Fundamentos de Redes

Objetivos Específicos

- Apropiar conceptos básicos de redes de comunicación.

- Distinguir las redes de comunicación LAN, WLNA, PAN, MAN Y WAN.

- Reconocer las capas de aplicación del Modelo OSI y Modelo TCP/IP.

- Diferenciar los Equipos de Red y Protocolos de Comunicación y Transferencia que pueden servir para realizar una Investigación Digital.

Contenidos

- Conceptos Básicos de Redes.

- Redes de Comunicación.

- Modelo OSI y Modelo TCP/IP.

- Equipos y Protocolos de Comunicación y Transferencia

Una red es una estructura que dispone de un patrón que la caracteriza. La noción de informática, por su parte, hace referencia a los saberes de la ciencia que posibilitan el tratamiento de datos de manera automatizada a través de computadoras (ordenadores).

Las personas utilizan las siguientes redes todos los días:

- Sistema de envío de correo

- Sistema telefónico

- Sistema de transporte público

- Red de computadoras corporativa

- Internet

TRASMISION DE DATOS

Un método de caracterizar líneas, dispositivos terminales, computadoras y modems es por su modo de transmisión o de comunicación.

Las tres clases de modos de transmisión son simplex, semidúplex y dúplex completo.

SIMPLEX

La transmisión simplex (sx) o unidireccional es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio, el paging unidireccional.

SEMIDUPLEX

En ocasiones encontramos sistemas que pueden transmitir en los dos sentidos, pero no de forma simultánea. Puede darse el caso de una comunicación por equipos de radio, si los equipos no son full dúplex, uno no podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en ese momento. En radiodifusión, se da por hecho que todo duplex ha de poder ser bidireccional y simultáneo, pues de esta manera, se puede realizar un programa de radio desde dos estudios de lugares diferente.

DUPLEX COMPLETO

Cuando los datos circulan en ambas direcciones a la vez,la transmisión se denomina full-duplex.A pesar de que los datos circulan en ambas direcciones,el ancho de banda se mide en una sola dirección.Un cable de red con 100 Mbps en modo full-duplex tiene un ancho de banda de 100 Mbps

REDES DE COMUNICACIÓN

Es un conjunto de medios (transmisión y conmutación), tecnologías (procesado, multiplexación, modulaciones), protocolos y facilidades en general, necesarios para el intercambio de información entre los usuarios de la red. La red es una estructura compleja.

LAN (Red de Área Local):

Las redes de computadoras se identifican según las siguientes características específicas:

- El tamaño del área que abarcan.
- La cantidad de usuarios conectados.

- La cantidad y los tipos de servicios disponibles.
- El área de responsabilidad

Redes WLAN y WPAN

También existen las redes inalámbricas WLAN y WPAN, las primeras (wireless Local Area Network) están delimitadas por la distancia de propagación del medio y de la tecnología empleada, en interiores hasta 100 metros y en exteriores varios kilómetros.

Redes MAN (Red de Área Metropolitana)

Una MAN es una colección de LANs o CANs dispersas en una ciudad (decenas de kilometros). Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL (Digital Subscriber Line), WDM (Wavelenght Division Modulation), ISDN, E1/T1, PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

Redes WAN (Red de Área Local)

Una WAN es una colección de LANs dispersadas geográficamente cientos de kilómetros una de otra. Un dispositivo de red llamado enrutador es capaz de conectar LANs a una WAN.

Las WAN utilizan comúnmente tecnologías ATM (Asynchronous Transfer Mode), Frame Relay, X.25, E1/T1, GSM, TDMA, CDMA, xDSL, PPP, etc. para conectividad a través de medios de comunicación tales como fibra óptica, microondas, celular y vía satélite.

Redes de Cliente y Servidor

Los servidores tienen software instalado que les permite proporcionar servicios, como archivos, correo electrónico o páginas web, a los clientes. Cada servicio requiere un software de Cliente para cada servicio requerido. Si en un cliente hay varios softwares de cliente Es la tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo y/o, a través de la organización, en múltiples plataformas. El modelo soporta un medio ambiente distribuido en el cual los requerimientos de servicio hechos por estaciones de trabajo inteligentes o "clientes, resultan en un trabajo realizado por otros computadores llamados servidores".

Direccionamiento de Red

Las huellas digitales de las personas no cambian y constituyen una manera de identificar físicamente a las personas. La dirección postal de una persona puede no mantenerse

siempre igual, dado que se relaciona con el sitio donde vive o donde recoge la correspondencia.

3. La promoción del desarrollo infantil implica el diseño de un paquete de programas que consideren un enfoque de costo- efectividad, sostenibilidad y participación activa de las comunidades.

Dirección IP

En la actualidad, es común que una computadora tenga dos versiones de direcciones IP. A principios del año 1990, había preocupaciones acerca del agotamiento de las direcciones de red IPv4. El Grupo de Trabajo de Ingeniería de Internet (IETF) comenzó a buscar un reemplazo.

Direccionamiento Estático

En una red con pocos hosts, es fácil configurar manualmente cada dispositivo con la dirección IP correcta. Un administrador de red que entienda de direccionamiento IP debe asignar las direcciones y saber elegir una dirección válida para una red particular. La dirección IP asignada es única para cada host dentro de la misma red o subred. Esto se conoce como “direccionamiento IP estático”.

MODELO OSI

Las capas de la OSI (Open Systems Interconnect) fueron creadas por la ISO (International Organization for Standarization) en 1974 con el propósito de abrir la comunicación entre diferentes sistemas sin recurrir a cambios a la lógica y fundamentos del hardware y software. El modelo de referencia OSI no es un protocolo, es un modelo para entender el diseño de una arquitectura de red que sea flexible, robusta y interoperable (Evelius, 2017).

MODELO TCP/IP

El modelo TCP/IP fue creado por investigadores del Departamento de Defensa (DoD) de los EE. UU. Está formado por capas que llevan a cabo las funciones necesarias para preparar los datos para su transmisión a través de una red. En la Figura 1 se muestran las cuatro capas del modelo TCP/IP (Cisco, 2017).

Arquitectura de la LAN Conmutada

ARQUITECTURA DE LA LAN/CONMUTADA

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. El propósito principal de la capa de

acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.
(David Alfonso Braojos, 2016)

CAPA DE ACCESO

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red.

El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

(David Alfonso Braojos, 2016)

CAPA DE DISTRIBUCION

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso.
(Slideshare, 2017).

CAPA NUCLEO

Es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto, debe poder reenviar grandes cantidades de datos rápidamente.
(Slideshare, 2017).

BENEFICIOS DE UNA RED JERARQUICA

Escalabilidad

- Redundancia

- Rendimiento

- Seguridad

- Facilidad de administración

- Capacidad de mantenimiento

HERRAMIENTAS DE RED

TCPDump

Es un software analizador de tráfico de paquetes de red, funciona a nivel de línea de comandos. Esta herramienta permite analizar el funcionamiento de aplicaciones, detectar problemas en la red o capturar datos que se transmiten por la red y se encuentre sin encriptación

NETWORKMINE

“Herramienta que permite capturar información de red. Permite analizarla aplicando filtros de búsqueda de datos”

(ARNEDO PEDRO JAVIER, 2014,).

NETWORK APPLIANCE FORENSIC TOOBIT

“Paquete de herramientas forenses desarrolladas en lenguaje Python, que se especializan en la captura de tráfico en la red y análisis del mismo”.

(ARNEDO PEDRO JAVIER, 2014,).

WireShark

“Es un software que permite capturar tramas y paquetes que circulan a través de una interfaz de red. Este aplicativo posee todas las características mínimas requeridas por un analizador de protocolos”.

(ARNEDO PEDRO JAVIER . 2014, p.31).

XPILCO

“Software que permite capturar el tráfico de la red, con la particularidad que permite extraer los datos transmitidos mediante el protocolo HTTP y los mensajes de correos electrónicos que tienen implementado los protocolos POP y SMTP”.

(ARNEDO PEDRO JAVIER, 2014,)

Splunk

Software que funciona en los sistemas operacionales más importantes del mercado, permite monitorear y analizar el tráfico de la red, detectando entre otros aspectos transacciones, registros de llamadas y lugares de navegación de los usuarios. Cuenta con un módulo de firmado de datos, que permite generar una prueba de autenticidad en cualquier proceso de análisis forense o auditor. Son establecidos a partir de relaciones de compañerismo y amistad entre sus miembros. No cuentan con una estructura formal, pero su constitución se lleva a cabo en el contexto de los grupos formales.

Snort

TCPDump

Es un software analizador de tráfico de paquetes de red, funciona a nivel de línea de comandos. Esta herramienta permite analizar el funcionamiento de aplicaciones, detectar problemas en la red o capturar datos que se transmiten por la red y se encuentre sin encriptación alguna