INTRODUCTION TO NETWORKS

1.6-1.9 Cisco.
Juan Pablo Vindas Suarez

1.

REDES CONFIABLES

Los arquitectos de redes deben tener en cuenta una serie de caracteristicas a la hora de elaborar redes las cuales son:

Tolerancia a fallas: Las redes tolerantes a fallas usan rutas redundantes y conmutación de paquetes para una recuperación rápida y proteger a los usuarios de los cambios de ruta.

Escalabilidad: Permite un rápido crecimiento para nuevos usuarios sin afectar el rendimiento de los usuarios existentes, facilitando la incorporación de nuevas redes y usuarios en la topología .

Calidad de servicio: Tambien conocido como (QoS) es esencial para garantizar una transmisión confiable y una experiencia óptima en las redes, gestionando la congestión y priorizando el tráfico de voz y video en tiempo real para cumplir las expectativas de los usuarios y evitar interrupciones en la transmisión de datos.

Seguridad de la red: Los administradores de red garantizan la seguridad de la información en los dispositivos conectados al protegerlos y prevenir el acceso no autorizado al software de administración. Se implementan medidas de seguridad, como el inicio de sesión, para proteger la red. Los administradores de red protegen los paquetes de datos transmitidos y la información en los dispositivos conectados al cumplir con los requisitos de confidencialidad, integridad y disponibilidad de datos.

2.

TENDENCIAS DE RED

Un rápido avance tecnológico Esto requiere que las empresas y Los consumidores se adaptan constantemente a modelos nuevos de las redes como:

Colaboraciones en línea: Teams, Skype, Discord, Cisco Webex y otras herramientas están fácilmente disponibles gracias a la tecnología moderna.

Comunicaciones por video: para una mejor comunicación, se reunió en una reunión con una cámara. Esto es bastante comparable a las colaboraciones en línea.

Tendencias tecnologicas en el hogar: Son los aparatos electonicos usados para mejorar el hogar con dispositivos como: hornos, parlantes inteligentes, servicios de limpieza dominados por una IA

BYOD: Conciste en tener un dispositivo que le permita realizar sus funciones. Entre estas se encunetran tablets, smartphones, labtops y lectores electronicos

Computacion en la nube: Se conoce como un lugar de almacenamiento donde se puede guardar informacion

nube publica: puede ser gratuito o se ofrecen en un modelo de pago por uso y esta abirto generalmente para todo el publico.

nube privada: por lo pertemecen a empresas o gobierno y conteinen informacion privada

Redes powerline: Permitir transmitir datos a través de la red eléctrica de una red domótica para brindar conectividad a los dispositivos.

Conexión inalámbrica de banda ancha: los proveedores de servicios de Internet (WISP) utilizan redes inalámbricas como WLAN para conectar ubicaciones inalámbricas o DSL. Para conectar dispositivos domésticos, la banda ancha inalámbrica con antenas compite con DSL y cable. Para las personas sin una opción de conexión convencional, es un método eficaz y asequible.

3.

SEGURIDAD DE LA RED

Amenazas de seguridad

Parte de la navegacion en las redes hay distantas amenas en contra de nuestra seguridad informatica, ejemplos de ellos son:

Virus,gudanos y caballos de troya: contienten malwares maliciosos que se ejecutan en un dispositivo.

Spyware y adwares: tipos de software que se instalan en el dispositivo de un usuario. Estos roban la informacion de los usarios

Ataques de día de cero: se produce el primer día que se concoe una vulnerabilidad.

Amanazas de Atacantes: una persona malintencionada ataca un dispositivio o una red en concreto.

Ataques por denegacion de servicios: ralentizan o bloquean las aplicaciones y procesos en un dispositivo de red.

Intercepcion y robo de datos: Roba los datos privados de una red de una organizacion.

Robo de identidad: ataca credenciales de inicio de seción de un usuario para tener acceso a datos privados.

4.

SEGURIDAD DE LA RED

Soluciones de seguridad

Antivirus y antispyware: estos ayudan a que los dispositivos no se infecten con sofware maliciosos.

Filtrado de Firewall: bloquea el acceso no autorizado dentro y fuera de la red.

Sistemas de firewall dedicados: ofrece funciones de cortafuegos más avanzadas para filtrar grandes cantidades de tráfico con mayor precisión.

Listas de control de acceso (ACL): filtran el acceso y reenvían el tráfico en función de las direcciones IP y las aplicaciones.

Sistemas de prevención de intrusiones (IPS):Estos detectan rápidamente amenazas peligrosas, como ataques nuevos y desconocidos.

- Redes Privadas Virtuales (VPN): Estos permiten que los empleados que trabajan desde casa accedan de forma segura a la red de la empresa.

5.

EL PROFESIONAL DE TI

CCNA: es importante conocer las habilidades necesarias para trabajar en TI. Es importante demostrar competencia en tecnologías avanzadas y adaptarse a las habilidades requeridas para tecnologías futuras.

Empleos de redes: La certificación CCNA abre puertas a diversos trabajos en el mercado actual gracias a las certificaciones las cuales abren puertas para empleos.

6.

REFERENCIAS

Cisco. (2022).Networking Academy CCNAv7 (modulo 1). Capítulo 1.6: Redes confiables.

Cisco. (2022).Networking Academy CCNAv7 (modulo 1). Capítulo 1.7: Tendencias de red.

Cisco. (2022).Networking Academy CCNAv7 (modulo 1). Capítulo 1.8: Seguridad de la red.

Cisco. (2022).Networking Academy CCNAv7 (modulo 1). Capítulo 1.9: El profesional en TI