**Programación sobre Redes**

**Trabajo Practico Teórico**

1. ¿Qué diferencias puede encontrar entre una conexión Coaxial, UTP o Fibra?

Las principales diferencias entre estos tipos de conexión de red radican en su material, método de transmisión y rendimiento.

Coaxial: Utiliza un cable con un conductor central de cobre y un blindaje metálico. Su diseño lo hace resistente a las interferencias electromagnéticas. Históricamente fue usado en redes de computadoras (Ethernet) y es común hoy en día en redes de televisión por cable.

UTP (Par Trenzado No Blindado): Consiste en pares de hilos de cobre trenzados, pero no tiene blindaje adicional. Es el tipo de cable más común en las redes de área local (LAN) debido a su bajo costo, flexibilidad y facilidad de instalación. Sin embargo, es más susceptible a las interferencias que el cable coaxial o la fibra óptica.

Fibra Óptica: Transmite datos a través de pulsos de luz que viajan por finos hilos de vidrio o plástico. Ofrece la mayor velocidad y capacidad de transmisión, con una mínima atenuación de la señal, lo que la hace ideal para redes de alta velocidad y largas distancias. Su principal desventaja es el costo y la complejidad de su instalación.

1. Según Cisco, ¿qué significa CCENT, CCNA y CCNP? Descripción breve del Track Routing & Switching y de algún otro a elección (ej. Wireless, Security, Cloud, etc).

Cisco ofrece un programa de certificaciones que valida los conocimientos y habilidades en redes.

CCENT (Cisco Certified Entry Networking Technician): Era una certificación de nivel inicial descontinuada por Cisco. Proporcionaba un conocimiento básico sobre redes y era un paso previo para la certificación CCNA.

CCNA (Cisco Certified Network Associate): Es una certificación de nivel asociado que cubre un amplio rango de fundamentos de redes, incluyendo enrutamiento, conmutación, seguridad y redes inalámbricas.

CCNP (Cisco Certified Network Professional): Es una certificación de nivel profesional. Se enfoca en la implementación y la solución avanzada de problemas de redes. Para obtenerla, se requiere aprobar varios exámenes.

Track Routing & Switching: Es el pilar fundamental de las redes de datos.

Routing (Enrutamiento): Es el proceso de seleccionar el mejor camino para enviar datos entre diferentes redes, utilizando direcciones IP. Los routers son los dispositivos que realizan esta función.

Switching (Conmutación): Es el proceso de dirigir el tráfico de datos dentro de una misma red local, utilizando direcciones MAC. Los switches son los dispositivos que realizan esta función.

Track Wireless (Inalámbrico): Este track se enfoca en redes que utilizan ondas electromagnéticas para transmitir datos, eliminando la necesidad de cables. La principal tecnología en este ámbito es Wi-Fi. Estas redes se clasifican según su alcance:

WLAN (Wireless Local Area Network): Redes inalámbricas de área local (hogares, oficinas).

WWAN (Wireless Wide Area Network): Redes de área amplia (redes móviles 3G, 4G, 5G).

1. Explique el modelo OSI.

El modelo OSI (Open Systems Interconnection) es un marco conceptual que divide la comunicación de red en siete capas. Cada capa tiene una función específica y se basa en la anterior, lo que facilita el diseño, la implementación y la solución de problemas en las redes.

Capa 7 - Aplicación: Es la más cercana al usuario final. Permite la interacción con aplicaciones de red (navegadores, clientes de correo electrónico).

Capa 6 - Presentación: Formatea, comprime y cifra los datos para que puedan ser comprendidos por la capa de aplicación.

Capa 5 - Sesión: Crea y mantiene la comunicación entre dispositivos, asegurando que la conexión permanezca abierta el tiempo necesario.

Capa 4 - Transporte: Divide los datos en segmentos y los reensambla. Se asegura de que la entrega sea completa (usando protocolos como TCP) o de que sea rápida (usando UDP).

Capa 3 - Red: Se encarga del enrutamiento. Los routers operan en esta capa para determinar la ruta óptima para enviar los datos a su destino, usando direcciones IP.

Capa 2 - Enlace de Datos: Organiza los datos en "tramas" y facilita la transferencia entre dispositivos en una misma red.

Capa 1 - Física: Se encarga de la transmisión de datos a nivel de bits (unos y ceros) a través de un medio físico, como cables o señales inalámbricas.

1. Explicar el estándar IEEE 802.3 regula la red. Cómo se implementa, ventajas y desventajas.

El estándar IEEE 802.3, conocido como Ethernet, define las reglas para las redes de área local (LAN). Es el estándar más utilizado en la actualidad.

Implementación: Se basa en un método llamado CSMA/CD (Acceso Múltiple con Detección de Señal Portadora y Detección de Colisiones), que permite a los dispositivos competir por el uso del medio de transmisión. Si se detecta una colisión de datos, la transmisión se detiene y se reintenta después de un breve periodo aleatorio.

Ventajas:

Alta velocidad: Ha evolucionado para soportar velocidades de hasta 100 Gbps o más.

Flexibilidad: Es compatible con diferentes tipos de medios de transmisión (cobre, fibra óptica) y diversas topologías de red (estrella, bus).

Estandarización: Su reconocimiento como estándar internacional garantiza la compatibilidad entre equipos de distintos fabricantes.

Desventajas:

Colisiones: En redes más antiguas o con mucho tráfico, el método CSMA/CD puede provocar colisiones que reducen el rendimiento.

1. Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4, conocido como Token Bus, fue un protocolo de red histórico utilizado en entornos industriales. Implementaba una red lógica en anillo sobre una red física de bus, usando un "testigo" (token) para controlar el acceso al medio de transmisión.

En una red Token Bus, solo el dispositivo que posee el testigo puede transmitir datos. Una vez que termina, pasa el testigo al siguiente dispositivo en el anillo lógico. Este método evitaba las colisiones y garantizaba tiempos de respuesta predecibles, lo que era crucial para aplicaciones industriales en tiempo real. Sin embargo, con el tiempo, fue superado por la popularidad de Ethernet.

1. ¿Qué protocolos se usan para enviar y recibir correo?

Los protocolos de correo electrónico son conjuntos de reglas que rigen la transferencia de mensajes.

SMTP (Simple Mail Transfer Protocol): Se utiliza para enviar correos electrónicos. Maneja la transmisión de mensajes entre clientes y servidores, y entre servidores de correo.

POP3 (Post Office Protocol versión 3): Se usa para recibir correos electrónicos. Al conectarse al servidor, este protocolo descarga los mensajes a tu dispositivo local y, por defecto, los elimina del servidor. Es ideal si solo accedes a tu correo desde un único dispositivo.

IMAP (Internet Message Access Protocol): Se usa para recibir correos electrónicos. A diferencia de POP3, IMAP te permite acceder y gestionar los mensajes directamente en el servidor. Esto significa que los mensajes permanecen en el servidor y se sincronizan en todos los dispositivos que utilices, lo que facilita la lectura y gestión del correo desde múltiples ubicaciones.

1. ¿Qué protocolo puede usarse para leer correo recibido?

Para leer correo recibido se utilizan principalmente dos protocolos:

IMAP (Internet Message Access Protocol): Permite acceder y sincronizar los correos directamente en el servidor. Los mensajes no se descargan por defecto y pueden ser leídos desde cualquier dispositivo.

POP3 (Post Office Protocol versión 3): Descarga los correos del servidor a un dispositivo local y los elimina del servidor. Los mensajes solo se pueden leer en el dispositivo donde fueron descargados.

1. Diferencias entre IPV4 e IPV6

IPv4 e IPv6 son dos versiones del Protocolo de Internet que permiten la comunicación entre dispositivos en una red. La principal diferencia radica en su estructura y sus capacidades.

Direcciones:

IPv4: Utiliza direcciones de 32 bits, lo que limita el número de direcciones únicas a aproximadamente 4.3 mil millones. Se representan en formato decimal (ej: 192.168.1.1).

IPv6: Utiliza direcciones de 128 bits, proporcionando un número de direcciones virtualmente ilimitado. Se representan en formato hexadecimal (ej: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Seguridad: IPv6 incluye IPsec como una característica obligatoria y nativa, lo que mejora la seguridad de las comunicaciones al proporcionar autenticación y cifrado. En IPv4, IPsec es opcional.

Configuración: IPv6 permite la autoconfiguración de direcciones (SLAAC), eliminando la necesidad de un servidor DHCP en muchos casos. También elimina el uso de NAT (Network Address Translation), lo que permite una conectividad más eficiente de extremo a extremo.

1. (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes? Ejemplos.: Accedo y configuro el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuro una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.

Spindler Carlos Daniel: No tengo ninguna experiencia en redes. Tampoco la tengo en TIC.