Unidad 1 / Escenario 2

Lectura fundamental

Arquitectura de redes

Contenido

Palabras clave: arquitectura de redes, retardos, pérdidas, tasas de transferencia, vulnerabilidad, ataque en redes.

1. Arquitecturas típicas de redes de datos

Para conocer más de las redes de datos, tenemos que diferenciar algunos conceptos que se usan a diario. LAN por sus siglas en inglés (*Local Area Network*), es un término muy usado en redes, este acrónimo indica que la red está acotada geográficamente, es decir que depende del área física en la cual opera, por lo general se trata de áreas pequeñas como salones, oficinas, pisos, y cuando son áreas mayores uno o varios edificios.

Las redes LAN están clasificadas de acuerdo con su configuración, diseño o topología. A continuación, vamos a describir cada topología sin ahondar en su funcionamiento, pues el objeto de todas es el mismo, interconectar dispositivos e intercambiar archivos de cualquier especie entre ellos.

1.1. Malla

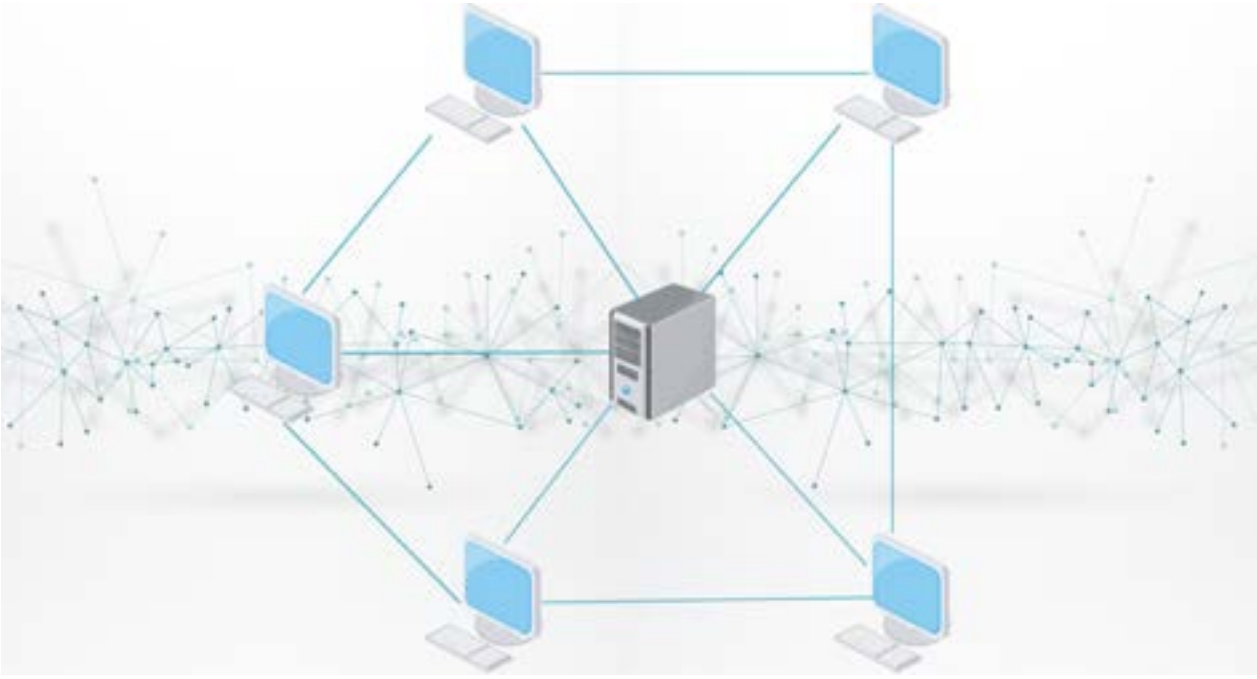

Figura 1. Red en malla

Fuente: elaboración propia

En esta topología, cada dispositivo tiene una línea de conexión contra los demás dispositivos de la red por lo que es llamada *full-mesh*. Esta fue una de las configuraciones más usadas a nivel de transmisión por empresas, sin embargo, también es la que más usa recursos de procesamiento en los equipos y mayores costos en medios de transmisión.

1.2. Bus

Figura 2. Red en bus
Fuente: elaboración propia

Esta topología ya casi no se usa pues se basaba en la conexión de dispositivos a través de un único bus central que unía todos los dispositivos. El bus central se basaba en un cable coaxial, que a medida del tiempo fue reemplazado por el UTP.

1.3. Anillo

Figura 3. Red en anillo
Fuente: elaboración propia

Esta topología al igual que la anterior usaba un cable coaxial, y sus velocidades dependían de la tarjeta de red que para su época no superaba los 10Mbps.

1.4. Estrella

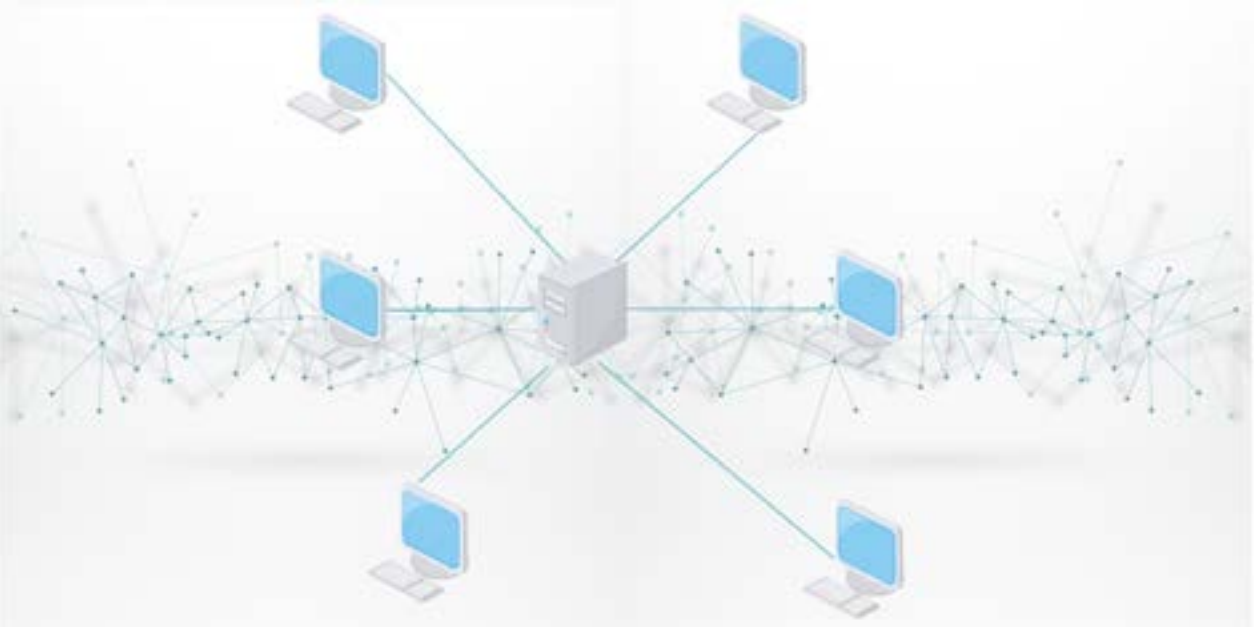

Figura 4. Red en estrella

Fuente: elaboración propia

Esta topología, la más común y más usada en estos días nos muestra que todos los dispositivos se conectan a un concentrador, y éste distribuye los archivos o peticiones de usuario inicial a usuario final.

1.5. WAN o red aérea

Otro de los conceptos a diferenciar es el termino WAN (*Wide Area Network*), o red de área extensa. Este concepto se usa para redes que tienen mucha distancia entre ellas, es decir, superan cuadras físicas de distancia en su mínima expresión y en la máxima para unir redes de país a país.

Figura 5. Esquema de una conexión WAN

Fuente: elaboración propia

Esta figura nos muestra una red unida de ciudad a ciudad, ejemplo de Bogotá hasta Medellín.

Las redes WAN, son propias de los ISP (Proveedores de Servicios) pues estos tienen la infraestructura para hacerlas operativas con sus tecnologías, varias de estas han evolucionado con el tiempo y reemplazándose unas a otras. Desde X.25, Frame Relay, ATM y por último MPLS son las tecnologías que se usan en las redes WAN, estas pueden ser punto a punto y/o punto multipunto.

Figura 6. Esquema de una conexión a través de un módem

Fuente: elaboración propia

Red punto a punto, establecida entre dos dispositivos.

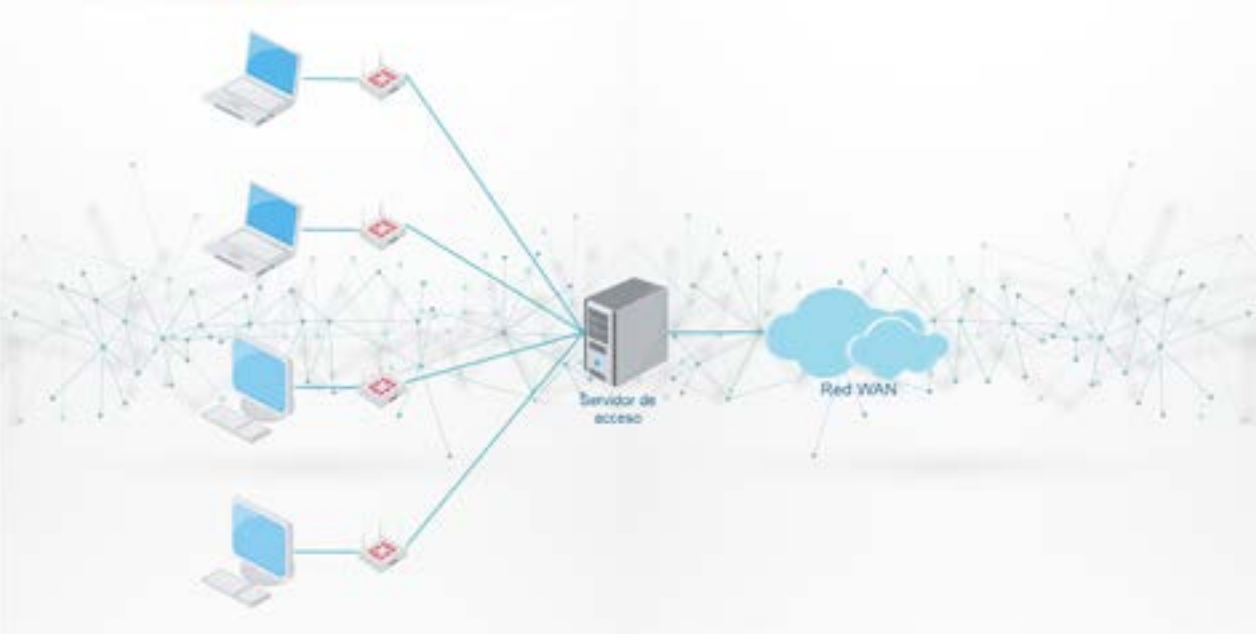

Figura 7. Conexión PPP

Fuente: elaboración propia

La red punto multipunto es aquella que conecta un dispositivo con varios, esta red fue la que utilizamos hace unos años cuando nos conectábamos a Internet por redes telefónicas conmutadas, donde todos los usuarios se conectaban a la red de algún proveedor de servicios. Después hubo grandes cambios tecnológicos y pasamos de la red conmutada a una red de mejor velocidad (ADSL) la cual funcionaba sobre el mismo par de cobre (línea telefónica), pero con una adición de un equipo modem (modulador-demodulador).

Estas redes WAN evolucionaron de la siguiente manera:

Tabla 1. Evolución de las redes WAN

RED	AÑOS	VELOCIDAD	ESTANDAR	EFERENCIA
X.25	1985-1996	9.6 – 64 Kbps		ITU-T CCITT
Frame Relay	1992-	64Kbps-2Mbps	ITU-T recomendación I.122	ITU-T
ATM	1996	34-155Mbps	RFC1754-2515-4454	IETF
MPLS	2001	20Mbps-10Gbps	IETF RFC 3031	IETF
METRO-ETHERNET	2003	1G-40Gbps	IEEE802.3–2000	IEEE-MEF-IETF

Fuente: elaboración propia

Teniendo en cuenta la información resumida en la tabla anterior vemos que las redes Frame Relay no tienen una fecha de finalización, a continuación, daremos luz a este interrogante.

Esto se debe a que aún hoy en día las usamos, aunque a Frame Relay no le queda mucho tiempo de vida pues la mayoría de empresas prestadoras de servicios de telecomunicaciones, que usaban estas tecnologías antiguas, ya están migrando sus redes a las nuevas. Esta evolución ha sido muy rápida porque cada día necesitamos más ancho de banda, ya no son simples correos, ahora demandamos video llamadas y canales de TV en HD por la red de datos.

Hay otro término que se encuentra en la mitad entre LAN y WAN, pero la verdad no es muy usada, las siglas MAN (Metropolitan Area Network), que es una mezcla de ambas redes, las cuales deben estar en una misma ciudad, sin embargo, con las distancias que hay entre ciudades grandes como Bogotá, no serían tan metropolitanas, pues ya cambiarían a WAN. Sobre todo, cuando las empresas grandes tienen que salir de la ciudad y estar en lugares especiales, como centros de acopio y zonas francas.

2. Análisis de retardos, pérdidas y tasas de transferencia en redes de datos

Los métodos más comunes de corrección y detección de errores se usan en la capa de enlace, estos son CRC, BER, CDMA/CS, FEC, Código de Hamming, Bit de paridad, Reed-Solomon.

Estos métodos previenen la pérdida de paquetes durante la transmisión de datos, pues los medios físicos por los cuales se transfieren los mismos no son óptimos, el aire no es igual al vacío, y los cables de cobre tienen pérdidas físicas inherentes a su material, uniones, terminales bañadas en oro para su mejor conducción, todos estos materiales tienen respuestas físicas y químicas que reaccionan de diferentes maneras al contacto eléctrico, pues los bits, como sabemos son pulsos de voltaje y corriente, pasan a altas frecuencias, por otro lado la fibra óptica es una fibra de vidrio que degrada la señal de luz inducida por los emisores y a veces no llega a sus receptores, lo que hace necesario el uso de repetidores y más equipos para regenerar las señales y puedan llegar más lejos.

Capacidades de los canales según Nyquist, C=2BW. Se determina que la velocidad máxima alcanzable debe ser 2 veces esa velocidad si no existe ruido. C es la velocidad de transmisión y BW en ancho de banda del canal. Y si esta señal tiene más de un nivel de bits la fórmula cambia de la siguiente manera: C= 2BW log2 M, donde M es el número de niveles.

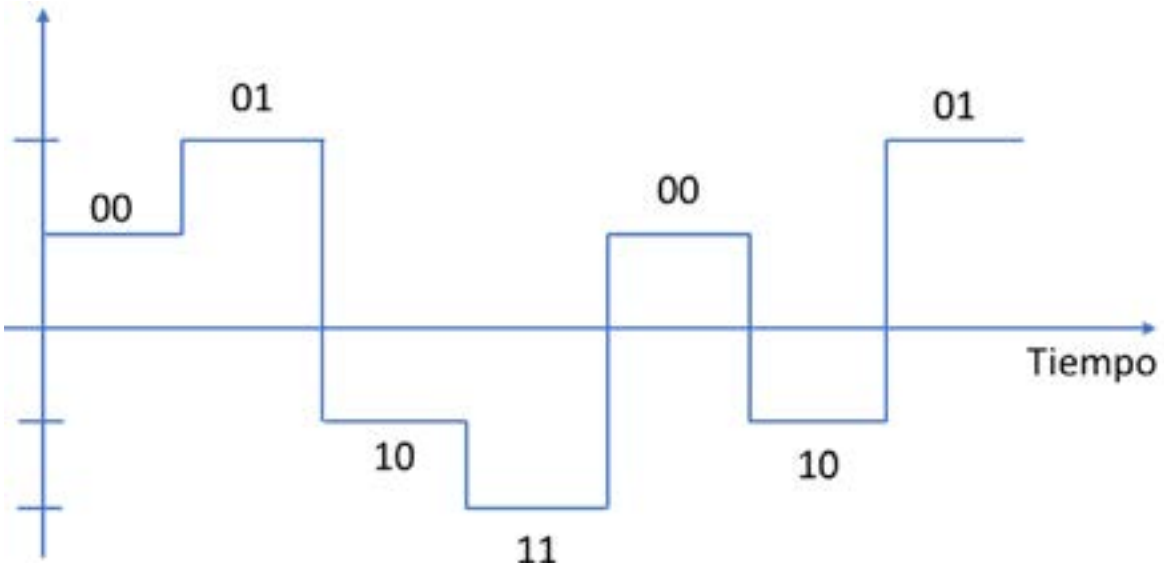

Figura 8. Conexión PPP

Fuente: elaboración propia. Modificado de Santos (2014)

Ancho de banda efectivo. El ancho de banda mínimo para transmitir una señal digital en su primer armónico es: BW= Tasa de bits / 2.

Por ejemplo, para una señal de 2 Mbps se debe utilizar un ancho de banda de 500 KHz como mínimo, para transmitir el primer armónico. Si se desea transmitir el primero, el tercero y el quinto se necesita un ancho de banda de 2,5 MHz (5 x 500 KHz).

3. Introducción a vulnerabilidades y ataques típicos en redes

La seguridad hoy en las redes es uno de los puntos más importantes en las empresas, pues su información vale oro textualmente, por tanto, hay puntos muy comunes que se deben tener en cuenta para ser protegidos.

Primero para tener referencia se tiene que hablar de la seguridad física, la ubicación de los equipos es transcendental, el acceso físico a ellos es de vital importancia y solo personal autorizado tendrá permisos a su control. La destrucción o pérdida de los equipos (servidores), puede tener un costo muy alto y su información algo mayor.

Problemas en sistemas operativos y aplicaciones es algo que no se puede detener, sin embargo, se pueden minimizar con sus actualizaciones, y lo hemos visto hace poco con los ataques a sistemas operativos conocidos y de última generación.

Ataques de *phishing* (correos fraudulentos solicitando información personal de cuentas), e ingeniería social dependen mucho de la enseñanza a los usuarios. Día a día se buscan nuevas formas de robar información en masa.

La no existencia de copias de seguridad es otra falla común y depende mucho de los administradores de los servidores y la misma red.

Los ataques a las redes mediante ping de la muerte y múltiples sesiones usando el SYN FLOOD, intentan tener acceso a los equipos y el control de su sistema operativo.

Tabla 1. Tabla resumen.

Problemas de seguridad	Defensas posibles
Inseguridad física.	Establecer perímetros de seguridad.
Vulnerabilidades del software.	Métodos seguros de actualización del software.
Pérdidas de datos sensibles.	Política correcta de copias de seguridad.
Ataques de acceso no permitido a sistemas.	Selección de contraseñas. Tarjetas token . Autenticación AAA. Firma digital. Sistemas biométricos.
Virus, troyanos, spyware, etc.	Sistemas antivirus y antispyware actualizados.
Ingeniería social.	Formación básica de usuarios.
Problemas de seguridad en redes en general.	Cortafuegos Sistemas de detección de intrusiones Detectores de vulnerabilidades.

Fuente: elaboración propia

Referencias

Santos, G. M. (2014). Sistemas telemáticos. Madrid, ES: RA-MA Editorial. Recuperado de: http://www.ebrary.com.loginbiblio.poligran.edu.co:2048

Simmons, G. J. (1992). A survey of Information Authentication". Contemporary Cryptology, The science of information integrity. Ed. GJ Simmons, IEEE Press, New York.

Oliva, N., Castro, G. M. A. y Díaz, O. G. (2013). Redes de comunicaciones industriales. Madrid, ES: UNED - Universidad Nacional de Educación a Distancia. Recuperado de: http://www.ebrary.com.loginbiblio.poligran.edu.co:2048

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Telecomunicaciones

Unidad 1: Conceptos básicos de las redes de datos e Internet

Escenario 2: Arquitectura de redes y seguridad

Autor: John Alirio Olarte Ramos

Asesor Pedagógico: Juan Felipe Marciales

Diseñador Gráfico: Karim Gaitán

Asistente: María Avilán