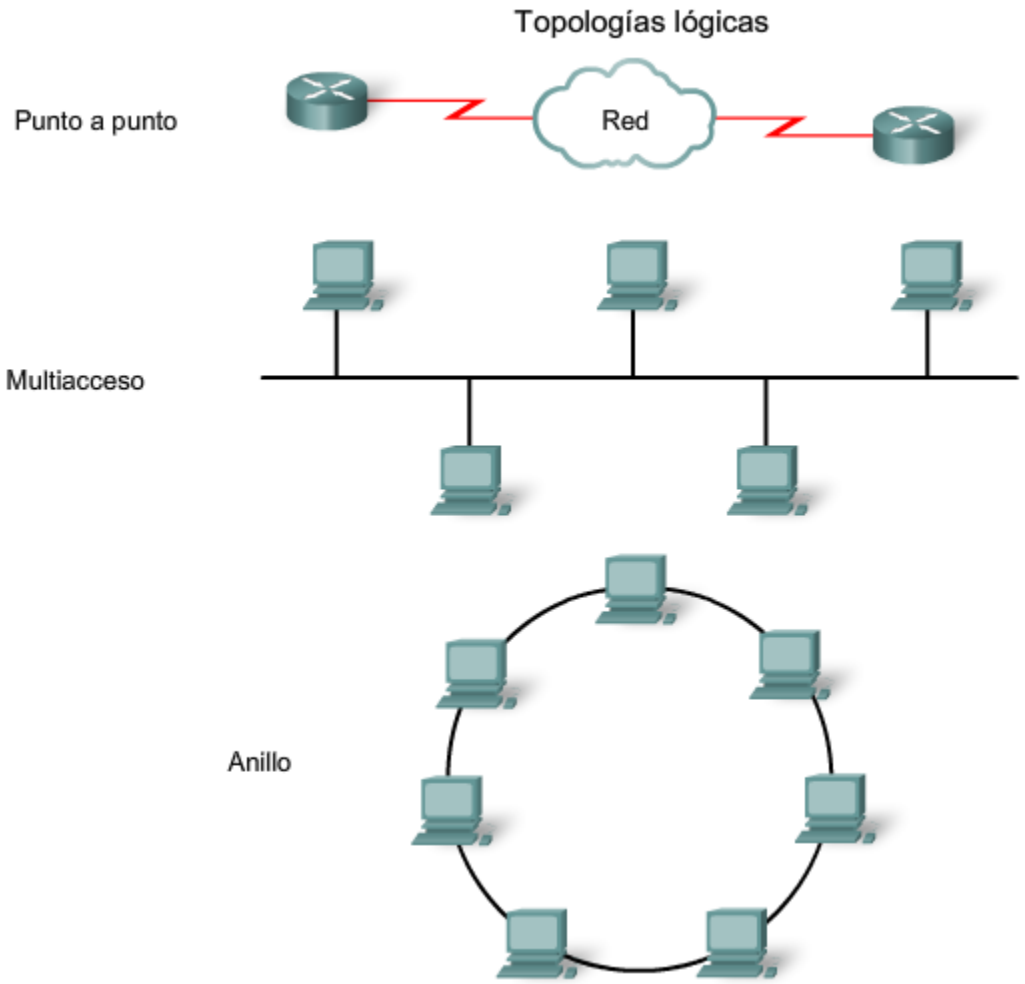
Los métodos de control de acceso al medio descritos en los protocolos de capa de enlace de datos definen los procesos por los cuales los dispositivos de red pueden acceder a los medios de red y transmitir marcos en diferentes entornos de red.
Son:

- Para medios compartidos: controlado (cada nodo tiene su propio tiempo para utilizar el medio) y basado en la contención (todos los nodos compiten por el uso del medio).
- Para medios no compartidos: full dúplex y half dúplex.

7. Control de acceso al medio para medios no compartidos (full dúplex y half dúplex).

En conexiones punto a punto:
Comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo.
En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento.
Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.

8. Topologías lógicas (esquemas).



9. Descripción de CSMA/CD y CSMA/CA

En CSMA/Detección de colisión (CSMA/CD), el dispositivo monitorea los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet usan este método.

En CSMA/Prevención de colisiones (CSMA/CA), el dispositivo examina los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo.
El dispositivo luego envía los datos. Este método es utilizado por las tecnologías de redes inalámbricas 802.11.

10. Descripción de pasos de tokens.

En una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso al medio llamada paso de tokens.

11. Protocolos de la capa de enlace de datos (para LAN y para WAN).

Protocolo Ethernet para LAN

Ethernet es una familia de tecnologías de interconexión de redes que se define en los estándares 802.2 y 802.3. Los estándares de Ethernet definen los protocolos de la Capa 2 y las tecnologías de la Capa 1. Proporciona servicio sin conexión y sin reconocimiento sobre un medio compartido utilizando CSMA/CD como métodos de acceso al medio.

Protocolo punto a punto para WAN

Utilizado para entregar tramas entre dos nodos. El estándar PPP está definida por RFC.

Protocolo inalámbrico para LAN

802.11 es una extensión de los estándares IEEE 802. El estándar IEEE 802.11, comúnmente llamada Wi-Fi, es un sistema por contención que utiliza un proceso de acceso al medio de Acceso múltiple con detección de portadora y prevención de colisiones (CSMA/CA).

CAPITULO 8. CAPA FÍSICA DEL MODELO OSI

12. Funciones esenciales de la capa física.

El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios una a la vez.
Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa.

13. Definición de tiempo de bit.

La capa física representa cada uno de los bits de la trama como una señal. Cada señal ubicada en los medios cuenta con un plazo específico de tiempo para ocupar los medios. Esto se denomina tiempo de bit.

14. Señalización de bit para los medios (enumerar solo lo que hay).

Señalización NRZ y Codificación Manchester

15. Definición de ancho de banda digital

El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado.

16. **Características de 100basetx, 1000baset, 100base-fx, 1000 base-sx**

Medios de Ethernet

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BA
Medios	UTP Categoría EIA/TIA 3, 4, 5, cuatro pares	UTP Categoría 5 EIA/TIA, dos pares	50/62.5 m fibra multimodo	STP	UTP Categoría 5 (o mayor) EIA/TIA, cuatro pares	fibra multimodo de 50/62.5 micrones	fibra m de 50/6 micron fibra monom 9 micro
Longitud de segmento máxima	100m (328 pies)	100m (328 pies)	2 km (6562 pies)	25 m (82 pies)	100 m (328 pies)	Hasta 550m (1804 pies) según la fibra utilizada	550 m (MMF) (SMF)
Topología	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Conector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)			

17. **Características de los medios de cobre en las comunicaciones de red.**

El cableado utilizado para las comunicaciones de datos generalmente consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización. Estos cables pueden utilizarse para conectar los nodos de una LAN a los dispositivos intermedios, como routers o switches. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos, como una compañía telefónica. Cada tipo de conexión y sus dispositivos complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física.

18. **Características del cable coaxial en comunicaciones de red.**

Consiste en un conductor de cobre rodeado de una capa de aislante flexible. Sobre este material aislante hay una malla de cobre tejida o una hoja metálica que actúa como segundo alambre del circuito y como blindaje para el conductor interno. La segunda capa o blindaje reduce la cantidad de interferencia electromagnética externa. La envoltura del cable recubre el blindaje.

19. **Características del cable de fibra óptica. Tipos.**

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar. Las fibras ópticas pueden utilizarse en longitudes mayores. Hay dos tipos:

- Fibra monomodo.
- Fibra multimodo.

20. **Tipos de redes inalámbricas. Incluir el estándar asociado.**

IEEE estándar 802.11: Comúnmente denominada Wi-Fi, se trata de una tecnología LAN inalámbrica (Red de área local inalámbrica, WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de Acceso múltiple con detección de portadora/Prevención de colisiones (CSMA/CA).

IEEE estándar 802.15: Red de área personal inalámbrica (WPAN) estándar, comúnmente denominada “Bluetooth”, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.

IEEE estándar 802.16: Comúnmente conocida como WiMAX (Interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.

Sistema global para comunicaciones móviles (GSM): Incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

21. Estándares de las redes 802.11.

IEEE 802.11b: opera en una banda de frecuencia de 2.4 GHz y ofrece velocidades de hasta 11 Mbps. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11ª.
IEEE 802.11g: opera en una frecuencia de banda de 2.4 GHz y ofrece velocidades de hasta 54 Mbps. Por lo tanto, los dispositivos que implementan este estándar operan en la misma radiofrecuencia y tienen un alcance de hasta 802.11b pero con un ancho de banda de 802.11ª.
IEEE 802.11n: el estándar IEEE 802.11n se encuentra actualmente en desarrollo. El estándar propuesto define la frecuencia de 2.4 Ghz o 5 GHz. La velocidad típica de transmisión de datos que se espera es de 100 Mbps a 210 Mbps con un alcance de distancia de hasta 70 metros.

CAPITULO 9

- **Describe brevemente la red Ethernet.**

Ethernet es un protocolo de acceso de red TCP/IP efectivo y ampliamente utilizado. Su estructura de trama común se implementó a través de una variedad de tecnologías de medios, tanto de cobre como de fibra, lo que la convierten en el protocolo LAN que más se utiliza en la actualidad.
Como implementación de los estándares IEEE 802.2/3, la trama de Ethernet proporciona direccionamiento MAC y comprobación de errores.

- **Qué es la dirección MAC. Estructura e indica un ejemplo.**

•El Control de acceso al medio (MAC) es la subcapa de Ethernet inferior de la capa de enlace de datos. El hardware implementa el Control de acceso al medio, generalmente en la tarjeta de interfaz de red (NIC) de la computadora.

•El IEEE obliga a los proveedores a respetar dos normas simples:
*Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.
*Se les debe asignar un valor exclusivo (código del fabricante o número de serie) a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) en los últimos 3 bytes.

•A0:B1:C2:D3:E4:F5.

- **Ethernet, unicast, multicast y broadcast en la capa 2.**

•El direccionamiento físico de la capa de enlace de datos (Capa 2) de OSI, implementado como dirección MAC de Ethernet, se utiliza para transportar la trama a través de los medios locales. Si bien brindan una dirección host única, las direcciones físicas no son jerárquicas. Estas direcciones se asocian a un dispositivo en particular, independientemente de su ubicación o de la red a la que esté conectado.

•Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.

•Recuerde que las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El intervalo de direcciones multicast es de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.

•Con broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Una gran cantidad de protocolos de red utilizan broadcast, como el Protocolo de configuración dinámica de host (DHCP) y el Protocolo de resolución de direcciones (ARP).

- **Diferencia entre dominio de colisión y dominio de broadcast.**

- **Características de 10 base 5, 10 base 2 y 10 base t.**

Las principales implementaciones de 10 Mbps de Ethernet incluyen:
10BASE5 con cable coaxial Thicknet
10BASE2 con cable coaxial Thinnet
10BASE-T con cable de par trenzado no blindado Cat3/Cat5

Las primeras implementaciones de Ethernet, 10BASE5 y 10BASE2 utilizaban cable coaxial en un bus físico. Dichas implementaciones ya no se utilizan y los más recientes estándares 802.3 no las admiten.

10 mbps Ethernet: 10BASE-T

La 10BASE-T utiliza la codificación Manchester para dos cables de par trenzado no blindado. Las primeras implementaciones de la 10BASE-T utilizaban cableado Cat3. Sin embargo, el cableado Cat5 o superior es el que se utiliza generalmente en la actualidad.

La Ethernet de 10 mbps se considera que es la Ethernet clásica y utiliza una topología en estrella física. Los enlaces de Ethernet 10BASE-T pueden tener hasta 100 metros de longitud antes de que requieran un hub o repetidor.

La 10BASE-T utiliza dos pares de cables de cuatro pares y finaliza en cada extremo con un conector RJ-45 de 8 pins. El par conectado a los pins 1 y 2 se utiliza para transmitir y el par conectado a los pins 3 y 6 se utiliza para recibir. La figura muestra la salida de pins RJ45 utilizada con Ethernet 10BASE-T.

La 10BASE-T generalmente no se elige para instalaciones de LAN nuevas. Sin embargo, todavía existen actualmente muchas redes Ethernet 10BASE-T. El reemplazo de los hubs por los switches en redes 10BASE-T aumentó notablemente la velocidad de transmisión (throughput) disponible para estas redes y le otorgó a la Ethernet antigua una mayor longevidad. Los enlaces de 10BASE-T conectados a un switch pueden admitir el funcionamiento tanto half-duplex como full-duplex.

- **Qué es un hub, un switch y un router.**

•La Ethernet clásica utiliza hubs para interconectar los nodos del segmento de LAN. Los hubs no realizan ningún tipo de filtro de tráfico. En cambio, el hub reenvía todos los bits a todos los dispositivos conectados al hub. Esto obliga a todos los dispositivos de la LAN a compartir el ancho de banda de los medios.

•Los switches permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

•El router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

- **Ejercicio 9.6.4**

- **Qué es ARP y ARP proxy.**

•Cuando se envía un paquete a la capa de Enlace de datos para que se encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de Enlace de datos que se mapea a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP.

•Hay ocasiones en las que un host puede enviar una solicitud de ARP con el objetivo de asignar una dirección IPv4 fuera del alcance de la red local. En estos casos, el dispositivo envía solicitudes de ARP para direcciones IPv4 que no se encuentran en la red local en vez de solicitar la dirección MAC asociada a la dirección IPv4 del gateway. Para proporcionar una dirección MAC para estos hosts, una interfaz de router puede utilizar un ARP proxy para responder en nombre de estos hosts remotos. Esto significa que la caché de ARP del dispositivo solicitante contendrá la dirección MAC del gateway mapeada a cualquier dirección IP que no se encuentre en la red local. Con el proxy ARP, una interfaz de router actúa como si fuera el host con la dirección IPv4 solicitada por la solicitud de ARP. Al "simular" su identidad, el router acepta la responsabilidad de enrutar paquetes al destino "real".

CAPITULO 10

- **Áreas existentes en la planificación de la instalación del cableado de red (cableado estructurado).**

•Costo
•Velocidad y tipos de puertos e interfaces
•Capacidad de expansión
•Facilidad de administración
•Características y servicios adicionales

- **Qué es MDI y MDIx.**

•La MDI (interfaz dependiente del medio) utiliza un diagrama de pines normal de Ethernet. Los pins 1 y 2 se utilizan como transmisores y los pins 3 y 6 como receptores. Dispositivos como computadoras, servidores o routers tendrán conexiones MDI.

•Los dispositivos que proporcionan la conectividad a la LAN (por lo general, hubs o switches) habitualmente utilizan conexiones MDIX (interfaz cruzada dependiente del medio). La conexión MDIX intercambia los pares transmisores internamente. Este intercambio permite que los dispositivos finales se encuentren conectados a un hub o switch utilizando un cable de conexión directa.

- **Tipos de conexiones WAN y tipos de conexión LAN.**

•UTP (Categorías 5, 5e, 6 y 7)
•Fibra óptica
•Inalámbrico

- **Qué es el DTE y el DCE.**

Equipo de comunicación de datos (DCE): Un dispositivo que suministra los servicios de temporización a otro dispositivo. Habitualmente, este dispositivo se encuentra en el extremo del enlace que proporciona el acceso WAN.

Equipo terminal de datos (DTE): Un dispositivo que recibe los servicios de temporización desde otro dispositivo y se ajusta en consecuencia. Habitualmente, este dispositivo se encuentra en el extremo del enlace del cliente WAN o del usuario.

CAPITULO 11

- **Métodos de acceso a un router CISCO.**

• Consola
• Telnet o SSH
• Puerto auxiliar

- **Tipos de archivos de configuración en un dispositivo CISCO.**

Un dispositivo de red Cisco contiene dos archivos de configuración:
• El archivo de configuración en ejecución, utilizado durante la operación actual del dispositivo
• El archivo de configuración de inicio, utilizado como la configuración de respaldo, se carga al iniciar el dispositivo.
También puede almacenarse un archivo de configuración en forma remota en un servidor a modo de respaldo.

- **Comandos CISCO.**

Modo EXEC del usuario

enable - Ingresar el modo EXEC privilegiado

Modo EXEC privilegiado

copy running-config startup-config - Copiar la configuración activa a la NVRAM.
copy startup-config running-config - Copiar la configuración en la NVRAM a la RAM.
erase startup-configuration - Borrar la configuración almacenada en la NVRAM.
ping ip_address - Hacer ping a esa dirección.
traceroute ip_address - Rastrear cada salto a esa dirección.
show interfaces - Mostrar las estadísticas para todas las interfaces de un dispositivo.
show clock - Mostrar el tiempo establecido en el router.
show version - Mostrar la versión de IOS cargada actualmente, hardware e información del dispositivo.
show arp - Mostrar la tabla ARP del dispositivo.
show startup-config - Mostrar la configuración almacenada en la NVRAM.
show running-config - Mostrar el contenido del archivo de configuración actualmente en ejecución.
show ip interface - Mostrar las estadísticas de IP para la/s interfaz/ces de un router.
configure terminal - Ingresar al modo Configuración de terminal.

Modo configuración de terminal

hostname hostname - Asignar un nombre de host al dispositivo.
enable password password - Establecer una contraseña de enable no encriptada.
enable secret password - Establecer una contraseña de enable encriptada en forma segura.
service password-encryption - Encriptar la visualización de todas las contraseñas, excepto la secreta.
banner motd# message # - Establecer un título con el mensaje del día.
line console 0 - Ingresar al modo Configuración de la línea de consola.
line vty 0 4 - Ingresar al modo Configuración de línea de terminal virtual (Telnet).
interface Interface_name - Ingresar al modo Configuración de interfaz.

Modo configuración de línea

login - Habilitar la comprobación de contraseñas en el inicio de sesión.
password password - Establecer la contraseña de línea.

Modo configuración de interfaz

ip address ip_address netmask - Establecer la dirección IP de la interfaz y máscara de subred.
description description - Establecer la descripción de la interfaz.
clock rate value - Establecer la frecuencia de reloj para el dispositivo DCE.