



# Actividades capítulo 3 y 4

**UNIVERSIDAD DEL CAUCA**

FECHA:

NOMBRE:

CÓDIGO DE SIMCA:

1. Leer el capítulo 3 y 4 del curso de Cisco.
2. Responder las preguntas de lectura y enviarlas en PDF.

# Preguntas de lectura: Capítulo 3

CCNA Exploration

Aspectos básicos de networking:

La vida en un mundo centrado en la

1. Describir las funciones de las tres capas superiores del modelo OSI y comAcotiviedasdteas sDel Curso D

Capa de Aplicación (Capa 7): Esta capa proporciona la interfaz entre el software de aplicación y el resto de la red. Ofrece servicios como el intercambio de datos entre aplicaciones a través de protocolos como HTTP (para la World Wide Web), SMTP (para correo electrónico) y FTP (para transferencia de archivos). Esta capa también maneja la autenticación, autorización y servicios de directorio.

Capa de Presentación (Capa 6): La función principal de esta capa es traducir, cifrar o comprimir los datos para garantizar que sean comprensibles por el destinatario. Esto incluye la conversión de datos de diferentes formatos (por ejemplo, ASCII a EBCDIC), la encriptación de datos para garantizar la seguridad de la comunicación, y la compresión de datos para optimizar el ancho de banda de la red.

Capa de Sesión (Capa 5): Esta capa establece, mantiene y finaliza las conexiones entre las aplicaciones en diferentes dispositivos. Proporciona servicios de gestión de sesiones, como la sincronización y el control del diálogo entre las aplicaciones. También maneja la recuperación de errores y la reanudación de sesiones en caso de desconexiones inesperadas.

1. Dentro de la capa de Aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios. Describir su respectiva función y/o propósito.

Aplicaciones: Son programas de software diseñados para realizar tareas específicas para el usuario final, como navegadores web, clientes de correo electrónico, clientes de mensajería instantánea, etc. Estas aplicaciones interactúan directamente con los usuarios y utilizan protocolos de aplicación (como HTTP, SMTP, FTP, etc.) para comunicarse a través de la red y acceder a los servicios ofrecidos por otros dispositivos.

Servicios: Son procesos de software que se ejecutan en un dispositivo de red para proporcionar funciones específicas a otras aplicaciones o dispositivos. Estos servicios incluyen servidores web, servidores de correo electrónico, servidores DNS, etc. Los servicios aceptan solicitudes de otras aplicaciones o dispositivos, procesan la solicitud y proporcionan una respuesta adecuada utilizando protocolos de aplicación específicos.

1. Explicar, por medio de un dibujo, el funcionamiento del modelo cliente-servidor y su relación con el término Daemon.
2. Describir la diferencia entre los términos: redes punto a punto y aplicaciones punto a punto (P2P).

Redes punto a punto se refiere a una topología de red donde todos los dispositivos están conectados directamente entre sí, sin un dispositivo central de control. Aplicaciones punto a punto (P2P), por otro lado, se refiere a sistemas de comunicación donde cada participante tiene igual capacidad y puede actuar como cliente o servidor, compartiendo recursos directamente entre ellos sin necesidad de un servidor central.

1. Explicar, con sus palabras, los procesos y protocolos de envío y recepción de un e- mail.

En el proceso de envío de un correo electrónico, el remitente redacta el mensaje y lo envía desde su cliente de correo electrónico a través del protocolo SMTP. El servidor SMTP del remitente transmite el mensaje al servidor SMTP del destinatario. Luego, el servidor POP3 o IMAP (Internet Message Access Protocol) del destinatario recibe y almacena el mensaje.

1. Describir la función de las aplicaciones TCP/IP conocidas, tales como World Wide Web e e-mail y sus servicios relacionados (HTTP, DNS, SMB, DHCP, SMTP/POP y Telnet).

World Wide Web (WWW): Permite la visualización y la transferencia de información en forma de documentos de hipertexto, a través del protocolo HTTP (Hypertext Transfer Protocol).

Correo electrónico (e-mail): Permite el intercambio de mensajes de texto entre usuarios a través de la red. Utiliza principalmente los protocolos SMTP (Simple Mail Transfer Protocol) para enviar correos electrónicos y POP (Post Office Protocol) o IMAP (Internet Message Access Protocol) para recibirlos.

Servicio de Nombres de Dominio (DNS): Traduce nombres de dominio legibles para los humanos en direcciones IP para que los dispositivos puedan comunicarse entre sí en la red.

Servicio de Mensajes de Bloque de Server (SMB): Facilita el intercambio de archivos e impresoras entre dispositivos en una red local.

Protocolo de Configuración Dinámica de Host (DHCP): Asigna automáticamente direcciones IP a los dispositivos de una red y configurar otros parámetros de red, como la máscara de subred y la puerta de enlace predeterminada.

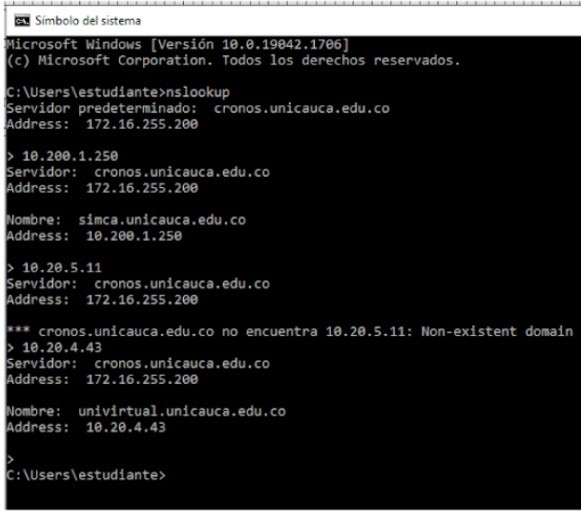
Telnet: Permite a un usuario controlar remotamente otro dispositivo a través de la red, utilizando el protocolo Telnet para la comunicación.

1. Investigar y explicar la diferencia entre Telnet y SSH

Telnet es un protocolo de red que permite el acceso remoto a otros dispositivos para ejecutar comandos y realizar tareas de manera similar a como se hace localmente, pero es menos seguro ya que la información viaja en texto plano.

SSH (Secure Shell) también permite el acceso remoto a dispositivos, pero de manera segura mediante la encriptación de la comunicación, proporcionando autenticación y protección contra ataques, a diferencia de Telnet.

1. Utilizando la utilidad **nslookup** obtener manualmente la dirección IP de al menos tres (3) sitios web que usted frecuente.
2. Conectado a la red de la Universidad del Cauca y utilizando la utilidad **nslookup** obtener manualmente la URL asociada a las siguientes direcciones IP: 10.200.1.250, 10.20.5.11, 10.20.4.43.



# Preguntas de lectura: Capítulo 4

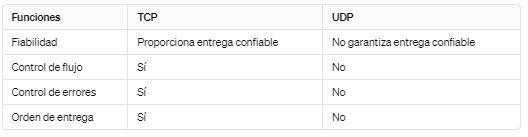
1. Describir las funciones de la capa de Transporte.

La capa de transporte se encarga de proporcionar un servicio de transferencia de datos confiable y eficiente entre dispositivos finales en una red. Esto incluye la segmentación y el reensamblaje de datos, el control de flujo y la corrección de errores para asegurar una entrega precisa y completa de la información. Además, esta capa también gestiona el establecimiento, mantenimiento y finalización de las conexiones entre los dispositivos.

1. ¿Por qué es importante la segmentación?

La segmentación es importante porque permite dividir los datos en unidades más pequeñas antes de ser enviados a través de una red. Esto mejora la eficiencia y la confiabilidad de la transmisión al reducir la posibilidad de errores y congestionamientos, además de facilitar el control de flujo y la retransmisión de datos en caso de pérdida parcial o total.

1. Describir a través de un cuadro de ideas, las funciones y diferencias de dos protocolos TCP/IP de la capa de transporte: TCP y UDP, además Identificar cuándo es apropiado usar TCP o UDP y proveer ejemplos de aplicaciones que usan cada protocolo.



Diferencias:

TCP garantiza la entrega de datos y el orden de entrega, mientras que UDP no lo hace.

TCP realiza control de flujo y control de errores, UDP no.

TCP es más lento debido a la verificación adicional, mientras que UDP es más rápido pero menos confiable.

Cuándo usar:

TCP es apropiado para aplicaciones que requieren entrega confiable de datos, como transferencia de archivos, correo electrónico.

UDP es adecuado para aplicaciones que pueden tolerar pérdida de datos, como transmisión de video, juegos en línea.

Ejemplos de aplicaciones:

TCP: Navegador web (HTTP), Correo electrónico (SMTP), Transferencia de archivos (FTP).

UDP: Transmisión de video (RTP), Voz sobre IP (VoIP), Juegos en línea.

1. Explicar cómo funciona y para que se utiliza el control de congestión de TCP.

El control de congestión de TCP se utiliza para evitar la congestión de la red y garantizar un flujo de datos eficiente. Funciona ajustando dinámicamente la velocidad de transmisión de los datos en función de la cantidad de datos en tránsito y las condiciones de la red, evitando así la saturación de los enlaces y la pérdida de paquetes. Esto se logra a través de técnicas como la ventana deslizante y la retransmisión rápida.

1. Explicar las funciones clave de la capa de Transporte incluyendo confiabilidad, direccionamiento de puerto y segmentación.

Confiabilidad: Garantiza que los datos sean entregados de manera confiable y sin errores mediante técnicas como la retransmisión de paquetes perdidos y la detección y corrección de errores.

Direccionamiento de puerto: Permite que múltiples aplicaciones se comuniquen en un mismo dispositivo utilizando diferentes puertos de origen y destino.

Segmentación: Divide los datos en segmentos más pequeños para una transmisión eficiente a través de la red, facilitando el control de flujo y la retransmisión de datos en caso de pérdida parcial o total.

1. ¿Cuáles son los diferentes tipos de número de puerto?

Puertos Bien Conocidos (Well-Known Ports): Numerados del 0 al 1023, están reservados para servicios específicos y son asignados por la Internet Assigned Numbers Authority (IANA). Ejemplos: HTTP (80), FTP (20 y 21), SSH (22).

Puertos Registrados (Registered Ports): Numerados del 1024 al 49151, están destinados para servicios específicos pero pueden ser registrados por cualquier usuario o aplicación. Ejemplos: MySQL (3306), Oracle Database (1521), HTTPS (443).

Puertos Dinámicos o Privados (Dynamic or Private Ports): Numerados del 49152 al 65535, son utilizados por aplicaciones efímeras y pueden ser asignados dinámicamente por el sistema operativo para conexiones salientes

1. Explicar, por medio de un dibujo, el establecimientoAspyectofsibnásaicloiszdaecnieótwnorkindge:

La vida en un mundo centrado en la

una

conexión TCP (intercambio de señales de tres vías).

Actividades Del Curso D

