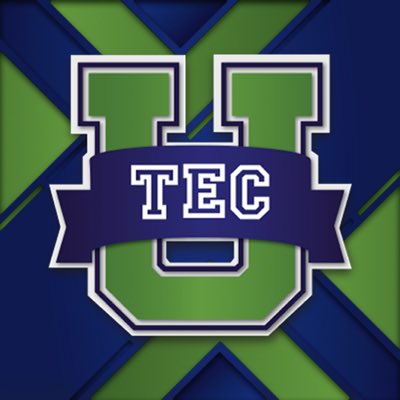
INTRODUCCION A WAN

Lee cuidadosamente el capítulo 1 Introducción a WAN, a continuación elabora un resumen de al menos dos cuartillas.



**YANET ISLAS YAÑEZ**

**ITI 91**

**CONCEPTOS DE WAN**

Las redes de área extensa (WAN) se usan para conectar redes LAN remotas. Una WAN puede proporcionar cobertura a una ciudad, un país o una región global.

Las WAN son de propiedad de un proveedor de servicios, y las empresas pagan una tarifa para usar los servicios de red WAN del proveedor.

Los estándares de acceso WAN funcionan en las capas 1 y 2 del modelo OSI, y la definición y administración de dichos estándares están a cargo de la TIA/EIA, la ISO y el IEEE. Una WAN puede ser de conmutación de circuitos o de conmutación de paquetes.

Existe terminología común que se usa para identificar los componentes físicos de las conexiones WAN y quién es responsable de qué componentes (el proveedor de servicios o el cliente).

Las redes del proveedor de servicios son complejas, y las redes troncales del proveedor de servicios constan principalmente de medios de fibra óptica de ancho de banda elevado. El dispositivo usado para la interconexión a un cliente es específico de la tecnología WAN que se implemente.

**¿POR QUÉ UNA WAN?**

Las WAN funcionan más allá del ámbito geográfico de una LAN, las WAN se usan para interconectar la LAN de la empresa a las LAN remotas en las sucursales y las ubicaciones de los empleados a distancia.

Una WAN es de propiedad de un proveedor de servicios. Para conectarse a sitios remotos, una organización debe pagar una tarifa para usar los servicios de red del proveedor. En cambio, las LAN normalmente son de propiedad de una organización y se utilizan para conectar computadoras, periféricos y otros dispositivos locales en un único edificio u otra área geográfica pequeña.

**¿SON NECESARIAS LAS WAN?**

Sin las WAN, las LAN serían una serie de redes aisladas. Las LAN proporcionan velocidad y rentabilidad para la transmisión de datos en áreas geográficas relativamente pequeñas. Sin embargo, a medida que las organizaciones se expanden, las empresas requieren capacidad de comunicación entre sitios geográficamente separados.

No se pueden conectar computadoras a través de un país, o del mundo, con cables físicos. Por lo tanto, las distintas tecnologías evolucionaron para admitir este requisito de comunicación. Internet se usa cada vez más como una alternativa económica a las WAN empresariales.

Las WAN, ya sea que se usen solas o en conjunto con Internet, permiten que las organizaciones y las personas cubran sus necesidades de comunicación en un área extensa.

**TOPOLOGÍAS WAN**

La interconexión de varios sitios a través de WAN puede incluir una variedad de tecnologías del proveedor de servicios y de topologías de WAN. Las topologías de WAN más comunes son:

**Punto a punto**

Una conexión punto a punto es transparente para la red del cliente, como si hubiera un enlace físico directo entre dos terminales. Los paquetes enviados desde un sitio se entregan a otro sitio y viceversa. Una conexión punto a punto es transparente para la red del cliente, como si hubiera un enlace físico directo entre dos terminales.

**De estrella**

Con una topología de estrella (hub-and-spoke) una sola interfaz a hub puede ser compartida por todos los circuitos de radio. Una topología de estrella (hub and spoke) también es un ejemplo de una topología de localización simple. Una de las desventajas de las topologías de estrella es que la comunicación debe pasar a través del hub.

**Malla completa**

Con una topología de malla completa con circuitos virtuales, cualquier sitio puede comunicarse directamente con cualquier otro sitio. La desventaja aquí es la gran cantidad de circuitos virtuales que se deben configurar y mantener.

**Topología de seguridad preventiva doble**

La desventaja de las topologías de seguridad preventiva doble es que son más costosas de implementar que las topologías de localización simple. Esto es porque requieren hardware de red, como routers y switches adicionales. Las topologías de seguridad preventiva doble son más difíciles de implementar porque requieren configuraciones adicionales y complejas. Sin embargo, la ventaja de las topologías de seguridad preventiva doble es que ofrecen redundancia de red, equilibrio de carga, computación o proceso distribuido mejorados, y la capacidad de implementar las conexiones del proveedor de servicio de respaldo.