COMUNICACIÓN Y REDES

EDUCA PANAMÁ

FACULTAD DE INFORMÁTICA ELECTRÓNICA Y COMUNICACIÓN

Tipos de Redes y Tecnologías WAN

Autor: Crisfor Gudiel

Lic. En Informática Aplicada

INTRODUCCIÓN

Presentaremos diversos tipos de red WAN y que es una red WAN es muy importante conocer para nuestro futuro como profesionales sobre los diversos tipos y que función realiza cada uno.

Se explicará sobre las tecnologías WAN alambradas y las inalámbricas y la seguridad en las redes inalámbricas. También cuales son las desventajas y desventajas de las redes WAN alámbricas e inalámbricas.

Existe una variedad de tecnologías WAN las cuales satisfacen las diferentes necesidades de las empresas y de igual manera existen muchas maneras de incrementar la cobertura de una red de datos, sin embargo, al agregar el acceso WAN, se presentan otros aspectos a tomar en cuenta con son la seguridad de la red y la administración de las direcciones, debido a estos aspectos el diseño de una WAN y la elección de los servicios de red adecuados no es algo simple.

REDES WAN Y SUS TIPOS

¿Qué es una Red WAN?

Es un grupo de redes de área local que se extienden por lo general sobre un área geográfica grande, utilizando una conexión de alta velocidad y tecnología costosa.

- **Conmutadas por Circuitos:** redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.
- **Conmutadas por Mensaje:** en este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.
- **Conmutadas por Paquetes:** en este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.
- **Redes Orientadas a Conexión:** en estas redes existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.
- Redes no orientadas a conexión: llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET.

- Red Pública de Conmutación Telefónica (PSTN): esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

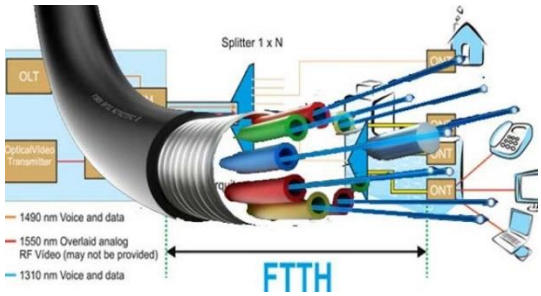
TECNOLOGIAS WAN ALAMBRADAS

Tecnología HFC:

La tecnología Hybrid Fibre Coaxial (HFC) es una combinación de cable y fibra óptica.

- Los datos se transportan por fibra óptica y luego se pasan al cable, que es el que llega realmente al hogar del usuario.
- Esta conexión utiliza un cable de fibra óptica para acercar a los usuarios de manera bidireccional, libre de problemas de ruidos, los servicios de internet, telefonía y televisión, transmitiendo los datos a través de nodos.
- A la hora de contratar servicio de internet los usuarios se encuentran con varias opciones: ADSL, fibra óptica (FTTH) y la fibra híbrida coaxial (HFC), que es el cable que ofrecen algunas compañías.

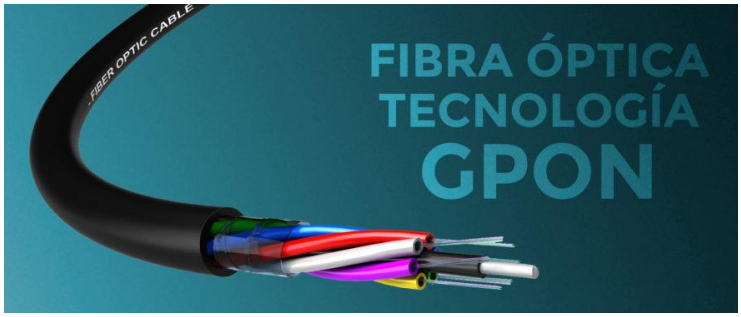
Tecnología FTTH:



Es una tecnología de telecomunicaciones que consiste en la utilización de cableado de fibra óptica y sistemas de distribución ópticos para la provisión de servicios de Internet, Telefonía IP y Televisión (IPTV) a hogares, negocios y empresas.

Es una tecnología que gradualmente se va incorporando en los servicios de Internet para hogares ofreciendo mayor velocidad, disponibilidad de contenidos y de mejor calidad. Como así también, preparando a las casas del futuro para la recepción de novedosos servicios y aplicaciones de valor agregado, tales como el video on demand, los canales HD o el almacenamiento en la nube.

Tecnología GPON:



Es una tecnología de acceso de telecomunicaciones que utiliza cableado de fibra óptica para llegar hasta el usuario, es decir, la última milla se compone de fibra óptica.

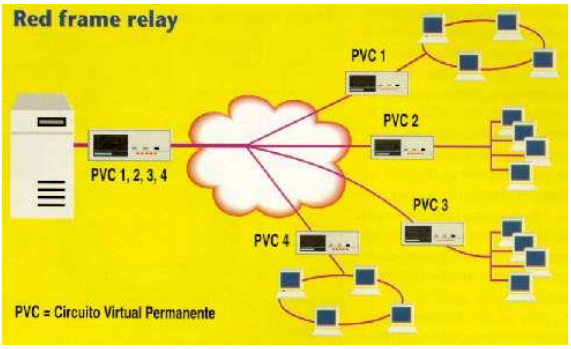
Esta tecnología de fibra óptica permite una mayor velocidad de transmisión y recepción de datos a través de una sola fibra, con una arquitectura de punto a multipunto, que permite fibra óptica al hogar (FTTH), o a un edificio (FTTB).

Modem:

Es un dispositivo capaz de convertir las señales digitales en analógicas, proceso llamado “modulación”, y también es capaz de convertir las señales analógicas en digitales, a cuyo proceso se le llama “demodulación”.

Lo que hace un modem básicamente es permitir la comunicación entre nuestro ordenador e Internet a través de la red de telefonía o del llamado cablemódem, que usa la red de televisión por cable, algo que ya nos sonará a antiguo.

Frame relay:



Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducido por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privad apunto a punto, esto quiere decir que es orientado a la conexión.

Wifi:

WiFi, es una tecnología que permite la conexión inalámbrica entre dispositivos electrónicos, ordenadores, smartphones, tablets, televisores, videoconsolas, etc. Wi-Fi es una marca de Wi-Fi Alliance o Alianza Wi-Fi, la organización que promueve dicha tecnología y que se encarga de certificar todos los productos que se ajustan a las normas establecidas de interoperabilidad.

Una tecnología que surgió por la necesidad de establecer una manera de conexión inalámbrica que fuese compatible con distintos dispositivos. Por lo tanto, el objetivo de la Alianza fue diseñar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad entre dispositivos.

SEGURIDAD EN REDES INALÁMBRICAS

Seguridad a nivel de protocolo: La seguridad a nivel de protocolo es la encargada de que los datos transmitidos por una WLAN no puedan ser descifrados por alguien ajeno a nuestra red. Para ello nuestra red ha de tener un algoritmo de codificación y gestión de claves. En primer lugar, el IEEE publicó un algoritmo de seguridad opcional en el estándar 802.11 llamado WEP.

WEP: El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso. RC4 consiste en generar una clave de forma pseudoaleatoria que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica XOR (O exclusiva), obteniendo como resultado un texto cifrado. La clave pseudoaleatoria se genera utilizando una clave secreta que define el propio usuario con una longitud de 40 o 104 bits y un vector de inicialización (IV) de 24 bits que lo genera aleatoriamente el sistema para cada trama. Pero wep tenía muchos defectos como era la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP. Por lo tanto, la IEEE trabajaba en otro algoritmo más potente, pero la Alianza Wi-Fi lanzó un algoritmo alternativo y más potente que WEP, llamado WPA.

WPA: WPA (Wifi Protect Access) es el protocolo de seguridad que lanzó la Alianza Wi-Fi para solucionar los problemas de seguridad del protocolo WEP. Este protocolo implementa las siguientes mejoras: • Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos). • Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits). • Utiliza el intercambio dinámico de claves mediante el protocolo TKIP (Temporal Key Integrity Protocol). • El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code). Posteriormente el IEEE publicó el estándar 802.11i, también conocido como WPA2.

WPA2: Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro. Incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes: • Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes.

Consejos de seguridad en Internet para proteger la red inalámbrica

A continuación, se incluyen varios pasos sencillos que puedes seguir para proteger tu red y routers inalámbricos:

- **Evita la utilización de la contraseña predeterminada**
  Es muy fácil para un hacker descubrir cuál es la contraseña predeterminada del fabricante de tu router inalámbrico y utilizarla para acceder a la red inalámbrica. Por lo tanto, es conveniente que cambies la contraseña de administrador de tu router inalámbrico. A la hora de establecer la contraseña nueva, trata de elegir una serie compleja de números y letras, e intenta evitar la utilización de una contraseña que pueda adivinarse fácilmente.
- **No permitas que el dispositivo inalámbrico indique su presencia**
  Desactiva la difusión del identificador de red SSID (Service Set Identifier) para evitar que el dispositivo inalámbrico anuncie su presencia al mundo que te rodea.
- **Cambia el nombre SSID del dispositivo**
  Al igual que antes, es muy fácil para un hacker descubrir cuál es el nombre SSID predeterminado del fabricante del dispositivo y utilizarlo para localizar la red inalámbrica. Cambia el nombre SSID predeterminado del dispositivo e intenta evitar la utilización de un nombre que pueda adivinarse fácilmente.

- **Cifra los datos**
  En la configuración de la conexión, asegúrate de que activas el cifrado. Si el dispositivo es compatible con el cifrado WPA, utilízalo; en caso contrario, utiliza el cifrado WEP.
- **Protección contra los ataques de malware e Internet**
  Asegúrate de que instalas un programa antimalware eficaz en todos los ordenadores y demás dispositivos. Con el fin de mantener actualizada la protección antimalware, selecciona la opción de actualización automática en el producto.

VENTAJAS Y DESVENTAJAS DE LAS REDES WAN ALÁMBRICAS

Ventajas:

- Costos relativamente bajos
- Ofrece el máximo rendimiento posible
- Mayor velocidad – cable de Ethernet estándar hasta 100 Mbps.

Desventajas:

- El ancho de banda se divide entre todos los usuarios que se encuentren, lo que afecta el rendimiento de la red.
- Mayor número de ataques por la red.
- Es más fácil obtener tu contraseña de acceso a Internet, o información confidencial.
- Personas ajenas a la red podrían recibir la señal y pirateársela

VENTAJAS Y DESVENTAJAS DE LAS REDES WAN INALAMBRICAS

Ventajas:

- No existen cables físicos: por lo tanto, no hay cables que se enreden, ni que entorpezcan la transitabilidad o que molesten estéticamente.
- La instalación de redes inalámbricas suele ser más económica.
- Permiten gran alcance; las redes hogareñas inalámbricas suelen tener hasta 100 metros desde la base transmisora.
- Permite la conexión de gran cantidad de dispositivos móviles.
- Posibilidad de conectar nodos a grandes distancias sin cableado, en el caso de las redes inalámbricas corporativas.
- Permite crear una red en áreas complicadas donde, por ejemplo, resulta dificultoso o muy cara conectar cables.
- Permite ampliar una red cableada en caso de redes mixtas (mezclas de inalámbricas con cableadas)

Desventajas:

- Son algo más inseguras que las redes cableadas
- El ancho de banda de las redes inalámbricas es menor que las cableadas; en otras palabras, la velocidad alcanzada por las redes cableadas es mayor.
- Las redes inalámbricas son un poco más inestables que las redes cableadas, pueden verse afectada por otras ondas electromagnéticas o aparatos electrónicos cercanos.
- La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, etc.

CONCLUSIÓN

Una red WAN trae muchas ventajas a las empresas para la mejorar su productividad y la eficiencia en un entorno de red empresarial. Las ventajas de aumentar el tamaño de la red, la sincronización y el intercambio de datos, y el software y los dispositivos compartidos se suman a hacer de la red WAN una herramienta esencial para cualquier empresa, también en un hogar tenga más de un usuario en su red.

Tenemos que tener muy claro todas las tecnologías que se explican, conocerlas y saber cada función que tiene cada una tanto como la alámbrica y la inalámbrica y sus ventajas y desventajas que tienen cada una.

En el ámbito personal o doméstico, la seguridad que existe actualmente con WPA2 es suficiente, ya que, la importancia de la información que se puede llegar a obtener en este tipo de ámbitos no merece la pena la dedicación de tiempo y recursos para poder obtenerla.

INFOGRAFÍA

https://sites.google.com/site/unidossomosmaz/asignaturas-estudio/home/modulo-uno/tipos-de-redes-wan

https://www.iptel.com.ar/que-es-ftth-o-fibra-al-hogar/

https://www.iptel.com.ar/que-es-gpon/

https://www.profesionalreview.com/2019/01/27/modem-que-es/

https://www.kaspersky.es/resource-center/preemptive-safety/protecting-wireless-networks

http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf

http://monicaparamo.weebly.com/alaacutembrica.html

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQd2oKX8y0Cm54cexxtrTOMo6dUuMVdtX8261nTIpANQ_ZfVnPgx8KICYaEtT13PLcjw7Q&usqp=CAU

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ8sUQ6IqKenomnFaxB0aCFFWnVBjLpKFhG7A&usqp=CAU

https://hotelplay.tv/wp-content/uploads/2019/02/fibra-gpon-blog-e1552984380188.jpg

https://pixabay.com/es/vectors/enrutador-inal%c3%a1mbrico-red-conexi%c3%b3n-157597/

https://ingetelecom.files.wordpress.com/2007/08/informe-frame-relay-i-2017.pdf

https://upload.wikimedia.org/wikipedia/commons/thumb/a/ae/WiFi_Logo.svg/2560px-WiFi_Logo.svg.png